UNIVERSIDAD AUTONOMA DE MADRID

ESCUELA POLITECNICA SUPERIOR

PROYECTO FIN DE CARRERA

SOLUCIÓN INTEGRAL EN MATERIA DE SEGURIDAD ELECTRÓNICA

Marta Naranjo Rico

Mayo 2008

SOLUCIÓN INTEGRAL
EN MATERIA DE SEGURIDAD ELECTRÓNICA

AUTOR: Marta Naranjo Rico
TUTOR: Antonio Aguilar Morales

Dpto. de Ingeniería Informática
Escuela Politécnica Superior
Universidad Autónoma de Madrid
Mayo de 2008

PROYECTO FIN DE CARRERA

Título: *Solución Integral en materia de Seguridad Electrónica*

Autor: Dª. Marta Naranjo Rico

Tutor: D. Antonio Aguilar Morales

Tribunal:

Presidente: Jose M. Martínez Sánchez

Vocal: Jose Alberto Hernández Gutiérrez

Vocal secretario: Antonio Aguilar Morales

Fecha de lectura:

Calificación:

Palabras clave

Seguridad, integración, CCTV, cámara, domo, intrusión, detector, barrera, central de alarmas, IP, ancho de banda, red IP, fibra óptica.

Resumen

En este proyecto se presenta un sistema de seguridad que pretende proteger a las personas y bienes materiales existentes en la implantación donde está instalado. Esta protección se conseguirá mediante un circuito cerrado de televisión, compuesto por domos y cámaras ip así como de servidores de vídeo, y un subsistema anti-intrusión tanto en el exterior del perímetro como en el acceso de los edificios, conectado a una central de alarmas, todo ello centralizado en un punto de control.
Así, cuando haya un siniestro, primero lo detectará, luego lo señalizará y posteriormente se iniciarán las acciones encaminadas a disminuir o extinguir los efectos: comunicación con central receptora de alarmas, se activarán las configuraciones apropiadas del sistema CCTV, comunicación entre el personal de seguridad, etc.

El medio utilizado para establecer la comunicación IP es la fibra óptica. El hecho de utilizar fibras ópticas en lugar de cables UTP se debe a las múltiples ventajas que tiene la fibra versus el cable UTP convencional, como son: el ancho de banda, bajas pérdidas (las mismas para cualquier frecuencia de señal), inmunidad electromagnética (no irradia ni es sensible a las radiaciones electromagnéticas), fiabilidad, mantenimiento, etc.

En los diferentes capítulos de este proyecto se hablará sobre los principales componentes del sistema de seguridad desarrollado. Se tratarán los principios básicos del Vídeo a través de la red IP, configuraciones, cámaras, servidores de vídeo, etc. Y se abordará igualmente la conveniencia que supone utilizar una integración de sistemas para programar la mayor cantidad posible de acciones ante todas las eventualidades reales y supuestas.

La integración y la arquitectura abierta permitirán que los diferentes sistemas de seguridad instalados puedan unirse y funcionar a la perfección creando buenas soluciones para la protección de los activos y las personas realizando el análisis de datos procedentes de los distintos sistemas de forma que provean de procesos más seguros eliminando el mayor número puntos débiles.

Abstract

This Project shows a security system which goal is to protect people and goods that exist in the place where it would be installed.

This protection will be done by installing a CCTV system with IP devices and an Anti-burglar alarm system.

These systems will be centralized, so that any time an intrusion occurs, the appropriate actions will be taken looking for the best effectiveness.

The IP communication will be made by optical fiber getting used of its several advantages as bandwidth, low loss or reliability.

The different chapters of the Project will deal with the mean components of the developed security system, explaining also how to integrate both systems to get the most efficient actions.

The integration and the open architecture will let the joint between the different installed systems in order to create good solutions for the protection preventing more secure process eliminating the weakest points as possible.

Agradecimientos

Gracias a mi tutor, Antonio, por servirme de ayuda en todo momento.

Gracias a Chema, por haberme dejado realizar este proyecto y estar siempre dispuesto a contestar mis dudas.

Gracias a mi hermano, por sus mimos y cuidados permanentes, por saber decirme todo sin hablar. A mi hermana, por la complicidad tan especial que siempre hay entre nosotras y ser la mejor amiga que se puede tener.

Gracias a mi madre, por darme las fuerzas suficientes para ver que solo necesito querer para conseguir todo lo que me proponga. Por alentarme sin descanso y ayudarme siempre a pintar la vida de colores. Por ser la persona que jamás me cansaré de admirar. A mi padre, por demostrarme cada día que el saber no ocupa lugar, y demostrarme que igualmente, me hará libre. Por servir de inspiración en todo lo que hago. Pero sobre todo, a los dos, por ayudarme a cumplir mis sueños, porque todo lo que soy, sin duda, es gracias a ellos. Este proyecto es vuestro.

Gracias a las bebes, por llenar mi vida de buenos momentos.

Gracias a todos los telekitos, que son sin duda, lo mejor que me llevo de estos 5 años. Por tantas horas de laboratorio, de césped, de risas, y por encima de todo, por lo que significan para mí, sin ellos, esto no se habría conseguido.

Gracias a todas las personas que de alguna forma han colaborado en este proyecto, con su ayuda ha salido adelante.

Gracias a David, por querer compartir estos sueños conmigo, por hacerlos suyos y por hacer de mi vida un cuento hecho realidad. Por querer seguir haciendo ruido a mi lado.

INDICE DE CONTENIDOS

INDICE DE FIGURAS

INDICE DE TABLAS

1. Introducción

1.1. Objetivos

Con este proyecto se busca mostrar el gran abanico de posibilidades con el que actualmente cuentan los sistemas de seguridad anti-intrusión así como los avances obtenidos respecto a los sistemas de CCTV gracias a la tecnología IP, y los múltiples beneficios de su integración.

Tras estudiar la diversidad de equipos de ambos subsistemas se establecerán las pautas necesarias para llevar a cabo un proyecto de sistema de seguridad compuesto por anti-intrusión y CCTV para más adelante presentar un caso de estudio en el que se realizará el desarrollo práctico del despliegue para unas instalaciones concretas.

Este estudio práctico expondrá la elección de equipos así como su ubicación en el plano y como estos serán integrados para una mayor efectividad. Se mostrará un estudio de costes que refleje todos los gastos asociados al proyecto.

1.2. Organización de la memoria

La memoria ha sido redactada de forma que se expliquen todas las tecnologías utilizadas en el desarrollo así como diversos aspectos de interés que pudieran resultar útiles en el diseño del sistema.

Los puntos que se han abordado son los que siguen:

i. Estudio de los equipos anti-intrusión
ii. Estudio de los equipos IP para CCTV
iii. Estudio de los pasos a seguir para el diseño de un sistema de seguridad
iv. Estudio caso práctico y desarrollo sistema de seguridad.

2. Estado del arte

2.1. Descripción General del Sistema

En la sociedad actual son múltiples y variados los peligros a los que se encuentran expuestos tanto las personas como los bienes, debiendo protegerse de las posibles amenazas mediante los instrumentos que ponen al alcance de las personas las diversas "seguridades": contra incendio, informática, vial.. la aparición de sistemas de protección en cada uno de estos campos ha estado fundamentada en la necesidad de mantener el orden público y dotar de la seguridad suficiente a una sociedad donde reinaría la inseguridad en ausencia de los citados medios y medidas de protección. Si se tiene en cuenta que la intrusión es considerada el origen de otras posibles amenazas (robo, hurto, agresiones, sabotaje, atentado, etc) y a ellas se exponen numerosas instalaciones y recintos se puede deducir que la protección contra esta amenaza se orientará en tres direcciones:

Prevención: medidas destinadas a anticiparse a la aparición de la intrusión.
Protección: actuaciones, medios y medidas destinados a evitar o reducir el riesgo de la amenaza.
Respuesta: medios destinados a neutralizar o anular este peligro.

Todos estos medios y medidas de seguridad contra la intrusión conforman un sistema de seguridad, el cual puede ser integral si se conjunta, coordina e interrelaciona con otros implantados en la instalación: incendio, control de accesos, CCTV, comunicaciones, etc.

Los medios técnicos de protección son uno de los pilares básicos de la seguridad, junto a los medios de protección humana y medios de protección organizativos. Dentro de los medios técnicos podemos establecer dos categorías:

◊ Medios técnicos pasivos: encargados de dificultar o retardar la materialización del riesgo: muros, vallas, puertas, verjas…

◊ Medios técnico activos o electrónicos: encargados de detectar e informar de la presencia de un riesgo, activar señales de alarma y facilitar información de su evolución: detectores, central de control y señalización, etc…

Por otra se encontrarían los siguientes medios o medidas:

◊ Medios Humanos: son capaces de actuar contra los intrusos para conseguir neutralizarles: vigilantes de seguridad, policías, etc.

◊ Medidas organizativas: englobaría todos aquellos documentos, normas, órdenes, planes, etc., que se establecen con la intención de coordinar el funcionamiento del conjunto de los medios citados.

Cada uno de los medios anteriormente citados desempeña unas funciones específicas:

- Prevención: se emplean medios pasivos para disuadir, obstaculizar, detener, retrasar, impedir, canalizar…, la evolución de la intrusión.

- Detección: la actividad de los medios humanos y electrónicos consistirá en vigilar, descubrir, identificar, comunicar,… la progresión de la amenaza.

- Reacción: consiste en la verificación, comprobación y evaluación del estado de la intrusión cuando se manifiestan, siendo realizados estos procesos con la ayuda de medios humanos y electrónicos.

- Respuesta: actividad primordial de los medios humanos, cuya misión consiste en neutralizar y/o anular la amenaza, aunque puede contar con el apoyo de ciertos medios electrónicos.

2.2. Detección Perimetral

Por detección perimetral se entiende todo sistema de vigilancia que, instalado en los límites de un espacio al aire libre, es capaz de señalar cualquier intento de intrusión a través de la línea que determina el contorno de dicho espacio.

Indudablemente la precocidad en la detección constituye una ventaja decisiva de la vigilancia perimetral, favoreciendo la interpretación del intruso o la puesta en fuga de éste, antes de que pueda aproximarse peligrosamente al bien a proteger.

Las condiciones ambientales desfavorables (nieve, granizo, niebla, animales en movimiento, objetos transportados por el viento, etc.) constituyen factores capaces de influenciar en la tasa de falsas alarmas, tanto mas si la elección, montaje o utilización del sistema no se llevan a cabo considerando minuciosamente las exigencias y posibilidades reales de estos equipos y del entorno en el que deberán funcionar.

La autoprotección contra el sabotaje del sistema, al igual que sucede en el resto de procedimientos de detección, no depende tanto del sistema elegido como del nivel tecnológico alcanzado por las firmas responsables de su fabricación e instalación.

Si para la vigilancia en espacios cerrados se cuenta habitualmente con fenómenos físicos característicos de la intrusión (apertura de puertas o ventanas, fractura de muros, desplazamientos del delincuente a través de zonas perfectamente delimitadas, etc.), en la vigilancia de zonas al aire libre, esta fenomenología no siempre resulta tan claramente perceptible para los equipos de detección, ya sea porque la sensibilidad de los mismos deba reducirse para limitar las alarmas intempestivas o porque el criterio de detección resulte excesivamente selectivo y por ello incapaz de captar todas y cada una de las alternativas de que dispone el intruso (túnel bajo tierra, acceso por encima de la zona de vigilancia, fractura o escalo de la cerca, etc.)

Teniendo en cuenta las prestaciones de los equipos de detección perimetral desarrolladas hasta la fecha, no existe el “procedimiento ideal” capaz de resolver satisfactoriamente todos los casos de vigilancia en el exterior. Será necesario por lo tanto, estudiar las

peculiaridades del proyecto, como condición indispensable para elegir el sistema de detección perimetral adecuado al caso en cuestión.

A pesar de los logros conseguidos, las instalaciones de vigilancia perimetral tienen cierta predisposición a provocar alarmas injustificadas. Es importante aclarar que en el número total de señales de alarmas generadas por un sistema de seguridad, podemos distinguir alarmas “ciertamente reales”, alarmas reales no deseadas, y falsas alarmas.

Las alarmas reales serán aquellas ocasionadas por un intento real de intrusión, mientras que las reales no deseadas, serán aquellas ocasionadas por eventos no controlables que provocan el correcto funcionamiento de los sistemas con la generación de la alarma. Por último se clasificarán como falsas alarmas, aquellas generadas por eventos o circunstancias controlables o no controlables, que no deberían provocar la generación de una señal de alarma.

2.2.1 Medios Pasivos

Los medios pasivos de protección, generalmente estáticos, se instalan con la intención de delimitar una propiedad o recinto, a la vez que se les exige ser capaces de disuadir a los posibles agresores. De no conseguirse este propósito deben detener, obstaculizar y dificultar la acción de los atacantes con el fin de retardar la progresión de la amenaza; de este modo se logran unos mayores tiempos de reacción para los otros medios de protección (humanos y electrónicos).

Estos medios se disponen en la zona periférica de las instalaciones con unas pretensiones y características muy concretas:

□ Sirven para delimitar la propiedad.

□ Deben constituir un elemento disuasorio: al ser visto por el intruso le hará desistir en sus intentos de agresión a la propiedad.

□ En caso contrario, deberá ser capaz de detener, obstaculizar o retardar los intentos de intrusión.

□ Adaptación a las características orográficas del terreno para garantizar una protección eficiente.

□ Canalizan las personas y vehículos hacia los puntos de acceso.

□ Se utilizan como soporte de ciertos medios electrónicos: cámaras de TV, dispositivos detectores, iluminación, etc.

□ Deben ofrecer continuidad en todo el perímetro instalado, ya sea en la combinación con puertas u otros elementos constructivos.

□ No deben ubicarse en las inmediaciones elementos ajenos (árboles, farolas, postes,...) o mobiliario urbano (contenedores de basura, papeleras, paradas de autobús,...), los cuales pueden colaborar en la superación de la barrera.

□ Se recomienda una altura superior a 2.5 metros.

□ Deben ser resistentes a las posibles condiciones meteorológicas adversas, propias del exterior: altas o bajas temperaturas, lluvia, nieve, granizo.

□ Actuación permanente y eficaz, durante las 24 horas del día.

□ No precisan un mantenimiento riguroso.

La consecución de estos objetivos, con los que se implantan los medios pasivos, implica obtener un aumento del tiempo de acción agresor para desarrollar la acción, permitiendo al resto de los medios disponibles, activos y humanos, dar la alarma y reaccionar para neutralizar la almenaza (tiempo de reacción).

2.2.1.1 Muros

Es el medio mayormente utilizado para proteger recintos de diversas extensiones, a pesar de los superiores costes de instalación. Consiste en una obra de albañilería que puede ser realizada en diferentes espesores y con materiales diversos (ladrillo, adoquín, piedras,...). superpuestos y unidos mediante una masa de yeso, cal o cemento.

Entre las características y requisitos de estos elementos se encuentran los descritos anteriormente para los medios pasivos y además destacan:

□ Resistencia y firmeza para obstaculizar y retardar la acción de los agresores, por medio de la escalada, superación, fractura, excavación.

□ Impide la visión y observación de las instalaciones o actividades en ella desarrolladas.

□ Utilización como soporte de ciertos medios electrónicos, cámaras de TV, dispositivos detectores, iluminación, etc.

□ En ocasiones se combinan en parte (hasta alturas de 50, 60, 80,... cm.) con otros medios de protección: vallas, alambradas, rejas, etc.

□ Deben ofrecer continuidad en todo el perímetro instalado, ya sea en la combinación con puertas y otros elementos constructivos.

2.2.1.2 Valla Electro soldada

Es una malla compuesta de varillas verticales y horizontales soldadas uniformemente en las intersecciones constituyendo formas cuadrangulares o rectangulares.

Básicamente sus características más importantes son semejantes a las anteriormente citadas para el muro, añadiendo entre otras que deben instalarse sobre postes anclados a tierra en base de hormigón, aunque también suele ir anclado sobre muro o murete.

También señalar que debe ofrecer continuidad en todo el perímetro instalado, ya sea en la combinación con puertas u otros elementos constructivos.

2.2.2 Sistemas Electrónicos

A la amplia variedad de Medios técnicos Activos, que se diseñan y fabrican con el fin específico de servir a la seguridad de las personas y los bienes, les vamos a denominar genéricamente Sistemas Electrónicos de Seguridad. Son un conjunto de elementos electromecánicos y electrónicos relacionados entre sí por una adecuada instalación, que a través de la información que nos proporcionan contribuyen al incremento del nivel de seguridad de un determinado entorno.

Entre las características reseñables de los sistemas electrónicos estarían:

Fiabilidad: asegurar la activación de los dispositivos de alarma en esta zona, que es la más alejada del objeto de protección.

Solidez: ofrecer resistencia a los actos de vandalismo e intentos de sabotaje.

Adaptación: inmunidad a las posibles condiciones meteorológicas adversas y cambiantes.

Sensibilidad: capacidad para diferenciar las personas de los animales de pequeño tamaño u otros objetos en el ambiente.

Disuasión: los agresores desisten de sus intenciones al percibir la implantación de los equipos.

Integración: estos sistemas pueden actuar conjuntamente con otros dispositivos electrónicos instalados en aras del objetivo de protección integral.

2.2.3 Sistemas de Intrusión

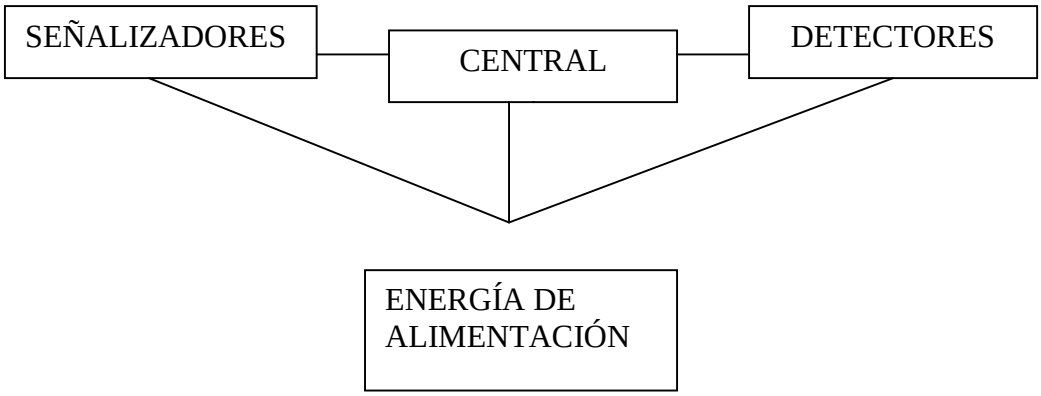
Son los elementos básicos en un sistema electrónico de seguridad que actúan como iniciadores de la alarma y su función es vigilar un área determinada y transmitir una señal al equipo de seguridad, al detectar una situación de alarma.

Están diseñados para proteger hogares y negocios. Si se produce una intrusión, se dispara la alarma y el sistema envía un aviso a la Central Receptora de Alarmas.

El sistema de seguridad anti-intrusión ideal debe alertar con la mayor rapidez posible de la entrada de un intruso, debe ser fácil de utilizar, de apariencia discreta, y capaz de proporcionar al usuario una tranquilidad absoluta.

Un sistema de seguridad anti-intrusión se basa en: control, detección y aviso. Si cualquiera de éstos tres elementos falla o produce resultados de baja calidad, es probable que el sistema no funcione adecuadamente. El sistema debe ser utilizado y controlado por personas autorizadas.

Básicamente un sistema de protección electrónica se puede distribuir en cuatro bloques:



2.2.3.1 Alimentación

Todo el sistema se alimentará de la red pública de suministro eléctrico, pero el sistema deberá ser capaz de funcionar en caso de ausencia de tensión en la red.

En la práctica la totalidad de los componentes de un sistema de protección electrónica se alimentan a doce voltios en corriente continua (12 VDC), por lo que se hace necesaria la instalación de una fuente de alimentación que transforme esos 220VCA en los 12VDC que precisa el sistema para su funcionamiento.

La potencia de estas fuentes de alimentación debe ser debidamente valorada para que pueda soportar la suma de todos los consumos de los distintos componentes del sistema de protección electrónica.

Al margen del suministro necesario para el funcionamiento del sistema de protección electrónica, la fuente de alimentación dispondrá de un dispositivo que permita la carga de unas baterías que serán las encargadas de alimentar el sistema en caso de corte del fluido eléctrico habitual.

El proceso de carga se realiza durante el suministro en condiciones normales de la red pública.

Normalmente, la capacidad de las baterías que se instalan para este propósito, es suficiente para que el sistema funcione durante unos minutos. En determinados sistemas, se utiliza como alimentación de apoyo, además de las baterías, un grupo electrógeno que asegure el suministro eléctrico durante un largo periodo de tiempo, en caso de ausencia de tensión en la red.

2.2.3.2 SAI: Sistema de Alimentación Ininterrumpida

Los equipos conocidos como SAI, sistema de alimentación ininterrumpida, o más conocido por sus siglas en ingles UPS (Uninterruptible Power Supply), es un dispositivo

que, gracias a su batería, puede proporcionar energía eléctrica tras un apagón a todos los dispositivos existentes en la red eléctrica.

Otra de las funciones de las UPS es la de mejorar la calidad de la energía eléctrica que llega a las cargas, filtrando subidas y bajadas de tensión y eliminando armónicos de la red en el caso de corriente alterna. Las UPS dan energía eléctrica a equipos llamados cargas críticas, que requieren tener siempre alimentación, equipos que deben permanecer conectados 24 horas al día, los 365 días del año a la corriente, y que ésta sea de calidad debido a la necesidad de estar en todo momento operativos y sin fallos (picos o caídas de tensión).

La unidad de potencia para configurar una UPS es el Volt Amper (VA), que es potencia aparente consumida por el sistema. Para calcular cuanta energía se requiere, debe saberse el consumo total de los equipos a proteger con la SAI. Si se conoce la potencia activa, se debe multiplicar la cantidad de Watts por 1.4 para tener en cuenta el factor de potencia.
Mientras que si los datos que se conocen de los equipos son la tensión y la corriente nominales, para calcular la potencia aparente (VA) se deberá multiplicar la corriente (Amps) por la tensión (Volts), por ejemplo: 3 Amps. X 220 Volts = 660 VA.

2.2.3.3 Señalizadores

Los señalizadotes serán los elementos encargados de avisar que se está produciendo una situación de alarma. Pueden ser de los siguientes tipos:

Local:

Sonoros ------ sirenas electrónicas / sirenas mecánicas

Visibles ------ luz destellante / flash / iluminación sorpresiva

A distancia:

Marcador telefónico / comunicaciones cableadas o vía radio.

Es conveniente utilizar simultáneamente varios tipos de señalizadotes con objeto de aumentar el grado de seguridad ante un posible intento de sabotaje de los mismos.

2.2.3.4 Detectores

Los detectores son los dispositivos encargados de informar a la central de alarmas sobre los cambios de estado producidos en los lugares protegidos.

Los detectores se pueden clasificar según el área de cobertura en:

• Puntuales: protegen un punto. Por ejemplo: contacto magnético (apertura de una puerta).

• Lineales: protegen una línea de puntos. Por ejemplo: rayos infrarrojos (pasillo).

• Superficiales: protegen una superficie. Por ejemplo: vibración, piezoeléctricos, sísmicos, microfónicos (cristal).

• Volumétricos: protegen un volumen. Por ejemplo: infrarrojos, microondas, ultrasonidos, mixtos (habitación).

2.2.3.4.1 Contactos Magnéticos

- Están basados en el empleo de un relé, constituido sus contactos por dos láminas que en presencia de campo magnético se atraen, cerrando un contacto eléctrico.

- Clasificación según la distancia máxima de apertura (separación del imán sin dar alarma): Pequeña potencia, Media potencia y Gran potencia.

- El relé se fijará en el marco y el imán en la parte móvil.

- Falsas alarmas: si la holgura de la puerta está próxima a la distancia de seguridad.

- Sabotaje: fácil.

2.2.3.4.2 Detectores De Vibración

- Detector superficial actuado por vibración. Se basan en el efecto péndulo, de forma que si existe una vibración al producirse el desplazamiento del péndulo, se ocasiona la apertura de un circuito eléctrico que genera la señal de alarma.

- Se debe tener en cuenta: la estabilidad del paramento donde se fijan, la superficie máxima de operación y la rigidez del paramento.

- Aplicación: muros y acristalamientos.

- Falsas alarmas: las producidas por vibraciones externas.

- Sabotaje: dificultad media.

2.2.3.4.3 Detectores Microfónicos

- Detector superficial actuado por vibración. Se basan en el uso de un micrófono y circuito de análisis, que registra y mide las ondulaciones acústicas producidas por la vibración. Se genera una alarma cuando se supere un valor predeterminado
.
- Diseño: no sobrepasar el área máxima de cobertura y se debe atender, según la protección que se pretende establecer, a los ajustes de sensibilidad variables.

- Aplicación: Rotura de acristalamientos, techos, suelos y muros.

- Registro del sonido producido por la rotura de cristales (detector instalado en elemento constructivo fuera de la superficie acristalada).
- Evaluación de las alteraciones sonoras ambientales en la zona a proteger (detector instalado en zona protegida).

- Falsas alarmas: pocas.

- Sabotaje: difícil.

- Coste elevado para grandes superficies.

2.2.3.4.4 Detectores Piezoeléctricos

- Detector superficial por rotura de paramentos rígidos. Reacciona ante vibraciones mecánicas producidas en las partículas del material al que están adheridos.

- Se basan en un elemento sensor capaz de distinguir alteraciones vibratorias y traducirlas en señal de alarma al superar unos niveles específicos.

- Diseño: no sobrepasar el radio máximo de cobertura y se debe atender, según la protección que se pretende establecer, a los ajustes de sensibilidad variables.

- Aplicación: cerraduras, acristalamientos, techos, suelos y muros.

- Falsas alarmas: escasas.

- Coste excesivo para grandes desarrollos.

2.2.3.4.5 Detectores Sísmicos

- Detector superficial por rotura de paramentos rígidos. Reacciona ante vibraciones mecánicas producidas en las partículas del material al que están adheridos.

- Es una aplicación de las utilidades de los microfónicos y del efecto piezoeléctrico.

- Comparativa con los detectores piezoeléctricos: estos cuentan con un “filtro paso bajo” que restringe las frecuencias a aquellas que están en el espectro de agresiones o ataques de carácter destructivo.

- En el diseño se debe tener en cuenta: no sobrepasar el área máxima de cobertura.

- Aplicación: cajas fuertes, cámaras acorazadas y muros.

- Falsas alarmas: muy pocas.

- Sabotaje: muy difícil.

2.2.3.4.6 Detectores Infrarrojos

- Están basados en la captación de energía infrarroja que emite un cuerpo humano por medio de un elemento piroeléctrico.

- Tipos de detectores:

* Abanico: cubren 90º con tres grados de inclinación.
* Lineales: larga distancia con pequeña apertura.
* Cortina: cubren un plano de 90º.
* Panorámico: tienen un modelo de detección de 360º.

- Para el diseño se tendrá en cuenta: el área máxima de cobertura, evitar dispositivos que generen corrientes de aire y respetar la altura de montaje.

- Falsas alarmas: producidas por corrientes de aire.

- Sabotaje: difícil si tiene la función anti-masking.

2.2.3.4.7 Detectores Microondas

- Están basados en la detección de movimientos mediante el efecto Doppler.

- Funcionamiento: el emisor emite una frecuencia que es reflejada por los objetos que le rodean. Esta señal es captada por un receptor asociado en el caso de que se desplacen los objetos. La frecuencia recibida es distinta a la emitida generándose una señal de alarma que produce la apertura de los contactos de un relé.

- Para el diseño se tendrá en cuenta: el ángulo de apertura y alcance y respetar la altura de montaje.

- Si se emplea más de un detector microondas, deben trabajar a frecuencias distintas para evitar que interfieran mutuamente.

- Cubren un volumen no confinado.

- Falsas alarmas: desplazamientos de objetos, movimiento del paramento al que están fijados, cañerías que recorren los muros y sobrepasar su alcance la zona de cobertura.

- Sabotaje: difícil si tiene la función anti-masking.

2.2.3.4.8 Detectores Ultrasonidos

- Están basados en la detección de movimientos mediante el efecto Doppler.

- Consta de:
* El transmisor de ultrasonidos que opera generalmente en frecuencias bajas
* Receptor que recoge las señales y las transforma a señal eléctrica
* El procesador electrónico que analiza la señal y la compara con la muestra predefinida

- Para el diseño se tendrá en cuenta: el ángulo de apertura y alcance y respetar la altura de montaje.

- Cubren un volumen confinado.

- Falsas alarmas: numerosos objetos pueden generar ultrasonidos (timbres, motores).

- Sabotaje: difícil.

- Coste elevado.

2.2.3.4.9 Detectores Mixtos, doble tecnología

- Se basan en el empleo simultáneo de un detector infrarrojos (sensible a variaciones de energía térmica) y un detector microondas (sensible a movimientos).

- Solamente se genera alarma cuando existe doble detección. Con esto se consigue la eliminación de la mayoría de las posibles falsas alarmas (corrientes de aire, caída de objetos, etc.).

- Para el diseño se tendrá en cuenta: el ángulo de apertura y alcance y respetar la altura de montaje.

- Sabotaje: difícil si tiene la función anti-masking.

2.2.3.5 Barreras de rayos IR

Equipo constituido por emisor de rayos infrarrojos y receptor que forman (verticalmente) una barrera invisible; la interferencia de elementos extraños en la continuidad de los rayos activará los dispositivos de alarma.

Entre sus características y requisitos se puede resaltar:

♦ El emisor genera los haces de luz infrarroja con una determinada longitud de onda y los dirige hacia el receptor.

♦ El receptor consta de un circuito electrónico cuya misión es analizar y verificar que los haces de luz infrarroja se reciben sin ser interrumpidos.

♦ Equipos desde un haz hasta columnas de varios haces diseñadas específicamente. Cuantos más haces se dispongan mayor garantía de detección.

♦ Programación de parámetros para activación de la alarma en función de las necesidades de protección y para evitar las falsas: al cortar un haz, dos,...simultáneo o alterno, temporizado, etc.

♦ Funcionamiento fiable en condiciones atmosféricas cambiantes mediante el ajuste automático de temperatura, la discriminación de objetos transportados en el aire, la lluvia, el granizo, la nieve, etc.

♦ Discriminación de animales, especialmente de menor tamaño y voladores (aves, insectos,..).

♦ Inmunidad a la luz solar, luces de vehículos, focos eléctricos, etc.

♦ Facilidad para la alineación óptica precisa de forma sencilla.

♦ Tanto el emisor como el receptor deben fijarse correctamente al suelo o soporte para impedir la pérdida de alineación a causa del fuerte viento o impactos.

♦ Posibilidad de montaje sobre mástiles, postes o paredes.

♦ Accesorios: contactos o tamper antisabotaje, carcasa antivandalismo, calefactor para ambientes fríos, termostato, etc.

♦ Alcance: superiores a 200 metros y con posibilidad de regulación.

2.2.3.6 Barreras de Microondas

Equipo constituido por emisor de radiación electromagnética y receptor que crean un espacio o volumen protegido invisible; la irrupción de elementos extraños en el campo creado activará los dispositivos de alarma.

Sus características y requisitos son:

♦ El emisor genera ondas electromagnéticas que se emiten en frecuencias próximas a los 10 Ghz y son dirigidos hacia el receptor. Un mismo dispositivo puede disponer de varias frecuencias de emisión.

♦ El receptor consta de un circuito electrónico cuya misión es analizar y verificar que las ondas se reciben sin sufrir modificaciones en su longitud de onda.

♦ Difícilmente vulnerable al crear un espacio protegido totalmente volumétrico.

♦ Programación de parámetros para activación de la alarma: incremento de la señal, variación dela frecuencia de modulación, desalineamiento, apertura de carcasa, etc.

♦ Control automático de ganancia.

♦ Ajuste de la anchura del volumen sensible y del margen de sensibilidad.

♦ Selector de canales.

♦ Ajuste del intervalo de tiempo de muestreo.

♦ Funcionamiento fiable en condiciones atmosféricas cambiante: lluvia, niebla, etc.

♦ Discriminación de animales.

♦ Tanto el emisor como el receptor deben fijarse correctamente al suelo o soporte para impedir la pérdida de orientación a causa del fuerte viento o impactos.

♦ Posibilidad de montaje sobre mástiles, postes o paredes.

♦ Accesorios: contactos o tamper antisabotaje, carcasa antivandalismo, calefactor para ambientes fríos, termostato.

♦ Alcances superiores a 200 metros y con posibilidad de regulación.

♦ Tipos de barreras: biestáticas, monoestáticas, seguidoras del terreno.

2.2.3.7 Barreras de Láser

Equipo constituido por emisor de rayos láser y receptor que forman (verticalmente) una barrera invisible; la interrupción de elementos extraños en la continuidad de los rayos activará los dispositivos de alarma. Sus componentes, características y requisitos son análogos a los detallas en el apartado de las barreras de infrarrojos, con la salvedad del empleo de luz coherente en la tecnología láser en vez de radiaciones infrarrojas.

Otra diferencia fundamental es el superior alcance de la barrera láser pero su elevado coste condiciona su elección frente a los infrarrojos.

2.2.3.8 Barreras Sensoras

Las barreras sensoras son dos opciones de seguridad en una. Son a la vez una barrera a la intrusión y un sistema de sensores. Los sensores de cable tensado son un ejemplo de una barrera sensora que ofrece una Tasa de falsas alarmas casi nula y una Probabilidad de detección insuperable. Estos sensores prácticamente no tienen limitaciones ambientales y pueden dar un servicio confiable durante muchos años.

2.2.3.9 Cable Sensor o Microfónico

Se trata de un cable coaxial (elemento sensor) que capta las vibraciones producidas en el soporte (valla, alambrada, paredes, concertinas...) para ser transmitidas a una unidad de proceso donde se analizan y procesan las señales aportadas por el transductor: vibración, fractura, empuje, presión doblamiento, etc.

Entre sus características destacan:

♦ Las vibraciones captadas son convertidas en sonidos diferenciados que permitirán distinguir las alarmas reales (corte, perforación, levantamiento, excavación,...) de las falsas alarmas (peso o impacto de aves, fuerza del viento y objetos transportados, lluvia, granizo, etc.)

♦ Programación del equipo mediante la selección de las señales que ocasionarán alarma: compensación de las condiciones climáticas, filtración de ruidos, zonificación variables, etc.

♦ Proporciona una detección lineal en toda la longitud del cable.

♦ Alcance: hasta 300 metros por cada tramo o zona.

♦ Adaptación a diferentes tipos de vallas y otros soportes.

♦ Etc...

2.2.3.10 Sensores montados en cercas

Los sensores montados en cercas o paredes, detectan al intruso cuando éste perturba el campo de detección o cuando la vibración producida por cortar o escalar una cerca metálica, dispara una alarma.

2.2.3.11 Campo Eléctrico

Los sistemas de detección de campo eléctrico de superficie requieren de un elemento que permita su fijación, puede ser incluso la propia valla o muro de delimitación, aunque también puede instalarse sin más que unos simples postes soporte. La aproximación del intruso ocasiona una perturbación en el campo eléctrico, suficiente para activar la alarma.

Este sistema resulta particularmente apropiado para vigilar zonas de orografía y contorno perimetral irregulares.

Estos sistemas ofrecen una notable seguridad en la captación del intruso y su instalación puede llevarse a cabo ocupando una zona de detección relativamente reducida.

Contrariamente este procedimiento comporta costos importantes, sobre todo en lo relativo a su montaje en el lugar.

2.2.3.12 Enterrados

En esta categoría se incluyen los sistemas de detección diseñados para su instalación debajo del suelo (del orden de 30cm como máximo)

Entre los más típicos se encuentran la detección neumática y la radiofrecuencia. Se basan en principios operativos radicalmente diferentes, pero ambos cumple idéntica función: detectan el paso por encima de sus elementos sensores, configurando una banda de terreno sensibilizado y totalmente invisible (una vez homogeneizado el terreno).

La detección neumática utiliza como criterio de detección las variaciones de presión del terreno, que ocasiona el intruso la desplazarse en las proximidades del sensor enterrado en el suelo; mientras que la radiofrecuencia puede considerarse como variante del sistema de campo eléctrico. Consiste en dos cables con apantallamiento especial que actúan como emisor y receptor de un campo de radio frecuencia, produciéndose la alarma cuando la señal que llega al cable detector, se atenúa por la presencia de un intruso en el interior de dicho campo.

2.2.3.13 Fibra Óptica

Entre las posibles aplicaciones como consecuencia del auge de la transmisión por fibra óptica se encuentra la de sistemas de protección enterrados, si bien no ha sido ni de lejos competencia para los dos sistemas expuestos anteriormente.

Consiste en un cable de fibra óptica que va enterrado a unos 6cm. de profundidad. El cable en sus extremos está conectado a un emisor y a un receptor láser. Cuando se pisa sobre el terreno la vibración producida provoca una deformación en el cable, lo que se transforma en una variación de la transmisión lumínica. Esta variación se analiza en la unidad de control, y si se sobrepasa un nivel preestablecido, se producirá una alarma.

2.2.4 Central de Alarma

La central de alarma es el cerebro de todo el sistema, posee un microprocesador que es el encargado, de acuerdo a su programación, de recibir las señales de los sensores y tomar acciones como activar una sirena, un emisor telefónico, etc. La central dispone de un cargador automático para batería que será la encargada de alimentar a todo el sistema en caso de corte del suministro eléctrico.

Los modelos disponibles de centrales parten de una base de 4 zonas y existen modelos hasta 128 zonas. Los modelos multiplexados (Particiones) permiten a partir de cuatro cables particionar una central de alarma funcionando la misma como si fueran dos o cuatro centrales independientes.

2.2.4.1 Funcionamiento y Partes

Equipo diseñado para el control y gestión de las alarmas generadas en los dispositivos de detección. Se integra en un Sistema Electrónico de Seguridad donde su misión consiste en:

- Recibir las señales emitidas por los detectores, pulsadores u otros iniciadores.

- Activar las señales, discriminar las alarmas y localizarlas.

- Advertir por medio de señales acústicas y/ u ópticas de las alarmas generadas.

- Transmitir señales de alarmas y pre-alarma a centrales receptoras de alarma.

- Memorizar o registrar información relativa a cierto número de alarmas.

- Supervisar continuamente la operatividad de la instalación y mostrar las averías o fallos detectados: cortes de líneas, sabotajes, interrupciones de alimentación, inactividad, cortocircuitos, etc.

- Generar señales de comunicación con otros dispositivos o equipos.

Los componentes principales son:

Entradas: puntos para conexión de las líneas que unen la centra y la red de detección, posibilitando la comunicación (información y señales) entre ambos.

Salidas: conexiones con otros dispositivos periféricos: sirena, ordenador, impresora...

Circuitos de análisis: analizan las señales recibidas para rehusar, o activar la alarma al cumplirse ciertos requisitos previamente programados.

Comunicación: el modo de transmisión de las señales e información entre la central y los iniciadores.

Elementos de control: permiten el control operativo del sistema de seguridad en las instalaciones (locales) o desde lugares alejados (remotos).

Alimentación: proviene de la red eléctrica, debiendo contar, además, con baterías que garanticen el funcionamiento en caso de interrupción del suministro eléctrico. Proporciona la energía necesaria a la central, enlaces y dispositivos de alarma.

Contenedor: es la caja, cuadro, armario, rack, etc. donde se hallan los circuitos electrónicos que controlan el funcionamiento de la central.

2.2.4.2 Características y Funciones

Se enumeran una serie de funciones y prestaciones generales de las centrales de intrusión, que convierten a estos equipos en adecuados para garantizar un nivel óptimo de seguridad:

Diseño modular: Fácil ampliación mediante módulos de expansión, de entradas y salidas (conexión en serie y/ o paralelo).

Control de un número variable de zonas, programables: retardadas, instantánea, pánico, alarma técnica, pre-alarma,...

Partición del sistema: posibilidad de crear conjuntos de zonas (y establecer una zona común) que operen independientemente.

Programación y control local desde el teclado integrado en la central.

Programación y control remoto por medio de uno o varios teclados u ordenador, equipado con módem y software apropiado, apto para entornos de uso generalizado.

Programación manual o ayudada por menús: condiciones de activación de la alarma, por zonas, tiempos, salidas de relés,...

Armado / desarmado total o parcial desde teclados, telemandos o lector de llave electrónica. Armado automático o al pulsar una tecla.

Establecer diferentes códigos: maestro de programación, de usuario, etc., asignables a todas las zonas o unas específicas, a determinadas horas, etc.

Tipos de circuitos: NA, NC, RFL, supervisados, etc.

Transmisión de alarmas mediante comunicador (vocal y/ o digital) en formatos multiprotocolo. Transmisión bidireccional, vía radio o cable.

Memoria de eventos, con fecha y hora, clasificados por grupos, opción de comunicación a central receptora u ordenador, recuperarlos e imprimirlos, visualizar en pantalla, salvaguardia entre cortes de corriente, etc.

Supervisión (autotest) permanente de la operatividad de la central: líneas, entradas, salidas,...

Enlace vía radio (sistemas inalámbricos) o *cable* (sistemas cableados) con medios de detección.

Conexión de periféricos, impresora, módem, sinópticos, etc.
Programación del tiempo de entrada/ salida, dentro de los intervalos establecidos.

Integración de medios de detección de incendios, de atraco/ robo, medios técnicos, etc.

Salidas de alarma: sirena interior o exterior, lanza destellos, luz estroboscópica, comunicación silenciosa, etc.

Caja de la central: equipada con cerradura y llave, tamper (para pared y/ o caja), protección contra la corrosión y vandalismo, de metal, de policarbonato, de chapa galvanizada,..

Respecto a una de las características anteriormente citada, medio de comunicación, sería bueno anotar que, en el estudio que se realice para la instalación de un subsistema anti-intrusión se debe considerar la posibilidad de llevar a cabo una instalación con sistemas vía radio. No obstante es importante matizar y señalar que dicha ventaja es únicamente estética y de instalación. Desde el punto de vista exclusivo de la seguridad es preferible y mucho más "ventajoso", la instalación de equipos cableados.

Las razones a grandes rasgos son las siguientes:

- Un detector cableado, no se puede sabotear, no se puede interferir, y no se puede cortar el cable sin que la central lo detecte.

- La tecnología vía radio siempre va ligada a la central y su correspondiente fabricante, por tanto obliga a la sustitución de todos los equipos en caso de cambio de la central.

- Los equipos vía radio pueden verse afectados, excepcionalmente, por interferencias locales. Este problema nunca afectará a un detector cableado.

Sin embargo, y a pesar de estos motivos, existen casos, en los que resulta inviable acometer una de estas instalaciones cableando. En todos estos casos el poder disponer de un elemento que ofrece una solución vía radio puede ser considerado como una "ventaja", aunque esta ventaja sólo sea por la posibilidad de poder elegir entre un elemento cableado o uno vía radio.

2.2.4.3 Componentes y Accesorios

En este apartado se exponen aquellos componentes que se pueden añadir a la central de señalización y control para incrementar sus prestaciones:

Módulos de expansión de zonas: permiten aumentar el número de zonas a controlar.

Módulos de salida de relés: activan funciones inherentes a las señales recibidas y analizadas.

Teclados de leds, alfanuméricos o de membrana: control y gestión de la central, tanto local como remotamente.

Comunicador, telefónico o vía radio: facilita la transmisión de alarmas, tests, escucha ambiental,... y permite la comunicación bidireccional, todo ello en tiempo real.

Marcador telefónico: posibilita el envío de mensajes pregrabados a una serie de números predeterminados por el titular de la instalación objeto de protección.

Fuente de alimentación: con información referente a fallo de red y batería, fusibles fundidos; voltaje regulable, programar un valor límite de consumo.

Lector de llave electrónica: la cerradura electrónica es un medio de control alternativo al teclado que permite la conexión/ desconexión desde el exterior de los espacios protegidos.

Módem: convierte las señales para su transmisión por redes de datos y su correcta recepción.

Software de programación y control, con interfaz gráfica intuitiva, fácil de usar y operando bajo un entorno de uso generalizado.

Software de gestión y control remoto, de idénticas características al anterior.

Interfaz para conexión de la central a ordenador.

Interfaz para la identificación individual de detectores.

2.2.4.4 Posibles Clasificaciones

En función de los criterios utilizados existen diversas clasificaciones para las centrales:

♦ En función de la aplicación de diseño:

◊ Centrales de intrusión.

◊ Centrales combinadas: integran las funciones de los sistemas de intrusión, incendio, atraco/ robo,... en el mismo equipo.

♦ Por la tecnología:

◊ Centrales convencionales.

◊ Centrales microprocesadas.

◊ Centrales computerizadas.

♦ Por el medio de transmisión de las señales e información:

◊ Centrales inalámbricas: la transmisión se efectúa vía radio, sin necesidad de instalar líneas de cableado.

◊ Centrales alámbricas: emplean el cable como medio de transmisión de señales y datos entre los diferentes componentes.

♦ Según la función de la central:

◊ Central principal.

◊ Central secundaria.

◊ Central auxiliar.

◊ Central repetidora.

2.2.5 Teclados

El teclado es el dispositivo que permitirá realizar las programaciones de la central de alarma así como también realizar el control del sistema como activación, desactivación, cancelación de zonas, etc.

Dentro de la programación se realizarán tareas tales como programación de claves, tiempos de entrada/salida, duración de la sirena, y diferentes tipos de zonas como ser perimetral, interna, temporizada, etc.

Los teclados podrán ser con leds (luces) indicadores o con display alfanumérico que a través del mismo se visualizarán palabras con indicaciones de fácil lectura.
Un sistema podrá disponer de más de un teclado como también podrá conectársele un control remoto para realizar activaciones y desactivaciones a distancia.

2.2.6 Software de Programación y Control

Las necesidades de protección obligan a la instalación de numerosos sensores y dispositivos, con prestaciones diversas y funcionamientos diferentes. Las aplicaciones informáticas posibilitan la gestión integral y conjunta de estos medios tan heterogéneos, además de facilitar la realización de las operaciones de control programación y gestión.

Entre sus características y prestaciones destacan:

- Compatibilidad con sistemas operativos de uso generalizado.

- Opción de diferentes idiomas, incluido el castellano.

- Configuración, programación y control de un mayor número de sensores, detectores, zonas, grupos teclados, horarios, usuarios, líneas BUS, etc., desde estaciones locales o remotas.

- Configuración del sistema según necesidades del cliente.

- Rapidez al realizar las operaciones, tanto local como remotamente: armado/ desarmado, inhibir, consultas, eventos, etc.

- Memorización, recuperación e impresión de eventos; posibilidad de guardar ficheros históricos.

- Presentación y gestión de gráficos, planos, esquemas, etc. En formatos compatibles con sistemas operativos convencionales. Esta prestación facilita la localización exacta de los diferentes medios.

- Posibilidad de intervenir directamente sobre dichos medios desde la pantalla, consiguiente una mayor prontitud en la actuación y, consecuentemente, un incremento del nivel de protección.

• Presentación de instrucciones en pantalla, cuando suceden fallos, averías o alarmas, con el fin de facilitar la toma de decisiones a los operadores.

El empleo de las aplicaciones específicas de programación, de control, de gestión, de control remoto,... está orientada hacia sistemas computerizados y aquellos con implantación en red, donde se hallan múltiples dispositivos ya que facilita las tareas de altas, bajas, modificación de condiciones, consulta de estados, registro y recuperación de eventos, agrupación de funciones, ejecución de tareas automáticas, elaboración de archivos históricos, etc.

2.2.7 Transmisión de Alarmas

Los medios de transmisión de alarmas garantizarán la emisión y recepción de las señales, mensajes y datos generados con el fin de mantener la fiabilidad y operatividad del sistema.

Los elementos imprescindibles para que se produzca la transmisión son: emisor, receptor y vía de transmisión (radio o cable).

Los medios cableados, redes telefónicas, son los más habituales para la transmisión de alarmas a centro de control o central receptora, empleándose los sistemas de radio como segunda vía de comunicación de alarmas. Cuando se trata de personas privadas la transmisión puede hacerse a teléfonos fijos (cable) o aprovechar las nuevas redes de telefonía móvil (GSM, UMTS). La transmisión vía radio permite, asimismo, la recepción de alarmas en buscapersonas.

2.2.8 Central Receptora de Alarmas, CRA.

La función de una CRA (central receptora de alarmas) es la recepción de señales emitidas debido a un salto de alarma por un intruso a las diversas instalaciones de seguridad.

Estas señales llegan a dicha Central a través de la línea telefónica, bien sea línea fija o GSM (móvil) a el receptor de alarmas, el cual está conectado a su vez con una red informática interna la cual gestiona toda la información recibida.

Una vez recibida, la CRA se pone en contacto con el cliente para verificar que no se trata de una falsa alarma, pidiéndole al conectado que se identifique con una clave.

Algunos equipos disponen del servicio habla y escucha, por lo que desde la misma central receptora pueden comprobar ruidos y distintos sonidos deduciendo si hay alguna intrusión.

El siguiente paso por parte de la CRA, es ponerse en contacto con el cuerpo de seguridad más cercano y dando aviso de un posible robo, la hora de la llamada queda registrada, por lo que se hace un seguimiento exhaustivo de las fuerzas de seguridad.

2.3. CCTV

El Circuito cerrado de televisión o su acrónimo CCTV, que viene del inglés: Closed Circuit Television, es una tecnología de vídeo vigilancia visual diseñada para supervisar una diversidad de ambientes y actividades.

Se le denomina circuito cerrado ya que, al contrario de lo que pasa con la difusión, todos sus componentes están enlazados.

Básicamente, el sistema consiste en varias cámaras colocadas en lugares estratégicos, que filman y transmiten imágenes a los monitores de la oficina central de vigilancia. El sistema ideal de CCTV debe proporcionar imágenes de excelente calidad tanto de día como en la oscuridad, ser flexible y fácil de usar y proporcionar imágenes para grabar evidencias o para ayudar a analizar cualquier incidente.

Los sistemas de CCTV pueden ser personalizados para adaptarse a la actividad de la propiedad o el establecimiento y a las necesidades del cliente. Pueden instalarse por varias razones, como por ejemplo para disuadir a posibles ladrones, observar actividades por motivos de seguridad o de información, documentar continuamente una zona o proceso, o analizar un incidente en particular.

Estos sistemas incluyen visión nocturna, operaciones asistidas por ordenador y detección de movimiento, que facilita al sistema ponerse en estado de alerta cuando algo se mueve delante de las cámaras. La claridad de las imágenes puede ser excelente, se puede transformar de niveles oscuros a claros... Todas estas cualidades hacen que el uso del CCTV haya crecido extraordinariamente en estos últimos años.

2.3.1 Descripción Sistema CCTV

El sistema de vigilancia por circuito cerrado de televisión consta de un conjunto de dispositivos que permiten captar y enviar imágenes y sonido desde la zona vigilada a los puestos de tratamiento de datos con el objetivo de controlar y proteger un espacio definido.

Los componentes de un CCTV pueden ser muy diversos en función de la aplicación específica, las necesidades o de criterios económicos:

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

Básicamente los sistemas de CCTV admiten desde sencillas instalaciones compuestas de cámaras, monitor y videograbador, hasta complejos sistemas integrados por múltiples y avanzados elementos multiplexores, videosensores, 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 en todo tipo de instalaciones con la pretensión de obtener imágenes de las zonas donde se produce la intrusión y almacenar las imágenes captadas. Por último reseñar que ciertas autoridades, competentes en materia de seguridad pública o privada podrán ordenar la instalación obligatoria de equipos o sistemas de captación y registro de imágenes en determinados establecimientos, como es el caso de los bancos, cajas de ahorro y demás entidades de crédito donde se custodien fondos o valores, e, incluso en la vía pública.

A pesar de la gran variedad de equipos existentes que pueden componer un CCTV solamente vamos a explicar aquellos que por el motivo del proyecto vayan a ser utilizados en nuestro diseño, mencionando solo algunos otros en caso de necesitarlo porque se les haga referencia en algún momento.

La cámara es el elemento básico de todo CCTV, cuya misión consiste en capturar imágenes (también sonidos) que se suceden en su campo de visión u observación.

Las señales ópticas captadas son transformadas en señales eléctricas para enviarlas, por los medios de transmisión (cables u ondas), hasta los puestos de tratamiento, donde los equipos (conversor, módem, monitor, etc.) restituyen la imagen tomada en el espacio vigilado.

Una posible clasificación de cámaras sería la diferenciación entre cámaras monocromas (blanco y negro) o de color.

Como criterio aplicable generalmente, sería positivo instalar las primeras en las zonas de escasa iluminación, ya que su sensibilidad es superior. Así mismo, para conseguir imágenes nítidas y definidas la resolución debe ser elevada, teniendo en cuenta que la información obtenida se presenta en la combinación de dos colores.

Por otra parte la menor sensibilidad propia a las cámaras en color convierte a estos dispositivos en imprescindibles cuando las condiciones de iluminación son buenas. En cuanto a la resolución, puede ser inferior a la de las cámaras monocromas ya que las imágenes captadas en color proporcionan una información más completa y detallada, información más real, muy valiosa para la identificación de situaciones, personas u objetos.

Así mismo, existen cámaras que operan en color durante las horas de máxima luminosidad y se pueden conmutar a B/N en condiciones de escasa iluminación (noche) debido a la mayor sensibilidad de las monocromas. Las prestaciones de la vigilancia nocturna se puede complementar mediante la instalación de focos de luz infrarroja. Por último, comentar la comercialización de cámaras falsas provistas de óptica simulada, cuyas funciones son la disuasión y el control psicológico.

Ambos tipos de cámaras cuando se ubiquen en el exterior serán resistentes a las inclemencias meteorológicas y la corrosión, mientras que cuando se instalen en ambientes contaminantes o agresivos deberán tolerar estos agentes.

Las cámaras pueden incorporar un videosensor, el cual no es un equipo, sino un procesador de la señal de vídeo que analiza la imagen captada por una cámara de televisión detectando cualquier variación que se produzca en la zona vigilada y comunicando el consiguiente estado de alarma. Entre otras opciones que pueden presentar destacan la instalación inalámbrica, la existencia de cámaras con iluminación infrarroja, ocultas, automáticas día/noche, sumergibles, blindadas, con conexión "plug and play", etc..

2.3.2 ¿En que consiste una cámara de CCTV?

Una cámara de CCTV está compuesta fundamentalmente por un dispositivo captador de imágenes, un circuito electrónico asociado (DSP) y una lente, que de acuerdo a sus características nos permitirá visualizar una escena determinada.

El dispositivo captador de imágenes, denominado comúnmente CCD o CMOS, está compuesto por cerca de 300.000 elementos sensibles denominados píxeles y su formato en las cámaras estándar es de 1/3" o 1/4". Las especificaciones más importantes son :

Alimentación: 220 VCA, 24 VCA y/o 12 VCC

Tipo de sensor: CCD o CMOS y su respuesta espectral (color, blanco y negro y/o infrarrojo).

El sensor de imagen de la cámara se encarga de transformar la luz en señales eléctricas. Cuando se fabrica una cámara, existen dos tecnologías de sensor de imagen disponibles:

■ CCD (Dispositivo de acoplamiento de carga)

■ CMOS (Semiconductor de óxido metálico complementario)

Los sensores CCD se fabrican usando una tecnología desarrollada específicamente para la industria de cámaras, mientras que los sensores CMOS se basan en una tecnología estándar ampliamente utilizada en los chips de memoria como por ejemplo, dentro de un PC.

Tecnología CCD

Los sensores CCD llevan utilizándose en las cámaras desde hace más de 20 años y presentan muchas ventajas de calidad, entre las cuales cabe destacar una mejor sensibilidad a la luz que los sensores CMOS. Esta mayor sensibilidad a la luz se traduce en mejores imágenes en situaciones de luz escasa. Sin embargo, los sensores CCD son caros ya que están fabricados siguiendo un proceso no estandarizado y más complejo para ser incorporados a una cámara. Además, cuando existe un objeto muy luminoso en la escena (como, por ejemplo, una lámpara o la luz solar directa), el CCD puede tener pérdidas,

provocando rayas verticales por encima y por debajo del objeto. Este fenómeno se llama "smear" (mancha).

Tecnología CMOS

Los recientes avances en los sensores CMOS los acercan a sus homólogos CCD en términos de calidad de la imagen, pero los sensores CMOS siguen siendo inadecuados para cámaras donde se exige la máxima calidad de imagen posible. Los sensores CMOS proporcionan soluciones de cámaras más económicas ya que contienen todas las funciones lógicas necesarias para fabricar cámaras a su alrededor. Hacen posible la producción de cámaras de un tamaño menor. Los sensores de tamaño mayor ofrecen una resolución megapíxel para una variedad de cámaras de red. Una de las limitaciones actuales de los sensores CMOS es su menor sensibilidad a la luz. En condiciones de luz normales esto no supone ningún problema, mientras que en situaciones de escasa luz se vuelve manifiesto. El resultado es una imagen muy oscura o una imagen con apariencia granular.

Tamaño del sensor: 1/4“, 1/3”, 1/2", 2/3", 1“

Resolución: es una medida de la calidad con que se reproducen los detalles finos de una escena. Cuantos más PIXELES posea el CCD mejor será la resolución de la cámara. Las cámaras estándar tienen 380 líneas de resolución (TVL), mientras que las cámaras profesionales van de las 420 a las 550 TVL. En la mayoría de las aplicaciones de CCTV se usan cámaras de resolución estándar (420TVL).

Audio: para escuchar el sonido del ambiente donde está instalada la cámara

Otras características de las cámaras CCTV

Sensibilidad: informa de la capacidad de reproducción de imágenes de video en condiciones de baja iluminación. Es la cantidad de iluminación mínima de una escena para obtener la señal de video. La sensibilidad se mide en LUX. Las cámaras blanco y negro tienen en general una sensibilidad de 0,01 LUX. En cambio las cámaras color tienen una sensibilidad aproximada de 0,1 a 1 LUX.

Iris Electrónico: también conocido como AES (Automatic Electronic Shutter), controla en forma automática la cantidad de luz que penetra en la cámara. Cuanto mayor es la velocidad de control, que puede variar entre 1/60 y 1/100.000 de segundo, mejor será la compensación de la imagen en condiciones de luz brillante. El concepto del iris electrónico es similar al de las lentes autoiris, pero como la compensación se realiza en forma electrónica, el rango de variación comparado con las lentes autoiris es menor y su aplicación se limita a cámaras de uso interior.

Montaje de la Lente: las cámaras de tipo profesional vienen preparadas para colocar diferentes tipos de lentes, que se seleccionan para la visualización de una escena determinada. Existen dos tipos de montajes: C y CS. La diferencia entre ambos es la distancia focal posterior mecánica entre la base de la lente y el área de enfoque de la imagen que es donde se encuentra el CCD. Esta distancia es de 17,526mm para una lente con montaje C, y de 12.50mm para las de montaje CS. Las cámaras actuales más populares de formato 1/3" vienen preparadas para lentes con montaje tipo CS. No obstante

puede usarse una lente con montaje tipo C colocándole una arandela de 5 mm para lograr la distancia focal necesaria.

Compensación de luz trasera: Cuando se debe visualizar una escena o un objeto que tiene una luz brillante detrás, se deberá seleccionar una cámara que posea compensación de luz trasera o BLC (Back-Light Compensation). Si la cámara está instalada en un ambiente interior, enfocada hacia una puerta de entrada o una ventana y no posee esta función, el reflejo del sol o luz diurna hace que la imagen en el monitor cuando una persona entre por la puerta o pase frente a la ventana, sea una silueta negra. La función del BLC es básicamente "engañar" electrónicamente a la cámara para que no registre la luz trasera, elimine el efecto de silueta y reproduzca una imagen clara en difíciles condiciones de luz generada a través de un oscilador interno de la cámara. Las cámaras que trabajan con CA se pueden sincronizar con la frecuencia de red (LLC – line lock control). El ajuste del nivel de fase del sincronismo vertical, evita saltos indeseables durante la reproducción del video en vivo o cuando se reproduce una grabación luego de ocurrido un evento.

Capacidad para aceptar lentes autoiris: La gran mayoría de las cámaras profesionales actuales aceptan lentes de tipo autoiris. Sin embargo existen dos tipos: control por video (VD – video drive) y control directo (DC – direct control). Cuando se realiza la elección de la cámara es importante comprobar que tipo de lente autoiris acepta. Las lentes autoiris del tipo DC son menos costosas que las del tipo video y tienen la misma función.

Relación Señal /Ruido (S/N - Signal Noise): Mide la inmunidad a ruido eléctrico proveniente de la línea de alimentación. Las normas recomiendan 46dB como mínimo.

AGC (Control Automático de Ganancia), valor típico: 30dB. Mantiene la salida de la señal de video en un nivel de 1V pico a pico, con una carga de 75ohms.

2.3.2.1 Lentes

Dependiendo de la iluminación de la escena a observar, su clasificación es la siguiente:

Lentes de Iris Fijo: Se utilizan cuando la iluminación es constante, como por ejemplo los interiores iluminados artificialmente.

Lentes de Iris Variable Manual: Cuando la iluminación interior puede tener variaciones por alternancias de luz artificial y/o natural, conviene utilizar estas lentes para lograr un ajuste de mayor precisión.

Lentes Autoiris: Es la lente adecuada cuando la cámara es instalada en el exterior, ya que controla en forma automática la cantidad de luz que penetra en la misma manteniendo una señal de video constante, con una efectividad superior al iris electrónico (AES), y logrando además una mayor profundidad de campo. Para observar una escena a una distancia determinada, debemos seleccionar la lente en función de la DISTANCIA FOCAL adecuada.

Figura 1: Lente cámara

Lentes Fijas: Cuando se ha definido fehacientemente la lente necesaria.

Lentes Varifocales: En las instalaciones donde el campo de visión es inseguro o el usuario debe definirlo una vez instalado el Sistema, se hace muy útil el uso de lentes varifocales que permiten ajustar en forma manual la distancia focal. Esto permite al instalador variar el campo visual en presencia del usuario y fijarlo en una posición, de común acuerdo con el mismo.

Lentes Zoom: Cuando se quieren observar imágenes cercanas y lejanas alternativamente, se deben utilizar lentes zoom. Estas cambian la magnificación de las imágenes enfocadas mediante el cambio de la distancia focal. Esto se realiza mediante un controlador que acciona el motor del zoom.

2.3.2.1.1 Selección lente cámara CCTV

La distancia focal es la distancia medida en mm entre el centro de la lente y el sensor CCD de la cámara. Cuanta más pequeña es la distancia focal, mayor será el campo visual. Las lentes con distancia focal de 2,8 a 4 mm son llamadas lentes gran angular y las que tienen distancia focal superior 6 mm, lentes telescópicas.

Figura 2: Campo visual y distancia focal

	1/3”	1/4"
99 º	2.8 mm	2.1 mm
64 º	4 mm	2.8 mm
47 º	6 mm	4 mm
35 º	8 mm	6 mm
27 º	12 mm	8 mm

Tabla 1: Campo visual y distancia focal

Requisitos de longitud focal

La longitud focal determina el campo de visualización horizontal a una distancia determinada; cuanto mayor sea la longitud focal, más estrecho será el campo de visualización.

La mayoría de los fabricantes ofrecen calculadores rotatorios sencillos que calculan la longitud focal del objetivo desde el tamaño de la escena y la longitud focal.

Para detectar la presencia de alguien en una pantalla, debería constituir como mínimo el 10 por ciento de la altura de la imagen. Para identificarlos con más precisión, deberá constituir el 30 por ciento o más de la imagen. Por esta razón, es importante comprobar las capacidades de las cámaras seleccionadas y ver las imágenes resultantes en la pantalla antes de grabar en directo.

Cálculo - metros

Para poder realizar un cálculo aproximado de la distancia focal necesaria para poder obtener una imagen con la cámara a una distancia determinada con un ancho de objeto concreto podemos utilizar la siguiente fórmula:

$$f = h \times D/H$$

donde f se corresponde con la distancia o longitud focal, h corresponde a la anchura del elemento CCD mientras que H es la anchura del objeto a visualizar y D la distancia a la que este se encuentra de la lente.

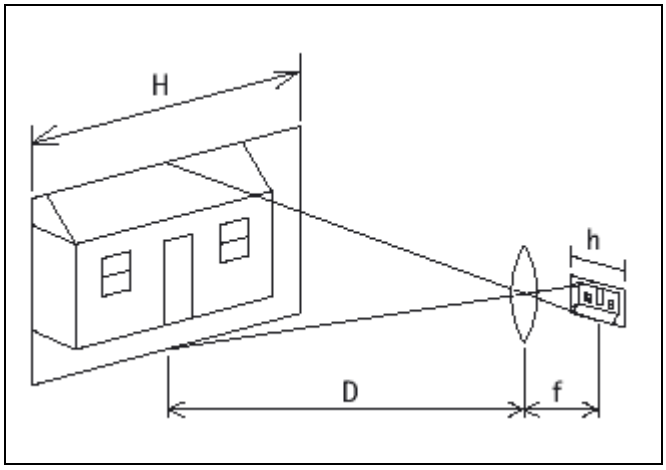


Figura 3: Cálculo Longitud Focal.

Objetivo y tamaño de sensor	1/2"	1/3"	1/4"
Longitud focal	12 mm	8 mm	6 mm

Tabla 2: Ejemplos de longitud focal para campo de visualización horizontal de 30º.

SENSOR CÁMARA	Valor h (mm)
1/2 “	6.4
1/3 “	4.8
1/4”	3.6

Tabla 3: Valor anchura CCD.

Utilizando esta fórmula y datos anteriores, proporcionados por uno de los proveedores, se podrán calcular el número de cámaras necesarias en función de las necesidades de cada caso.

2.3.2.2 Funcionalidad Día/Noche

Algunos entornos o situaciones limitan el uso de luz artificial, haciendo que las cámaras de infrarrojos (IR) sean particularmente útiles. Esto incluye aplicaciones de vigilancia por vídeo con escasa iluminación, donde las condiciones de luz no son óptimas, así como

situaciones de vigilancia discretas y encubiertas. Las cámaras sensibles a infrarrojos, que pueden utilizar luz infrarroja invisible, pueden utilizarse, por ejemplo, en zonas residenciales ya que, de noche, no se molesta a los residentes con el uso de focos u otras fuentes de iluminación. También son útiles cuando la instalación de cámaras requiere discreción.

2.3.2.2.1 Percepción de la luz

La luz es una forma de energía de onda de radiación que existe en un espectro. Sin embargo, el ojo humano puede ver sólo una parte (entre longitudes de onda de ~400-700 nanometros o nm). Por debajo del color azul, justo fuera del alcance que los humanos pueden percibir, se encuentra la luz ultravioleta y por encima del rojo se encuentra la luz infrarroja.

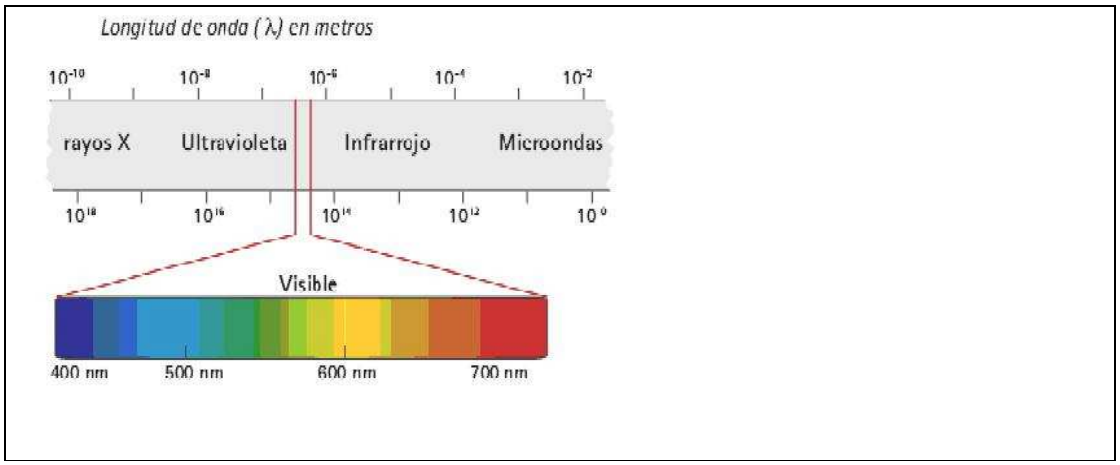


Figura 4: Percepción de la luz

La energía infrarroja (luz) es emitida por todos los objetos: los humanos, animales y la hierba, por citar algunos ejemplos. Los objetos que desprenden más calor tales como las personas y los animales destacan de fondos típicamente más fríos. En condiciones de luz escasa como, por ejemplo, por la noche, el ojo humano no puede percibir el color y la tonalidad, sólo el blanco y el negro y matices de gris.

2.3.2.2.2 Filtro IR

Mientras que el ojo humo sólo puede registrar luz entre el espectro azul y rojo, el sensor de imagen de una cámara en color puede detectar más. El sensor de imagen puede percibir una radiación de infrarrojos de onda larga y en consecuencia “ver” la luz infrarroja. Si el sensor de imagen capta infrarrojos en condiciones de luz diurna, distorsionará los colores que los humanos ven. Por esta razón, todas las cámaras en color están equipadas con un filtro IR, una pieza óptica de cristal que está colocada entre el objetivo y el sensor de imagen, para extraer la luz IR y ofrecer las imágenes que el ojo humano está acostumbrado a percibir.

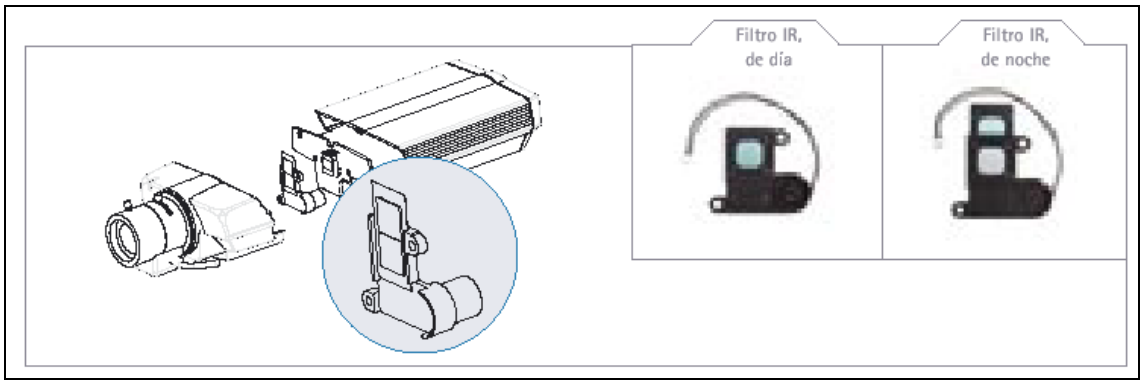


Figura 5: Filtro IR

Como la iluminación se reduce y la imagen se oscurece, el filtro IR en una cámara diurna y nocturna puede extraerse automáticamente para permitir que la cámara utilice luz IR a fin de que "vea"incluso en un entorno muy oscuro. Para evitar las distorsiones de color, la cámara a menudo cambia a modo blanco y negro, permitiendo de este modo generar imágenes en blanco y negro de alta calidad. El filtro IR en las cámaras IP diurnas/nocturnas puede también extraerse manualmente a través de la interfaz de la cámara.

**La capacidad para extraer o colocar automáticamente el filtro IR situado frente a un sensor de imagen de la cámara depende de la fabricación de la misma.*

2.3.3 Grabador Digital

Estos equipos tienen como misión la grabación digital de vídeo en disco duro, DVD, cinta de vídeo digital,… con capacidades muy dispares en función del soporte y la ampliación e integración en red de varios dispositivos (más de 100Gb).

Consta de entradas de vídeo, de audio y de alarmas, además de salidas para monitor, impresora, puertos de comunicaciones, etc.

Este tipo de equipos permite la programación del inicio y duración de la grabación así como condicionarla a eventos o alarmas, permiten la grabación digital de imágenes a velocidad que permiten la percepción real (25 ips), ya sea de forma individual o simultánea de cada cámara. Puede realizar grabaciones de imágenes previas y posteriores a alarmas, con diversas formas de grabación. Permite búsqueda de imágenes bajo diferentes criterios, es capaz de detectar la pérdida de la señal de vídeo y entre otras de sus características está la de ir equipado con puertos de comunicación como RTC, RDSI, X.25, Ethernet, Frame Relay,… utilizando como protocolo TCP/IP

Figura 6: Grabador Digital

2.3.4 Cámaras de red

Una cámara IP puede describirse como una cámara y un ordenador combinados para formar una única unidad. Capta y transmite imágenes directamente a través de una red IP, permitiendo a los usuarios autorizados visualizar, almacenar y gestionar vídeo de forma local o remoto mediante una infraestructura de red que se basa en una tecnología IP estándar.

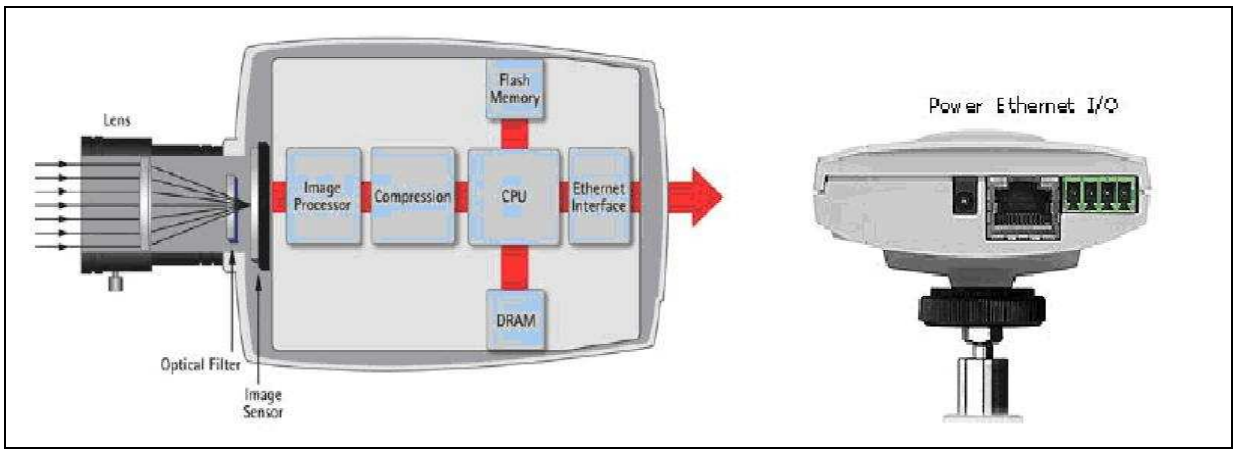


Figura 7: Interior cámara IP

Una cámara de red tiene su propia dirección IP. Se conecta a la red y lleva incorporado un servidor web, servidor o cliente FTP, cliente de correo electrónico, gestión de alarmas, capacidad de programación y mucho más. Una cámara IP no necesita estar conectada a un PC, funciona independientemente y puede colocarse en cualquier lugar donde haya una conexión de red IP. Por otra parte, una cámara web es algo totalmente diferente, ya que necesita estar conectada a un PC a través de un puerto de conexión USB o IEEE1394 y un PC para funcionar.

Además del vídeo, una cámara IP también incluye otras funcionalidades e información que se transmiten a través de la misma conexión de red como, por ejemplo, entradas y salidas digitales, audio, puerto(s) serie para datos en serie o control de mecanismos con movimiento vertical, horizontal y zoom.

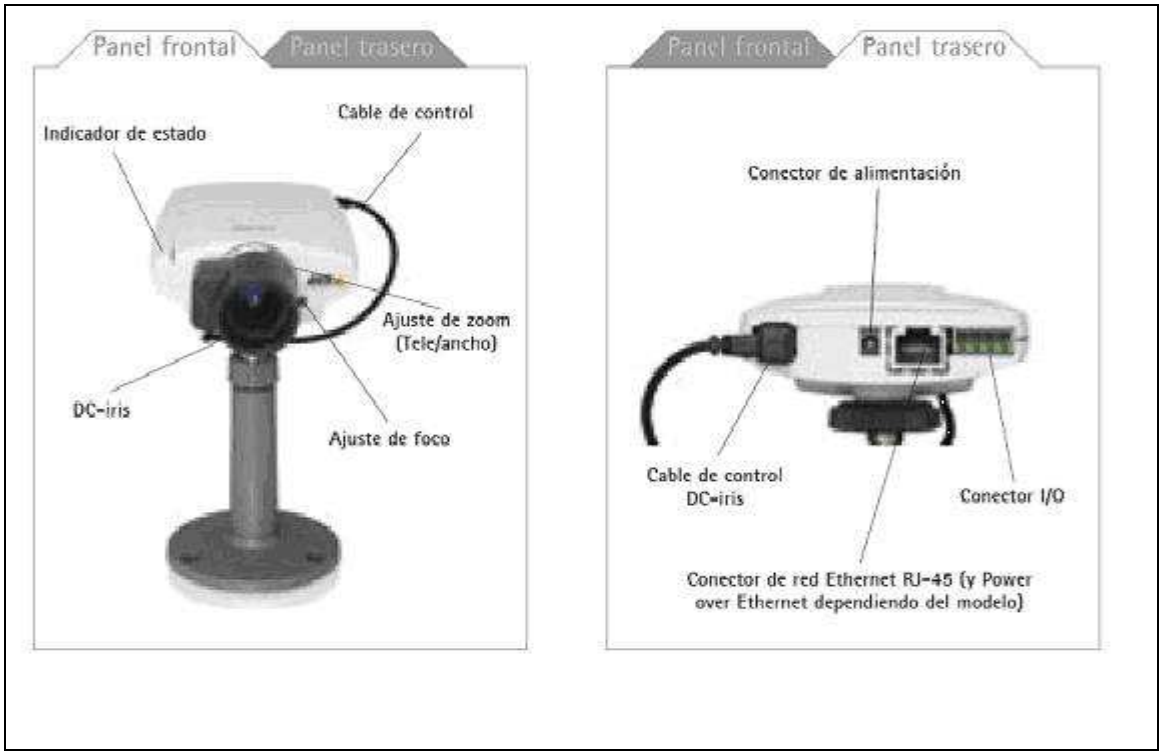


Figura 8: Panel frontal y trasero cámara IP

2.3.4.1 Funcionamiento

Una cámara de red posee su propia dirección IP y funciones de servidor independiente integradas. Todo lo necesario para ver las imágenes a través de la red está incluido dentro de la cámara. La cámara se conecta directamente a la red como cualquier otro dispositivo de red, tiene su propio software integrado, servidor FTP, cliente FTP y cliente e-mail (FTP).

Incluye también entradas de alarma y salidas para relé. Según el modelo de cámara podrá ir equipada con muchas otras funciones como entre otras son la detección de movimiento o la salida de vídeo analógico.

Los componentes de cámara de las cámaras de red capturan la imagen, que se puede describir como luces con diferentes longitudes de onda y la transforman en señales eléctricas. Estas señales son convertidas entonces del formato analógico al digital y se transfieren al componente ordenador de la cámara donde la imagen es comprimida y enviada a través de la red.

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

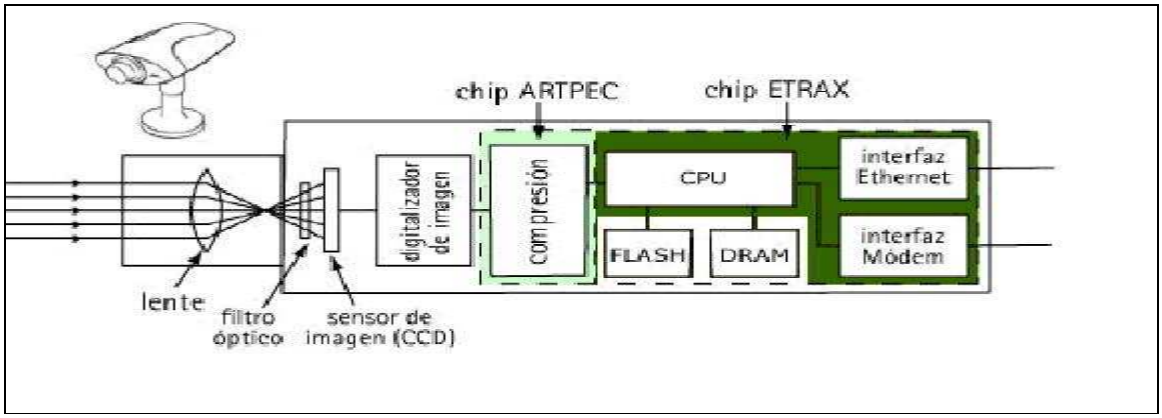


Figura 9: Elementos cámara IP

El chip de compresión de vídeo comprime la imagen digital a una imagen con la información reducida para su eficiente envío a través de la red. En algunas ocasiones este chip realiza igualmente las funciones de control de la cámara como son la gestión de la exposición, el balance de blancos (ajusta los niveles de color), la nitidez de la imagen y otros aspectos de la calidad de la imagen.

La conexión Ethernet de la cámara se consigue gracias a una solución de sistema en un chip que permite conectar periféricos a la red. Dicho chip incluye una CPU de 32bit, conectividad 10/100Mb Ethernet, funcionalidad DMA (Direct Memory Access) avanzada y un amplio rango de interfaces de Entrada/Salida.

La CPU, memoria Flash y la memoria DRAM representan el "cerebro" o funciones de ordenador de la cámara y están diseñadas específicamente para aplicaciones de red. Juntas, gestionan la comunicación con la red y el servidor web.

2.3.4.2 Diferencias entre cámaras de red y cámaras analógicas

A lo largo de los últimos años, la tecnología de la cámara IP ha alcanzado la tecnología de la cámara analógica y en la actualidad reúne los mismos requisitos y cumple con las mismas especificaciones. Las cámaras IP incluso superan, en muchos aspectos, el rendimiento de las cámaras analógicas.

En pocas palabras, una cámara analógica es una portadora de señal unidireccional que finaliza a nivel del usuario y el DVR, mientras que una cámara IP es completamente bidireccional, integrando e impulsando el resto del sistema a un nivel superior en un entorno escalable y distribuido. Una cámara IP se comunica con diversas aplicaciones en paralelo para realizar varias tareas, tales como la detección de movimiento o el envío de diferentes secuencias de vídeo.

2.3.4.3 Clasificación cámaras IP

2.3.4.3.1 Cámaras Fijas

2.3.4.3.1.1 Cámara Fija

Las cámaras fijas formadas por un cuerpo y un objetivo representan el tipo de cámara tradicional. En algunas aplicaciones, resulta sumamente útil que la cámara sea muy visible. Si éste es el caso, una cámara fija representa la mejor elección, puesto que la cámara es claramente visible al igual que la dirección hacia la cual apunta. Otra ventaja es que la mayoría de cámaras fijas disponen de objetivos intercambiables con montura C/CS. Para una mayor protección, las cámaras fijas pueden instalarse en carcasas diseñadas para interiores o exteriores.

Figura 10: Cámara Fija IP

2.3.4.3.1.2 Cámara domo fija

Las cámaras domo fijas, también conocidas como mini domo, constan básicamente de una cámara fija preinstalada en una pequeña carcasa domo. La cámara puede enfocar fácilmente el punto seleccionado en cualquier dirección. La ventaja principal radica en su discreto y disimulado diseño, así como en la dificultad de ver hacia qué dirección apunta la cámara. Una de las limitaciones es que las cámaras domo fijas casi nunca disponen de objetivos intercambiables, y en caso de que ofrezcan una selección de objetivos, las posibilidades de intercambiarse se ven limitadas por el espacio en el interior de la carcasa domo.

Figura 11 Cámara domo fija IP

2.3.4.3.2 Cámaras con movimiento

Hasta este momento las cámaras mencionadas han sido fijas con lentes de longitud focal determinada. En muchas aplicaciones el área a cubrir pudiera necesitar muchas cámaras fijas. La solución para esto es la aplicación de cámaras montadas en una plataforma móvil. Esta plataforma puede ser controlada desde un lugar remoto. La plataforma puede simplemente girar en un plano horizontal. En forma alternativa, la plataforma puede ser controlada tanto en el plano horizontal o vertical y es conocida generalmente como una unidad Pan Tilt.

La aparición de Domos con cámaras interna movibles en los últimos años cumplen con las exigencias de prácticamente cualquier tipo de aplicación gracias a sus capacidades de movimiento. Los controladores para este tipo de domos tienen la versatilidad de generar posiciones prefijadas por el usuario así como controlar decenas de domos desde un mismo punto.

Las cámaras pueden ser instaladas en interiores y/o exteriores. Cuando se utilizan en exteriores éstas siempre requieren de una cubierta para protección. Para aplicaciones en interiores el medio ambiente o el contenido estético dictarán cuando se requiere una cubierta. Los sistemas pueden contener una combinación de ambos tipos de cámaras, fija y móvil.

2.3.4.3.2.1 Cámaras PTZ

Las cámaras con movimiento vertical/horizontal/zoom (PTZ) poseen la ventaja de obtener una visión panorámica, inclinada, alejada o de cerca de una imagen, manual o automáticamente. Para un funcionamiento manual, la cámara PTZ puede, por ejemplo, utilizarse para seguir los movimientos de una persona en un comercio. Las cámaras PTZ se utilizan principalmente en interiores y en aquellos lugares donde resulte apropiado ver la dirección hacia la cual apunta la cámara. La mayoría de cámaras PTZ no disponen de un movimiento horizontal completo de 360 grados, y tampoco están hechas para un funcionamiento automático continuo, conocido como “recorrido protegido”. El zoom óptico oscila entre 18x y 26x.

Figura 12: Cámara PTZ IP

2.3.4.3.2.2 Cámaras domo

Una cámara domo, en comparación con una cámara PTZ, añade la ventaja de permitir una rotación de 360 grados. Asimismo ofrece la resistencia mecánica para un funcionamiento continuo en recorridos protegidos donde la cámara se desplaza de forma continua entre por ejemplo unas 10 posiciones predefinidas, un día tras otro. Con recorridos protegidos, una cámara puede abarcar una zona donde se precisarían 10 cámaras fijas para llevar a cabo el mismo trabajo. La principal desventaja es que sólo se puede supervisar una ubicación en un momento dado, dejando así las otras 9 posiciones sin supervisar. El zoom óptico oscila, normalmente, entre 18x y 30x. Sin embargo, para instalaciones en el exterior, los factores de zoom superiores a 20x resultan inadecuados debido a las vibraciones y movimientos causados por el viento.

Figura 13: Cámara domo IP

2.3.4.3.2.3 Cámaras PTZ no mecánicas

Con la introducción de las cámaras IP, llega al mercado una nueva línea de cámaras PTZ, las llamadas cámaras PTZ no mecánicas. Gracias al sensor de megapíxels, la cámara puede abarcar entre 140 y 360 grados y el usuario puede obtener una visión panorámica, inclinada, alejada o de cerca con la cámara, en cualquier dirección, sin tener que realizar ningún movimiento mecánico. La ventaja primordial es que no se produce un desgaste de las piezas móviles. Ofrece además un movimiento inmediato a una nueva posición, lo que en una cámara PTZ tradicional puede tardar hasta 1 segundo. En la actualidad, las mejores cámaras PTZ no mecánicas utilizan un sensor de 3 megapíxels. Con el fin de garantizar una buena calidad de imagen, el movimiento vertical y horizontal deberá limitarse a 140 grados y el zoom a 3x. Para un zoom o una cobertura mayor, la calidad de la imagen se verá seriamente perjudicada.

Figura 14: Cámara PTZ IP no mecánica

Se encuentran disponibles diversas variaciones de los tipos de cámaras descritos anteriormente, entre las que se incluyen:

- Versiones a prueba de agresiones, en función de la carcasa de protección que se use.

- Versiones resistentes a las condiciones climáticas, en función de la carcasa de protección que se use.

- Versiones de visión diurna / nocturna, lo que significa que la cámara puede cambiar automática o manualmente entre modo diurno con vídeo en color y modo nocturno con imágenes en blanco y negro en situaciones de poca luz que pueden mejorarse usando iluminadores de infrarrojos.

2.3.4.4 Alimentación a través de Ethernet

La alimentación a través de Ethernet (Power over Ethernet, PoE) es una tecnología que incorpora alimentación eléctrica a una infraestructura LAN estándar. Permite que la alimentación eléctrica se suministre al dispositivo de red como, por ejemplo, un teléfono IP o una cámara IP, usando el mismo cable que se utiliza para una conexión de red. Elimina la necesidad de utilizar tomas de corriente en las ubicaciones de la cámara y permite una aplicación más sencilla de los sistemas de alimentación ininterrumpida (SAI) para garantizar un funcionamiento las 24 horas del día, 7 días a la semana. Power over Ethernet se regula en una norma denominada IEEE 802.3af y está diseñado de manera que no haga disminuir el rendimiento de comunicación de los datos en la red o reducir el alcance de la red. La corriente suministrada a través de la infraestructura LAN se activa de forma automática cuando se identifica un terminal compatible y se bloquea ante dispositivos preexistentes que no sean compatibles. Esta característica permite a los usuarios mezclar en la red con total libertad y seguridad dispositivos preexistentes con dispositivos compatibles con PoE.

El estándar proporciona una alimentación de hasta 15,4 W en el lado del conmutador o midspan, lo que se traduce en un consumo eléctrico máximo de 12,9 W en el lado del dispositivo/cámara, haciendo que resulte perfecto para cámaras de interior. Las cámaras de exterior así como las cámaras domo y PTZ poseen un consumo eléctrico superior a éste, por lo que la funcionalidad PoE resulta menos adecuada. Algunos fabricantes ofrecen también productos patentados que no son estándar y que proporcionan un suministro adecuado a esas aplicaciones, aunque debería tenerse en cuenta que, al tratarse de productos no estándar, no es posible una interoperabilidad entre marcas distintas. La norma 802.3af proporciona soporte para la llamada clasificación de energía eléctrica, que permite una negociación del consumo eléctrico entre la unidad PoE y los dispositivos, lo que significa que un conmutador inteligente puede garantizar un suministro suficiente y no superfluo para el dispositivo (la cámara), ofreciendo la posibilidad de que el conmutador pueda permitir más salidas PoE.

2.3.4.4.1 Como usar Power over Ethernet

PoE funciona a través de un cableado de red estándar (es decir, cat 5) para suministrar alimentación directamente desde los puertos de datos a los que están conectados los dispositivos de red. Hoy en día, la mayoría de los fabricantes ofrecen switches de red con soporte PoE incorporado. Si se dispone de una estructura de red/conmutador existente, los clientes pueden beneficiarse de la misma funcionalidad añadiendo al switch el llamado Midspan, que añadirá alimentación al cable de red. Todas las cámaras de red que no disponen de PoE incorporado, pueden integrarse en un sistema PoE usando un Active Splitter.

El diagrama siguiente le muestra cómo la cámara IP puede recibir alimentación a través de un cable de red y es capaz de seguir funcionando cuando se produce un fallo eléctrico.

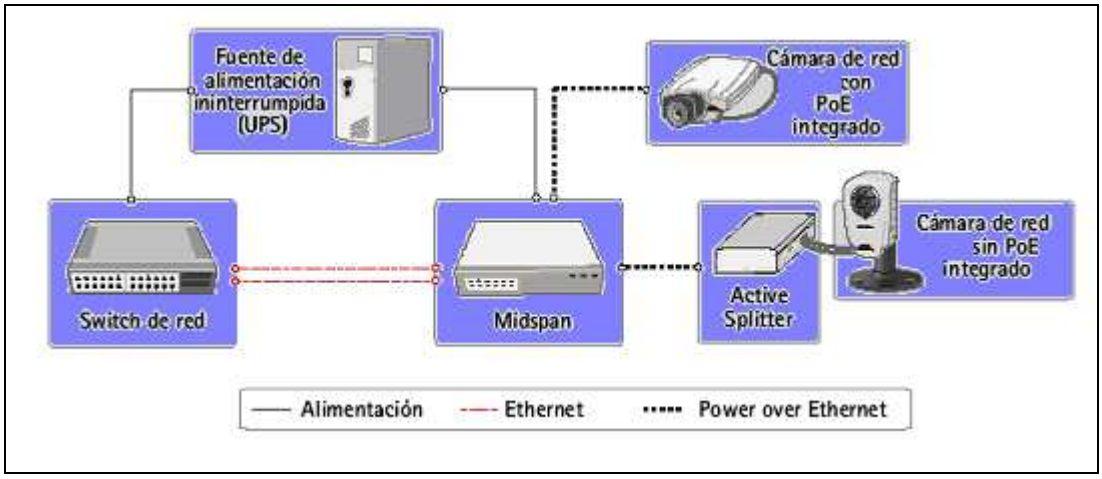


Figura 15: PoE

2.3.4.5 Detección de movimiento

La detección de actividad o movimiento consiste en el análisis de las imágenes para descubrir las modificaciones por la cantidad de píxeles que las conforman. Esta situación genera una causa de alarma, procediendo según programación: grabar prioritariamente donde se detecta actividad, avisar al operador con señalización visible o acústica, al tiempo que muestra en pantalla imágenes tomadas por la cámara de zona, etc. Muy apropiado para optimizar la grabación en vídeo al eliminar imágenes poco significativas. Es conveniente que disponga de ajuste de sensibilidad a fin de eludir falsas alarmas.

La tarea de grabación por detección de movimiento utiliza solo la detección de movimiento generada por el software, no por las propias cámaras, cuya detección de movimiento se utilizará para la generación de alarmas únicamente.

La principal ventaja de este proceso radica en que las grabaciones resultantes muestran algo que puede no ser importante, pero que reflejan acción. Con ello se evitan las grabaciones de larga duración en las que es preciso buscar aquello que interesa entre enormes cantidades de información.

Existen dos procesos de detección de movimiento:

Movimiento detectado por el software. Útil para poder detectar movimiento en cámaras y sistemas que no tengan por sí mismos esta capacidad. Sirve para optimizar las grabaciones programadas en base a tareas, de tal manera que el sistema sea capaz de grabar solo aquello que signifique variación de imágenes respecto de las inmediatas anteriores. El sistema procesa continuamente (a una o dos imágenes por segundo y cámara) la información que le llega desde la cámara y la compara con las imágenes inmediatamente anteriores. De esta manera, si la cantidad porcentual de movimiento o variación de imagen supera el umbral de sensibilidad asignado a la cámara, el sistema recopilas las secuencias inmediatamente anteriores al evento y las asocia a la grabación que se produce mientras la cantidad de variación supera dicho umbral.

De igual manera, se empaquetan en la grabación las imágenes inmediatamente posteriores a que la situación vuelve a normalizarse. Así, la grabación dispone de PRE movimiento, movimiento y POST movimiento.

El movimiento detectado por software provoca consumo de ancho de banda y capacidad de proceso, y por lo tanto debería estudiarse detenidamente las consecuencias y capacidades de comunicaciones y procesamiento del equipo en el que se encuentra instalado el sistema. La detección de movimiento por software sirve también para generar un evento de alarma.

Detección de movimiento de la cámara o videoservidor. Se utilizará en el caso de preservar el ancho de banda del sistema de comunicaciones y/o descarga de tareas y procesos al sistema central, ya que cada cámara realiza su propia detección de movimiento.

La gran ventaja de esta solución es que el sistema no se ve repercutido por el número de cámaras que se instalen, ni sus procesos, ya que cada una de ellas realiza sus propias tareas. Además no existe tráfico desde la cámara al PC para que este analice las imágenes, ya que es la propia cámara la que ejecuta el proceso.

Figura 16: Detección de movimiento

2.3.4.6 Entradas y salidas digitales (I/O)

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

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

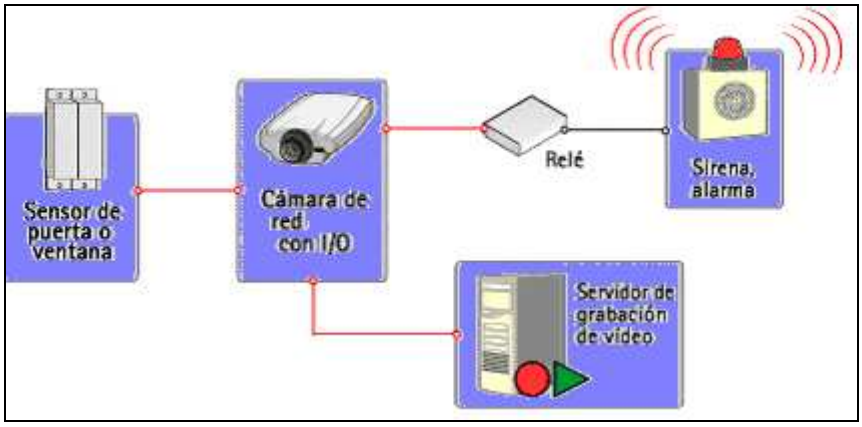


Figura 17: Entradas y salidas digitales

A continuación se muestran 2 tablas con algunas de las diferentes posibilidades de entradas y salidas digitales a conectar.

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

	ser activado por la cámara)	produciendo una imagen animada a pantalla completa y enviando notificaciones

Tabla 4: Entradas Digitales

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

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

Tabla 5: Salidas Digitales

2.3.4.7 Servidor de vídeo

Un servidor de vídeo permite avanzar hacia un sistema de vídeo IP sin necesidad de descartar el equipo analógico existente. Aporta nueva funcionalidad al equipo analógico y elimina la necesidad de equipos exclusivos como, por ejemplo, el cableado coaxial, los monitores y los DVR. Estos dos últimos no son necesarios ya que la grabación en vídeo puede realizarse utilizando un servidor de PC estándar.

Un servidor de vídeo normalmente dispone de puertos analógicos para conectar las cámaras analógicas, así como un puerto Ethernet para la conexión a la red. Al igual que las cámaras IP, dispone de un servidor Web integrado, un chip de compresión y un sistema operativo para que las entradas analógicas puedan convertirse en vídeo digital, transmitirse y grabarse a través de la red informática para facilitar su visualización y accesibilidad.

Además de la entrada de vídeo, un servidor de vídeo también incluye otra información y funcionalidades que se transmiten a través de la misma conexión de red: entradas y salidas digitales, audio, puerto(s) serie para datos en serie o control de mecanismos con movimiento horizontal, vertical y zoom. Un servidor de vídeo puede conectarse también a una amplia variedad de cámaras especiales, tales como cámaras de gran sensibilidad en blanco y negro, cámaras en miniatura o cámaras microscópicas.

2.3.4.7.1 Características de los vídeo servidores

Facilita la visualización de imágenes (también audio) utilizando el navegador desde cualquier lugar y en todo momento.

Compresión de la imagen en formato jpeg, mjpeg,...

Distintas velocidades: 30, 25, 20... fps.

Control de brillo, saturación, contraste,...

Varias entradas de vídeo: para 1, 2, 4, 9, 16,... cámaras.

Diversos puertos de conexión, serie y paralelo.

Otras características: procesador, memoria ROM, memoria RAM,...

Protocolos TCP/IP, FTP, HTTO, SMTP, TELNET, UDP, ARPICM,...

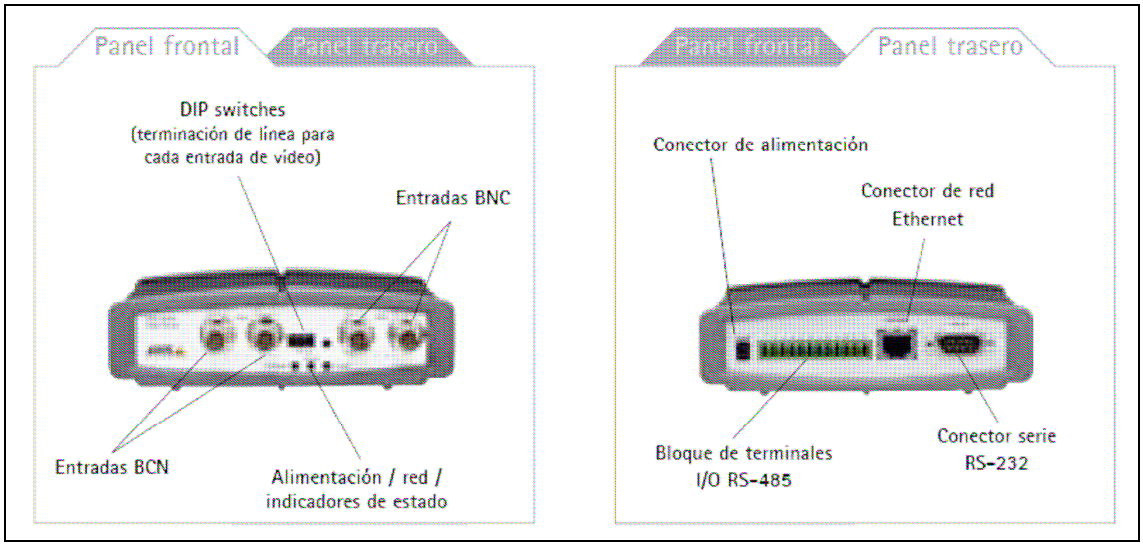


Figura 18: Panel frontal y trasero vídeo servidor

2.3.4.7.2 Uso de cámaras analógicas con servidores de vídeo

Se pueden integrar cámaras analógicas de cualquier tipo como por ejemplo cámaras fijas, domo, de interior, de exterior, domo fijas, con movimiento Pan/tilt/zoom, así como las cámaras especializadas, en un sistema de vídeo IP utilizando los servidores de vídeo. El cable coaxial de la cámara analógica se conecta fácilmente a la entrada analógica del servidor de vídeo que, a continuación, digitaliza, comprime y transmite la imagen de vídeo mediante una red local o a través de Internet. Una vez que el vídeo está en la red, el proceso es idéntico a una transmisión procedente de una cámara IP y está preparado para integrarse a los sistemas de vídeo IP. En resumen: un servidor de vídeo convierte una cámara analógica en una cámara IP.

2.3.4.7.3 Servidores de vídeo montados en rack

La mayoría de las empresas utilizan una sala de control exclusiva para centralizar el equipo en una ubicación y controlar de forma eficiente las operaciones dentro de un entorno seguro para la información de vital importancia. En un edificio con gran número de cámaras analógicas habrá gran cantidad de cableado coaxial que confluye en la sala de control.

Si todo el cableado coaxial ya ha sido instalado y está disponible desde la sala central, supondrá una gran ventaja para la instalación el empleo de un rack de servidores de vídeo, que permite que un gran número de servidores de vídeo en tarjeta se monten en un rack y se administren de forma centralizada. El rack contiene ranuras para un máximo de 12 servidores de vídeo en tarjeta intercambiables y suministra conexión a red, comunicación serie y conectores I/O en la parte trasera de cada ranura, así como una fuente de alimentación común.

2.3.4.7.4 Servidores de vídeo independientes

En un sistema de vigilancia donde se han realizado inversiones en cámaras analógicas pero aún no se ha instalado el cableado coaxial, resulta útil conectar un servidor de vídeo independiente cerca de las cámaras analógicas del sistema. Además del reducido coste de cableado para transmitir el vídeo, se añade el beneficio de no disminuir la calidad de la imagen debido a la distancia, que es lo que ocurre con el cableado coaxial en el cual la calidad de la imagen se reduce en distancias mayores. Un servidor de vídeo produce imágenes digitales, por tanto la calidad no se ve reducida a causa de la distancia.

2.3.4.7.5 Servidores de vídeo con cámaras PTZ y domo

Las cámaras PTZ pueden conectarse a servidores de vídeo independientes así como a servidores de vídeo montados en rack, usando el puerto serie (RS232/422/485) integrado en los servidores de vídeo. En los casos en los que se utiliza un servidor de vídeo de un

solo puerto con la cámara, se añade el beneficio de no tener que instalar cableado serie independiente para controlar el mecanismo PTZ. También ofrece la función de realizar un control PTZ a lo largo de grandes distancias a través de Internet. Deberá estar disponible un controlador específico en el servidor de vídeo para controlar una cámara PTZ determinada. En un servidor de vídeo, existen controladores PTZ disponibles para las cámaras domo y PTZ más conocidas y pueden transferirse al servidor de vídeo. También puede usarse un controlador que se encuentra en el PC que ejecuta el software de gestión de vídeo si el puerto serie se ha establecido como un servidor serie que se desplaza a través de los comandos.

2.3.4.8 Sistemas de vídeo en red

Un sistema de vídeo en red utiliza como red troncal (backbone) para el transporte de información redes LAN/MAN/WAN/Internet, en vez de las líneas punto a punto dedicadas que se utilizan en los sistemas de vídeo analógicos. Muchos negocios ya usan redes informáticas para una amplia cantidad de funciones. La tecnología de vídeo en red utiliza y amplía esta misma infraestructura para la monitorización remota y local.

En este sistema la transmisión de vídeo, del audio y de los paquetes de datos tiene lugar sin la presencia de una infraestructura física dedicada que conecte la cámara al monitor. El crecimiento del vídeo en red para tareas de vigilancia monitorización está siendo impulsado no sólo por un aumento general de la necesidad de seguridad, sino también por su mayor rendimiento y los ahorros que proporciona su flexibilidad en el acceso a la información y la facilidad de distribución de imágenes, por su capacidad de integración, escalabilidad y muchos otros factores.

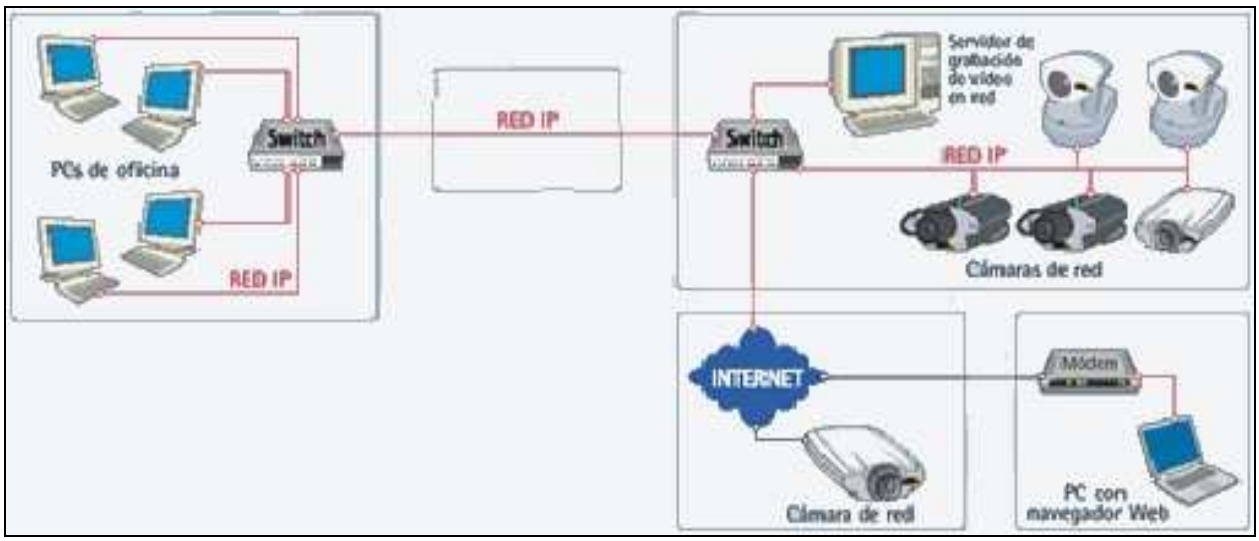


Figura 19: Sistema de vídeo en red

2.3.4.9 Migración analógica a digital

Muchas empresas y organizaciones ya realizaron inversiones importantes en Circuitos Cerrados de TV (CCTV) analógicos. Mientras esos sistemas sigan aportando valor, es

lógico que no haya motivos para cambiarlos. Sin embargo pueden ser mejorados con tecnología IP, sin necesidad de erradicar la infraestructura existente.

El alcance actual de la tecnología digital ha cubierto muchas de las limitaciones de la tecnología analógica. Los sistemas de CCTV analógicos generalmente precisan un mantenimiento intensivo, no ofrecen accesibilidad remota y son notablemente difíciles de integrar con otros sistemas.

Para poder cubrir esta demanda, se requieren productos que permitan combinar los equipos antiguos con dispositivos actualizados y obtener las ventajas que ofrece la tecnología digital: accesibilidad remota, rentabilidad, flexibilidad, escalabilidad, integración y funcionalidad actualizable y óptima calidad de imagen.

Como bien se ha dicho implementar un sistema digital no exige deshacerse de las cámaras por las que ya se ha pagado. Con la Vigilancia-IP, se pueden utilizar las cámaras, lentes y cables ya instalados a través de una migración paso a paso hacia la tecnología digital. Y si esta no es una razón con suficiente peso como para considerar una actualización, hay que tener en cuenta la calidad actual de las imágenes grabadas, que es a menudo, insatisfactoria, en particular si se usa en investigaciones oficiales. Con la introducción de la tecnología del Grabador de Vídeo Digital (DVR), el medio de almacenamiento ya no volverá a depender de la intervención de un operador o de la calidad de las cintas. Y con la tecnología de Vigilancia IP, el servidor de vídeo y el servidor de red representan el siguiente nivel de mejora al conectar las cámaras actuales a la red con un servidor de vídeo y entonces almacenar las imágenes en el servidor de red.

2.3.4.9.1 El embudo de los CCTV se sitúa en el grabador

En una instalación con videograbador digital y cámaras analógicas la carga de trabajo se sitúa en el videograbador. Las cámaras analógicas únicamente capturan las imágenes y las envía al videograbador. Es éste quien tiene que realizar el trabajo de digitalizar y comprimir, por ello, se dice que “el embudo de los CCTV digital o analógico se sitúa en el grabador”. En una instalación con videograbador IP y cámaras IP este embudo no se produce ya que son las propias cámaras las que digitalizan y comprimen las imágenes. El videograbador no recibe esa carga de trabajo añadida que se da en las instalaciones CCTV. Añadir una cámara en instalaciones de vídeo IP no significa añadir carga de trabajo al videograbador, sino que, al añadir una cámara estamos añadiendo capacidad de proceso, un “cerebro” más.

Todo este proceso se puede ver gráficamente en el siguiente esquema.

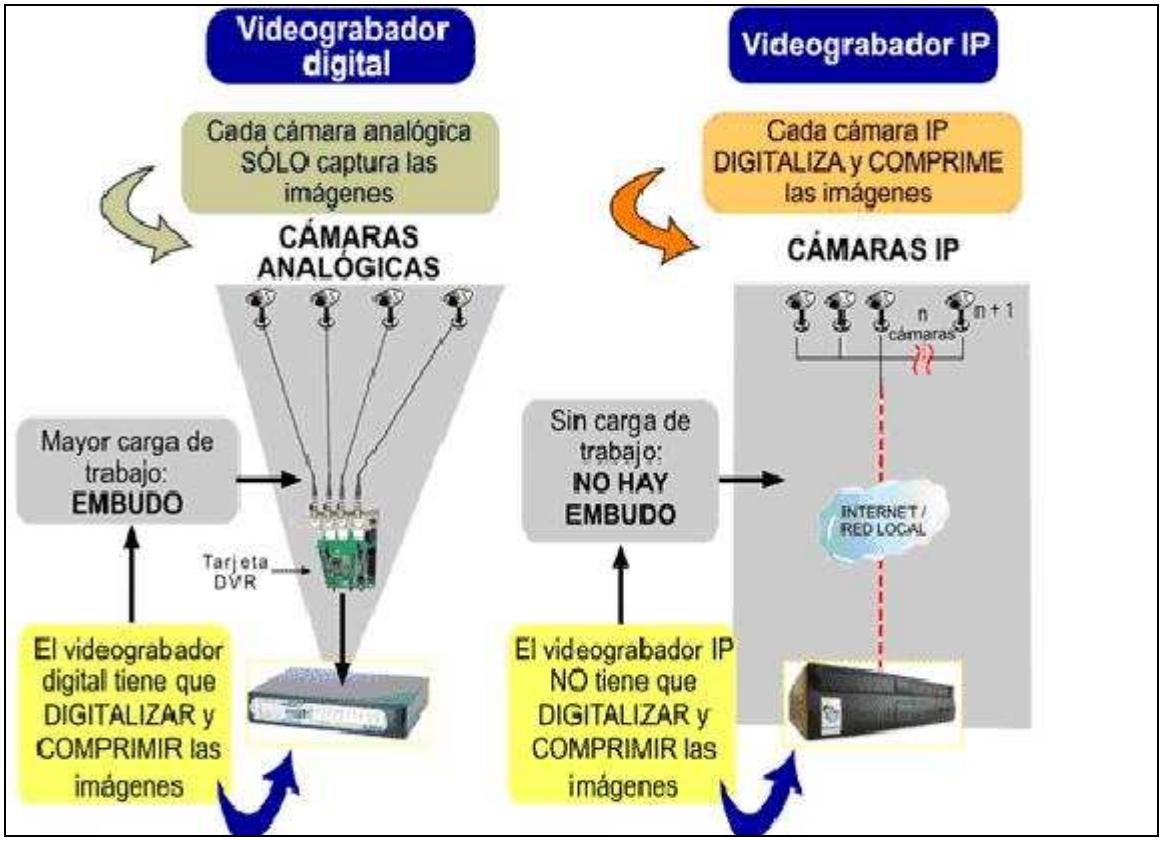


Figura 20: Embudo CCTV

2.3.4.9.2 Los múltiples beneficios de lo digital

Con la expansión de la tecnología de grabación digital, sus múltiples ventajas se han hecho bastante aparentes: facilidad de uso, capacidades avanzadas de búsqueda, grabación y visualización simultáneas, sin pérdida de calidad de imagen, mejora de la compresión y el almacenamiento, y mayor potencial de integración, entre otras. Pero con la tecnología digital y su núcleo, la Vigilancia IP ofrece todas esas ventajas y más:

Accesibilidad remota. El principal beneficio de la conexión de las cámaras analógicas a la red es que a partir de ese momento el usuario puede visualizar imágenes de vigilancia desde cualquier ordenador conectado a la red, sin necesidad de ningún hardware o software adicional. En las instalaciones ordinarias de CCTV que operan en modo punto a punto y precisan cableado dedicado para cada cámara, la visualización solo puede llevarse a cabo desde monitores específicos y teclados de operarios conectados al sistema. Si tiene un puerto para Internet, puede conectarse de forma segura desde cualquier parte del mundo para ver el edificio seleccionado o, incluso, una cámara de su circuito de seguridad. Con el uso de Redes Privadas Virtuales (Virtual Private Network, VPN) o intranets corporativas, se pueden gestionar accesos protegidos por contraseña a imágenes del sistema de vigilancia. Tan seguro como el pago por Internet, las imágenes y la información del usuario quedan seguras y sólo puede acceder a ellas el personal autorizado.

Escalabilidad: un sistema digital es flexible y totalmente escalable para satisfacer las necesidades concretas de cualquier usuario. Lo digital ha sido diseñado para proporcionar funcionalidades de "plug and play" tanto para instalaciones pequeñas como para grandes aplicaciones profesionales. Los sistemas de vigilancia IP pueden escalar desde una a miles de cámaras en incrementos de a una sola cámara. Además, no existen los límites de los 16 canales que se encuentran en el mundo de los DVR. Se puede aumentar la tasa de cuadro y de almacenamiento agregando discos duros y servidores a la red y, además, cualquier tasa de cuadro en cualquier cámara puede estar disponible cuando se la requiera. Frente a la mayoría de sistemas analógicos, un sistema de vídeo en red puede ser ampliado sin necesidad de reemplazar componentes del sistema.

Almacenamiento seguro e ilimitado. Se almacenan tantas horas de imágenes como se quiera en función de la capacidad de los discos duros. Y puede realizarse dicha función desde cualquier lugar en casos donde la monitorización y el almacenamiento son de misión crítica o necesiten back-up.

Distribución flexible y pro-activa de imágenes. Uno de los mayores problemas con los sistemas analógicos es la falta de un sentido eficiente de la distribución de la información. En el entorno del vídeo digital toda la información se trata como ficheros de datos, que pueden contener secuencias de vídeo o imágenes estáticas. Un fichero se puede distribuir fácilmente a un número ilimitado de receptores, o puede "colgarse" en una página web en pocos segundos. Esta distribución de la información visual puede realizarse sin degradación alguna de la calidad de las imágenes.

Con el vídeo digital también es posible conseguir instantáneas de un intruso o un incidente y hacer que sean enviadas por e-mail a la policía o las autoridades apropiadas. También, la policía u otros colaboradores con acceso protegido por contraseña podrán conectarse a las cámaras y ver la actividad en los alrededores de las instalaciones del usuario.

Alertas automáticas. El servidor de vídeo y las cámaras IP pueden enviar automáticamente mensajes de correo electrónico con una imagen de alarma a las direcciones de correo especificadas, de forma que las personas idóneas tengan la información que necesitan para pasar a la acción en el momento preciso.

Rendimiento y Coste Total de Propiedad (TCO). Una cámara de red actualmente es más cara cuando se compara su precio con el de una cámara analógica "similar". Sin embargo un análisis que contemple todos los factores de la inversión total en el sistema hace que la decisión sea más favorable a la solución de vídeo digital. Los costes de instalación son generalmente inferiores dado que el cableado de red es más económico que el coaxial. Ya no serán necesarios los grabadores de lapsos de tiempo, ni las cintas de vídeo ni su cambio o clasificación. Los costes de mantenimiento también son inferiores. Y mientras el rendimiento y los resultados del sistema aumentan notablemente el coste total de propiedad a través del tiempo continúa decreciendo.

Otro factor que impacta positivamente en el TCO se encuentra en el lado operativo. Las potentes herramientas de los sistemas digitales, tales como herramientas para buscar, localizar y distribuir imágenes de vídeo interesantes aumentan la eficiencia y eficacia de los operadores. Cuando se incorporan todos estos factores de mantenimiento y operativos a la ecuación, el análisis de costes es aún más beneficioso para la solución digital, especialmente si se precisa grabación de vídeo.

La Vigilancia IP proporciona toda la funcionalidad superior asociada a la tecnología digital y además los tremendos beneficios de una mayor accesibilidad, de un almacenamiento y distribución de imágenes mejorada y unas imágenes con mayor relación coste/beneficio.

Infraestructura más rentable. El sistema digital utiliza una red normal basada en IP para la transmisión y distribución de vídeo, con lo que se elimina la necesidad de una costosa instalación de cableado delicado, a esto añadir que la mayoría de las instalaciones ya cuenta con cableado de infraestructura de pares trenzados, de modo que no se necesita ningún tipo de cableado adicional, una parte muy costosa de cualquier instalación de CCTV. En los sitios en donde no hay infraestructura, la instalación de pares trenzados es más económica que un cable coaxial. Además, se pueden utilizar redes inalámbricas cuando el cableado no es una solución práctica.

Integración de sistemas y convergencia de redes. La tecnología de vigilancia IP ofrece una plataforma fácilmente integrada y abierta. A medida que la integración de sistemas se vuelve cada vez más crítica, es necesario asegurarse de que el control de acceso, la calefacción y la ventilación, los controles de proceso y otros sistemas y aplicaciones puedan integrarse efectivamente. Una sola red conecta y administra la empresa en cuanto a traspaso de datos, video y voz, etc., haciendo que la administración sea más efectiva y rentable.

Cámaras Inteligentes: Detección de movimiento, búsqueda de eventos, entrada con sensor, salida por relé, fecha y hora y otras capacidades incorporadas permiten que la cámara tome decisiones inteligentes acerca de cuándo enviar alarmas y en qué cuadro, mejorando así el acceso a la información y la toma de decisiones.

Alta confiabilidad: El transporte de datos basado en IP permite el almacenamiento externo y la posibilidad de usar infraestructura redundante, y la arquitectura de almacenamiento y servidores. Al utilizar servidores estándares y equipamiento de redes, el tiempo de reemplazo, en caso de que alguna parte del equipo deba ser cambiada, es considerablemente menor cuando se utilizan soluciones DVR. El software de administración ofrece un estado de operación del sistema en tiempo real e información en cuanto a medidas preventivas.

2.3.4.10 Tecnología IP

Hoy en día, el protocolo de Internet (IP) constituye el protocolo de comunicación informática más ampliamente utilizado. Es el protocolo básico empleado para la comunicación por Internet, como el correo electrónico, web y multimedia. Una de las razones de la aceptación de este protocolo es su escalabilidad. En otras palabras, funciona perfectamente tanto en instalaciones muy pequeñas como en instalaciones muy grandes y es compatible con una gama cada vez más amplia de tecnologías y equipos de gran rendimiento, bajo coste y eficacia contrastada por el sector. A continuación se expone una visión general de las distintas tecnologías empleadas, basadas en IP, para sacar el máximo partido de un sistema de vídeo IP.

2.3.4.10.1 Ethernet

En las oficinas de hoy en día, lo más probable es que los ordenadores utilicen una red TCP/IP conectados a través de una red Ethernet. Ethernet ofrece una red rápida a un precio razonable. La mayoría de ordenadores modernos se suministran con una interfaz Ethernet integrada o permiten alojar fácilmente una tarjeta de interfaz de red Ethernet (NIC, Network Interface Card).

Tipos de Ethernet más comunes:

◊10 Mbit/s (10Mbps) Ethernet

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

◊ Fast Ethernet (100 Mbit/s)

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

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

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

◊ Gigabit Ethernet (1000 Mbit/s)

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

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

1000BASE-SX/LX (FIBRA)

La fuerza de tareas IEEE 802.3z ha desarrollado una solución Ethernet Gigabit en fibra que soporta transmisión semidúplex y dúplex completo a velocidades de 1Gbps (1000mbps). La norma 1000Base-SX se desarrolló para soportar canalizaciones de fibra multimodo de menor costo en aplicaciones de subsistema horizontal y de menor longitud. La norma 1000Base-LX se desarrolló para soportar subsistemas de fibra multimodo para edificios y subsistemas de campo con fibra monomodo. La norma 1000Base-LX soporta longitudes multimodo de 550m y longitudes monomodo de 3km. Las soluciones 1000Base-T serán compatibles con versiones anteriores de tecnologías 10Base-T y 100Base-T.

MM 62.5/125	SX (850 nm)	Distancia	LX (1300 nm)	Distancia
	160MHz x Km	220 m.	500Mhz x Km	550 m.
	200MHz x Km	275 m.	500Mhz x Km	550 m.
MM 50/125	400MHz x Km	500 m.	400Mhz x Km	550 m.
	500MHz x Km	550 m.	500Mhz x Km	550 m.

Tabla 6: Distancias máximas Gigabit Ethernet IEEE (802.3z)

◊ 10 Gigabit Ethernet (10 000 Mbit/s)

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

2.3.4.11 Funciones de seguridad

Con cualquier sistema de vigilancia por vídeo, la privacidad es de suma importancia. El vídeo inteligente y las cámaras IP pueden funcionar para mitigar algunas de estas preocupaciones. A diferencia de las cámaras analógicas de circuito cerrado de TV que sólo envían una transmisión de vídeo única que puede ser interceptada, una cámara IP puede cifrar el vídeo que se envía a través de la red para asegurarse de que no pueda visualizarse ni interferirse. El sistema también se puede configurar para autentificar la conexión mediante certificados cifrados que sólo acepten una cámara IP específica, con lo que se elimina la posibilidad de que cualquier persona pueda espiar la línea.

Para atenuar la amenaza de la manipulación de imágenes digitales, ahora es posible utilizar técnicas tales como los sellos de fecha y hora y el marcado de agua. La creación de pistas de auditoria permite conocer qué imágenes han sido vistas y por quién y si se han realizado cambios.

Con el marcado de agua, la cámara IP agrega marcas de agua cifradas al flujo de datos de vídeo. Estas marcas de agua contienen información sobre la hora, la ubicación y los usuarios así como información sobre qué alarmas estaban conectadas a una secuencia de grabación específica. Las marcas de agua digitales están diseñadas para que sean completamente invisibles para los visualizadores, lo cual se logra dispersando la información sobre marcas de agua aleatoriamente por todo el archivo, de forma que no puedan ser identificadas ni manipuladas por usuarios no autorizados.

2.3.4.12 Software de manejo de vídeo

El software de manejo de video es un componente importante en lo relacionado con los sistemas de vigilancia IP. Los requerimientos de cada control de vídeo dependerán del número de cámaras, el rendimiento necesario, la escalabilidad y la habilidad de integrar otros sistemas. Las soluciones a ello puede ir desde un solo PC hasta avanzados software basados en cliente / servidor para proporcionar múltiples usuarios simultáneos y miles de cámaras

No obstante existen ciertas características comunes a casi todo el software de manejo de vídeos, independientemente del tipo o el tamaño:

▫ *Visualización y grabación simultánea de video en directo de múltiples cámaras*: la gestión de vídeo habilita a varios usuarios ver gran cantidad de cámaras diferentes al mismo tiempo, y permite que las grabaciones tengan lugar simultáneamente. El software de gestión puede igualmente aumentar la resolución de las cámaras con actividad o alarmas.

▫ *Diversos modos de grabación*: continuo, por alarma y/o detección de movimiento e incluso programado (el cual puede combinar continuo y basado en instrucciones de grabación por alarma). El vídeo por detección de movimiento puede ser realizado tanto a nivel de cámara, lo cual es preferible, o residir en el software. El software puede proporcionar la función de detección de movimiento a las cámaras de red o servidores de vídeo que no dispongan de ella.

▫ *Gestión de alarmas*: por ejemplo, los parámetros pueden ser establecidos de manera que las alarmas no son enviadas durante las horas de actividad normal, como podría ser de 8 a.m. a 9 p.m. de lunes a viernes. Por tanto, si el movimiento es detectado a las 3 a.m. de un sábado, el sistema sabrá que la actividad no es normal, y podrá enviar mails o mensajes de texto para alertar a las autoridades que corresponda.

▫ *Control del frame rate*: la gestión de vídeo posibilita a los usuarios definir la tasa de las cámaras seleccionadas, y predeterminar si la actividad es detectada, si la tasa de grabación se debería incrementar o en caso contrario decrementar.

▫ *Gestión de cámara*: la gestión del vídeo permite a los usuarios administrar y gestionar las cámaras desde una sola interfaz. Esto resulta útil para tareas como la detección de cámaras en la red, gestión de direcciones IP, y definir resolución, compresión y niveles de seguridad. Las cámaras están habitualmente situadas en puntos distantes y de difícil alcance, lo cual hace impracticable la actualización de cada cámara in situ. Mediante los sistemas de gestión de vídeo se puede acceder a todas las cámaras de la red que serán actualizadas automáticamente mediante firmware.

Cierto software de gestión puede incluir soporte para audio en tiempo real full-duplex, así como herramientas que mejoren los detalles de las imágenes o proporcionen información útil a los usuarios. Los programas con mejoradores de imagen, por ejemplo, pueden mejorar la calidad de la imagen tomada en condiciones climáticas adversas como lo son la lluvia, la niebla o la nieve.

La mayoría de los sistemas de gestión se encuentran disponibles en Windows, aunque también existen opciones para UNIX, Linux y Mac OS.

Puede utilizarse una amplia variedad de aplicaciones de software. La elección de la misma depende de la aplicación que le vaya a dar el usuario final y sus necesidades específicas. Un ejemplo de una aplicación de software es Milestone's Xprotect, un avanzado software de vigilancia con detección de movimiento incorporada, una rápida base de datos y acceso Web. Otro ejemplo es un software de gestión de SeeTec, un software para configurar y gestionar remotamente las cámaras, para control directo o automático de las cámaras y otro equipamiento accesorio, para la representación de imágenes y para la visualización y el reenvío de mensajes. Un tercer ejemplo es Softsite32 de JDS Digital Security System. Softsite32 es una aplicación autónoma que permite la visualización, la grabación y la gestión de imágenes de vídeo e imágenes instantáneas. Es muy robusto y escalable y tiene una instalación y configuración rápidas.

2.4. Fibra Óptica

2.4.1 Introducción

La tecnología de transmisión asociada a las líneas ha estado siempre a la expectativa de nuevas mejores técnicas; sin embargo, las novedades revolucionarias no existen. Precisamente, con el desarrollo del láser semiconductor y de la fibra óptica (FO), así como de la tecnología digital avanzada, se abrió el paso a una revolución en las transmisiones: las señales eléctricas podían ser convertidas en señales ópticas y conducirse, a través de fibras del espesor de un cabello, fabricadas de vidrio, a lo largo de grandes distancias, con lo que se irrumpía en una nueva era de las telecomunicaciones, en cuyo transcurso se irá pasando gradualmente de la era del cable de cobre a la del cable de fibra óptica. Ciertamente, en el curso de la digitalización de las redes de telecomunicación se seguirán utilizando los cables de cobres existentes, pero lo nuevos enlaces o trazados de cable se instalarán, a escala mundial, exclusivamente, con cables de fibra óptica.

Con su gran anchura de banda y baja atenuación, la fibra óptica es un medio excelente para la transmisión de señales digitales. Si al comienzo se utilizó un margen de longitud de onda de λ = 850nm, actualmente domina el espectro de los 1300nm, siendo ya accesible, con el estado actual de la técnica, la tercera ventana óptica en el margen de los 1550nm.

2.4.2 Que es la FO

Una fibra óptica es un filamento de vidrio sumamente delgado y flexible (de unas 125 micras) capaz de conducir rayos ópticos (señales en base a la transmisión de luz). Las fibras ópticas poseen capacidades de transmisión enormes, del orden de miles de millones de bits por segundo. Se utilizan varias clases de vidrios y plásticos para su construcción. Normalmente, esta luz es de tipo infrarrojo y no es visible al ojo humano. La modulación de esta luz permite transmitir información tal y como lo hacen los medios eléctricos, con un grosor del tamaño de un cabello humano. Poseen capacidad de transmisión a grandes

distancias con poca pérdida de intensidad en la señal y transportan señales impresas en un haz de luz dirigido, en vez de utilizar señales eléctricas por cables metálicos.

Al conducir luz por su interior, la fibra óptica no es propensa a ningún tipo de interferencia electromagnética o electrostática.

Además, y a diferencia de los pulsos electrónicos, los impulsos luminosos no son afectados por interferencias causadas por la radiación aleatoria del ambiente.

2.4.3 Conceptos básicos

Las fibras ópticas involucran la transmisión de información mediante luz a lo largo de fibras transparentes fabricadas de vidrio o deplástico. Una fuente de luz modulada un diodo emisor de luz (LED) o un láser, que se enciende, apaga o varía su intensidad de excicación, de tal manera que representa la señal eléctrica de entrada que contiene la información. La luz modulada se acopla a una fibra óptica a través de la cual se propaga la luz. Un detector óptico y el circuito electrónico asociado (Receptor Óptico)en el lado opuesto de la fibra recibe la señal óptica modulada y la convierte en una señal eléctrica idéntica a la señal de entrada al Transmisor.

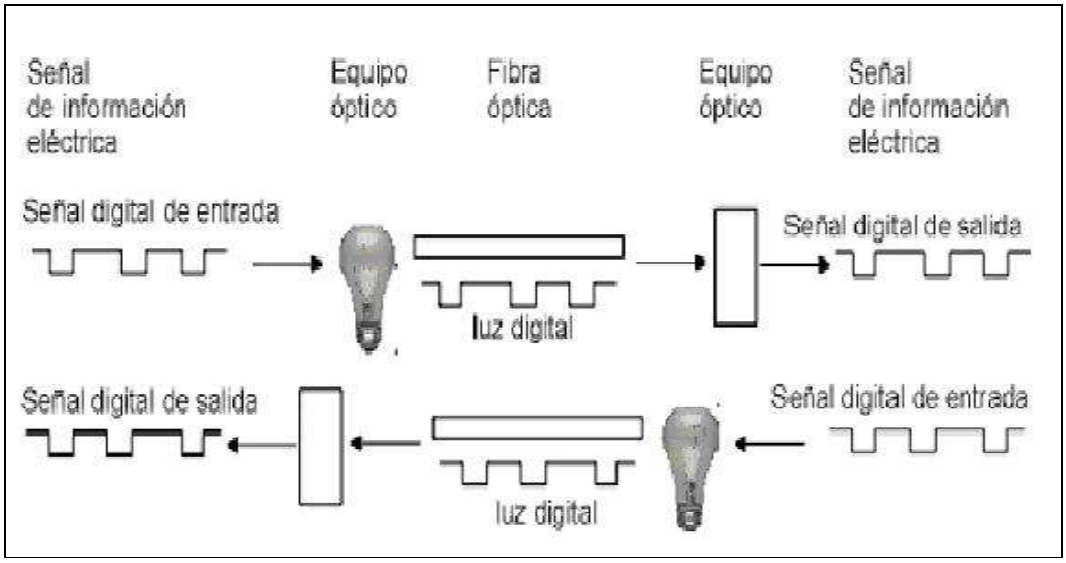


Figura 21: Comunicación por FO

Las señales luminosas digitales se propagan en la f.o. gracias a lo que se conoce como modulación digital.

En este proceso las señales analógicas se convierten a un formato digital utilizando un conversor analógico-digital (conversor A/D) antes de la etapa de modulación. Las señales luminosas digitales se propagan así en la fibra óptica.

En el otro extremo la señal de luz digital se convierte en una señal digital eléctrica mediante un detector. A continuación, un segundo convertidor analógico-digital convierte la señal digital de vuelta a su forma analógica original. Esta técnica proporciona a la señal el mismo formato que otras señales digitales y permite que se puedan agregar un gran

número de señales utilizando equipamiento de multiplexado. Las técnicas de transmisión solo muestran la transmisión de información en un sentido. Sin embargo, la mayoría de los sistemas requieren comunicaciones simultáneas y completas en ambos sentidos. Por tanto, se implemente un segundo grupo idéntico de dispositivos de modulación y detección en sentido opuesto para formar un sistema de comunicación bidireccional completamente funcional.

2.4.4 Ventajas y desventajas de sistemas de FO

Puesto que existen principalmente tres implementaciones diferentes del canal físico, cable de red cat5, ca6 y la fibra óptica, resulta importante justificar la utilización de la fibra óptica, ya que de su elección vendrán determinadas las especificaciones del sistema final
.
Algunas de las ventajas más importantes de este medio son:

■ Ancho de banda: la fibra óptica tiene la capacidad de transmitir grandes cantidades de información. Con la tecnología presente se pueden transmitir más de 60.000 conversaciones simultáneamente con dos fibras ópticas. El ancho de banda de las fibras excede ampliamente de los del cable de cobre.

■ Bajas pérdidas: las pérdidas limitan la distancia a la cual la información puede ser enviada sin necesidad de regeneración de la señal. En un cable de cobre, la atenuación aumenta con la frecuencia de modulación. En una fibra óptica, las pérdidas son las mismas para cualquier frecuencia de la señal hasta muy altas frecuencias.

■ Inmunidad electromagnética: la fibra no irradia ni es sensible a las radiaciones electromagnéticas. Esto las convierte un medio de transmisión ideal cuando el problema a considerar son las EMI (Interferencia Electromagnética).

■ Seguridad: la fibra óptica ofrece un alto grado de seguridad. Es extremadamente difícil intervenir una fibra y, virtualmente imposible hacer la intervención indetectable, por ello es altamente utilizada en aplicaciones militares.

■ Tamaño y peso: un cable de fibra óptica tiene un diámetro mucho más pequeño y es más ligero que un cable de cobre de capacidad similar.

■ Aislamiento: la fibra óptica es un dieléctrico. Las fibras de vidrio eliminan la necesidad de corrientes eléctricas para el camino de la comunicación. Un cable de fibra óptica propiamente dieléctrico no contiene conductores eléctricos y puede suministrar un aislamiento eléctrico normal para multitud de aplicaciones. Puede eliminar la interferencia originada por las corrientes a tierra o por condiciones potencialmente peligrosas causadas por descargas eléctricas en las líneas de comunicación, como los rayos. Es un medio intrínsecamente seguro que se utiliza a menudo donde el aislamiento eléctrico es esencial.

■ Fiabilidad y mantenimiento: la fibra óptica es un medio constante y no envejece. Los enlaces de fibra óptica bien diseñados son inmunes a condiciones adversas de humedad y temperatura y se pueden utilizar, incluso para cables subacuáticos. La fibra óptica tiene también una larga vida de servicio, estimada en más de treinta años para algunos cables. El mantenimiento que se requiere para un sistema de fibra óptica es menor que el requerido

para un sistema convencional, debido a que se requieren pocos repetidores electrónicos en un enlace de comunicaciones; y el cable no se ve afectado por cortocircuitos, sobretensiones o electricidad estática.

■ Versatilidad: los sistemas de comunicación por fibra óptica son los adecuados para la mayoría de formatos de comunicaciones de datos, voz y vídeo.

■ Expansión: los sistemas de fibra óptica bien diseñados se pueden expandir fácilmente. Un sistema diseñado para una transmisión de datos a baja velocidad se puede transformar en un sistema de velocidad más alta, cambiando la electrónica. El cable de fibra óptica puede ser el mismo.

■ Regeneración de la señal: la tecnología presente puede suministrar por fibra óptica más allá de los 70km. antes de que se requiera regenerar la señal. Los sistemas de cable eléctrico convencional pueden, en contraste requerir repetidores cada pocos kilómetros.

Las desventajas más importantes de las comunicaciones por fibra óptica son las siguientes:

■ Conversión electro-óptica: antes de conectar una señal eléctrica de comunicación a una fibra óptica, la señal debe convertirse al espectro luminoso (850, 1.310 o 1.550 nanómetros (nm)). Esto se realiza por medios electrónicos y la convierte en una señal óptica usando un LED o un láser semiconductor. A continuación, esta señal óptica se propaga por la fibra óptica. En el extremo del receptor de la fibra óptica se debe convertir otra vez en señal eléctrica antes de poder ser utilizada para lo cual se utiliza un fotodiodo.

■ Instalación especial: debido a que la fibra óptica es predominantemente vidrio de sílice, son necesarias técnicas especiales para la ingeniería e instalación de los enlaces. Ya no se aplican los métodos convencionales de instalación de cables de hilos como, por ejemplo, sujeción, soldadura, etc. También se requiere un equipamiento adecuado para probar y poner en servicio las fibras ópticas.

■ Reparaciones: un cable de fibra óptica que ha resultado dañado no es fácil de reparar. Los procedimientos de reparación requieren un equipo de técnicos con mucha destreza y habilidad en el manejo del equipamiento.

2.4.5 Composición de las FO

El conductor de fibra óptica esta compuesto por dos elementos básicos:

El núcleo (core) y el recubrimiento (cladding), cada uno de ellos formando por material con distinto índice de refracción, para conformar así un guiaondas propagador de las ondas luminosas. Así cuando hablamos de fibras de 50/125, 62.5/125 o 10/125mm, nos estamos refiriendo a la relación entre el diámetro del núcleo y el revestimiento.

Otro parámetro importante en una fibra es su apertura numérica. En los conductores de fibra óptica se utiliza el efecto de la reflexión total para conducir el rayo luminoso por su interior. El ángulo necesario para acoplar al núcleo un rayo luminoso desde el exterior recibe el nombre de ángulo de aceptación. Pues bien, el seno de este ángulo se denomina

apertura numérica (AN). A mayor AN mayor será la potencia luminosa acoplada a una fibra óptica procedente de una fuente de luz, i.e. led.

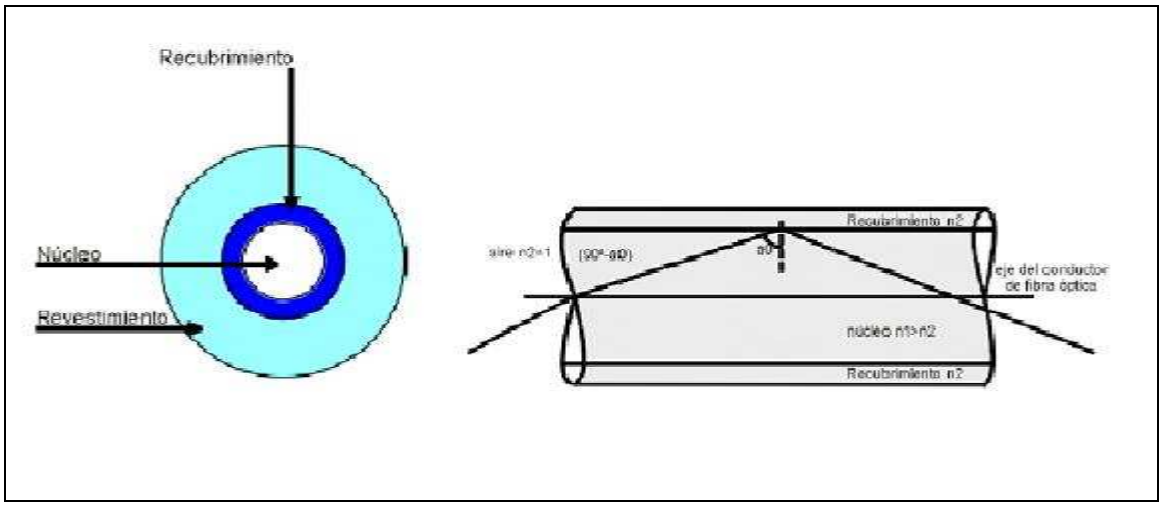


Figura 22: Composición FO

2.4.6 Conducción de la luz en un conductor de FO

Un parámetro extrínseco a la fibra óptica es la ventana de trabajo. Cuando hablamos de ventanas de trabajo nos referimos a la longitud de onda central de la fuente luminosa que utilizamos para transmitir la información a lo largo de la fibra. La utilización de una ventana u otra determinará parámetros tan importantes como la atenuación que sufrirá la señal transmitida por kilómetro. Las ventanas de trabajo más corrientes son: Primera ventana a 850nm, segunda ventana a 1300nm y tercera ventana a 1550nm. La atenuación es mayor si trabajamos en primera ventana y menor si lo hacemos en tercera. El hecho de que se suela utilizar la primera ventana en la transmisión de una señal es debido al menor coste de las fuentes luminosas utilizadas, al ser tecnológicamente más simple su fabricación.

2.4.7 Tipos de FO

Se pueden realizar diferentes clasificaciones acerca de las fibras ópticas, pero básicamente existen dos tipos: fibra multimodo y fibra monomodo.

Fibras multimodo. El término multimodo indica que pueden ser guiados muchos modos o rayos luminosos, cada uno de los cuales sigue un camino diferente dentro de la fibra óptica. Este efecto hace que su ancho de banda sea inferior al de las fibras monomodo. Los enlaces basados en este tipo de fibras y con diodos LED, como fuente de luz, puede resultar enlaces competitivos en coste.

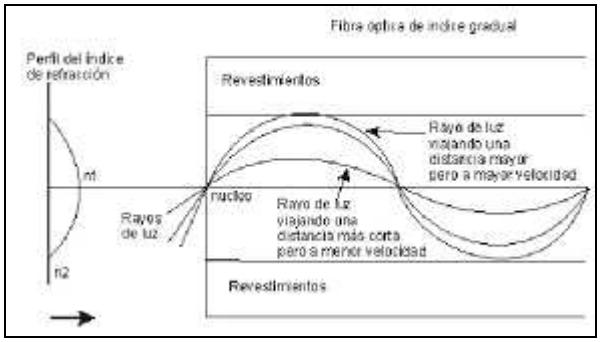


Figura 23: Fibra multimodo

Fibras monomodo. El diámetro del núcleo de la fibra es muy pequeño y sólo permite la propagación de un único modo o rayo (fundamental), el cual se propaga directamente sin reflexión. Este efecto causa que su ancho de banda sea muy elevado, por lo que su utilización se suele reservar a grandes distancias, superiores a 10Km, junto con dispositivos de elevado coste (LÁSER).

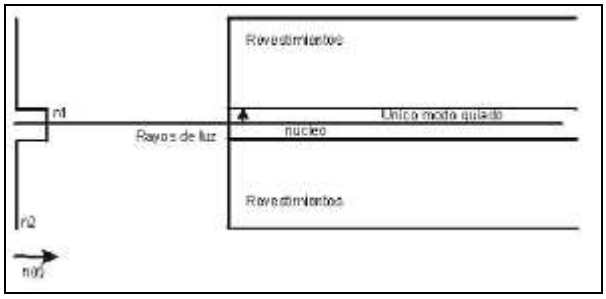


Figura 24: Fibra monomodo

Sistemas de transmisión basados en fibra monomodo y fuentes de luz LASER de altas prestaciones son los usados por los operadores de telecomunicación para los enlaces de gran capacidad y larga distancia.

2.4.8 Estructura de los cables de FO

El objetivo de los cables es proteger y asegurar las propiedades de la fibra óptica a lo largo del ciclo de vida: instalación y operación. Por consiguiente, existen numerosas estructuras de cables de fibras ópticas dependiendo de su aplicación. A continuación se explican dos de las estructuras más destacadas.

Estructura ajustada: está formado por un tubito de plástico o vaina en cuyo interior se encuentra alojado, en forma estable, el conductor de fibra óptica. La vaina debe ser fácil de manejar de forma similar a un cuadrete o un par coaxial. Pueden ser cables tanto monofibra, como multifibra. Sus aplicaciones más frecuentes son: cortas distancias,

instalaciones en campus, instalaciones en interiores, instalaciones bajo tubo, montaje de conectores directos y montaje de latiguillos.

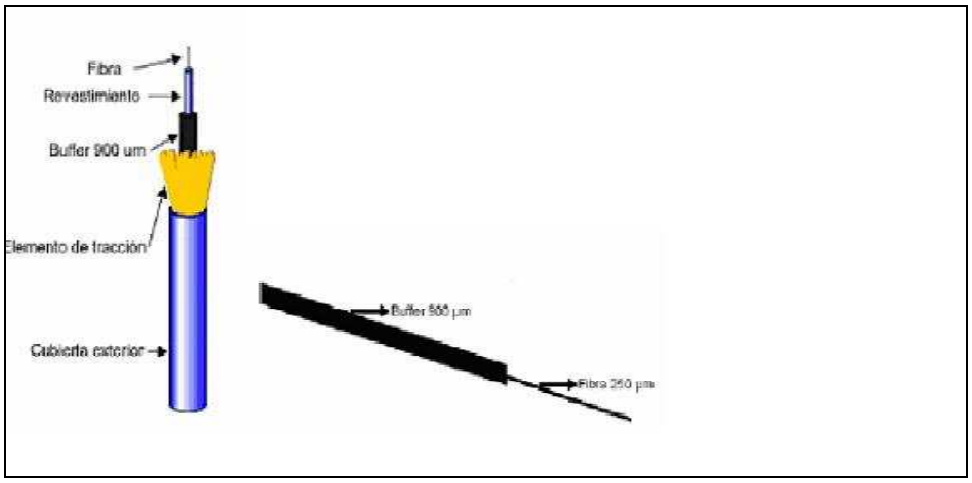


Figura 25: FO estructura ajustada

Estructura holgada: en lugar de un solo conductor se introducen de dos a doce conductores de fibras ópticas en una cubierta algo más grande que la vaina del caso anterior, de ésta forma los conductores de fibra no se encuentran ajustados a la vaina. Además se suele recubrir todo el conjunto con un gel para que no penetre el agua en caso de rotura del cable. Principalmente se dividen en cables multifibras armados (antihumedad y antirroedores con fleje de acero) y cables multifibra dieléctrico (cable totalmente dieléctrico). Como aplicaciones más importantes tenemos conexiones a largas distancias e instalaciones en exteriores.

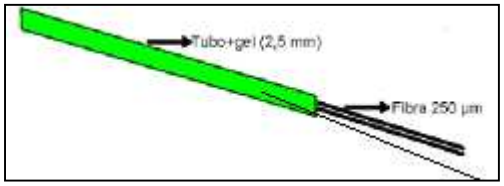


Figura 26: FO construcción holgada

2.5. Seguridad Integrada

Si por integrar entendemos “contribuir, unirse o entrar a formar parte de un todo o conjunto” podemos deducir que la aplicación de este concepto al sector de las seguridades nos permite afirmar que la integración consistiría en conjuntar y vincular diferentes sistemas autónomos para su control y supervisión desde una plataforma central.

Los objetivos que se persiguen con la integración son:

- Relacionar diversos sistemas autónomos para optimizar los recursos disponibles.

▫ Centralizar las informaciones y comunicaciones generadas para facilitar la toma de decisiones.

▫ Mejorar la eficacia de los medios técnicos y de la gestión de seguridad.

▫ Incrementar la seguridad en la explotación del sistema: operaciones, procesos, procedimientos, actuaciones,...

▫ Reducir los costes (instalación, mantenimiento, equipos,...) y consumos de energía.

Entre las posibilidades, más frecuentes, de integración con sistemas de vigilancia óptica destacamos:

• Los propios medios del CCTV: captación, transmisión, almacenamiento, reproducción, control, etc.

• Sistemas de detección de intrusión.

• Sistemas de control de accesos.

• Sistemas de protección contra incendios.

• Equipos de transmisión y verificación de alarmas.

• Sistemas de control de rondas y vigilancia de instalaciones.

• Sistemas de comunicación: interfonía, megafonía y telefonía.

• Sistemas de climatización, calefacción, aire acondicionado, iluminación,...

La principal finalidad que se persigue al integrar sistemas de CCTV es obtener imágenes reales y que corroboren las incidencias producidas en otros sistemas: una intrusión, un acceso no permitido, un incendio, verificar una alarma, una avería, etc. Por ello es indispensable disponer, además de los equipos de captación de diferentes medios de registro y almacenamiento de imágenes.

2.6. Centro de Control

El Centro de Control es el espacio físico donde se centralizan y gobiernan los diferentes sistemas, aunque gracias a los avances tecnológicos (Internet, telefonía móvil), es posible la administración del sistema desde cualquier lugar del mundo y a cualquier hora mediante un programa informático navegador o el teléfono móvil.

Para controlar todas las funciones se instalan equipos compuestos de procesador central y controladores inteligentes a los que se conectan los diferentes dispositivos a integrar.

Un sistema integral se debe componer de diferentes medios de protección adaptados a las necesidades de seguridad de la instalación o de las personas, de tal manera que garanticen la seguridad del objeto de protección reduciendo el número de vulnerabilidades; estos medio serían los ya expuestos previamente en la descripción de los sistemas anti-intrusión: Medios pasivos, activos, humanos y medidas organizativas.

3. Metodología del Proyecto de despliegue

3.1. Despliegue de un Sistema de Seguridad

3.1.1 Introducción

Para el seguimiento de la actividad podemos establecer cinco fases claramente diferenciadas:

1) Diseño del sistema.
2) Elaboración de la propuesta.
3) Implantación del proyecto.
4) Entrega del sistema.
5) Mantenimiento y seguimiento del cliente.

Cualquier actividad que realicemos llevará de forma intrínseca el desarrollo de todas y cada una de las citadas fases, en mayor o menor medida en función de la complejidad y envergadura del proyecto y de la idiosincrasia del cliente.

3.1.2 Fases de la actividad

La actividad puede ser dividida en las siguientes fases:

• Diseño del sistema.

• Dentro de esta fase de la actividad podemos diferenciar tres puntos:

• Estudio de las características definidas por el cliente.

• Toma de datos

• Realización del diseño.

3.1.2.1 Diseño Sistema

El diseño del sistema contempla el análisis de las pretensiones técnicas y económicas que el cliente expone. Ello nos lleva a un preestudio de lo que en realidad pretende el cliente y de las posibilidades de llevarlo a la práctica.

Una vez definidas las necesidades del cliente, se realiza la toma de datos necesarios, siendo ésta uno de los puntos más importantes de todas las fases de la actividad. En dicha toma de datos se deberán evaluar los siguientes puntos:

Elección de los sistemas y equipos de seguridad que se adecuen con mayores posibilidades a la detección de los riesgos que se pretenden minimizar. Dicha elección implica un análisis pormenorizado de los condicionantes ambientales y funcionales que incidirán de manera directa o indirecta en los equipos propuestos.

Determinación en cuanto a magnitud y dificultad, de las canalizaciones y obra civil necesaria para la implantación del sistema elegido.

Análisis del emplazamiento donde se ubicarán los equipos de centralización, en cuanto a dimensionado e idoneidad.

Dimensionamiento de los medios técnicos y humanos necesarios para llevarlo a cabo.

Por último, y tras el estudio de todos los datos e indicaciones recogidas se procede a la realización de los cálculos necesarios.

3.1.2.2 Elaboración del Proyecto

Realizada la toma de datos necesaria y el estudio correspondiente se procede a la confección de la oferta. Dicha oferta deberá ser:

● Clara y precisa, sin dar lugar a ambigüedades.

● Con profusión de datos y documentación, debidamente clasificados, que arropen la propuesta.

● Con valoraciones económicas pormenorizadas.

● Con una buena organización y presentación del documento.

3.1.2.3 Implantación del Proyecto

Una vez aceptada la oferta, entramos en la fase definitoria del producto que nos ocupa. En dicha fase podemos distinguir los puntos que a continuación se pasan a describir:

1.- Reunión de lanzamiento: En esta reunión se retoman los contactos iniciados en las fases anteriores concretando las acciones a llevar a cabo y si procede alguna variación al proyecto original.

2- Replanteo de obra: Tras la reunión de lanzamiento, normalmente se prevé una visita a las instalaciones objeto de la implantación del proyecto. En esta reunión a pie de obra se confirman todos los pequeños detalles que hubieran quedado por definir. Es a partir de este momento, donde empieza a contar el plazo de entrega comprometido en oferta. Este momento normalmente se documenta con lo que denominamos el acta de inicio de obra.

3.- Elaboración del proyecto de detalle: una vez definido hasta el último detalle que consideremos de importancia es el momento de descomponer el proyecto en cuantas actividades y subactividades sea preciso para el posterior control de la marcha de la obra.

Dicho proyecto estará de acuerdo, en extensión y profundidad, con el volumen, complejidad y desarrollo en tiempo de la implantación del sistema.

4.- Planning de ejecución: Con objeto de poder controlar y corregir en tiempo las posibles desviaciones del desarrollo de la implantación es aconsejable, cuando no imprescindible, el realizar un planning de ejecución.

5.- Realización de pedidos de materiales: Como ya se ha comentado en capítulos anteriores, los materiales (equipos y sistemas) suponen uno de los puntos vitales del producto, es por ello que la realización de los pedidos de los materiales necesarios para nuestra instalación, ha de suponer el esfuerzo preciso en negociaciones con proveedores para optimizar las condiciones económicas y plazos de entrega.

6.- Acopios de materiales: Realizados los pedidos debemos velar por el cumplimiento de la programación realizada, no dejando a iniciativa de los proveedores el cumplimiento o no de los plazos comprometidos. Para ello será necesario realizar los seguimientos oportunos para asegurar dicho acopio.

7.- Ejecución de la instalación: Una vez realizado el planning de ejecución, independientemente del seguimiento en el acopio de materiales, será necesario controlar las posibles desviaciones que se puedan producir en las partidas de mano de obra, potenciando las dotaciones si ello fuera necesario para el cumplimiento de la programación. Debemos tener en cuenta que el tiempo perdido en estas partidas es irrecuperable muchas veces.

8.- Pruebas de control de calidad: Durante el desarrollo de la instalación, se deben prever la realización de las pruebas de control de calidad necesarias que nos puedan asegurar que la instalación se está llevando a cabo según los parámetros exigidos. Aunque esto muchas veces nos pueda suponer considerables retrasos por localizaciones de elementos o partidas que no superen las pruebas realizadas, a la larga será un tiempo ganado.

3.1.2.4 Entrega de la Instalación

Una vez realizada la instalación y quizás uno de los momentos mas críticos de esta es el momento de la recepción por parte del cliente. En efecto será en este momento cuando se compruebe si las expectativas del cliente, a la hora de contratar dicho servicio, se cumplen en la instalación realizada. Con este fin se procede de acuerdo a los siguientes pasos:

1.- Elaboración del protocolo de pruebas: dicho documento recogerá las pruebas que deben realizarse y cuales han de ser los resultados obtenidos. Estos resultados son difícilmente objetivos en algunas circunstancias, por lo que es aconsejable tener acordados de antemano, si es posible en la reunión de lanzamiento.

2.- Ejecución del protocolo de pruebas: es el momento de demostrar al cliente que lo que se le entrega responde a sus expectativas. Para ello se llevan a cabo la realización de las pruebas definidas en el protocolo de pruebas y se cotejan los resultados obtenidos con los previstos.

3.- Entrega de la instalación: Si los resultados obtenidos en las pruebas realizadas se ajustan a los previstos, se hace entrega de la instalación al cliente documentando dicha situación con el "Acta de entrega". Este acta, en algunas circunstancias se denomina "Acta de recepción provisional", dejando la realización del "Acta de recepción definitiva" una vez haya transcurrido el periodo de garantía establecido, normalmente de un año de duración.

4.- Entrega del manual de funcionamiento: Coincidiendo con la entrega de la instalación, se hace entrega del manual de funcionamiento al cliente. Dicho manual habrá sido desarrollado en la fase de ingeniería del proyecto tras la elaboración del proyecto de detalle y en el se recogen todos los datos y planos necesarios para el conocimiento en profundidad del sistema instalado.

5.- Facturación: Recepcionada la instalación se procede a la facturación. En algunas circunstancias ésta se ha ido realizado con certificaciones parciales a lo largo de la implantación, liquidándose en el momento de la entrega.

3.1.2.5 Mantenimiento

Es obvio el interés del cliente en que la inversión y los objetivos conseguidos con la implantación del sistema se mantengan el máximo tiempo posible, para ello no hay mejor solución que un mantenimiento programado que implique una serie de visitas preventivas, complementadas con las acciones correctivas que vayan siendo precisas.

Para ello se pueden articular distintos tipos de contratación en función de la cobertura requerida por el cliente. Según esto tendremos:

Mantenimiento Preventivo: Supone la realización periódica de una serie de tareas, que evite el desgaste, envejecimiento prematuro o malfuncionamiento de los equipos y garantice su amortización en el plazo inicialmente previsto.
Mantenimiento Correctivo: Supone la realización de una actuación requerida por el cliente por el malfuncionamiento de alguno de los equipos. Son intervenciones esporádicas que en gran medida podrán ser minimizadas si existe un buen mantenimiento preventivo.
En los dos supuestos hasta ahora expuestos la sustitución o cambio de los materiales es normalmente a cuenta del cliente.

3.1.3 Requisitos del Cliente

La finalidad del proyecto consiste en la "**Realización de un diseño de integración en materia de seguridad electrónica**", por lo que restringiremos las condiciones del cliente a las siguientes permisas:
:
● Seguridad perimetral tutelada por un sistema de CCTV basado en red IP, que contemple una posible futura ampliación de medios.

● CCTV interior en los posibles puntos conflictivos

● Detección intrusión edificios

● Protección superior en edificio central, así como integración con el nuevo sistema.

● Todo este sistema de seguridad deberá ser centralizado en un punto de ubicación a la entrada del perímetro, cuerpo de guardia o garita de vigilante donde estará bajo vigilancia permanente, con opción remota de configuración y gestión de los subsistemas, tanto de CCTV como anti-intrusión.

● Respecto al tema económico, se plantearán aquellas soluciones que supongan un desembolso menor.

Igualmente aclarar que la toma de datos se ha basado en la búsqueda de los equipos que mejor se adecuen a las necesidades y con una buena relación calidad/coste Por otro lado, la magnitud de la obra civil no se ha tomado en cuenta en la elaboración del proyecto, considerando que la infraestructura dispone de las canalizaciones necesarias que comunican todos los edificios entre sí y que cuentan con espacio libre para introducir nuevos cableados.

Previamente al paso del desarrollo de la instalación es necesario responder a una serie de cuestiones que determinarán la forma del diseño y ayudarán a sacar el máximo rendimiento a las posibilidades. Con este fin se realiza un esfuerzo de optimización de dichos medios, bajo el prisma de incluirlos en un sistema integrado de seguridad donde, lejos de contemplar a cada edificio y al perímetro exterior como una entidad aislada, se constituya un conjunto cuyos recursos de seguridad son compartidos. Las opciones ofrecidas van dirigidas a mejorar la capacidad de respuesta existente, y disminuir el nivel de riesgo.

3.1.4 CCTV

Las actuaciones que se propongan en el subsistema de circuito cerrado de televisión deben referirse a la optimización del sistema integrado de seguridad. Pretendiendo, por un lado centralizar los sistemas ya existentes dotándoles de tecnología IP, (puesto que se quiere realizar una instalación basada en IP y como se observa en los planos existen equipos ya instalados), y por otro instalar nuevas cámaras ya dotadas de esta tecnología. En este caso el sistema estará formado por las cámaras analógicas y los servidores de vídeo requeridos para la migración, así como por las nuevas cámaras IP a instalar en lo que a CCTV se refiere.

En la arquitectura ideada, el sistema estará basado en múltiples cámaras analógicas (existentes), digitales (las nuevas, ahora propuestas), y servidores de vídeo que adaptarán la señal en banda base proporcionada por las cámaras para su transmisión por redes basadas en protocolo IP.

Siguiendo con el escenario es necesario determinar cuales son los puntos principales a vigilar. Partiendo de estas ubicaciones se debe valorar la distinta importancia de cada uno de esos puntos, las condiciones de iluminación de las que se dispone o el ángulo requerido de visión. Igualmente el entorno en el que nos encontremos y el escenario determinarán si es necesario la instalación de un tamper en los equipos o que estén preparados como antivandálicos.

En lo referente a las condiciones de iluminación habría que distinguir entre un uso de las cámaras para interiores o exteriores (existen cámaras IP que pueden ser utilizadas en los dos ámbitos), o plantear la posibilidad de las cámaras con visión diurna / nocturna que proporcionan imágenes en color durante el día e imágenes en blanco y negro durante la noche, pensando en la sensibilidad lumínica de la cámara IP en ambos entornos.

Para poder supervisar correctamente los objetos desde las cámaras es necesario posicionarlas ajustándose al ángulo de visión requerido (ancho, estrecho, general o cobertura detallada, determinando la amplitud de la escena que se necesita ver). Las cámaras IP suelen ser suministradas con enfoque y ángulo fijo así como variable que permite ajustar a distancia el movimiento horizontal/vertical/zoom para ampliar la zona de cobertura. Respecto al área de cobertura, una cámara PTZ o un domo son capaces de cubrir un área mayor que la que cubriría una cámara fija. Cuanto mayor sea el área, mayor será el número de cámaras necesitadas.

3.1.4.1 Factores subsistema CCTV

3.1.4.1.1 Determinación necesidades de aplicación

Es necesario tener en cuenta si el control de toda la seguridad de la infraestructura se va a llevar a cabo de manera remota, si se van a utilizar activaciones de entrada y salida de las cámaras integrando otros equipos, así como si se implantará un sistema de vigilancia inteligente con gestión avanzada de eventos. Todo esto es respondido según las necesidades que se planteen.

Igualmente es necesario establecer unos requisitos de almacenamiento de la grabación en función de cómo se programe la actuación de todas las cámaras, realizando estimaciones de saltos de alarmas que provoquen grabaciones o de actividad en las zonas de grabación programada. Este estudio lleva consigo la necesidad de calcular igualmente los requisitos de ancho de banda antes de decidir el número de cámaras, la tecnología a utilizar así como el medio de transmisión necesario.

3.1.4.1.2 Factores sobre redes

Dado que los sistemas digitales utilizan redes informáticas como medio de transporte para contenidos, el diseño de red afectará al rendimiento global del sistema de vídeo, así como al rendimiento global de la red.

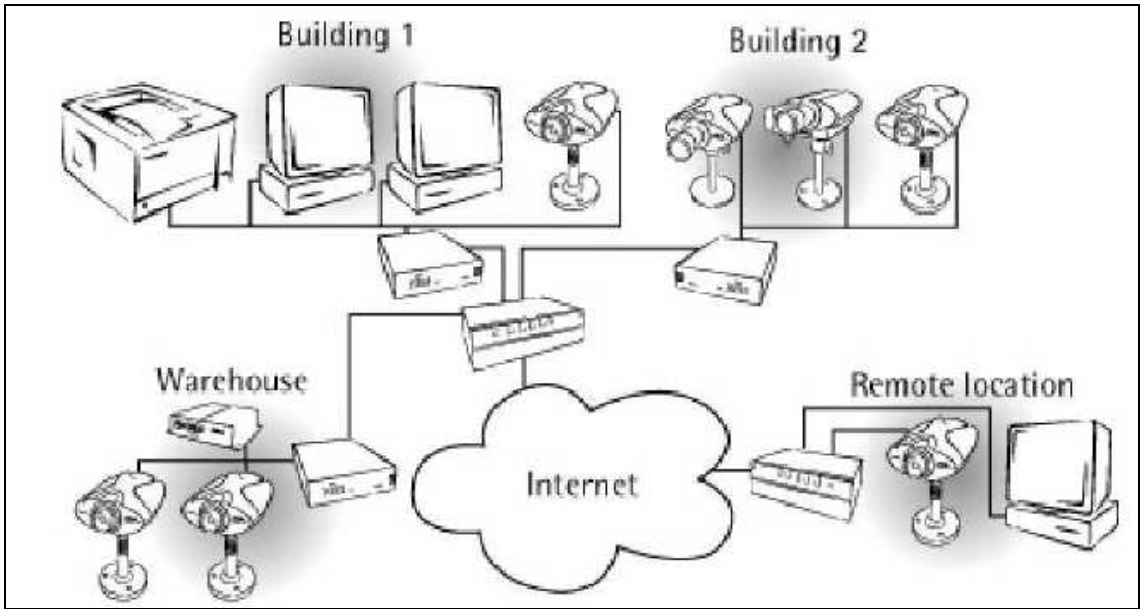


Figura 27: Ejemplo de un sistema de video en red.

En el diseño habría que tener en cuenta la exclusividad o no de la red para el sistema de CCTV así como la ubicación de los puntos de red, infraestructura dispersa en puntos distantes o bien concentrados en un mismo área, así como la facilidad de realizar un cableado o en caso de existir previamente, testar el estado en que se encuentre.

3.1.4.1.2.1 Consideraciones previas respecto al ancho de banda

Los switches de red permiten a los distintos equipos como son las cámaras de red, los servidores o PCs comunicarse y compartir información, en algunos casos, con una conexión común de Internet. Los diseños de la red pueden tomar muchas formas y pueden variar en términos de desarrollo y seguridad.

Como ya se comentó, el primer paso necesario sería determinar cual es el uso que se le está dando a la red actualmente así como su nivel de congestión, tanto si se trata de una red de área local LAN o bien de área mayor como una WAN.

Si se trata de un caso donde se implementará un pequeño sistema de vigilancia donde solo se trate de unas 8 o 10 cámaras, se debería ser capaz de usar un switch de red básico de 100Mbits sin tener que considerar limitaciones de ancho de banda, en la mayoría de los casos se puede implementar un sistema de vigilancia de este tamaño considerando la red ya existente.

No obstante si se trata de un sistema mayor de 10 cámaras, se debe estimar la carga de red que se necesitará, partiendo de las siguientes permisas:

Una cámara utilizará aproximadamente de 2 a 3Mbits de ancho de banda cuando sea configurada para enviar imágenes de alta calidad a una resolución alta.

Con más de 12 o 15 cámaras, se debe considerar el uso de un switch con capacidad de gigabit, Gbit. Si se utiliza un switch que soporte gigabit, el servidor que contenga el software de gestión de vídeo deberá tener instalado un adaptador de red de gigabit.

Es necesario determinar los niveles de congestión durante unos periodos dados para averiguar si se debe o no instalar ancho de banda adicional en la red, o si por el contrario con la red ya instalada es suficiente. Podría ser que el tráfico de la red disminuyera durante la noche y los fines de semana, momentos en los que el sistema de vigilancia debe ser activado.

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

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

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

Frecuencia de imagen condicionada a sucesos:
En la mayoría de las aplicaciones no es necesario disponer de 30 imágenes por segundo (ips) en todo momento en todas las cámaras. Las posibilidades de configuración y los sistemas inteligentes incorporados a las cámaras de red o el servidor de vídeo permiten establecer frecuencias de imagen menores (por ejemplo, 1-3 ips), reduciendo drásticamente el consumo de ancho de banda. En caso de alarma, si está activada la detección de movimiento, la frecuencia de imagen de la grabación puede aumentarse automáticamente hasta un nivel superior.
En la mayoría de los casos, la cámara sólo enviará vídeo a través de la red si merece la pena grabar las imágenes, lo que por regla general únicamente supone el 10% del tiempo. El 90% restante no se transmite nada a través de la red.

3.1.4.1.3 Ancho de banda de la red

Calcular las necesidades del ancho de banda:

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

▪ Resolución de la imagen (mayor resolución, más ancho de banda requerido).

▪ Tipo de compresión (Motion JPEG a menudo requiere mayor ancho de banda que MPEG-4).

▪ Ratio de compresión (cuanto mayor sea la compresión, menos ancho de banda se usará).

▪ Frame rate (cuanto más alto, más lo será también el ancho de banda usado).

▪ Complejidad de la imagen (la más complejo utilizará un ancho de banda mayor.)

Un calculador de ancho de banda permite determinar el ancho de banda que un producto de vídeo IP utilizará, basándose en el tamaño de la imagen y la velocidad de imagen. También calculará la cantidad de espacio que necesitaría una secuencia de imágenes grabada.

3.1.4.2 Métodos de Grabación

Para cada cámara se puede seleccionar uno de los 3 métodos de grabaciones a usar:

Continuo: se puede fijar la cantidad de tramas por segundo y su frecuencia (como por ejemplo cada pocos segundos entre imágenes) la cámara debería enviar imágenes al software para su grabación. Si se realiza de forma continua se utilizará mayor espacio en disco que por ejemplo usando la grabación dependiente de movimiento.

Activado por movimiento o alarma: En este tipo de grabación, simplemente definiendo la alarma para la cámara seleccionada, se grabará cuando la alarma sea disparada, igualmente se puede determinar la longitud del buffer de almacenamiento de imágenes previo y posterior a la alarma, cuantos segundos se quieren grabar antes y después de que la alarma salte. Esto dará una imagen más extensa del evento. Grabando únicamente cuando se detecte movimiento o salte la alarma, se ahorrará mucho espacio en disco comparado con la grabación continua.

Programado por horario: Con la grabación programada, se establecen horarios para tanto grabación continua como basada en alarma / detección, resultando una combinación de ambas formas de grabación.

3.1.4.3 Almacenamiento

Los requerimientos de almacenamiento en discos duros dependen del ratio de imágenes por segundo del vídeo que se desee almacenar. Si desea almacenar todo el vídeo a 30 imágenes por segundo (30 frames per second, fps) como oposición a almacenar 1 fps, debe saber que precisará 30 veces más capacidad de almacenamiento. Cada aplicación tiene diferentes necesidades de grabación y almacenamiento en términos de imágenes por segundo en el vídeo y los requerimientos de almacenamiento en disco diferirán en función de ellos.

3.1.5 Protección Anti-Intrusión

El perímetro es la "primera línea de defensa" de cualquier propiedad y debe formar parte de una estrategia integral de protección. No se debe permitir que esta "línea" sea sobrepasada por intrusos. Nuestro perímetro cuenta con un muro que lo acordona, que nos servirá para la ubicación de nuestro subsistema así como suponer un impedimento más al acceso interior.

A excepción de otros sistemas, la Seguridad Perimetral funciona las 24 horas y su "presencia" además de ser un formidable Sistema de Defensa, representa un factor psicológico "altamente disuasivo". De no conseguirse este propósito debe detener, obstaculizar y dificultar la acción de los intrusos con el fin de retardar la progresión de la amenaza; de este modo se logra unos mayores tiempos de reacción para los otros medios de protección (humano y electrónico). Estos medios se disponen en la zona periférica de las propiedades, con objetivos concretos: deben delimitar la propiedad, y como bien se ha dicho deben constituir un elemento disuasorio.

Los sensores perimetrales pueden usarse como complemento de los sensores interiores de seguridad o como seguridad primaria si nuestro proyecto a desarrollar posee unas condiciones en las que no es factible la seguridad interior.

Las condiciones ambientales (temperaturas extremas, lluvia, nieve, animales, basura que levanta el viento, terreno, tráfico, entre otras) deben ser tenidas en cuenta, de manera tal que, aún operando bajo efectos adversos, el sistema siga ofreciendo alta probabilidad de detección, se minimicen las alarmas accidentales (de causa ambiental) y las falsas alarmas (de causa desconocida). Los sensores pueden instalarse totalmente ocultos: esto los hace difíciles de eludir y los preserva del vandalismo. Pero hay sensores muy visibles, que se colocan así para crear un efecto disuasivo. Por otra parte, los sensores volumétricos generan un campo de detección invisible tan grande, que difícilmente puedan ser vulnerados

3.1.6 Subsistema de Centralización (Centro de Control de Seguridad, CCS)

Permite la integración de los subsistemas de Detección de Intrusión y CCTV. Este control implica las tareas de recepción de alarmas, telemando sobre parámetros de los subsistemas, registro de incidencias y en general, apoyo a la toma de decisión sobre las emergencias. También incluye la alimentación eléctrica de todos los elementos electrónicos de los diferentes subsistemas. Este subsistema debe ubicarse en un punto estratégico de las instalaciones

4. Desarrollo

La infraestructura planteada a utilizar como base para la instalación de un sistema de seguridad es la que se muestra en el plano 1:*"Plano General"* ubicado al final del documento en el anexo A. En ella se instalarán los distintos equipos de ambos sistemas, anti-intrusión y CCTV, que provean de una mayor seguridad. Este plano será el punto de partida de toda decisión como si una toma de datos se tratase.

4.1. Subsistema de Intrusión

4.1.1 Perímetro Exterior

La implantación de un sistema anti-intrusión busca establecer un perímetro de seguridad en las zonas previstas, durante las horas en las que las distintas dependencias debieran permanecer desocupadas, alertando en las situaciones en las que se produzca una situación de alarma por intento de intrusión al Subsistema de Centralización.

Partiendo de la situación en la que se encuentra ubicado el recinto a cubrir, así como sus características delimitadoras (todo el perímetro está rodeado por un muro de una altura aproximada de 4 m.) se ha optado por instalar un sistema anti-intrusión basado en barreras. Se descartan desde un principio los alambrados o detectores enterrados por no ser posible su colocación.

En función de que el terreno de la parcela sea liso o abrupto, las barreras se instalarán infrarrojas o microondas. Para terrenos llanos donde los equipos pueden "verse" entre si, la barrera por infrarrojo es la ideal.

Cuando el terrero es irregular o presenta obstáculos para que los dos postes "se vean" claramente, se debe prever la instalación de barreras microondas. Estos equipos generan un campo de detección con forma de elipse, y tienen la capacidad de poder atravesar pequeños obstáculos o irregularidades del terreno.

Instalando equipos de calidad y con un criterio adecuado, los problemas serán mínimos o inexistentes. Para tener certeza de si una alarma es realmente una intrusión es por lo que, entre otras, se complementará la instalación de una detección perimetral con un circuito cerrado de televisión y su correspondiente almacenamiento de imágenes, y así analizar que ha ocurrido realmente en un salto de alarma.

Por lo anteriormente descrito finalmente se optará por la instalación de barreras infrarrojas. Estas se adecuan mejor al perímetro exterior, donde no existen obstáculos que impidan la visibilidad. Así mismo las barreras infrarrojas cuentan con la principal ventaja de la reducida anchura del haz, lo que nos permite su utilización en nuestras instalaciones donde la detección resultaría insuficiente para un sistema de microondas (aproximadamente de 6m).

A lo largo de todo el perímetro del recinto cubierto por muro, se colocarán distintas barreras infrarrojas de un alcance u otro en función del punto del perímetro en el que nos encontremos, de forma que quede todo completamente cubierto. Las barreras son colocadas mediante unos postes en la parte superior del muro que proporcionen su fijación al mismo.

Como inconveniente característico cabe citar la influencia desfavorable que la niebla abundante, las tormentas de lluvia o nieve, e incluso el paso de aves en vuelo, tienen para el buen funcionamiento del sistema, pudiendo ser causa de alarmas indeseables.

Para aquellos puntos en los que por los cambios de orientación del muro que rodea a la ubicación resulta imposible la detección de intrusión por medio de las barreras colocadas, se dispondrán detectores cubriendo los posibles puntos muertos. Esto son las localizaciones que se convierten en puntos débiles y de fácil acceso por no quedar controladas por alguna de las barreras.

4.1.1.1 Barreras y Detectores

Para establecer el número de barreras a colocar dividimos el plano en 8 lados, como bien aparecen referenciados en el plano 1:*"Plano General"*, diferentes distinguibles en la figura de la instalación, los cuales cuentan con las siguientes medidas:

LADO PERÍMETRO	LONGITUD (metros)	BARRERAS A COLOCAR
Lado 1 (puerta acceso)	46	1 (50m)
Lado 2 (delimitación dcha. 1)	60	1 (100m)
Lado 3 (delimitación dcha. 2)	85	1 (100m)
Lado 4 (limite inferior)	380	4 (100m)
Lado 5 (delimitación izq. 1)	180.15	2 (100m)
Lado 6 (delimitación izq. 2)	80	1 (100m)
Lado 7 (delimitación izq. 3)	75	1 (100m)
Lado 8 (limite superior)	280	3 (100m)
Lado 9 (delimitación dcha. sup.)	95	1 (100m)
TOTAL BARRERAS 100metros		14
TOTAL BARRERAS 50metros		1

Tabla 7: Distancia perimetral, colocación barreras

Como se aprecia en la tabla las barreras a instalar tendrán un alcance de 100 o 50 metros dependiendo del lugar donde se coloquen. Ver el detalle de la configuración en el plano 2:*"Barreras"* (anexo A).

En la actualidad existen barreras con un alcance en el exterior de 200metros, no obstante se ha considerado oportuno establecerlas de 100metros dado que si un suceso causase fallo en una de las barreras resulta preferible la pérdida de 100metros sin control que no 200m. Bajo esta misma teoría podría pensarse un mejor subsistema anti-intrusión el formado

únicamente por barreras de 50metros, no obstante esto supondría un mantenimiento mayor y un número excesivo de puntos a centralizar y, evidentemente, un coste superior.

Como bien se ha comentado anteriormente, hoy en día en el mercado se pueden encontrar barreras de 1, 2 y hasta 4 haces. Como es obvio pensar, un mayor número de haces permitirá una detección mayor, no obstante la elección de uno u otro irá en base del grado de seguridad requerido. Puesto que buscamos la mayor seguridad posible nuestra elección es la de barreras de 4 haces.

Con la instalación de barreras de 4 haces se conseguirá prevenir un mayor número de falsas alarmas; desde caídas de hojas o pequeños animales. No obstante, los detectores pueden configurarse para generar una alarma tanto cuando los cuatro haces son bloqueados a la vez o como cuando esto sólo sucede en los superiores o en los inferiores. Esta particularidad además de evitar las falsas alarmas elimina la posibilidad de que el intruso pueda ingresar arrastrándose.

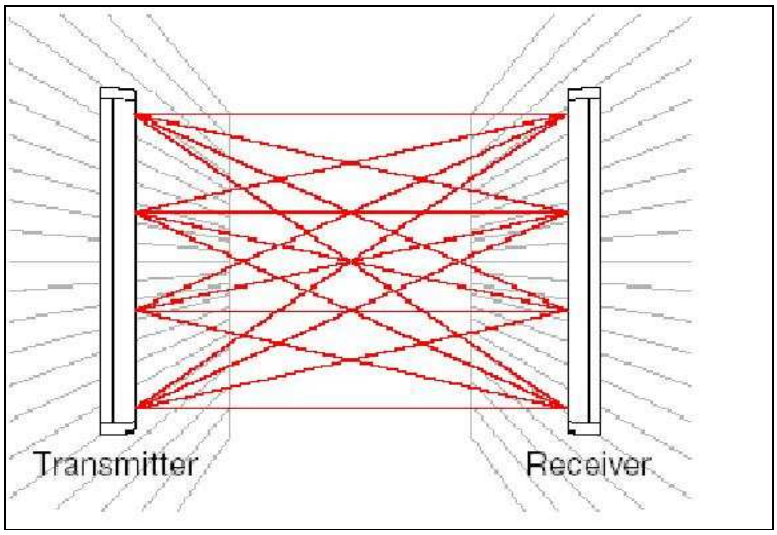


Figura 28: Barrera IR de 4 haces.

Como bien se observa en la figura 28, los distintos haces se disponen en el interior de las columnas debidamente camufladas tras metacrilatos opacos, que permitan el paso de los haces de infrarrojos, pero que imposibiliten la visión desde el exterior. De esta manera la ubicación de los distintos haces dentro de la columna no será visible desde el exterior, permitiendo el disponer tantos haces como se precisen en función del grado de seguridad requerido.

La marca elegida para las barreras es Pulnix cuyas especificaciones técnicas, al igual que la del resto de equipos utilizados, se encuentran anexadas al final del documento.

Dentro del funcionamiento básico de las barreras cabe destacar que las alarmas no se inician de forma inmediata al interrumpir el haz, se producirá el arranque al mantener el haz interrumpido durante un tiempo predeterminado. Esto se consigue gracias a la selección del tiempo de detección. El jumper permitirá seleccionar el tiempo de detección del receptor a una interrupción del haz. Como norma general este tiempo suele venir seleccionado de fábrica como 160mseg., sin embargo en nuestro caso optaremos por un

tiempo de respuesta recomendado de 320mseg por no querer detectar la interrupción por objetos rápidos. Esta selección de respuesta de tiempos diferentes es también aplicable de forma independiente para las funciones AND y OR.

Estas barreras disponen de un control automático de la sensibilidad en situaciones atmosféricas adversas como son la niebla, lluvia fuerte o nieve, así mismo los haces funcionarán sin interrupciones en condiciones de escarcha o polvo gracias a la carcasa protectora. Por otro lado las barreras contienen un módulo de ambiente incorporado que emitirá una señal de avería cuando el nivel de detección del receptor se reduzca a niveles no aceptables (descalificador).

Aparte de la salida de relé de alarma por detección, de contacto NC (normalmente cerrado) o la alarma de la salida ambiente, también dispone de una salida para detección de apertura de la cubierta de la barrera, comúnmente llamado “tamper” de salida relé NC. Esta salida producirá una alarma en el momento que alguna de las barreras intente ser manipulada.
Por último apuntar que las barreras contienen cuatro frecuencias de ajuste diferentes de manera que se evitan interferencias en sistemas de columnas o lineales de larga distancia.

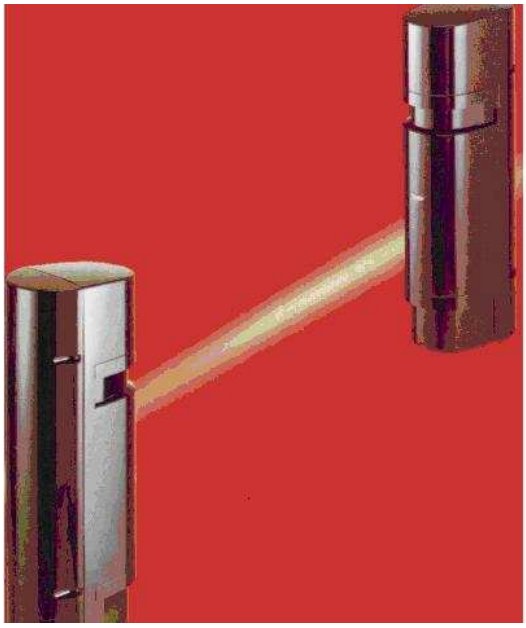


Figura 29: Barrera IR Pulnix

Las características expuestas corresponden a para todas las barreras independientemente de la distancia que cubran.

Una vez colocadas todas las barreras, como bien se comentó, existen puntos descubiertos donde podría producirse la intrusión. En estos puntos se ha optado por la colocación de sensores de doble tecnología, pero aquellos que extienden un campo con una forma similar a la de una cortina.

Estos puntos coinciden como bien se anotó, con todos los cambios de orientación del muro. Estos cambios hacen un total de 7 giros, que por tanto necesitarán la instalación de 7 Volumétricos, representados en el plano 3: *"Barreras y Detectores"*.

PUNTO COLOCACIÓN SENSOR	**# SENSORES**
Lado 2 a Lado 3	1
Lado 3 a Lado 4	1
Lado 4 a Lado 5	1
Lado 5 a Lado 6	1
Lado 6 a Lado 7	1
Lado 7 a Lado 8	1
Lado 8 a Lado 9	1
TOTAL DETECTORES DT CORTINA EXTERIORES	**7**

Tabla 8: Volumétricos

Estos sensores originan una superestrecha pantalla de protección de 3º (como una cortina) para asegurar accesos y zonas abiertas contra intrusos. Puesto que se ubicarán en el exterior es necesaria una característica de impermeabilidad. Como bien se determinó se busca satisfacer un alto grado de seguridad, por ello que se eligieran barreras de 4 haces, y por tanto los volumétricos elegidos deben proporcionar una gran capacidad de detección y una gran fiabilidad.

Por ello mismo se ha elegido un detector SI-DT-CORTINA. Este está equipado con una excelente protección contra todo intento de desactivar su funcionamiento mediante el bloqueo (enmascarado) de su campo de visión cercano. La protección contra el enmascarado del campo de visión cercano del detector se consigue mediante un escaneo constante con haces de infrarrojos activos. SI-DT-CORTINA puede detectar casi cualquier clase de material que bloquee (enmascare) su campo de visión cercano. También detecta objetos transparentes como un cristal claro o una bolsa de plástico. Incluso puede activar una alarma si sus lentes son pintadas con spray o cubiertas con un adhesivo. SI-DT-CORTINA combina dos tecnologías de detección, Microondas e Infrarrojos Pasivos (PIR), y verifica todas las intrusiones con ambas. Un avanzado y exclusivo algoritmo permite su funcionamiento en las condiciones medioambientales más difíciles y donde se requieran altas condiciones de seguridad, manteniendo a su vez una inmunidad a falsas alarmas única.

Figura 30: SI-DT Cortina

En el plano 3 (anexo A): *"Barreras y Detectores"* se aprecia la distribución final de las barreras y los volumétricos del subsistema anti-intrusión en el perímetro exterior.

4.1.1.2 Central Intrusión

Una vez colocadas las barreras y todos los sensores será necesaria la unificación de todos ellos en una central que pueda gestionar desde un solo punto el correcto funcionamiento del perímetro de seguridad. La central elegida para ello, es la central de intrusión de Galaxy-500.

La Galaxy-500 es una central de altas prestaciones, completamente direccionable y de alta seguridad. El sistema comprende una Unidad de Control, con un máximo de 63 módulos remotos de entradas/salidas (RIO), 32 teclados remotos y 16 módulos de control de accesos (MAX), adaptándose a cualquier instalación a través de 4 líneas de comunicación de datos de dos hilos con una longitud máxima de 1.000 metros por línea.

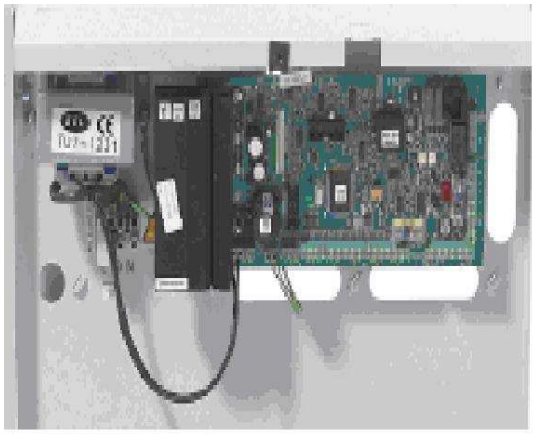


Figura 31: Central intrusión Galaxy**.**

Esta central será instalada en el centro de control, donde se dispondrá de un ordenador de gestión que permita controlar las distintas centrales y sistemas asociados en tiempo real, mostrando mediante un entorno gráfico la localización de las distintas señales de alarma y posibilitando actuaciones bidireccionales de forma instantánea.

El término zona engloba todos aquellas salidas de los equipos que se encuentren activas y conectadas con la central, de esta forma aquí se encontrarían las salidas de alarma, de ambiente y las de tamper, donde la primera de todas es únicamente aplicable al receptor. La cantidad de zonas que pueden ser conectadas en la placa base de la central es únicamente de 16 y dado que el número de zonas es superior a este valor, es necesario contar con módulos expansores. Estos módulos expansores, denominados RIO/B, actúan como concentradores de zonas unificándolas para poder gestionarlas desde la central en una única ubicación.

Cada uno de ellos cuenta con multiplexado de 8 zonas identificadas individualmente y con doble balanceamiento además de 4 salidas lógicas programables para ampliación de sistemas Galaxy.

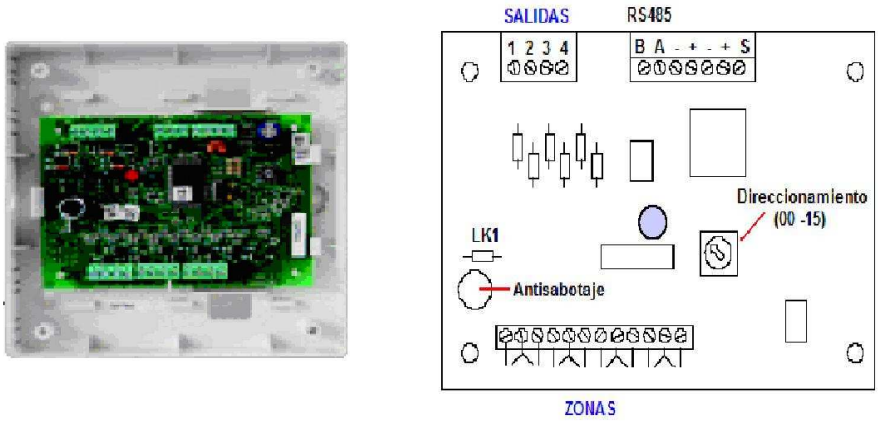


Figura 32: RIOB

4.1.1.2.1 Zonas y Resistencia Final de Línea

Para calcular el número de zonas con las que contamos y las cuales es preciso manejar, partimos del número de barreras colocadas. En total se colocarán 15 barreras cubriendo todo el perímetro, cada una de estas barreras estará formada por su correspondiente emisor y receptor, donde el emisor contará con 2 salidas (salida ambiente y salida tamper) mientras que el receptor a su vez contará también con la salida alarma que se activará en caso de intrusión propiamente dicho. Por lo que se contará con un total de 5 zonas por cada pareja de barreras que se tenga.

No obstante, aprovechando la cualidad de la resistencia de final de línea podemos decir que por cada pareja de barreras, emisor y receptor, cada una de ellas contará con 2 zonas diferentes.

Esta reducción del número de entradas, zonas, se debe a unificar dos de esas entradas como una sola, es decir que cuantifiquen como una sola pero que provoque salto de alarma en caso de que cualquiera de las dos entradas se active, salida de alarma y de tamper para los receptores.

Esta resistencia es una resistencia de valor fijo, fijada por el fabricante de la central, cuya función es la de carga del circuito y que debe colocarse en el interior de la barrera. Como se aprecia en el dibujo se colocaría una resistencia en paralelo con un circuito normalmente cerrado, que a su vez estarían en serie con otra resistencia de su mismo valor, en nuestro caso 1KΩ.

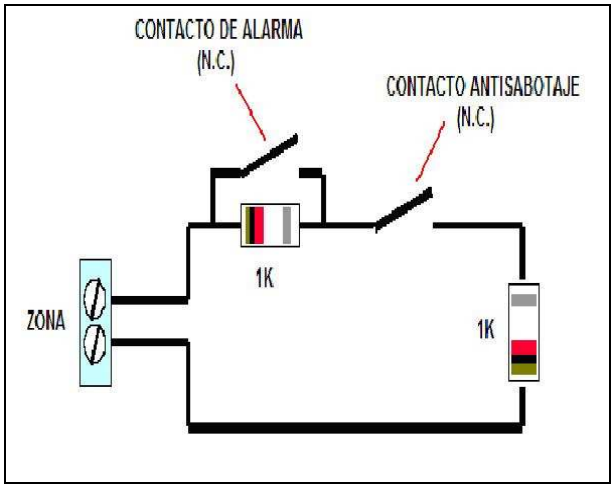


Figura 33: RFL

- En un sistema de **circuito normalmente cerrado**, el circuito eléctrico está cerrado cuando la puerta está cerrada. Esto significa que mientras la puerta se mantenga cerrada, electricidad puede fluir desde un extremo del circuito hasta el otro. Pero si alguien abre la puerta, el circuito se abre y la electricidad deja de fluir. Esto activa una alarma.
- En un sistema de **circuito normalmente abierto**, el abrir la puerta cierra el circuito, permitiendo el flujo de electricidad. En este sistema, la alarma es activada cuado el circuito se completa.

En función de cual sea la acción que se realice sobre la barrera la resistencia de carga del circuito variará hacia un valor u otro. Los valores que aparecerán reflejados en la central según la acción son los mostrados en la tabla 8 mostrada a continuación.

RESISTENCIA DE ZONA	CONDICIÓN
0 – 800 Ω	Cortocircuito
800 Ω - 900 Ω	Baja resistencia
900Ω - 1K2	Normal (cerrado)
1K2 – 1K3	Alta resistencia

1K3 – 12K	Alarma (abierto)
12K - ∞	Támper

Tabla 8: Valores RFL

Por tanto finalmente el número de zonas queda como sigue:

Barreras: 15
1 emisor: salida tamper + salida ambiente = 2
1 receptor: salida intrusión + salida tamper + salida ambiente = 3.

O

1 receptor: (salida intrusión + salida tamper) + salida ambiente = 2.
15 barreras * 4 zonas (2 emisor y 2 receptor) = 60 zonas.

Con un total de 64 zonas harían falta exactamente 8 expansores, RIO/B. No obstante no se han tenido en cuenta en este sumatorio las salidas provenientes de cada uno de los detectores exteriores de cortina, que supondría el uso de un RIO/B adicional, ni tampoco el subsistema de anti-intrusión exterior. Por todo lo anterior el número de RIOs a utilizar no podrá ser determinado hasta tener conocimiento exacto del número de equipos que comprendan el subsistema.

4.1.1.2.2 Bus Datos Intrusión

Para poder conectar todos los dispositivos del subsistema anti-intrusión y que exista una comunicación entre ellos, se utilizará un par trenzado apantallado con un sistema en bus de transmisión multipunto diferencial, RS-485. Este protocolo de comunicaciones en bus resulta ideal para transmitir a altas velocidades sobre largas distancias. Sin dejar de tener en cuenta que la distancia del bus de comunicaciones no debe exceder de los 1000metros.

El perímetro de la instalación a cubrir es superior a este valor, 1282metros, por lo que es clara la necesidad de utilizar dos buses de comunicación diferente donde quede repartido todo el perímetro de forma que no se exceda de los 1000metros en ninguno de los casos. Esto es posible gracias a que la central exigida soporta hasta 4 buses diferentes para comunicación, pudiendo conectar por tanto ambos buses.

Por otra parte se debe tener en cuenta que la limitación de distancia entre los detectores y barreras hasta los módulos RIO no podrá superar los 500metros. La división en dos buses de comunicación queda reflejada en el plano 4: *"Buses de Comunicación"*

Toda esta comunicación se llevará a cabo gracias a la instalación de un tubo de acero que colocado por encima de todo el muro perimetral, contendrá todo el cableado pertinente.

La central elegida ofrece la posibilidad de integrar un módulo externo, E080-2. Este módulo es un comunicador bidireccional Ethernet para los sistemas Galaxy, con comunicación a través de LAN/WAN y configurable desde teclado o software con protocolo encriptado TCP/IP.

Con este módulo opcional se conseguiría igual que como se consigue con los sistemas de CCTV IP realizar una gestión y control desde un punto remoto a la ubicación en sí vigilada, si así se quisiera.

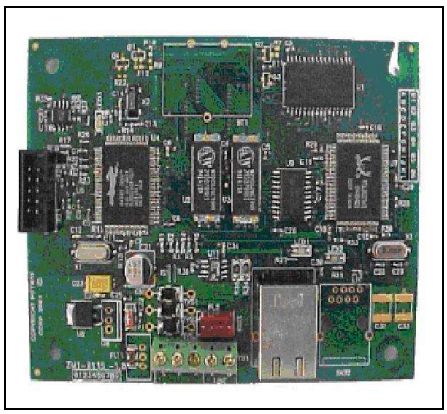


Figura 34: Módulo comunicador E080-2

4.2. Subsistema Anti-Intrusión Edificios Perímetro Interior

Dentro de todos los edificios que se sitúan en el interior del perímetro no todos requieren un mismo nivel de seguridad, por ello en cada edificio se han decidido instalar unas medidas diferentes.

Todos los edificios contarán con la instalación de contactos magnéticos en sus puertas, y aquellos en los que así se establezca se incorporarán además otros dispositivos al subsistema anti-intrusión. Como bien se explicó, mediante este contacto, cuando se produzca la apertura de la puerta en la que se sitúe se activará una señal de alarma que será visualizada en el centro de control. De esta forma se tendrá constancia de intrusión en los edificios si se consiguiera acceder al recinto sin ser percibido.

Se cuenta con un total de 6 edificios cada uno con 1 o más accesos a su interior, contabilizando el número de puertas se requieren 9 contactos magnéticos para cubrir todos los edificios.

El único edificio que requiere un nivel de seguridad mayor corresponde con el edificio central, por encontrarse en él objetos cuyo valor es importante, según se impuso en las premisas de diseño. El edificio cuenta con un gran número de ventanales a lo largo de los 4 lados, como se aprecia en el plano 5: "*Edificio Central*". Puesto que estos ventanales suponen un punto de vulnerabilidad al acceso se colocarán en cada uno de ellos también contactos magnéticos, no obstante al tratarse de cristal el lugar de ubicación de los mismos los contactos elegidos serán de detección por vibración. El total de ventanas con el que cuenta el edificio es de 12, es decir habrá 12 detectores. Igualmente, en el interior de la

habitación de control del CCTV que ya está instalado se ubicará un detector de doble tecnología advirtiendo la presencia de extraños cuando corresponda.

Para la elección de los detectores a instalar nos basaremos principalmente en el precio, eligiendo entre las principales marcas, puesto que no existen diferencias entre ellas respecto a eficiencia.

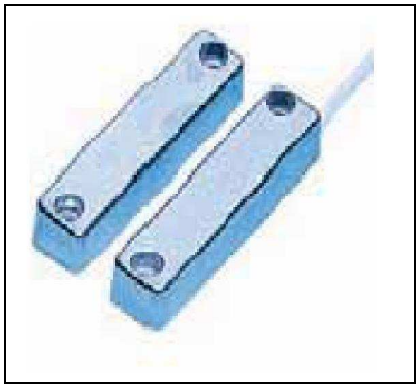


Figura 35: Contacto magnético de superficie

4.3. Ubicación módulos expansores

La siguiente tabla muestra las conexiones que se realizarán entre cada equipo perteneciente al subsistema anti-intrusión y un módulo expansor. Los RIOs han sido colocados en las ubicaciones que permitan el menor cableado posible alcanzando a todos los equipos.

Comenzando a recorrer el perímetro desde la puerta principal en sentido descendente comienza la colocación.

La dinámica a seguir fue básicamente la siguiente:

El primer RIO fue colocado en el principio del perímetro, conectándose a él todos los dispositivos cercanos sumando un total de 7 zonas.

Continuando por el perímetro, el siguiente punto de confluencia de equipos, en el punto situado a 60m de la entrada se colocará el siguiente RIO, para así poder conectar el emisor y receptor así como el detector de cortina situados en ese punto. Igualmente, se conectaron a este RIO los contactos magnéticos correspondientes a las dos puertas de acceso del edificio 5. A pesar de que el contacto magnético 1 se encuentra a una distancia inferior de algún RIO colocado en otro punto del perímetro, resulta menos costosa la tirada de cable para ambos contactos del edificio hacia un mismo RIO, que no realizar esta tirada por dos canalizaciones diferentes. Esta decisión ha sido tomada en todos los edificios que ocurriera esta misma situación.

Así sucesivamente se han ido disponiendo los RIO como se aprecia en el plano 6: *"RIOs"*. Destacar que los dispositivos ubicados en el edificio 6 han sido agrupados en 2 RIOs diferentes. Estos están situados cada uno a la menor distancia posible, diagonalmente

hacia el perímetro, de forma que también queden enganchados con alguno de los dos buses de datos.

Con un total de 93 zonas se han utilizado 12 RIOs ubicados a lo largo de todo el perímetro conectándose así a un bus de comunicaciones.

La conexión de los equipos con los RIOs quedan representadas en el plano 7: *"Conexiones RIOs"* y esquematizadas en la siguiente tabla.

BUS DE DATOS	# RIO	# ZONA	EQUIPO CONECTADO	DISTANCIA (m) hasta RIO correspondiente
1	0	1	Contacto Magnético 1	128
1	0	2	Contacto Magnético 2	50
1	0	3	Volumétrico Exterior 1	40
1	0	4 y 5	Tamper y Ambiente Emisor Barrera 1	1
1	0	6 y 7	Tamper + Intrusión y Ambiente Receptor Barrera 0	1
1	1	1 y 2	Tamper + Intrusión y Ambiente Receptor Barrera 1	1
1	1	3 y 4	Tamper y Ambiente Emisor Barrera 2	1
1	1	5	Detector Cortina 1	1
1	2	1 y 2	Tamper + Intrusión y Ambiente Receptor Barrera 2	1
1	2	3 y 4	Tamper y Ambiente Emisor Barrera 3	1
1	2	5	Detector Cortina 2	1
1	3	1 y 2	Tamper + Intrusión y Ambiente Receptor Barrera 3	47.5
1	3	3 y 4	Tamper y Ambiente Emisor Barrera 4	47.5
1	3	5 y 6	Tamper + Intrusión y Ambiente Receptor Barrera 4	47.5
1	4	1	Contacto Magnético 3	158
1	4	2	Contacto Magnético 4	36.2
1	4	3 y 4	Tamper y Ambiente Emisor Barrera 5	47.5
1	4	5 y 6	Tamper + Intrusión y Ambiente Receptor Barrera 5	47.5
1	4	7 y 8	Tamper y Ambiente Emisor Barrera 6	47.5
1	5	1 y 2	Tamper + Intrusión y Ambiente Receptor Barrera 6	45
1	5	3 y 4	Tamper y Ambiente Emisor Barrera 7	45
1	5	5	Detector Cortina 3	45
1	5	6 y 7	Tamper + Intrusión y Ambiente	45

			Receptor Barrera 7	
1	5	8	Contacto Magnético 5	120
1	6	1 y 2	Tamper y Ambiente Emisor Barrera 8	90
1	6	3 y 4	Tamper + Intrusión y Ambiente Receptor Barrera 8	1
1	6	5 y 6	Tamper y Ambiente Emisor Barrera 9	1
1	6	7	Detector Cortina 4	1
2	7	1 y 2	Tamper + Intrusión y Ambiente Receptor Barrera 9	37.5
2	7	3 y 4	Tamper y Ambiente Emisor Barrera 10	37.5
2	7	5	Detector Cortina 5	37.5
2	8	1 y 2	Tamper + Intrusión y Ambiente Receptor Barrera 10	47
2	8	3 y 4	Tamper y Ambiente Emisor Barrera 11	47
2	8	5	Detector Cortina 6	47
2	8	6	Contacto Magnético 6	120
2	8	7	Contacto Magnético 7	40
2	9	1 y 2	Tamper + Intrusión y Ambiente Receptor Barrera 11	47
2	9	3 y 4	Tamper y Ambiente Emisor Barrera 12	47
2	9	5 y 6	Tamper + Intrusión y Ambiente Receptor Barrera 12	47
2	9	7 y 8	Tamper y Ambiente Emisor Barrera 13	47
2	10	1 y 2	Tamper + Intrusión y Ambiente Receptor Barrera 13	1
2	10	3 y 4	Tamper y Ambiente Emisor Barrera 14	1
2	10	5	Contacto Magnético 8	140
2	10	6	Contacto Magnético 9	65
2	10	7	Detector Cortina 7	1
2	11	1	Contacto Magnético 10	230
2	11	2	Detector Rotura 12	206
2	11	2	Detector Rotura 1	185
2	11	4	Detector Rotura 2	157
2	11	5	Detector Rotura 3	150
2	11	6	Detector Rotura 4	183
2	11	8	Detector doble tecnología	193
1	12	1	Detector Rotura 5	201.25
1	12	2	Detector Rotura 6	224
1	12	3	Detector Rotura 7	191.5
1	12	4	Detector Rotura 8	159
1	12	5	Detector Rotura 9	126.5
1	12	6	Detector Rotura 10	146

1	12	7	Detector Rotura 11	172
Directamente Conectado	-------	1 y 2	Tamper + Intrusión y Ambiente Receptor Barrera 14	24
Directamente Conectado	-------	4 y 5	Tamper y Ambiente Emisor Barrera 0	20

Tabla 9: Conexionado RIOs

4.4. *Software de gestión de instalaciones Galaxy Graphics*

El software elegido para realizar la gestión de todos los equipos de intrusión es el Galaxy Graphics, propio de la central de alarmas que hemos instalado.

Mediante este software de gestión se pueden crear planos de las instalaciones así como importarlos desde otras fuentes. El plano correspondiente, cuando se reciba una señal de alarma, será mostrado automáticamente en pantalla.

El software proporciona una gestión gráfica que permite la asociación dinámica de las zonas de manera que estos simbolicen en cada momento el estado de los detectores.

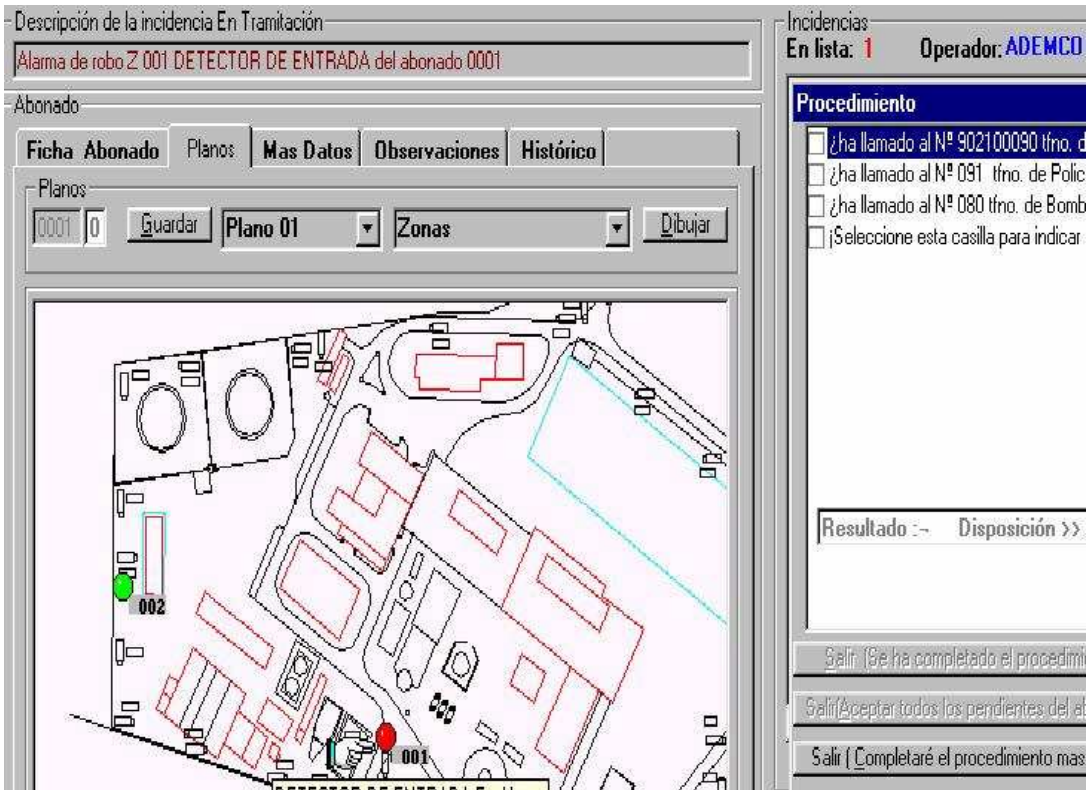


Figura 36: SW Galaxy, plano salto de alarma

Resaltar, por otro lado, que el Software de Gestión Galaxy Graphics permite la conexión, al mismo PC, de hasta 5 unidades de control unificando la gestión de todas ellas.

4.5. CCTV Perímetro exterior, instalaciones e infraestructura

Para poder cubrir la necesidad de un perímetro completamente vigilado por un circuito cerrado de televisión se plantea el problema de las largas distancias que es necesario controlar. Por otro lado, para que realmente resulte efectiva toda la seguridad del perímetro exterior es necesaria la perfecta complementación de los subsistemas, como se comentó anteriormente, para la verificación real de la existencia de alarma.

4.5.1 Entrada Perímetro

Evidentemente el principal punto de acceso a las instalaciones, puerta de entrada, será vigilado con una cámara que se encuentre grabando de forma permanente. Para ello la mejor opción por tanto es una cámara fija. Estas cámaras son utilizadas en los puntos donde se requiere, como aquí, una vigilancia absoluta localizada en un solo punto. Para una rigurosidad mayor y una visión más completa se instalará una cámara en cada sentido de orientación de la entrada, para controlar tanto la salida como la entrada de vehículos y personas a las instalaciones.

Puesto que la vigilancia de este punto se requiere durante las 24 horas del día es obvia la necesidad de cámaras capaces de ofrecer imágenes en condiciones bajas de iluminación, por lo que se optará por cámaras día/noche que proporcionen: por un lado vídeo en color cuando haya suficiente luz para, como ya se comentó en las características de las cámaras, proporcionar una información más completa y detallada, y en blanco y negro en condiciones de oscuridad por la baja iluminación.

Para cumplir estos requerimientos será necesario que posea una sensibilidad lumínica adecuada. Igualmente como se especificó en las cámaras monocromas para conseguir imágenes nítidas y definidas la resolución debe ser elevada.

La cámara que se encuentre enfocando la entrada al perímetro se situará en un poste a una altura de 4 metros para así disponer de una visión más completa. Por ello mismo para proporcionar seguridad a dicha cámara bajo ella, en ese mismo poste, se colocará un volumétrico exterior que pueda detectar un acercamiento a la ubicación de la cámara, provocando un salto de alarma en caso de que así fuera. Por otra parte la cámara enfrentada a esta se situará en el muro que acordona todo el perímetro gozando de esta forma también de altura.

Tras consultar distintos catálogos, comparando precios y características la cámara que se ha escogido es la Pixord-428.

Figura 37: Cámara IP Pixord-428

La Cámara IP Pixord-428, es un modelo día/noche basado en un CCD 1/3" Sony Interlaced con iris mecánico y una luminosidad mínima de 0 Lux gracias a sus potentes iluminadores de infrarrojo que nos permite alcanzar una distancia de visión de entre 80 y 100 metros en condiciones nulas de luminosidad. Incorpora una lente varifocal de 7,5 a 50 mm. Esta construida en aluminio resistente que le permite soportar la instalación en exteriores gracias a su protección Ip66.

Aunque la detección de movimiento no sea una de las características de la cámara, esto puede solventarse utilizando un software de manejo de imágenes que incorpore la detección.

4.5.1.1 Ubicación cámaras

Para calcular la ubicación de la cámara en relación a la distancia de la entrada principal, utilizamos la fórmula citada en otro apartado.
Siguiendo dicha fórmula y utilizando los datos facilitados en las tablas de dicho apartado y partiendo de una serie de datos referentes a las características de la cámara podremos decir:

Cámara ip fija distancia focal, f= 7.5 - 50 mm. h (1/3”) = 4.8 mm

Sabiendo que la anchura a cubrir es de aproximadamente 30metros (H = 30m.) podremos calcular la mínima distancia a la que se debe colocar:

$$f = h \times D/H$$

$f > 7.5$ $7.5 < 4.8 \times D/30$ $225 / 4.8 < D$ $D > 46.875$ m.

Por tanto el poste que sujetará la cámara y el volumétrico se situará a una distancia de 47metros.

Respecto a la cámara que vigila la salida del perímetro, para calcular su distancia focal llevamos a cabo la misma operación que para la otra cámara. La anchura que se desea cubrir es un poco superior, de 40m así como la distancia, para obtener una visualización más completa

$f = h \times D/H$ H = 40m. D = 70m. $f = 4.8 \text{ X } 70/40 = 8.4$mm.

4.5.2 Perímetro Exterior

Para todo el perímetro exterior se busca un control absoluto, por tanto, si se colocarán cámaras fijas el número de estas sería excesivamente elevado dado su alcance, dado que si quisiéramos visualizar una intrusión alertada por una barrera en un punto alejado, nos resultaría imposible sin tener que añadir una óptica mayor a las cámaras.

Por esto mismo se ha optado por la instalación de cámaras domos IP. Además de por su mayor alcance, este tipo de cámaras pueden ofrecer un almacenamiento en memoria de diferentes posicionamientos, es decir permite la modificación de su orientación sin necesidad de realizarlo manualmente desde el centro de control, pudiéndose hacer manualmente si así se desease. De esta forma se conseguirá reducir el número de cámaras puesto que modificando la orientación se pueden cubrir diferentes zonas con una sola de ellas.

Si bien las cámaras fijas no tienen un alcance con visión adecuada como el que pueden disponer los domos, si recalcar que el objeto enfocado por una cámara fija se encuentra bajo vigilancia constante, por el contrario con un domo durante la visualización de una de sus posiciones, el resto de sus posibles presets, posicionamientos, quedarán al descubierto durante las sucesivas rondas que realizaría la cámara.

Aunque esto sea una desventaja en el sentido de control total durante todo el tiempo, queda prácticamente solventada con la integración de las cámaras al subsistema anti-intrusión, de forma que si alguna alarma fuese activada, la cámara o cámaras que más cercanas a la barrera que produjo la alarma se encuentren, enfocarían directamente al punto requerido, previa configuración de las posibilidades distintas de posición que cada cámara es capaz de almacenar.

Los rangos de longitudes ópticas que podremos disponer varían entre 4 y aproximadamente 120mm, que son las ópticas máximas que contienen algunos de los domos del mercado. Sabiendo que se desea tener una imagen de una anchura de aproximadamente 5m, podremos determinar cuales son los alcances máximos en metros que podremos obtener.

La tablas siguientes muestran la relación entre longitud focal y distancia para un tamaño de sensor de 1/4”, por tanto h será 3.6mm, y para un tamaño de 1/3” donde h será 4.8mm.

1 / 4 ”			1 / 3 ”	
Longitud Focal (mm)	Distancia (m)		Longitud Focal (mm)	Distancia (m)
4	6,67		4	5
10	16,67		10	12,5
20	33,33		20	25
30	50,00		30	37,5
40	66,67		40	50
50	83,33		50	62,5
60	100,00		60	75
70	116,67		70	87,5
80	133,33		80	100
90	150,00		90	112,5

100	166,67		100	125
110	183,33		110	137,5
120	200		120	150

Tabla 10: Relación distancia-longitud focal.

Si se observa el plano se verá como la mínima distancia que un domo debiera de cubrir estará en torno a los 80m, valor del mayor de los lados inferior a 100m, para que los lados de menor longitud del perímetro necesiten solamente una cámara. Por tanto la máxima longitud focal disponible debe ser superior a 50mm en un caso y 70mm en el otro.

De esta manera quedan establecidos todos los requisitos que los domos a instalar en el perímetro deben tener.

Tras analizar catálogos de diversos proveedores, con domos de fabricantes diferentes la mejor oferta finalmente encontrada corresponde a domos IP infinova de syscom, que cumplen con todos las cualidades buscadas. La tabla siguiente muestra las posibilidades a elegir con sus correspondientes precios.

Especificación	**V1726N-L0S2B6**	**V1748N-L0S2B6**	**V1749N-L0S3B6**
Tipo	Color	Color / Día / Noche	Color / Día / Noche
Resolución	480 TVL, CCD 1/4" HITACHI	480/550 TVL, CCD 1/4" SONY	540/720 TVL, CCD ¼" SONY
Zoom	22X Óptico / 12X Digital	26X Óptico / 12 Digital	35X Óptico / 12X Digital
Longitud Focal	4mm - 88mm	3.5mm - 91.0mm	3.4mm - 119mm
Iluminación Min (color)	0.1 Lux	0.1 Lux	0.05 Lux
Iluminación Min (B/N)	-	0.01 Lux (Shutter Variable)	0.01 Lux (Shutter Variable)
Wide Dynamic Range	Encendido / apagado	N/A	MD1/MD2/OFF
Aplicación de Carcasa	Interior	Exterior	Exterior
Mica	Color Humo	Color Humo	Color Humo
Antivandalismo	-	-	-
Precio	**1766 euros**	**2127 euros**	**2367 euros**

Tabla 11: Comparativa domos IP

Todos los domos anteriores poseen 128 presets posibles, así como 4 entradas de alarma con salidas programables.

El domo para interior se descarta, quedando 2 posibilidades más, las cuales cumplen con la especificación ip66 de montaje en exterior.

Nos fijamos en una primera instancia únicamente en la longitud focal posible, dejamos las otras características dado que cumplen los requisitos estimados, y pasando después al precio.

Si utilizáramos los domos de óptica máxima 91mm., como se observa en al plano 8: *"7 domos"*, se necesitarían instalar un total de 7 domos para cubrir todo el perímetro, mientras que si utilizamos el domo con 119mm., necesitaremos únicamente 5, como se ve en el plano 9:*"5 domos"*.

Por tanto ahora únicamente quedará determinar que opción resulta más económica.

Si instaláramos el domo V1748N-L0S2B6 supondría un desembolso de
2127 x 7 = 14889 euros
mientras que si instalamos el domo V1749N-L0S3B6 el gasto sería de
2367 x 5 = 11835 euros

De esta forma no solo se ahorrará por un menor gasto sino que al instalar dos domos menos se requerirá menos trabajo de configuración y mantenimiento.

Todos los domos necesitan una carcasa protectora dada su instalación en exterior, igualmente en función de cual sea su ubicación, pared, techo, o poste, se necesitan adaptadores para el montaje, complementos que se han tenido en cuenta en el estudio económico final expuesto más adelante. Para mayor seguridad la carcasa que se instalará será antivandálica. Este tipo de carcasa, ofrecen una resistencia mucho mayor ante golpes por estar hecha con acero, además se encuentra fijada mediante tornillos especiales para evitar su desarme y manipulación, igualmente su cristal es de una gran resistencia.

Figura 38: Domo IP infinova

4.5.3 Perímetro interior

Una vez conseguida la visualización absoluta del perímetro exterior de las instalaciones, se considera necesaria la instalación de diversas cámaras en el interior del mismo aumentando de esta forma la seguridad y vigilancia. En esta ocasión no se pretenda vigilar de forma exhaustiva todo el interior, sino controlar principalmente los accesos a los distintos edificios que componen el perímetro.

Las cámaras, como se observa en el plano 10: *"CCTV perímetro interior"*, son colocadas para vigilar la entrada y salida de los edificios. Aprovechando la situación de los edificios las cámaras son colocadas en las paredes de los mismos, evitando así la utilización de postes que pueden ser más fácilmente manipulados y requieran una detección de manipulación extra a la de la propia cámara, como ocurre en el caso de la cámara establecida para la vigilancia de la entrada al perímetro.

Las cámaras a utilizar serán las mismas que las instaladas para la entrada y salida del perímetro, el modelo Pixord-428, sin embargo en esta ocasión interesa que las imágenes que sean captadas por estas cámaras abarquen la mayor distancia posible para así controlar mayor puntos del interior. Por tanto la longitud focal será fijada en un valor de 32mm, de forma que se observen objetos a 100 metros de distancia con una anchura de 15metros.

4.5.4 Interior edificios; Migración

En las condiciones previas establecidas al comienzo del diseño de la instalación no se busca instalación de cámaras en el interior de los edificios. No obstante dada la versatilidad de los sistemas IP la instalación de las mismas no supondría un complicado proceso. Sin embargo en uno de los edificios del perímetro existe ya un despliegue de CCTV previo instalado tiempo atrás. Este CCTV del edificio numerado bajo el número 6 esta compuesto por un total de 5 cámaras, como bien muestra el plano 11: *"CCTV analógico"*.

Todas ellas están gestionadas desde un cuarto de control situado en la entrada del edificio el cual cuenta con los equipos necesarios para una visualización, y almacenamiento correcto de las imágenes (monitor y grabador digital). Sin embargo buscándose una integración total de todos los equipos se pretende la migración del sistema analógico al sistema IP que se está desarrollando.

Como se explicó anteriormente es posible la migración mediante unos equipos denominados servidores de vídeo. Estos servidores poseen una conexión Ethernet que habilitará el control a través de una red IP. También se explicó que el número máximo de cámaras que un servidor es capaz de soportar es únicamente de 4, al contar con una instalación de 5 cámaras analógicos será necesario instalar dos servidores de vídeo, uno con capacidad para 4 cámaras y otro servidor de vídeo para un canal más.

Aclarar que existen grabadores digitales que según sus especificaciones pueden proporcionar una conexión TCP/IP, en este caso no sería necesario la instalación de servidores de vídeo, incluso si las cámaras instaladas fueran domo algunos grabadores proporcionan el control de los mismo mediante telemetría a través de la red.
En nuestro caso el equipo de almacenamiento de imágenes no cuenta con una conexión TCP/IP por tanto la migración mediante servidores sigue siendo necesaria.
El servidor de 4 canales elegido es el FLEXWATCH 3450.

Figura 39: Servidor de vídeo Flexwatch 3450

FlexWATCH 3450 es un servidor web de vídeo de 4 canales de última generación y características profesionales permite ver hasta 4 cámaras por Internet desde cualquier parte del mundo. El servidor incluye además detección de movimiento integrada, envío de imágenes por mail y FTP ante cualquier tipo de evento, 4 entradas de alarmas, 4 salidas de relé, control de dispositivos de domótica X10, gestión independiente de usuarios, control de cámaras con movimiento etc.

El vídeo servidor posee doble sistema de compresión MJPEG y MPEG4 que nos proporcionará la máxima calidad y fluidez de visionado independientemente del ancho de banda disponible. También posee una salida de vídeo en quad que permite la conexión a una televisión o monitor para ver localmente las 4 cámaras en la misma pantalla de forma simultánea, consiguiendo así un útil efecto disuasorio. Su reducido tamaño, tan solo 15.5cm x 14cm, nos permitirá colocarlo en cualquier parte teniendo además la ventaja que todas las conexiones se encuentran en la parte trasera de manera que evitaremos molestos cables de por medio. Añadir que posee una sólida carcasa de aluminio que mejora la ventilación y reduce el calor.

El servidor permite la utilización de cualquier tipo de cámaras, lo que supone una gran ventaja. FlexWATCH 3450 convierte en cámaras IP las 4 cámaras que se le conectan a el, obteniendo las prestaciones y calidad digital de las cámaras IP.

En lo referente a la seguridad, dispone de un completo sistema de registro de usuarios para restringir el acceso solo a personas autorizadas por el administrador del equipo. Así puede crear un usuario que solo pueda ver la cámara 1y 2 y evitar el acceso de usuarios no autorizados. También se puede controlar el acceso al movimiento de las cámaras, el control del audio y las salidas de alarma, con lo que las posibilidades se multiplican. Otras funciones son filtración de IP, opción de rechazo de cliente y encriptación segura de imagen.

Para el servidor de vídeo de 1 canal, se ha decidido instalar el servidor de vídeo IP PIXORD 1000 que permite conectar 1 cámara analógica a una misma dirección IP a través de una red Ethernet. Las características principales detalladas para el servidor anterior de 4

canales son extendidas a este equipo, permite la visualización de una cámara a través de Internet o intranet, con el servidor se puede realizar una grabación de video en local o remotamente así como enviarnos un mail cuando se produzca un alarma predefinida.

Igualmente que para el servido anterior dispone un chipset que le habilita para poder enviar vídeo comprimido en tiempo real usando los algoritmos de compresión JPEG y MJPEG. El servido de vídeo IP PIXORD 1000 también dispone de Detección de Movimiento incorporado, así como de 4 entradas de alarmas opto acopladas y un relé de salida.

Figura 40: Servidor de Vídeo IP PIXORD 1000

Puesto que las 5 cámaras del edificio central deben separarse en dos grupos de 4 y 1 cámaras respectivamente dado que se utilizan dos servidores de vídeo, la opción escogida es la de conectar la cámara analógica dedicada al control de la entrada del edificio al servidor de vídeo de 1 canal y las cuatro restantes al otro servidor.

La configuración final para la migración del CCTV analógico quedará como la siguiente imagen.

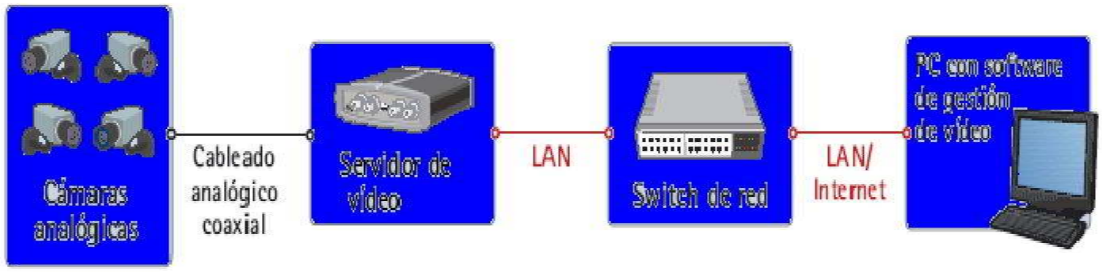


Figura 41: Representación migración

4.5.5 Software manejo de vídeo

En la actualidad existen gran cantidad de software para le manejo de un sistema de CCTV, no obstante muchos de ellos son exclusivos de un fabricante por lo que requiere que las cámaras a gestionar sean igualmente de ese fabricante. De entre los posibles software se ha optado por el software de gestión Milestone. La tabla siguiente muestra las distintas posibilidades que se tienen dentro de este software

milestone
Open Platform IP Video Surveillance

	XProtect Basis + 4.0	XProtect Professionnal 4.6	XProtect Enterprise 6.0	XProtect Corporate 1.5
Accesibilidad	Total	total	Necesita certificación	Necesita certificación
Tipo de instalación	1 servidor	1 servidor	Servidores múltiples	Servidores múltiples
Nº de cámaras	4,6,9,16,25	4,6,9,16,25, 36,50,64	Ilimitada (licencia por cámara)	Ilimitada (licencia por cámara)
Grabación	MJPEG: 600,000 imágenes/cámara/día MPEG-4: 600,000 I frames (+P frames)/cámara/día	MJPEG: 600,000 imágenes/cámara/día MPEG-4: 600,000 I frames (+P frames)/cámara/día	Sin límite con grabación	Sin límite con grabación
Volcado de imágenes	Diario (disco local)	Diario (disco local ó externo)	Por horario (disco local ó externo)	Por horario (disco local ó externo)
Modo de búsqueda	Por día/ hora, alarma, detección de movimiento	Por día/ hora, alarma, detección de movimiento y búsqueda avanzada	Por día/ hora, alarma, detección de movimiento y búsqueda avanzada	Por día/ hora, alarma, detección de movimiento y búsqueda avanzada
Entradas máx	4 cámaras	16 cámaras	64 cámaras	Ilimitada
Accesos remotos	Cliente Web 1-4 cámaras	Cliente Web 1-4 cámaras y cliente remoto 1-16 cámaras	Cliente Web 1-4 cámaras y cliente remoto 1-16 cámaras, cliente Smart 1-64 cámaras cliente PDA 1 cámara	
Protocolo de telemetría	Manual - 25 prepos.	Rondas manuales y auto, con pausas hasta 50 prepos	Rondas manuales y auto, con pausas hasta 50 prepos	Rondas manuales y auto, con pausas con prepos ilimitados
Ent./Sal. De alarma	Entradas	Ent./Sal. y detección de movimiento	Ent./Sal. y detección de movimiento	Ent./Sal. y detección de movimiento
Aplicación de Matriz	no	opcional	incluído	incluído
Monitor principal	no	sí	sí	sí
Secuencia	no	sí	sí	sí
Exportación	Jpeg/Avi/Wav	Jpeg/Avi/Wav + Base nativo	Jpeg/Avi/Wav + Base nativo	Jpeg/Avi/Wav + Base nativo
Cliente PDA		opcional	integrada	
Otros				Gestión centralizada de cámaras y usuarios

Tabla 12: SW Milestone

Nuestro diseño cuenta con un total de 15 cámaras IP, más 5 cámaras analógicas conectadas a través de un servidor de vídeo, por lo que con un software para 25 cámaras será suficiente.
A continuación se comentan diversos aspectos del software

Administración
El software soporta cámaras IP y videoservidores que se conectan directamente a una red LAN de oficina u otra red TCP/IP, almacenando directamente en un disco duro del PC. En el módulo de administración de XProtect Basis+ se configuran dichas cámaras de red,

los servidores de vídeo y los usuarios del sistema. En un sencillo interfaz puede definir cuántas cámaras de red quiere ver, así como su programación, las preferencias de archivo, y el envío de alertas por correo electrónico. También en esa pantalla podrá concretar los derechos de cada usuario.

Monitor
El Monitor de XProtect Basis+ permite ver simultáneamente la emisión de, entre 16 y 25 cámaras por servidor, desde una localización centralizada.
El Visor puede reproducir grabaciones en una pantalla que muestra 4 cámaras a la vez.

Detección de Movimiento
La detección de movimiento es en tiempo real, integrada y completamente ajustable a las necesidades que se requieran, además ofrece la posibilidad de excluir zonas de detección.
Igualmente las cámaras pueden ser configuradas para acelerar el número de fotogramas cuando se detecte movimiento, o cuando ocurra un evento, de forma que no se almacenen gran cantidad de imágenes innecesarias.
XProtect Basis ofrece control manual Pan/Tilt/Zoom y ofrece la posibilidad de preestablecer 25 posiciones PTZ por cámara. Es decir el número de presets posibles vendrá determinado por el software. El zoom PTZ puede realizarse en el rectángulo señalado con ciertas cámaras PTZ.

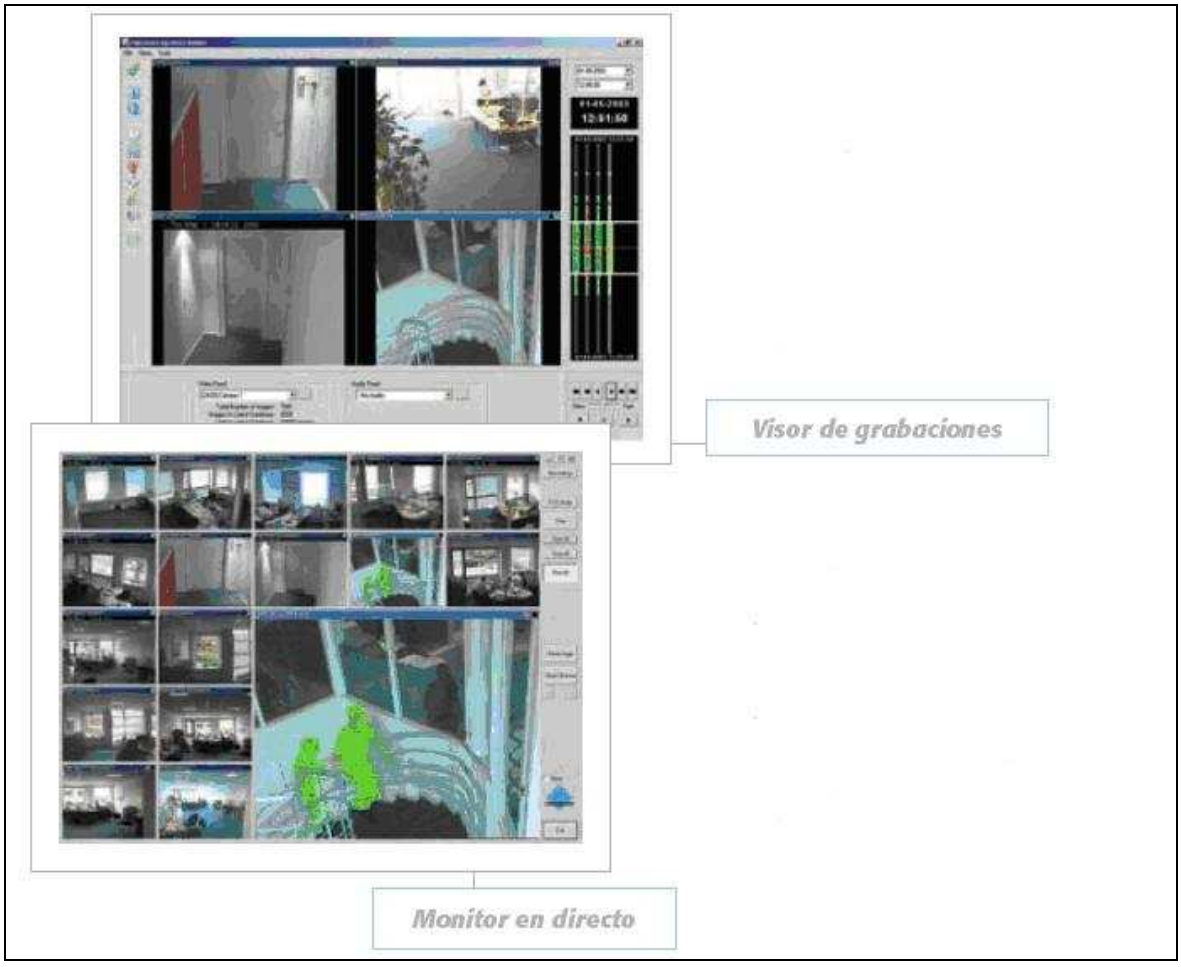


Figura 42: Imágenes Milestone

Grabación de Imagen y Sonido
El software permite grabación y reproducción simultánea de imágenes grabadas y en directo, también ofrece también grabación de sonido (un canal) y reproducción instantánea en tiempo real. Aunque para nuestro diseño esta aplicación no va a ser utilizada.

Milestone proporciona una velocidad de grabación y visualización de más de 30 fotogramas por segundo y cámara, con la única limitación del hardware, donde la calidad de grabación depende completamente de las posibilidades de las cámaras y servidores de vídeo. El software no limita en modo alguno, soportando imágenes JPEG y vídeo MPEG4. Para la versión del software elegida se dispone de una capacidad de grabación de 600.000 imágenes por cámara y día.

Las búsquedas de grabaciones pueden realizarse por fecha y hora, y por actividad y alarma (Video detección de movimiento). Los resultados pueden ser generados como una imagen JPEG o una película AVI.

Acceso Remoto
XProtect Basis+ cuentan con un servidor de red para acceder al sistema de vigilancia desde localizaciones remotas mediante el "Microsoft Internet Explorer". El programa proporciona acceso remoto completo a grabaciones e imágenes en directo en una vista cuádruple en Basis+.

Integración
Como ya se comentó la forma de integración con dispositivos de seguridad como alarmas de acceso o de intrusos se realiza a través de entradas de relé de cámara, utilizando los puertos de cámara E/S (I/O). Por ejemplo, la entrada (input), será un sensor que controla el "ir a" una posición preestablecida de una cámara PTZ que, a su vez, iniciará la grabación en vídeo desde ese lugar.

La integración del software de vigilancia garantiza que una cámara PTZ se mueva para grabar imágenes de personas que entran o salen de un determinado lugar.

En el momento en que alguna alarma sea detectada por parte de alguna cámara, ya sea por detección de movimiento o bien por su conexión con algún dispositivo del subsistema anti-intrusión, dicha cámara aparecerá en la pantalla de visualización automáticamente, con el preset que corresponda. Las alarmas igualmente pueden realizar una activación de alertas por correo electrónico.

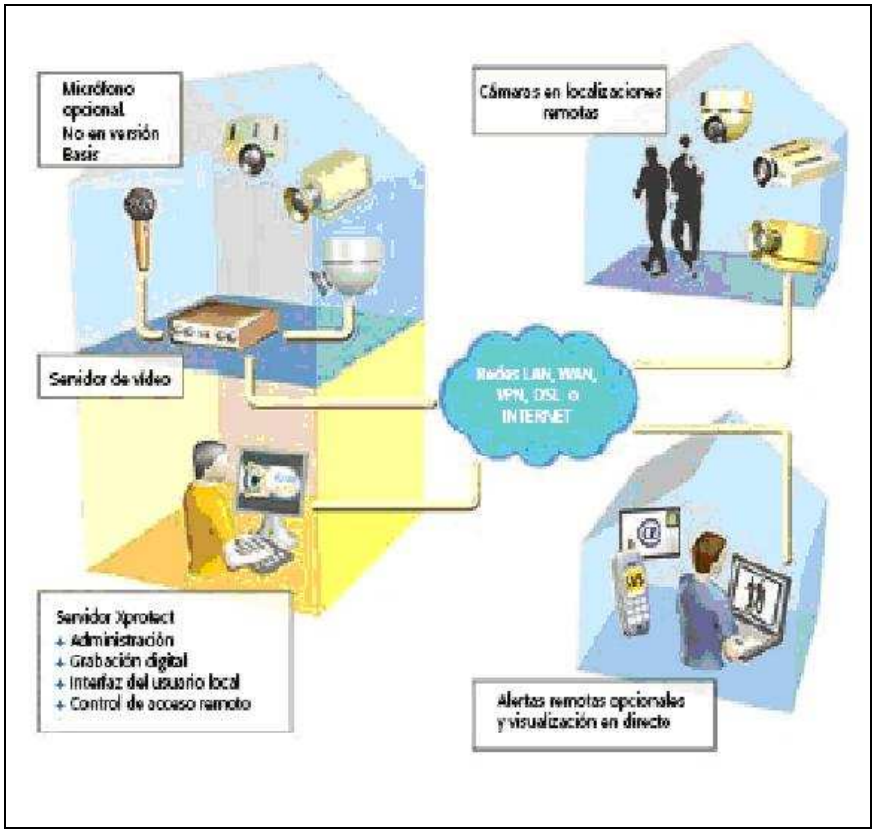


Figura X: Representación aplicaciones Milestone.

4.5.6 Configuración e integración de cámaras

4.5.6.1 Integración cámaras

Como bien se anotó previamente, todas las cámaras domo IP que son instaladas para la vigilancia del perímetro dan la posibilidad de conectar dispositivos a sus entradas y salidas digitales, igualmente las cámaras fijas pero esta opción no será realmente utilizada, quedando abierta para posibles futuras aplicaciones. De esta forma vamos a llevar a cabo un conexionado de los RIOs a las cámaras con el fin de posicionarlas, según presets establecidos en el momento que se detecten alarmas, consiguiendo una verificación de la misma mediante la visualización del lugar donde se haya detectado el salto.

Cada domo puede conectar con 4 entradas de alarmas con salidas programables.
A continuación se establecen esas conexiones según que zonas estén dentro del campo visual de cada cámara:

# DOMO A CONECTAR	# RIOs CONECTADOS COMO ENTRADAS
Domo ip 1	RIO 0, RIO 1, RIO 2 y RIO 3
Domo ip 2	RIO 4, RIO 5 y RIO 6
Domo ip 3	RIO 5, RIO 6 y RIO 7
Domo ip 4	RIO 7, RIO 8 y RIO 9
Domo ip 5	RIO 9, RIO 10 y Centro Control

Tabla 13: Conexionado domo-RIOs

Esto será la conexión de las cámaras domos con los RIOS, el cableado que representa la conexión queda plasmado en el plano 12: *"Integración CCTV Intrusión"*.

Dentro de las cámaras fijas establecidas, como ya se comentó en su configuración, realizarán determinadas acciones en el momento en el que detecten movimiento; no obstante la cámara C1, enfocada a la entrada del perímetro, estará conectada a una de las salidas del RIO0 de forma que también lleve a cabo la misma actuación que con la detección de movimiento en caso del salto de alarma por parte de este RIO.

Como especifican las características de los domos, estos son capaces de almacenar 128 posicionamientos diferentes, sin embargo como bien se anotó el software de manejo de vídeo únicamente proporciona capacidad para 25 presets por cámara. Mediante estos presets los domos realizarán rondas de vigilancia del exterior del perímetro.

4.5.6.2 Configuración

A continuación se detalla la programación de las cámaras instaladas, las horas donde se realizarán las grabaciones de imágenes, las imágenes por segundo de las visualizaciones y grabaciones, y las acciones en función de los acontecimientos. Las decisiones se han tomado en base a los horarios de actividad en el interior del perímetro (7 a.m. a 6 p.m.) y las necesidades del cliente.

Cámaras Entrada y Salida del Perímetro
07:00 – 18:00: visualización y grabación a 30 ips.
18:00 – 07:00: visualización y grabación a 3 ips. En caso de producirse detección de movimiento por la cámara, o bien por la recepción de una señal de alarma, los valores pasarán automáticamente a 30 ips.
Fines de semana: visualización y grabación a 3 ips. En caso de producirse detección de movimiento por la cámara, o bien por la recepción de una señal de alarma, los valores pasarán automáticamente a 30 ips.

Cámaras Perímetro Interior
07:00 – 18:00: visualización y grabación a 30 ips.
18:00 – 07:00: visualización a 3 ips. En caso de producirse detección de movimiento por la cámara, los valores pasarán automáticamente a 30 ips en visualización y comenzará la grabación, para una mayor seguridad se hará uso de la posibilidad de grabación pre y post alarma, que se fijará durante la configuración.
Fines de semana: visualización y grabación a 3 ips. En caso de producirse detección de movimiento por la cámara, los valores pasarán automáticamente a 30 ips.

Cámaras edificio 6
En este edificio se llevará a cabo la misma configuración que para las cámaras del interior del perímetro, añadiendo la particularidad de cambiar los valores a 30 ips de visualización y comenzar la grabación en el caso que se produzca un salto de alarma. Señalar que, tratándose de CCTV analógico, la detección de movimiento será proporcionada por el software, aunque pudiera ser también obtenida por el servidor de vídeo.

Cámaras Perímetro Exterior

La colocación de las cámaras rodeando el perímetro no busca más que servir de apoyo en situación de alarma, verificándolas y pudiendo ser utilizadas posteriormente como reconocimiento, por tanto no es necesaria la transmisión de imágenes a una frecuencia de 30 ips, ni tampoco su grabación. Por ello durante las 24 horas la visualización y grabación será a 3 ips pasando a 30 en caso de alarma, utilizando como en casos anteriores la utilidad de pre-post alarma, los 7 días de la semana.

4.5.7 Diseño red IP

Para poder decidir cual es la tecnología de red que más se adecua a nuestras necesidades, como bien se explicó en el apartado de diseño, son necesarias ciertas consideraciones acerca del ancho de banda de la red.

4.5.7.1 Ancho de Banda

Para calcular el ancho de banda que requieren todas las cámaras que conforman nuestro sistema de CCTV se hará uso de una herramienta de cálculo de ancho de banda para cámaras IP. En esta herramienta se fijan los valores de resolución, compresión, imágenes por segundo y el número de cámaras del sistema.

La primera configuración de cámaras que hemos fijado sería para hallar el máximo de ancho de banda que en un momento determinado podría llegar a ser necesitado. La situación en la que se daría este máximo requerimiento de ancho de banda podría darse en algún momento entre las horas de actividad del perímetro donde las cámaras del perímetro interior así como las cámaras de entrada y salida o las del edificio 6 se encuentran transmitiendo a 30 ips. A esto añadir una situación de alarma por todo el perímetro exterior que hiciera que todos los domos comenzarán la visualización y grabación igualmente a 30 ips.

Por tanto para rellenar los campos de la calculadora de ancho de banda, habría un total de 20 cámaras, con una resolución de 640x480 y MPEG4 como método de compresión.

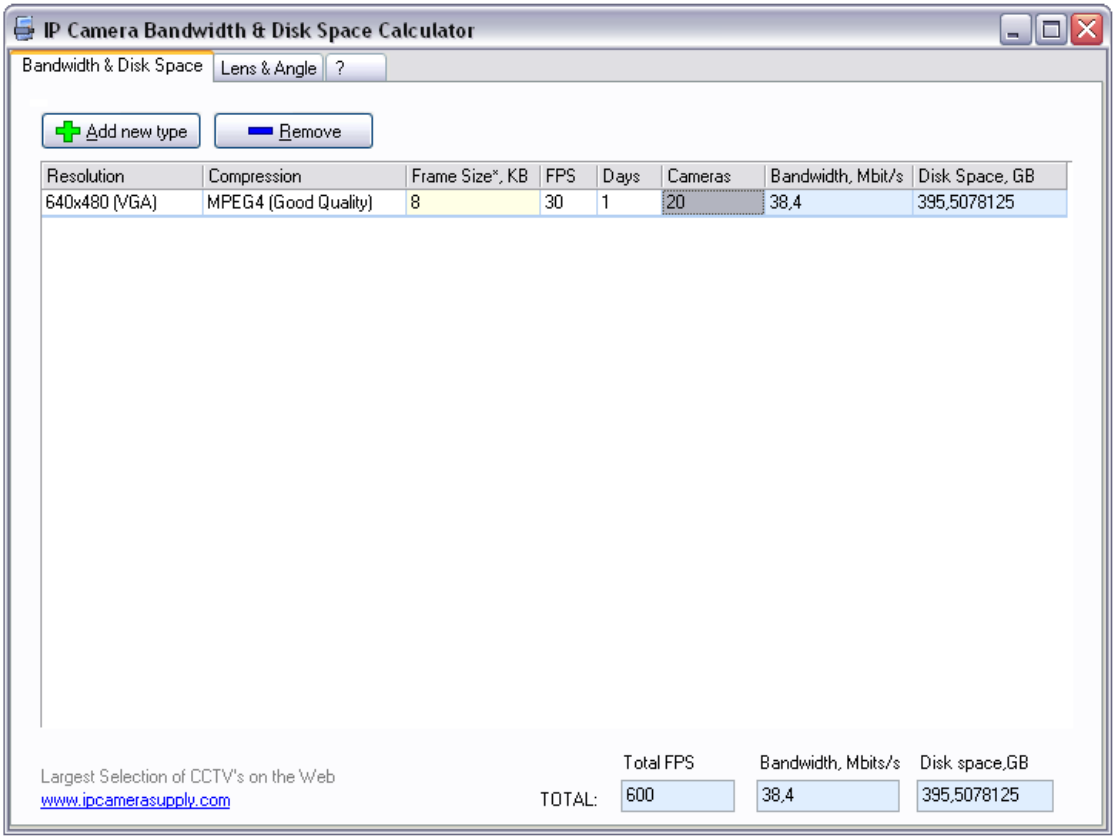


Figura 43: Calculadora ancho de banda

El estándar FastEthernet ofrece una tasa de bits de 100 Mbit/s, por lo que esta opción se ve razonable y suficiente para dar cabida a todos nuestros equipos, no obstante esta red podría ser utilizada como LAN o se podrían querer instalar nuevas cámaras en un futuro, por lo que habría una exigencia de ancho de banda que podría no cubrirse con esta instalación. El estándar que sería capaz de dar cabida a un crecimiento en el sistema de CCTV es el Gigabit Ethernet (1000 Mbit/s).
.

4.5.7.2 Tecnología y Topología

Partiendo de la decisión de utilizar el estándar Gigabit Ethernet se decide que la tecnología necesaria será la de fibra óptica y no un cable cat5 o cat6 por sus deficiencias en cuanto a la distancia que, por otro lado, la f.o. suple.
Por tanto para cubrir las necesidades de comunicaciones a lo largo de la línea, se utiliza un sistema de transmisión por fibra óptica altamente confiable que proporcione la infraestructura necesaria para las necesidades planteadas y sea suficiente para absorber las demandas a corto, mediano y largo plazo, dejando abiertas las puertas a los avances de la tecnología.

La red se realizará como un anillo de fibra óptica; La topología de anillo esta diseñada como una arquitectura circular, con cada nodo conectado directamente a otros dos nodos. Toda la información de la red pasa a través de cada nodo hasta que es tomado por el nodo apropiado.

Por tanto lo que finalmente tendremos será un sistema de CCTV en el que la comunicación entre los diferentes elementos que componen el sistema se realiza a través del protocolo IP, conectando los equipos a una red Ethernet.

4.5.7.3 Descripción anillo

Para poder conformar una red en anillo es necesario que los equipos IP, en nuestro caso cámaras de red y video servidores, se conecten a un switch para poder establecer la comunicación. Dado que el medio de comunicación es la fibra óptica, los switchs deberán contar con la posibilidad de conexionado de fibra, para una comunicación Gigabit.

Según la ubicación de las cámaras se han establecido 5 nodos para formar el anillo de comunicación y proporcionar conexión a las cámaras, estos se representan en el plano 13: *"Anillo FO"*, donde también se aprecia la conexión de las diferentes cámaras a dichos switchs.

La tabla que sigue muestra que cámaras se encuentran conectadas en cada switch así como la distancia que las separa.

SWITCH	**CÁMARA**	**DISTANCIA (metros)**
SWITCH 1	Cámara 3	91
SWITCH 1	Cámara 4	60
SWITCH 1	Domo 1	90
SWITCH 2	Cámara 2	40
SWITCH 2	Domo 2	70
SWITCH 3	Cámara 1	60
SWITCH 3	Cámara 8	70
SWITCH 3	Domo 3	80
SWITCH 3	Domo 4	30
SWITCH 4	Cámara 7	70
SWITCH 4	Servidor de vídeo 1	1
SWITCH 4	Servidor de vídeo 2	1
SWITCH CENTRAL	Cámara 5	70
SWITCH CENTRAL	Cámara 6	70
SWITCH CENTRAL	Domo 5	80
SWITCH CENTRAL	Cámara entrada	10
SWITCH CENTRAL	Cámara salida	80

Tabla 14. Conexionado y distancias switches.

La conexión entre las cámaras y el switch correspondiente, se realizará mediante un cable de red cat5, que proporciona el suficiente ancho de banda para el envío de imágenes desde las cámaras independientemente, siempre y cuando la distancia entre los equipos no supere 100 metros. En nuestro caso no es superada, puesto que los switch se han ubicado en el interior de cada edificio de forma que esto no ocurra. En la situación en la que por algún

motivo no pudiera ser así y al distancia excediera de los 100 metros, se valoraría la opción de instalar en los puntos donde se requiera, hubs, que sirvan de regeneración de la señal.

Como se observa, el máximo número de cámaras que se conectará a un switch es de 4, por tanto con un switch que cuente con 8 puertos resultaría suficiente para los nodos, y un switch de 16 para el nodo central; se podría contemplar la posibilidad de instalar switchs que alberguen un mayor número de puertos si así se especificará en el pliego de condiciones, o por deseo del cliente.

El switch elegido para los nodos es un Switch Linksys de 8 puertos y para el nodo central un Linksys de las mismas características con 16 puertos 10/100.

Figura 44: Swithes Gigabit de 8 y 16 puertos

Como bien aparece en la hoja técnica de características del producto, anexada al final. este switch cuenta con dos puertos GigaEthernet y dos puertos para fibra óptica que se conectan al cableado mediante pequeños conversores. Por último, está el puerto de consola para configurar el router.

Figura 45: Ranura Gigabit

Los puertos para fibra óptica son unas ranuras de expansión denominadas mini-GBIC o SFP. En ellas se instala un módulo que añade un puerto de fibra óptica LC dúplex compatible con 1000Base-SX (1000Mbps), permitiendo una distancia máxima de 550 nm, a una longitud de onda de 850 nm, LC multi-modo (MM).

Figura 46: Mini-GBIC

Puesto que la comunicación a través de fibra óptica es simplex, es obvia la necesidad de contar con un cable que al menos albergue 2 fibras, de las cuales una de ellas se destinará a la comunicación desde los distintos nodos hasta el switch central para el envío de imágenes, mientras que la otra será como vía de comunicación entre este nodo central y el resto. Se utilizarían entonces dos fibras para la implementación de nuestra red cosiendo un switch con otro, hasta completar el anillo, donde cada switch regenera la señal.

Puesto que contamos con comunicación en dos sentidos diferentes, nuestro anillo es clasificado como un anillo bidireccional, puesto que el tráfico de transmisión y el de recepción viajan alrededor del anillo en direcciones opuestas. Añadir que los anillos bidireccionales se prestan mejor para aquellos casos, como el nuestro, en que el tráfico está equilibrado entre los distintos nodos.

Existen también anillos bidireccionales de cuatro fibras, en los cuales un par de fibras se reserva para protección, o para conducir tráfico igualmente, por lo que para agilizar el envío de imágenes dentro de este anillo se opta por la instalación de un cable que contenga un mayor número de fibras. Se podrá optar directamente por un cable de 4 fibras, o por el contrario, con un número mayor, pudiéndose utilizar como repuesto o bien para otras aplicaciones. En el informe económico final se ha hecho una valoración del precio para un cable de mayor número de fibras, de las mismas características.

La protección se conseguirá gracias a los avanzados switchs que han sido instalados. Estos proporcionan una visión del estado actual de todas las conexiones de sus puertos utilizados así como la posibilidad de realizar pruebas para verificar el funcionamiento del cableado. Gracias a esto si un fallo se produce en algún cable nos avisaría e incluso indicaría el lugar donde este fallo ocurre. Por tanto se podría llevar a cabo alguna acción mientras la información es enviada en otro sentido gracias al Spanning Tree Protocol (explicado en el apartado siguiente), y a la existencia de más fibras en el cableado.

Siguiendo con la instalación de un solo anillo de fibra óptica, las fibras no utilizadas y reservadas como back-up, podrían ser utilizadas para el envío de tráfico sobre ellas, fibras "de protección" en caso de fallo de las fibras "en funcionamiento".

Otro mecanismo de protección conocido dentro de la topología en anillo, sería el establecer otro anillo de fibra (1+1) de la misma configuración que se utilizará en caso de fallo del anillo primero. No obstante para poder instalar un anillo distinto nuevo, se requeriría nuevamente toda la cantidad de fibra ya instalada, además de unos equipos con capacidad para albergar más de 2 entradas de fibra, por tanto la opción que prevalece será la de instalar un cable de fibra con un número superior de fibras al requerido.

Estas fibras formarán el anillo introducidas en la canalización ya existente que posee espacio libre para su ubicación, únicamente añadir que la fibra escogida es adecuada para instalaciones en el exterior, resistente a la humedad y con los componentes necesarios anti roedores y una cubierta adecuada para una protección eficiente.

Basándonos en las tablas de caracterización de las fibras así como en los estándares Ethernet, se determina que la fibra a instalar será de 50/125, puesto que provee de una mayor ancho de banda, que aunque en un principio con la instalación realizada no vaya a ser completamente aprovechado, resultará de mayor utilidad en futuras ampliaciones.

Como bien se comentó, todo este cable de fibra irá bajo tierra, y dadas las distancias tampoco precisará de ningún empalme, gracias a que se disponen de las canalizaciones suficientes para ello, además de nuevamente aclarar que el tema de obra civil no compete a este proyecto, y por tanto no se profundizará en él.

4.5.7.4 Protocolos

Los equipos instalados realizarán un Protocolo de interconexión de datos: Ethernet, Fast Ethernet, Gigabit Ethernet.

Por otro lado, como bien se ha dicho, se cuenta con más de una fibra en cada cable para poder realizar la comunicación desde los nodos al switch central en ambos sentidos. Como toda redundancia puede provocar inundaciones o copias de varias tramas, así como un posible desperdicio de ancho de banda. Por lo que se ha optado por la utilización de un protocolo de gestión para este tipo de fallos, Spanning Tree Protocol.

Spanning Tree Protocol (STP) es un protocolo de red de la segunda capa OSI, (nivel de enlace de datos), que gestiona enlaces redundantes (por ejemplo: redes en anillo), previniendo bucles infinitos de repetición de datos en redes que presenten configuración redundante.

Para configurarlo en nuestros switches, evitando así que se formen bucles en la transmisión de datos, se debe configurar cada puerto así como una prioridad para direccionar el tráfico a través del mismo. La opción de configuración aparecerá en el menú de la página de gestión del dispositivo.

Figura 47: Configuración STP

4.5.7.5 Asignación direcciones IP

Todos los equipos conectados a la red, disponen de una dirección IP privada, de esta forma desde el centro de control, se puede llevar a cabo la configuración de los mismos. Las direcciones IP privadas existentes son:

- Clase A: 10.0.0.0 a 10.255.255.255 (8 bits red, 24 bits hosts)
- Clase B: 172.16.0.0 a 172.31.255.255 (16 bits red, 16 bits hosts)
- Clase C: 192.168.0.0 a 192.168.255.255 (24 bits red, 8 bits hosts)

Si se quisiera acceder independientemente a cada una de estas cámaras, o bien a alguno de los servidores de vídeo, se podría hacer mediante la configuración en el router de comunicación con el exterior de lo que se conoce como PAT. Este mecanismo mapea varias direcciones IP privadas a una sola dirección IP pública. Esto es posible gracias a que cada dirección privada se diferencia por el número de puerto, estos números de puerto origen son únicos, y sirven en la dirección IP global interna para distinguir entre las traducciones.

No obstante, como bien se especifica en la hoja técnica, los equipos disponen de aplicaciones de seguridad para que el acceso a los mismos sea restringido.

Si únicamente se quisiera configurar el sistema de forma que el único acceso posible a las imágenes fuera con la visualización que está teniendo lugar en los monitores del centro de control, bastaría con la obtención de una ip fija para el PC donde estuviera el software de gestión. Con restricciones de acceso igualmente.

La gráfica siguiente muestra la dirección IP privada asignada a cada equipo de la red.

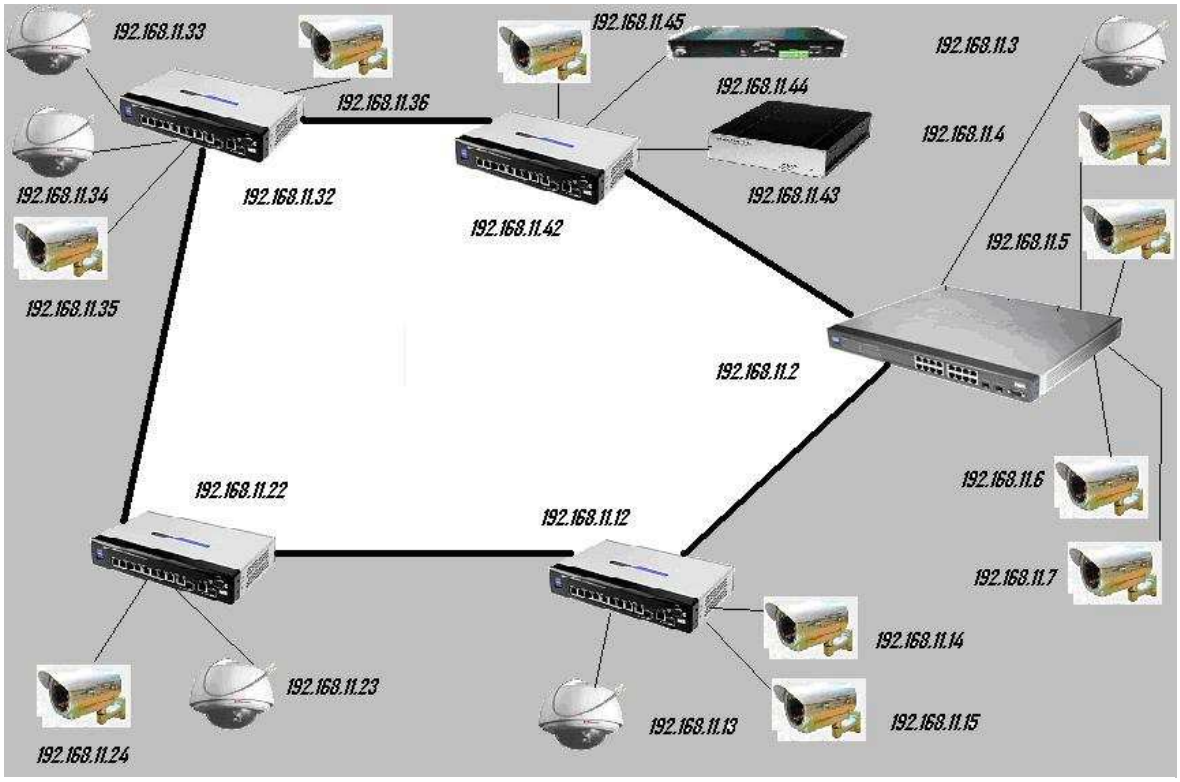


Figura 48: Anillo con direcciones IP

4.5.7.6 Almacenamiento

Para poder añadir equipos para el almacenamiento de las imágenes, volvemos a hacer uso de la herramienta de cálculo que nos proporcionará un valor de espacio en disco requerido.

Los datos que hemos introducido nos permiten conocer los GB para una grabación de 1 día completo, 24hr, grabando a 3 ips y a 30 ips únicamente una cámara, y de ahí extrapolaremos a toda la instalación.

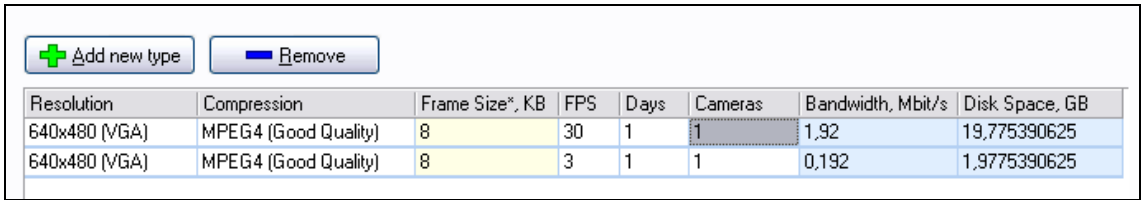


Figura 49: Calculadora espacio en disco.

Según los resultados, para una sola cámara a 30 ips se necesitarían 19.8 GB de disco duro, por tanto 1 hora de grabación requerirá 0.825 GB.
Según los horarios establecidos de grabación durante 11 horas al día cada día de lunes a viernes, habrá 11 cámaras con esa necesidad de almacenamiento por hora, por tanto tenemos que:

11 horas x 0.825 GB/hr = 9.075 GB/cámara

9.075 GB/cam x 15 cam = 136.125 GB

Contabilizando un mes natural de 30 días, 8 de ellos serán fin de semana, por tanto durante los 22 restantes se lleva a cabo la grabación anterior, entonces necesitaremos:

136.125 GB/día x 22 días = 2994.75 GB

A esto habría que añadir la cantidad de disco duro para almacenar las grabaciones de imágenes a 3 ips. Como bien anota la calculadora una cámara a 3 ips durante un día de grabación necesitará 1.98 GB.

5 cámaras perímetro exterior x 1.98 GB/ dia = 9.9 GB
9.9 GB x 30 días = 297 GB
15 cámaras(Edif.+ perim. Int+ e/s) x 0.0825 GB/hr x 13hr/ día x 22 días = 353.925 GB
15 cámaras(Edif.+ perim. Int+ e/s) x 1.98 GB/ día x 8 días (fin de semana) = 237.6 GB

Todos los valores anteriores hacen un total de espacio requerido de 3883.275 GB sin contar situaciones que pudieran producir alarma, todo esto si se quisieran almacenar imágenes durante 30 días, máximo tiempo permitido por ley de almacenamiento de imágenes. Por tanto incluyendo un sistema de almacenamiento por medio de disco duros hasta alcanzar 4Teras, será suficiente para prácticamente mantener almacenadas imágenes durante 30 días. Se ha escogido un Western Digital MyBook G2NC20000E, de capacidad 2.0 Terabyte que nos permitirá igualmente compartir los archivos a través de la red.

Figura 50: Disco duro Western Digital

Estos dos discos duros serán conectados al ordenador que contenga el software de manejo de vídeo en el centro de control y se irán almacenando ahí las visualizaciones, igualmente el software permite un borrado de imágenes en el momento que se detecte que el disco duro se encuentra en su máxima capacidad, comenzando a borrar los archivos más antiguos, liberando espacio y almacenando los nuevos.

Como ya se comentó en apartados anteriores, para una mayor seguridad en el almacenamiento de imágenes este puede realizarse igualmente en otra ubicación remota del perímetro como salvaguarda, acción que es permitida por el software instalado.

4.6. Subsistema de emergencias

Este Subsistema contempla todos los equipos que en caso de emergencia eviten que deje de funcionar el Centro de Control y los ordenadores de seguridad.

Se utilizarán para ello sistemas de alimentación interrumpida, SAI.

Para ello calculamos los VA que necesitaremos para cubrir toda nuestra necesidad, según lo explicado en otro apartado anteriormente.

EQUIPO	CONSUMO MÁXIMO / UNIDAD (VA)	UDS TOTALES	TOTAL CONSUMO (VA)
Barrera IR 50 m	1.14	1	1.14
Barrera IR 100 m	1.26	14	17.64
Cámara IP fija	12	10	120
Domo IP	35	5	175
Servidor Vídeo 1 canal	12	1	12
Servidor Vídeo 4 canales	51.6	1	51.6
Switch 8 puertos	15.4	4	61.6
Switch 16 puertos	35	1	35
PC	560	2	1120

TOTAL	1.5Kva

Tabla 11: Cálculo consumo equipos

Con el resultado anterior, se prevé una instalación de una SAI de 2KVA, que nos permitirá una autonomía de aproximadamente 10 min. Lo que se busca con su instalación es proporcionar un margen de tiempo en el que tras haber ocurrido un fallo eléctrico los equipos puedan ser apagados correctamente, de forma que no se produzcan picos de tensión que pudiera provocar daños. Este equipo es instalado en el cuerpo de guardia, donde según especificaciones del cliente, habrá siempre una persona vigilando los monitores, por tanto, en el momento que algún fallo ocurra y la SAI empiece a actuar emitirá un sonido y otro, especificado en la hoja técnica, en función del fallo detectado.

Figura 51: SAI Integra

4.7. Centro de Control

Este centro, como bien quedo especificado en las permisas a seguir en el desarrollo del proyecto, se situará en el cuerpo de guardia que se sitúa a la entrada del perímetro.

En este centro de control se gestionará toda la red IP CCTV así como todo el despliegue del subsistema anti-intrusión.

Para el primero de todos, red IP CCTV, como se ha ido comentando se instalará el switch central donde se recibirán las imágenes y estás serán visualizadas en un monitor. Este punto, será también el de comunicación con Internet, para poder realizar las configuraciones o visualizaciones remotamente. El software de manejo de vídeo será instalado en un PC que se ubicará en dicho centro de control, y se conectará al switch central, y desde el que se realizarán las visualizaciones y toda la gestión necesaria. En este mismo monitor se detectarán las alarmas por detección de movimiento, así como se configurarán las rondas, y se podrá actuar directamente sobre todas las cámaras. Se podría añadir un monitor más, de forma que se distribuyeran más cámaras entre ambos, utilizando una tarjeta gráfica.

Respecto al subsistema anti-intrusión, se colocará otro PC, donde se centralizarán todo el subsistema y se instalará el software elegido para la gestión. La central de alarmas elegida, Galaxy, se conectará con dicho ordenador igualmente y de esta forma se enviarán las señales que correspondan para el control del subsistema.
Por último también se ubicará en el centro de control la SAI proveedora de alimentación en caso de fallo.

El centro de control de nuestra instalación de seguridad se recoge una gran cantidad de información. Este caudal de datos será aprovechado al máximo, tanto desde el punto de vista de la operatividad inmediata como para le posterior análisis de los hechos y la mejora de la seguridad global de la instalación con la experiencia adquirida.

4.8. Estudio de Costes

Como se observa en el estudio de costes, el resultado total de toda la instalación ascendería hasta un valor de 80.412,75 euros, únicamente cubriendo gastos y sin aplicar un margen de comisión que toda empresa realiza para obtener beneficios. No obstante aclarar que, las empresas que se dedican a este tipo de instalaciones, sistemas de seguridad a gran escala, poseen un descuento respecto al PVP de los proveedores, que les permite jugar a la hora de competir con otras grandes empresas. Dichos descuentos suelen encontrarse entre un 30 y un 60 por ciento del precio estipulado.

Utilizando el descuento explicado anteriormente, y realizando una media hacia la baja, de que todos los equipos recibieran un porcentaje de descuento del 35 por ciento, obtendríamos que el coste por los materiales sería de: 25.00 euros en lugar de los 40.000 anteriores. Ahorro considerablemente atractivo para los instaladores.

TOTAL GENERAL	
TOTAL MATERIALES	**39.293,25 €**
TOTAL CANALIZACIONES Y CABLEADOS	**32.219,50 €**
TOTAL MANO DE OBRA	**8.900,00 €**
TOTAL COSTES	**80.412,75 €**

SUBSISTEMA DE INTRUSIÓN							
ITEM	**DESCRIPCIÓN**	**PROVEEDOR**	**MARCA**	**MODELO**	**UDS.**	**PRECIO UNITARIO**	**PRECIO TOTAL**
1	Central de alarmas. Control de 0-504 Zonas programables. Soporta zonas RF. 16 Particiones. 4-256 Salidas. 500 códigos de usuario. Función de Autoconfiguracion y Autodiagnóstico. Registro de 1000 Eventos. Fuente de alimentación de 3A	HONEYWELL	HONEYWELL	**GALAXY - 500/3A o similar**	1	600,00 €	600,00 €
2	Módulo expansor multiplexado de 8 zonas identificadas individualmente y con doble balanceamiento + 4 salidas lógicas programables, para ampliación de sistemas Galaxy.	HONEYWELL	HONEYWELL	**RIO/B o similar**	13	130,00 €	1.690,00 €
3	Fuente de alimentación de 12 Vcc/ 5 Amperios en caja.	HONEYWELL	HONEYWELL	**12V5AB o similar**	15	143,80 €	2.157,00 €
4	Sensor Cortina de doble tecnología antienmascaramiento (Infrarrojo + microondas) para exterior o interior de pequeño Angulo de apertura 3º y rango de detección de 12 mx 0,60 m.	INMORA	INMORA	**SI-DT-CORTINA o similar**	8	150,00 €	1.200,00 €
5	Detector volumétrico de doble tecnología.	HONEYWELL	C&K	**DT7450EU o similar**	1	49,09 €	49,09 €
6	Detector por contactos magnéticos. Varios modelos según puertas.	EULEN	ADEMCO	**7945 o similar**	10	12,98 €	129,80 €
7	Sensor Rotura de cristal electrónico, alcance 3 m de radio.	CASMAR	SENTROL	**SENTROL**	12	15,77 €	
8	Barreras de infrarrojos de 4 haces de 100 metros	TURSON	PULNIX	**PB-IN-100-HFo similar**	14	242,00 €	3.388,00 €
9	Barreras de infrarrojos de 4 haces de 50 metros	TURSON	PULNIX	**PB-IN-50-HF o similar**	1	222,00 €	222,00 €
10	Soportes especiales para ubicación de barreras sobre muro.	TURSON	PULNIX	**PULNIX**	15	45,00 €	675,00 €
11	Ml aproximado de manguera para transmisión de señales VV-K500v de 12x 0,75 mm².	REPEL	REPEL	**REPEL**	1300	0,65 €	845,00 €
12	Ml. De manguera de alimentación 3 x 2, 5 mm²	PHERCAB	PHERCAB	**PHERCAB**	750	0,77 €	577,50 €
13	Ml. De manguera de alimentación 3,5 x 6 mm².	PHERCAB	PHERCAB	**PHERCAB**	1500	2,15 €	3.225,00 €
14	Ml aproximado tubo de acero de métrica 60.	REPEL	REPEL	**REPEL**	1300	11,72 €	15.236,00 €
15	Cableados, pequeño material, mano de obra de instalación, conexionado, programación, pruebas, puesta a punto y curso de formación en el manejo de los sistemas.	Empresa Sub contratada	Empresa Sub contratada	**Empresa Subcontratada**	1	4.200,00 €	4.200,00 €

SUBSISTEMA DE CCTV							
ITEM	**DESCRIPCIÓN**	**PROVEEDOR**	**MARCA**	**MODELO**	**UDS.**	**PRECIO UNITARIO**	**PRECIO TOTAL**
1	Cámara IP Día/Noche basado en un CCD 1/3"con lente varifocal de 7,5 a 50 mm. Esta construida en aluminio resistente que le permite soportar la instalación en exteriores gracias a su protección Ip66.	TURSON	PIXORD	**IP Pixord-428**	10	790,00 €	7.900,00 €
2	Domo IP PTZ, con servidor de vídeo integrado, día/noche longitud focal 3.4-119 mm, con cárcasa para exterior antivandálica,IP 66.	Sistemas Fotónicos S.L.	INFINOVA	**V1749N**	5	2.480,75 €	12.403,75 €
3	Fuente de alimentación de 24 V 3 Amperios en caja.	CASMAR	CASMAR	**CASMAR**	5	153,77 €	768,85 €
4	Columna de 4 m con adaptador para soporte de cámara.	A definir	A definir	**A definir**	1	195,00 €	195,00 €
5	Cable de interconexión RJ45 categoría 5	CENTER CABLE	CENTER CABLE	**CENTER CABLE**	1000	0,50 €	500,00 €
6	Cable de fibra óptica para instalaciones exteriores, con 4 fibras multimodo 50/125 en estructura libre (unitubo) con gel hidrófugo resistente a la humedad, refuerzo mecánico de fibra de vidrio resistente a los roedores y cubierta de polietileno.	OPTRAL	OPTRAL	**OPTRAL**	1000	4,55 €	4.550,00 €
7	Cable de fibra óptica para instalaciones exteriores, con 6 fibras multimodo 50/125 en estructura libre (unitubo) con gel hidrófugo resistente a la humedad, refuerzo mecánico de fibra de vidrio resistente a los roedores y cubierta de polietileno.	OPTRAL	OPTRAL	**OPTRAL**	1000	5,53 €	5.530,00 €
8	Ml. De manguera de alimentación 3 x 2, 5 mm^2	PHERCAB	PHERCAB	**PHERCAB**	200	0,77 €	154,00 €
9	Ml aproximados de canaleta unex de 90x60.				100	9,37 €	937,00 €
10	Cableados, pequeño material, mano de obra de instalación, conexionado, programación, pruebas, puesta a punto.	Empresa Sub contratada	Empresa Sub contratada	**Empresa Subcontratada**	1	4.000,00 €	4.000,00 €

SUBSISTEMA DE CENTRALIZACIÓN							
ITEM	**DESCRIPCIÓN**	**PROVEEDOR**	**MARCA**	**MODELO**	**UDS.**	**PRECIO UNITARIO**	**PRECIO TOTAL**
1	Modulo de RS-232 para sistema Galaxy. Comunicación Bidireccional Local o remoto (mediante PC).	HONEYWELL	HONEYWELL	**RS232/I/B o similar**	1	299,48 €	299,48 €
2	Software grafico 1 GY, Windows 95/98 de controles Galaxy. Iconos dinámicos. 2 niveles de planos asociados.	HONEYWELL	HONEYWELL	**GY-GRAPH/WIN**	1	1.081,92 €	1.081,92 €
3	Teclado alfanumérico con display de cristal liquido de 2 líneas x 16 caracteres para la programación y gestión de las centrales Galaxy.	HONEYWELL	HONEYWELL	**MK-7**	1	170,00 €	170,00 €
4	Interfase de conversión a salida de 4 reles desde la salidas de los módulos RIO	HONEYWELL	HONEYWELL	**MR-4E**	13	39,07 €	507,91 €
5	Software de gestión: grabación, monitorización y gestión remota de vídeo IP, hasta 25 cámaras.	HONEYWELL	MILESTONE	**XPB+25**	1	2.090,00 €	2.090,00 €
6	Unidad de alimentación ininterrumpida 2 Kva montaje rack con autonomía de 15 minutos.	INTEGRA	INTEGRA	**PLUS 2K**	1	390,77 €	390,77 €
7	PC	A definir	A definir	**PENTIUM IV**	2	600,00 €	1.200,00 €
8	Switch gestionable 8 puertos 10/100/1000 + 2 puertos expansión mini GBIC	ACUISTA (web)	LINKSYS	**LINKSYS 8+2**	4	187,42 €	749,68 €
9	Switch gestionable 16 puertos 10/100/1000 + 2 puertos expansión mini GBIC	ACUISTA (web)	LINKSYS	**LINKSYS 16+2**	1	315,00 €	315,00 €
10	Adaptador SFP Gigabit Ethernet SX Mini-GBIC	TWENGA (web)	LINKSYS	**MGBSX1**	10	111,00 €	1.110,00 €
11	Ml. De manguera de alimentación 2 x 2 x 0,5 mm².	PHERCAB	REPEL	**REPEL**	100	0,65 €	65,00 €
12	Cuadro eléctrico	A definir	A definir	**A definir**	1	600,00 €	600,00 €
13	Cableados, pequeño material, mano de obra de instalación, conexionado, programación, pruebas, puesta a punto y curso de formación en el manejo de los sistemas.	Empresa Sub contratada	Empresa Sub contratada	**Empresa Subcontratada**	1	700,00 €	700,00 €

4.9. Estudio Analógico

A modo comparativo se ha realizado un estudio del desarrollo del diseño de seguridad en el caso de haber utilizado un CCTV analógico, en lugar de tecnología IP.
Los equipos referentes al subsistema anti-intrusión serían los mismos que para el diseño IP, sin agregar el módulo Ethernet de la central.

Si se hubieran utilizado cámaras analógicas, se plantearía un primer problema en cuanto a equipararlo con el sistema desplegado. Se eligieron domos IP para reducir el número de cámaras así como para poder ofrecer una vigilancia superior en caso de alarma o intrusión, por tanto si se quisiera visualizar todo el perímetro exterior se requeriría un mayor número de cámaras, además de encontrar cámaras con la óptica apropiada o bien incorporar objetivos a las cámaras. Podrían instalarse igualmente cámaras domos que alcanzaran dichas distancias sin embargo su movimiento para enfocarlas hacia una posición u otra se tendría que hacer manualmente gracias a la telemetría desde el centro de control.

Supongamos que queremos instalar cámaras fijas, contando con una óptica de 5-50mm., se instalarían 14 cámaras en el perímetro exterior.

Respecto a las cámaras del perímetro interior así como las dos de entrada y salida, puesto que en el sistema IP se utilizó una óptica como la escogida ahora el número de cámaras no variaría, haciendo un total de otras 11 cámaras más sus respectivos objetivos. Estas cámaras deberán ser igualmente día noche para obtener un sistema equivalente al nuestro.

El uso de un sistema analógico requiere la instalación de grabadores digitales para el almacenamiento de las imágenes, y en el caso en que la cantidad de imágenes a almacenar sea muy grande se necesitaría una extensión de la memoria de almacenamiento de imágenes por lo que se debería añadir un disco duro al grabador.
Si se quisiera igualmente integrar las cámaras del edificio central al nuevo punto de control, no se utilizaría un servidor de vídeo para sistemas IP, sino un multiplexor.

Un multiplexor es un dispositivo para el proceso de señales de vídeo que divide y multiplexa imágenes de varias cámaras y las presenta como una sola señal. Un microprocesador de alta resolución se encarga de multiplexar / demultiplexar las entradas de cámara con salidas para monitores y videograbadoras. Al contar con 5 canales con un multiplexor de 4 entradas no sería suficiente por lo que se requeriría uno de mayor capacidad, un multiplexor de 9 entradas, que envíe las señales de video sobre 1 fibra óptica multimodo 62,5/125, de igual forma en el punto de recepción de dichas imágenes se deberá colocar un Multiplexor receptor con tratamiento digital de hasta 9 señales de vídeo para poder tratar correctamente las imágenes.

Puesto que se trata de cámaras analógicas el cableado necesario para la transmisión de la señal de vídeo ya no es un cat5 como en nuestro sistema IP, sino cable coaxial. No obstante este cable también presenta limitaciones en distancia por lo que normalmente se suele utilizar cuando las distancias entre los distintos componentes de un sistema de CCTV no exceden los 200 m. La transmisión de video por par trenzado es una opción muy

conveniente frente al cable coaxial con amplificadores de video ya que estos amplifican también las interferencias.

Otra opción posible sería el uso de enlaces inalámbricos, estos se usan para transmitir en forma inalámbrica una imagen de CCTV a una distancia entre los 100 mts y 8.000 mts. La señal de video se modula con una frecuencia que pertenece a la región de las microondas del espectro electromagnético. En la práctica, sin embargo, las frecuencias típicas que se usan para la transmisión de video están entre 1GHz y 10GHz.
Las conexiones de microonda transmiten un ancho de banda muy grande de señales de video así como también otros datos si es necesario (incluyendo audio y /o control de PTZ). El ancho de banda depende del modelo del fabricante. Para una unidad bien construida, un ancho de banda entre 6MHz y 7MHz es suficiente para enviar señales de video de alta calidad sin una degradación visible. Para un correcto enlace, se necesita tener visión óptica entre el transmisor y el receptor. Las distancias que se pueden alcanzar con esta tecnología dependen de la potencia de salida del transmisor y de la ganancia de las antenas.

Aunque el número de cámaras sea superior el desembolso económico será muy inferior con respecto a las cámaras IP, de todas formas lo que realmente encarece este tipo de obras donde las distancias a cubrir son muy grandes es las grandes tiradas de cable que se requieren, que en ambos casos serán necesarias.

El resto de elementos necesarios en el diseño son semejantes a los del sistema IP, por lo que no se mencionan aquí ni se les referencia económicamente, como pueden ser las carcasas, los soportes, los cables de alimentación o los monitores de visualización.

A continuación se exponen unos posibles equipos correspondientes a los citados anteriormente, se debe tener en cuenta que los pecios pueden variar enormemente en función del fabricante de los equipos.

Uds	Descripción	Precio Unidad	PVP TOTAL
25	PELCO Cámara día/noche con sensor de 1/3". Rango Dinámico ampliado hasta 60 dB. Elementos 752x582. Cuerpo de estilo compacto. Resolución 480 líneas en color y 530 líneas en B/N. Iluminación mínima 0.02 lux en color y 0,002 lux en B/N. Montura C/CS. 12Vdc/24 Vac. Configurable mediante menú en pantalla o mediante RS485 (compatible Pelco P y D), compensación de contraluz.	989,44 €	24736 €
25	PANASONIC Cámara conmutable color-B/N digital con CCD de 1/3". Elementos 752x582. Resolución 480 líneas color y 570 líneas B/N. Iluminación 1 lux (F1.4) color y 0.15 lux (F1.4) B/N. 220 Vac. Montura C/CS. Relación señal/ruido 50 dB. Compensación de contraluz.	468,75 €	11718,75 €
1	BFI OPTILAS Multiplexor Transmisor con tratamiento Digital de hasta 4 cuatro señales de video sobre 1 fibra óptica multimodo 62,5/125.	618 €	618 €
1	BFI OPTILAS Multiplexor receptor con tratamiento Digital (8 bits) de hasta cuatro señales de video sobre 1 fibra óptica multimodo 62,5/125. 1210 nm. Montaje en Rack. Distancia máximas 4 Km.	618 €	618 €
2	A5: Unidad de grabación digital con video sensor avanzado para 16 entradas de video, resolución seleccionable CIF, 2 CIF y 4 CIF, 200 i.p.s. Ethernet 10/100.	2469 €	4938 €

5. Conclusión

La instalación de los sistemas de seguridad como medio de protección de bienes y personas busca minimizar los intentos de intrusión y proporcionar una acción efectiva y rápida ante dichos intentos.

La integración de diferentes sistemas permite una acción conjunta de todos los participantes que unidos por fibra y dirigidos por la red IP ofrece una solución óptima para el mercado de sistemas de seguridad, ofreciendo ventajas que el usuario final no encuentra en los sistemas independientes.

A lo largo del desarrollo del proyecto hemos podido comprobar que la integración y la arquitectura abierta permiten que los diferentes sistemas de seguridad instalados pueden unirse y funcionar creando buenas soluciones para la protección de los activos y las personas, realizando el análisis de datos procedentes de diferentes fuentes proporcionando así procesos más seguros y eliminando el mayor número de puntos débiles.

Las principales ventajas que pueden concluirse respecto a la integración de sistemas y el uso de las tecnologías IP son las siguientes:

- Unificación de sistemas en un único punto de control.
- Posibilidad de centralización in situ y remoto.
- Configuración remota de equipos.
- Aumento en la eficiencia de las respuestas ante posibles ataques gracias a la acción conjunta.
- Disminución del número de equipos por los actuales alcances de las cámaras domos.
- Visualización de las zonas detectadas con alarmas gracias a la integración entre equipos y los diferentes opciones de presets de los domos IP.
- Detección de movimiento integrado en los equipos CCTV que supone un apoyo a los sistemas anti-intrusión.
- Aprovechamiento de los equipos previamente instalados, migrando a las nuevas tecnologías utilizándose igualmente en la integración.
- El diseño se ha concebido de forma que la adaptación a los nuevos avances tecnológicos del futuro sea viable con un mínimo coste gracias a la instalación de fibra óptica.

6. Referencias

Toda la información que se han utilizado para realizar este proyecto ha sido tomada de páginas Web que son referenciadas a continuación junto con material didáctico del “Curso superior de planificación y gestión de seguridad” realizado por Asimag y la Universidad Complutense de Madrid

www.axis.com
www.hispazone.com
www.seguridad-online.com.ar
www.cablestocks.com
www.syscomcctv.com
www.belt.es
www.4security.com
www.borrmart.es
www.tsbvi.edu/technology/cctv.htm
www.siemon.com/es/
www.ordenadores-y-portatiles.com
www.guiadelaseguridad.com.ar
www.tech-faq.com
www.fibraopticahoy.com
www.sci-spain.com
www.scati.com
www.nexo.tech.com
www.voxdata.com.ar
www.ipronet.es
www.auditoressiglo21.com
www.sicuralia.com
www.adi-intl.com
www.adt-es.com
www.wut.de
www.fluidmesh.com
www.segurycontrol.com
www.etechconsulting.net
www.latinoseguridad.com
www.topalarmas.es
www.alarmas.teoriza.com
www.iceseguridad.com
www.boschsecurity.us
www.almacenpc.solostocks.com
www.targetseguridad.com
www.cctv.bfioptilas.com
www.whitepapers.zdnet.com
www.ipcctvcameras.co.uk
www.paguito.com
www.geocities.com
www.linksys.com/
www.hard-h2o.com
www.infinova.com

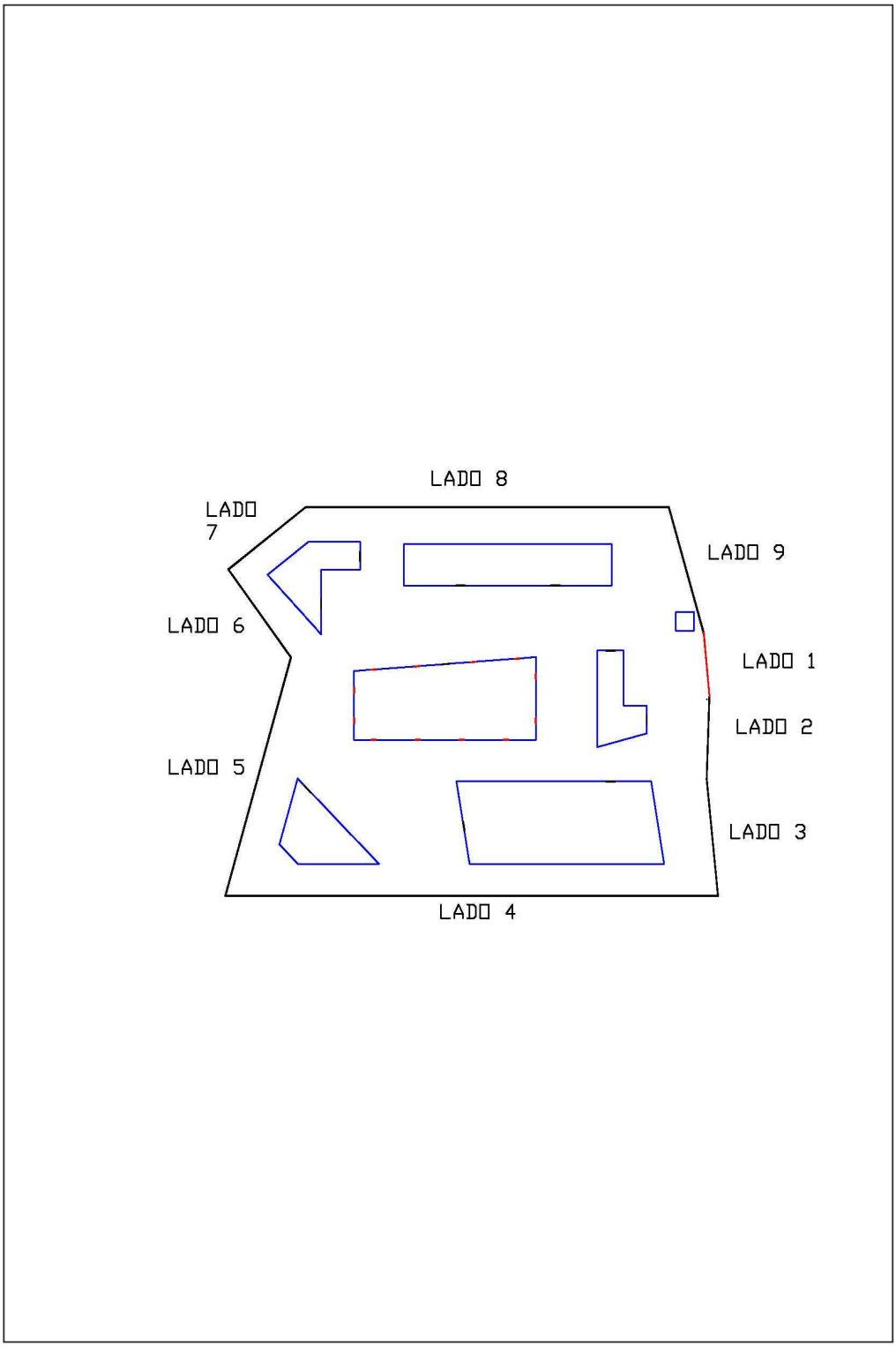
www.turson.com
www.configurarequipos.com
www.integra-ups.com
www.casmar.es
www.indigovision.com
www.euroshop.de
www.dipsoft.com
www.domaut.com
www.solostocks.com
www.twenga.es
www.teknicenter.com
www.acuista.com
www.domaut.com
www.linksys.com
www.soloingenieria.net
www.clasedigital.com
www.ip-center.es
www.construmatica.com

7. Glosario

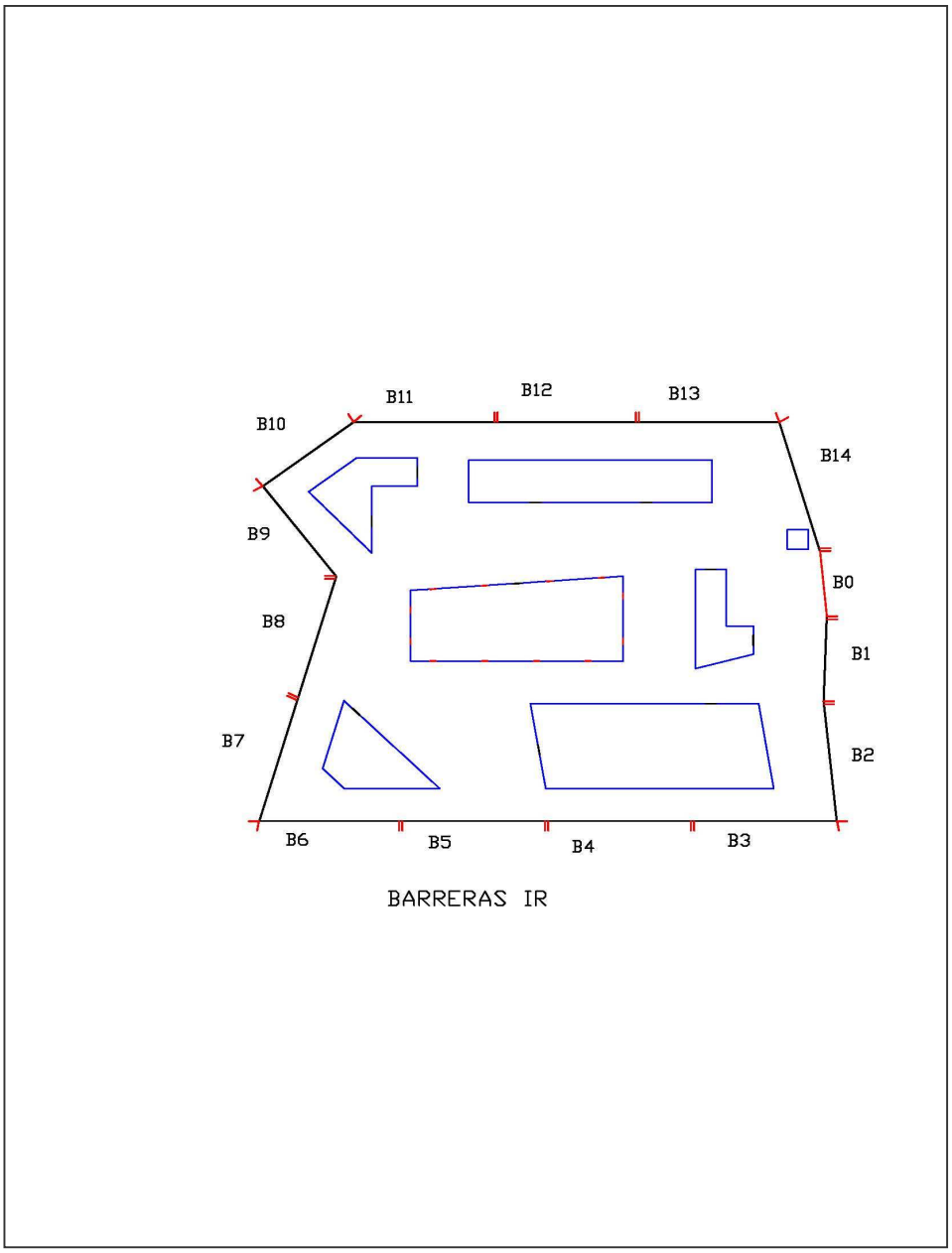
CCTV	Circuito Cerrado de Televisión
IPS	Imagen Por Segundo
FPS	Frames Per Second
PTZ	Pant/Hill/Zoom
DVR	Digital Video Recorder
MPEG	Moving Pictures Expert Group
MJPEG	Motion JPEG
JPEG	Joint Photographic Experts Group
RFL	Resistencia Final de Línea
NA	Normalmente Abierto
NC	Normalmente Cerrado
IR	Infrarrojo
E/S	Entrada/Salida
I/O	Input/Output
POE	Power Over Ethernet
IP	Internet Protocol
IEEE	Institute of Electrical and Electronics Engineer
FO	Fibra Óptica
MM	Multimodo
SAI	Sistema de Alimentación Ininterrupida
STP	Spanning Tree Protocol
PAT	Port Address Translation

ANEXO A: PLANOS

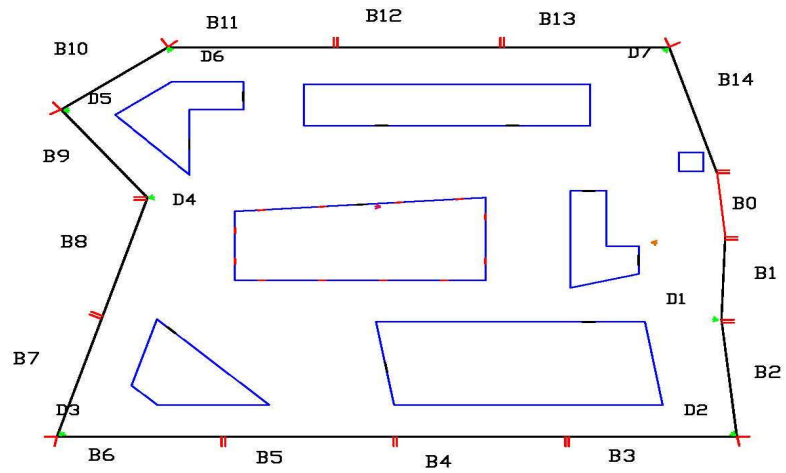
Plano 1. PLANO GENERAL



Plano 2. BARRERAS

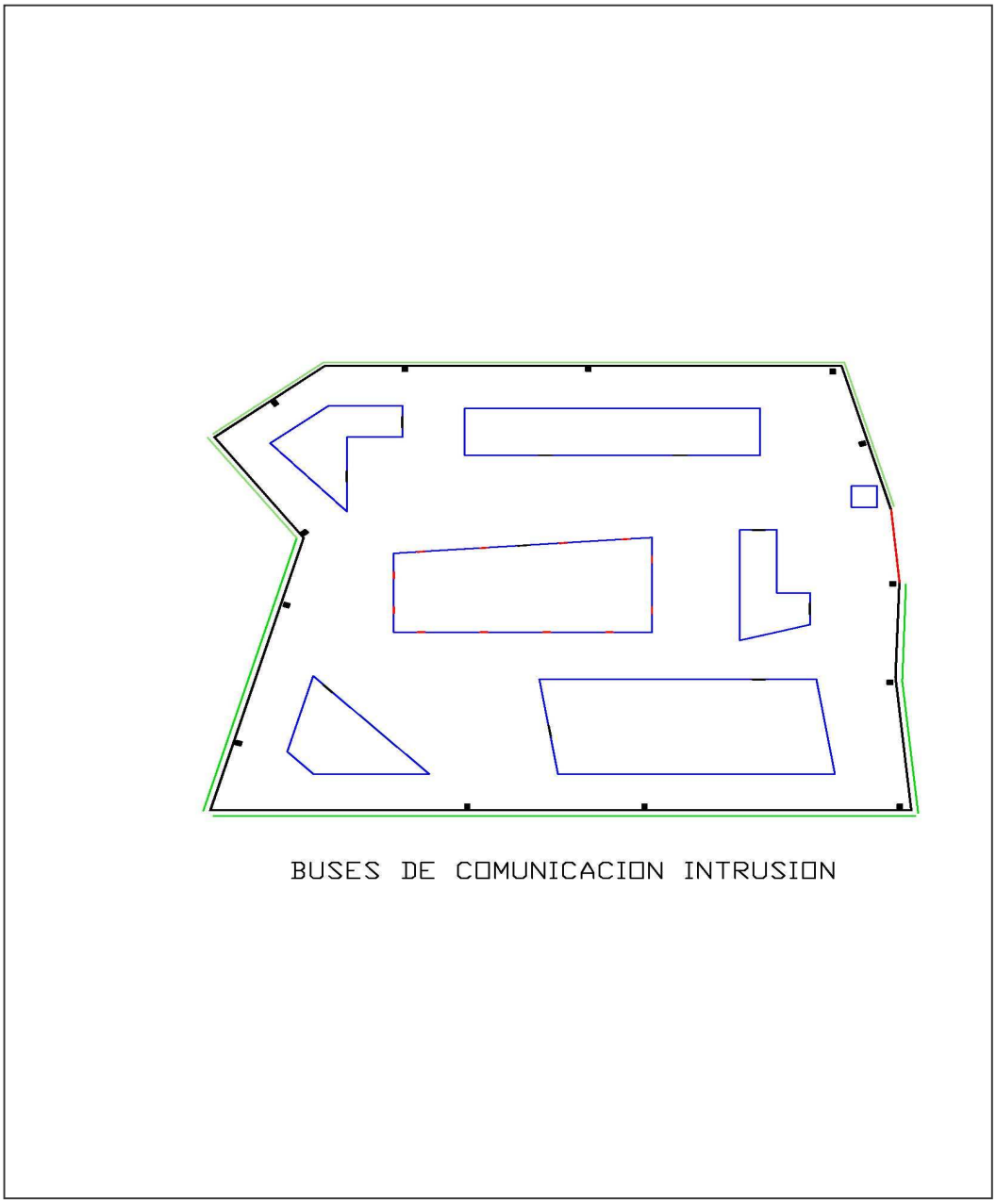


Plano 3. BARRERAS Y DETECTORES

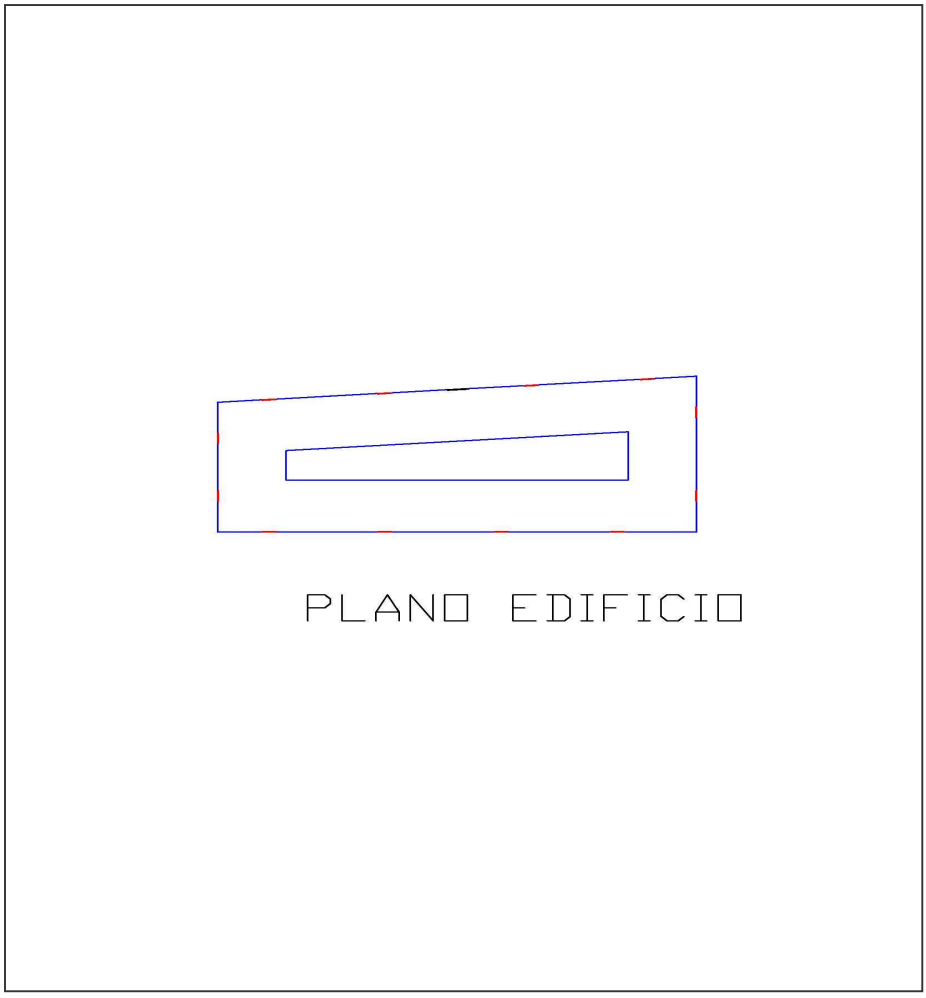


BARRERAS IR Y DETECTORES CORTINA

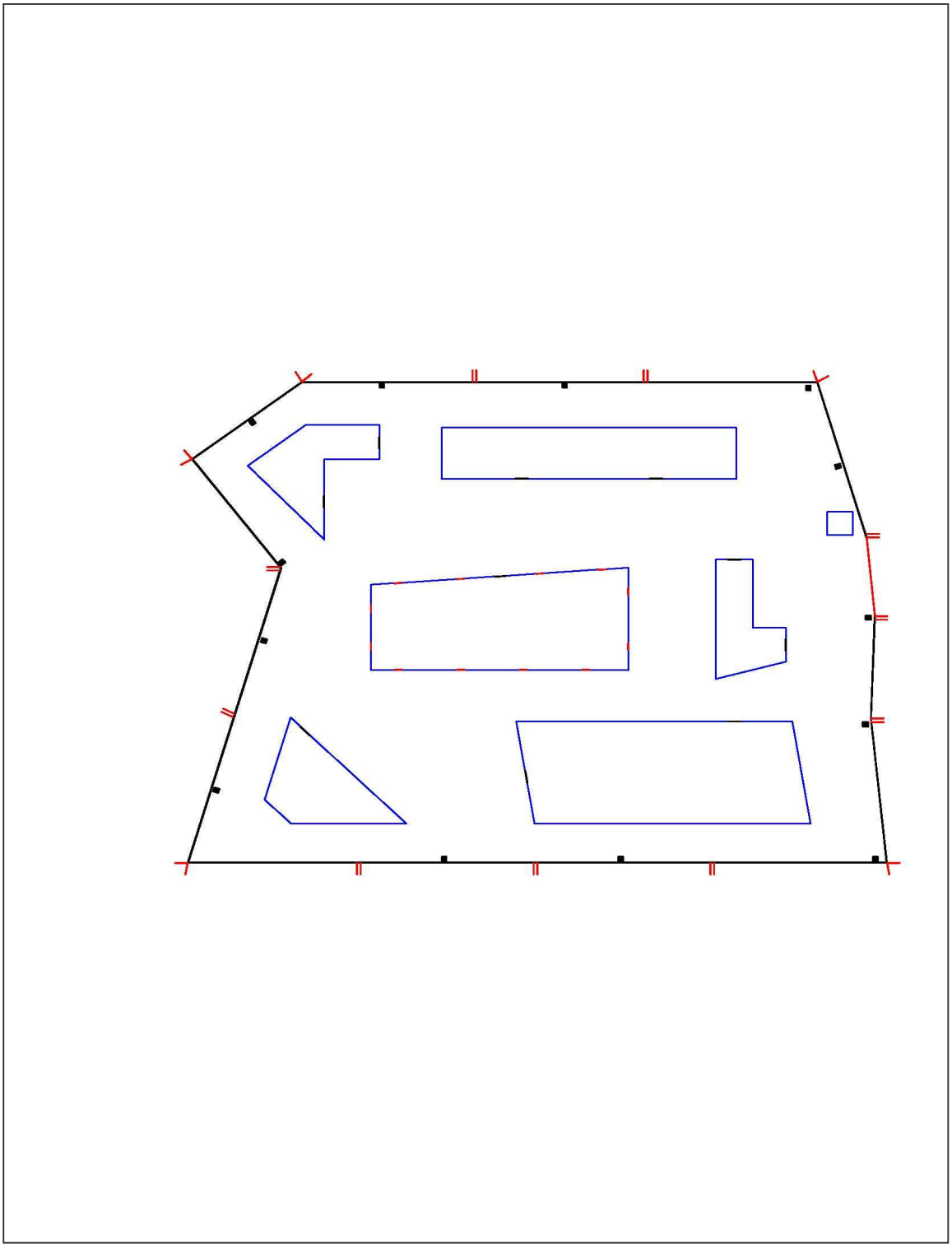
Plano 4. BUSES DE COMUNICACIÓN



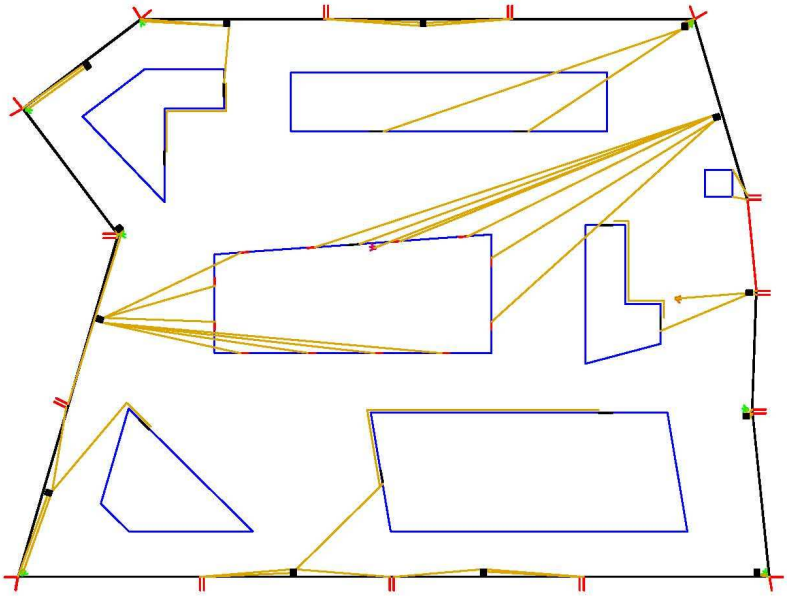
Plano 5. EDIFICIO CENTRAL



Plano 6. RIOS

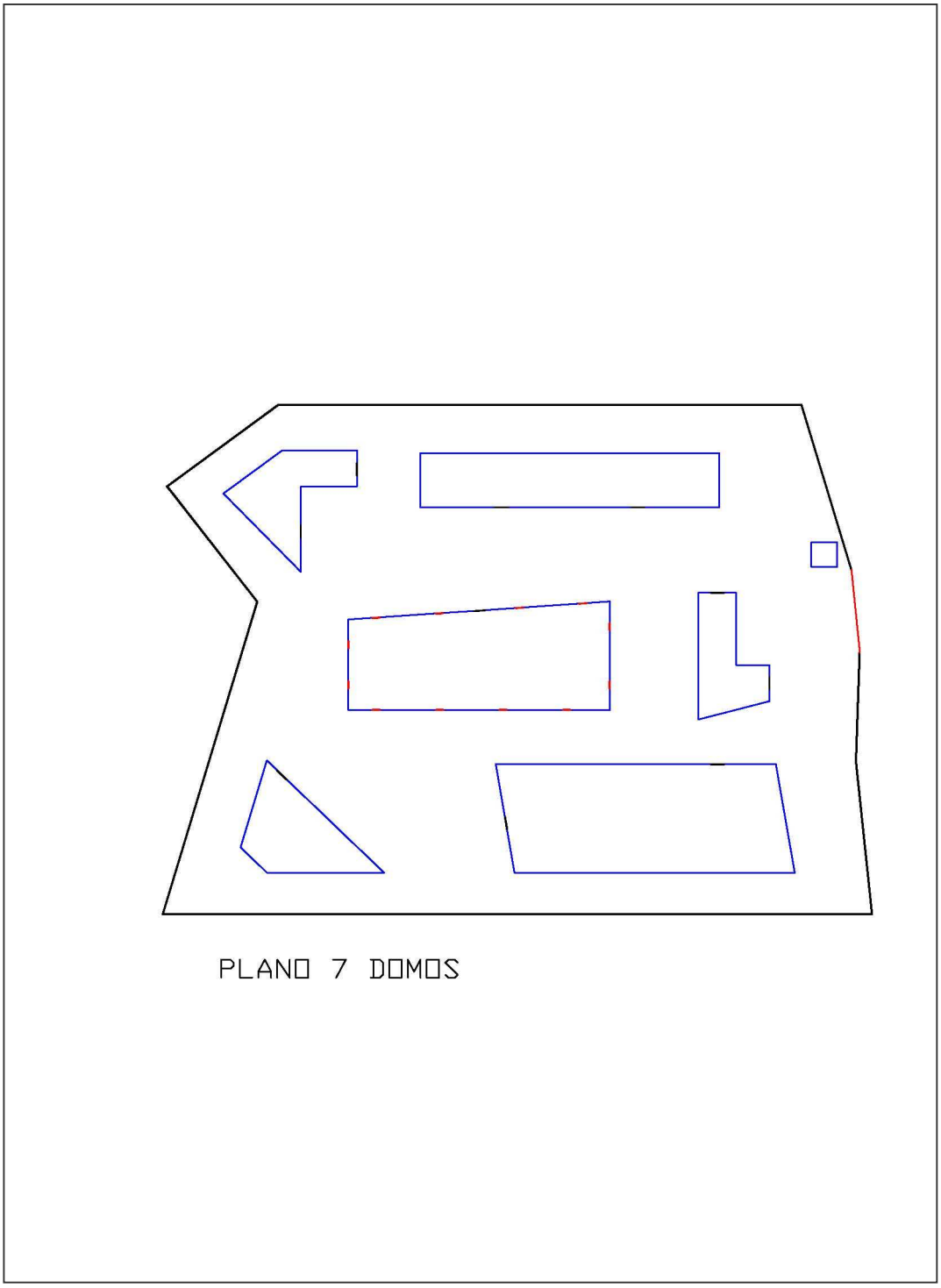


Plano 7. COMUNICACIONES RIOs

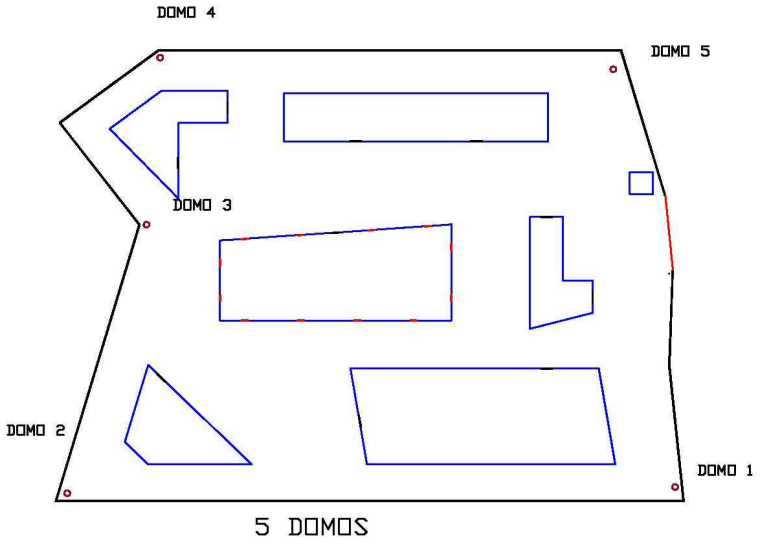


CONEXIóN RIOS

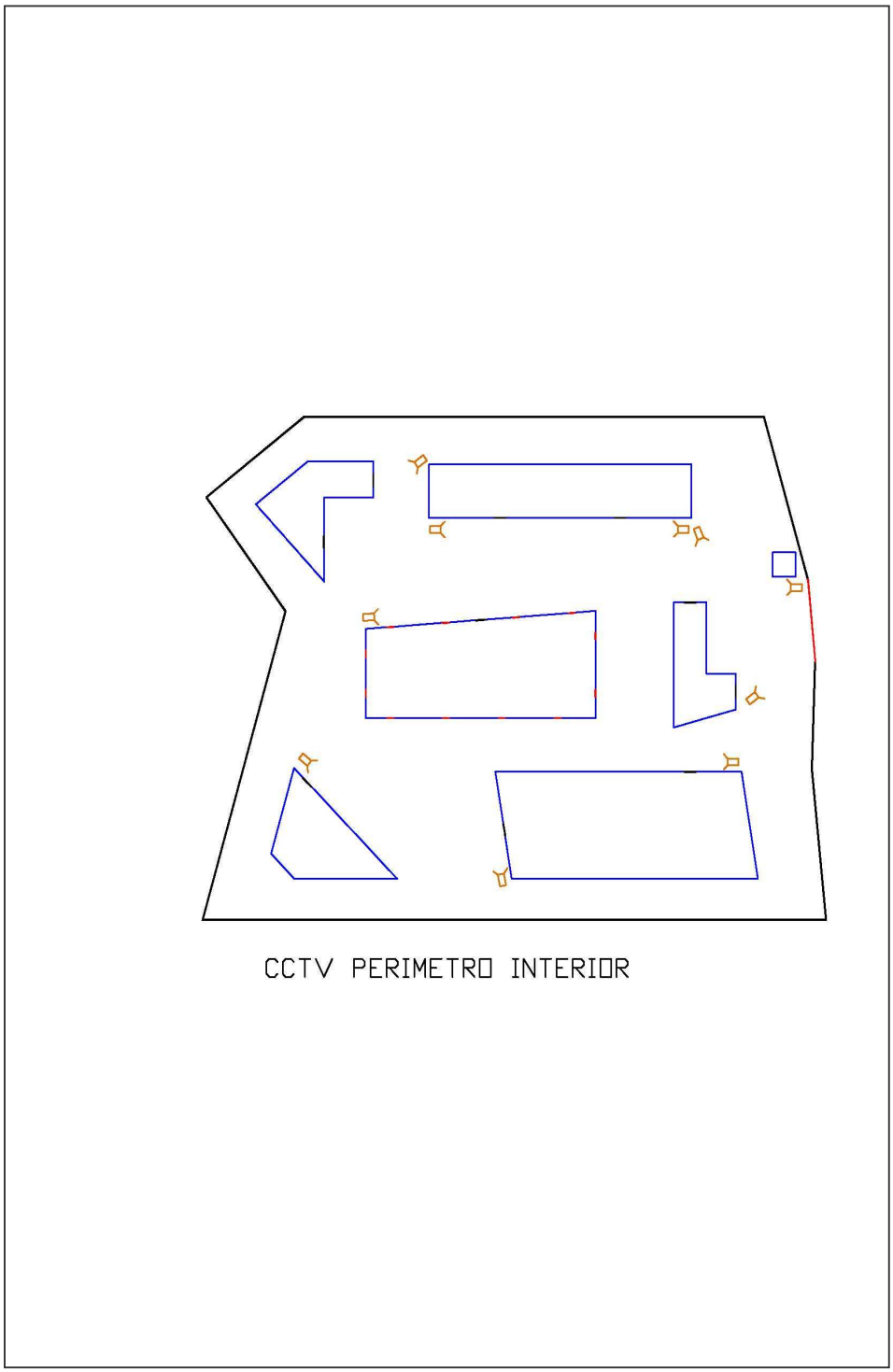
Plano 8. 7 DOMOS



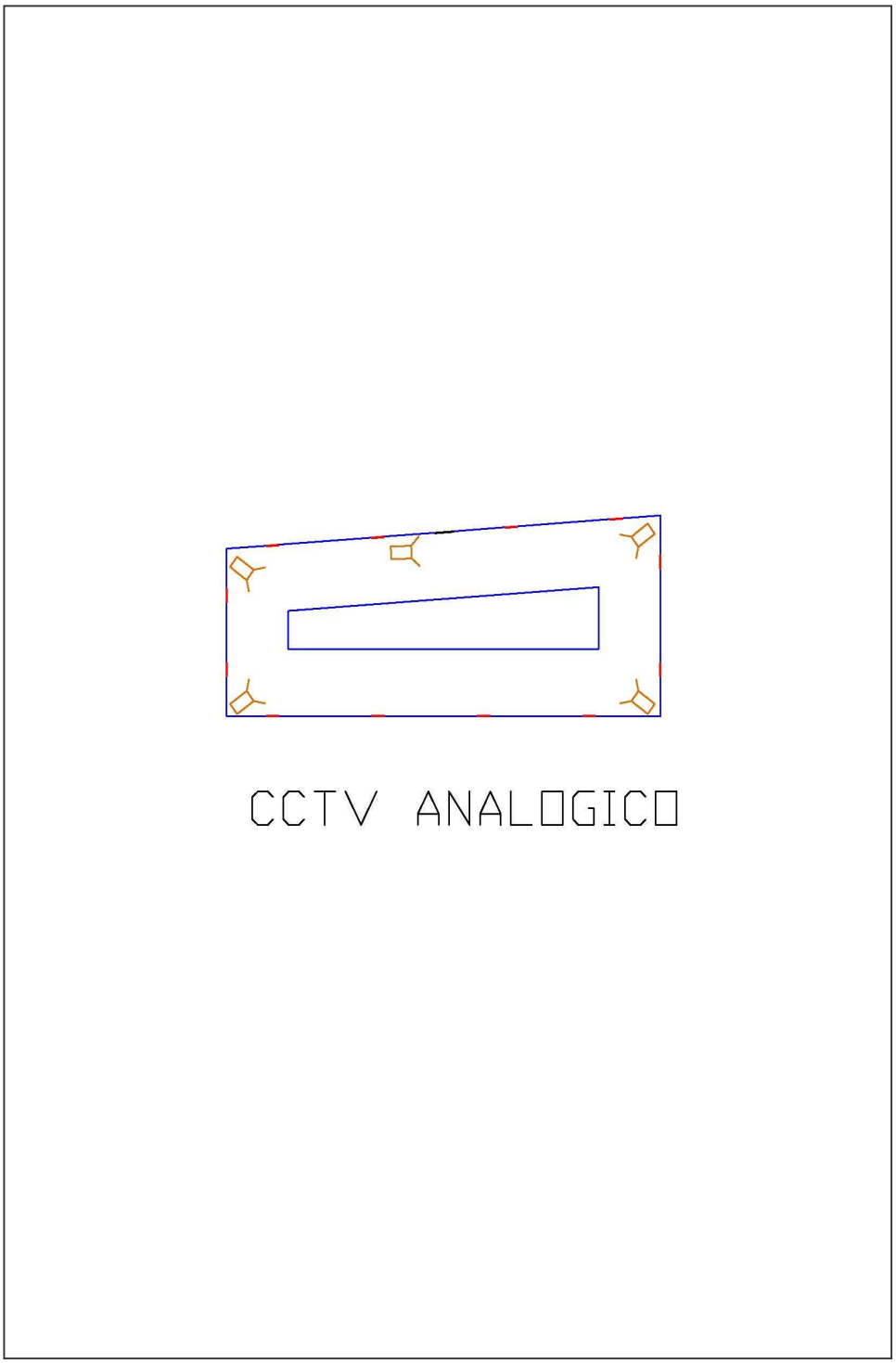
Plano 9. 5 DOMOS



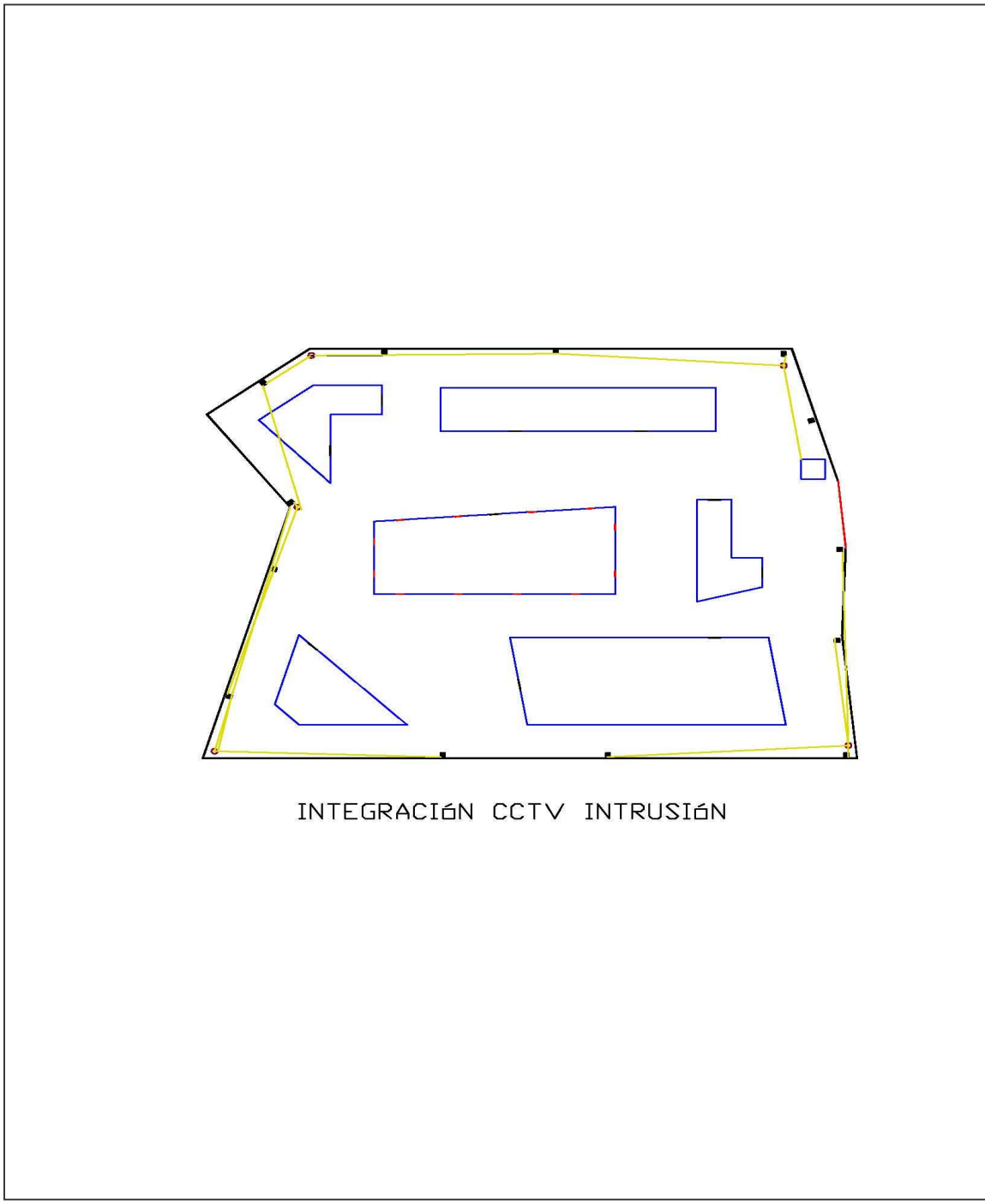
Plano 10. CCTV PERIMETRO INTERIOR



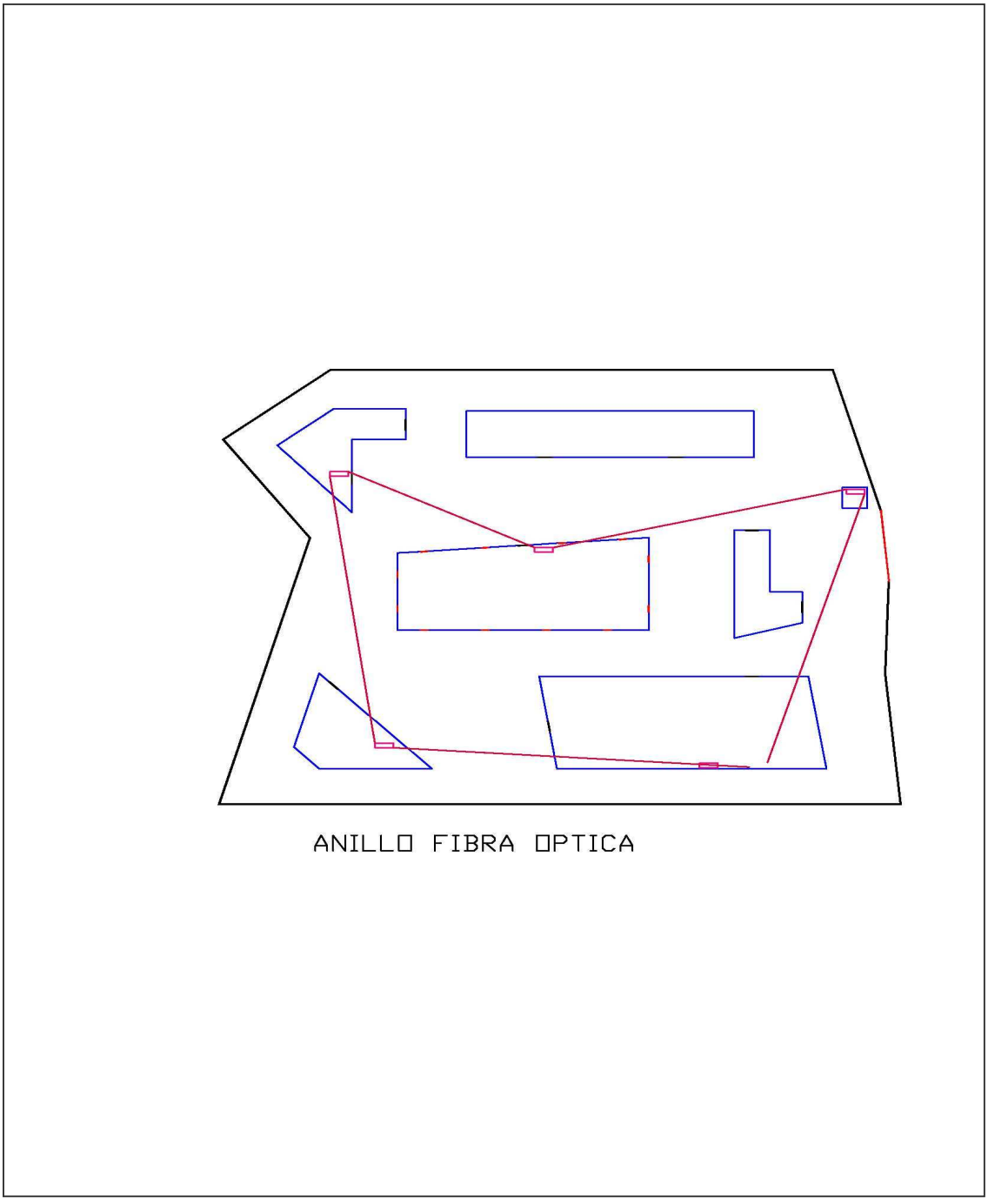
Plano 11. CCTV ANALÓGICO



Plano 12. INTEGRACIÓN CCTV INTRUSIÓN



Plano 13. ANILLO FO



ANEXO B: HOJAS TÉCNICAS EQUIPOS

Barrera IR

HAZ SENSOR
FOTOELECTRICO

Serie Quad Inteligente

PB-IN-50HF Exterior 50m
PB-IN-100HF Exterior 100m
PB-IN-200HF Exterior 200m

PULNiX

El equipo Pulix Quad inteligente de haz fotoeléctrico esta especialmente diseñado para protección exterior. Los haces Quad están sincronizados para trabajar conjuntamente y reforzar el rango y la estabilidad en condiciones ambientales sev. Los haces de las series PB-IN-HF están equipados con muchas prestaciones las cuales facilitan un amplio campo de selección de opciones. Estas opciones resultan en una considerable flexibilidad para una variedad de aplicaciones necesarias.

Características

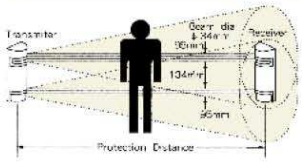
- 4 Infrarrojos Sincronizados de Alta Potencia (patentado)
  - 4 haces están "y forman barrera", para prevenir falsas alarmas desde caida de hojas o pequeños animales.
  - La transmisión activa del infrarrojo es excepcionalmente potente con una distancia máxima de llegada diez veces superior a la distancia de protección especificada.
  - La luz externa del circuito de compensación proporciona una excelente tolerancia, contra la luz solar, las luces de los automóviles, la luz fluorescente o la luz de mercurio.
- Selecciones de Cuatro Frecuencias
  4 posibilidades separadas de frecuencia evitan llamada cruzada en instalaciones apiladas o en instalaciones lineales largas.
- Selección de Potencia del Haz Transmisor
  Pueden ser establecidos 2 niveles de potencia de transmisión para ajustar la distancia de protección.
- Cierre de Auto Ganancia
  La sensibilidad optima de ganancia es fijada automáticamente para cubrir cualquier distancia para una distancia máxima de protección. El cierre o fijación de la Auto Ganancia es fácilm confirmada por el sonido de chequeo.
- Fácil Alineamiento del Haz
  - Alineamiento mediante una señal audible (Modelo Utilitario) tono de alineamiento hace posible con rápido ajuste de los haces. El tono se incrementar al máximo en el pico de nivel del haz.
  - Luces Led de atenuación de la sensibilidad creando el nivel d haz es atenuado el cual indica baja sensibilidad.
  - Clavija de salida del monitor.
- AGC Programado
  La sensibilidad aumenta automáticamente en malas condicion atmosféricas para contrarrestar la niebla, lluvia fuerte, escarch nieve.
- Memoria de alarma
  El Led de memoria de alarma está localizado en el receptor y puede ser automáticamente rearmodo (5 minutos después de la alarma, parpadeando durante 55 minutos, entoces se rearma automáticamente) o puede ser controlado manualmente.
- Módulo ambiental incluido
  La señal de dificultad ambiental es enviada cuando el nivel de Recepción del haz se reduce por debajo de un nivel aceptable.
  - Ajuste de amplitud (horizontal ±90°, vertical ±10°).
  - Salida de tamper.
  - Excelente cobertura anti-golpe de policarbonato.
  - Accesorios opcionales

Especificaciones

Modelo	Haz Sensor Fotoeléctrico (Serie Quad Inteligente)		
Modelo N°	PB-IN-50HF	PB-IN-100HF	PB-IN-200HF
Sistemas de Detección	Sistemas de interrupción próximo al haz infrarrojo (TR-RE. Interrupción simultanea de 4 haz infrarrojo)		
	Double modulación pulsed beam by LED		
Distancia de protección	Exterior 50m o menos	Exterior 100m o menos	Exterior 200m o menos
Max.Distancia de alcance	Décuplo 500m	Décuplo 1000m	Décuplo 2000m
Tempo de respuestas	De 50mseg. A 700mseg. Variable (Estándar: 50mseg.)		
Alimentación elétrica	12V a 30V DC (no polaridad)		
Consumo corriente	60mA o menos a la protección (Max. 95mA o menos)	70mA o menos a la protección (Max. 105mA o menos)	85mA o menos a la protección (Max. 120mA o menos)
Salinda de alarma	Relé de salida por contacto seco: 1c Rearme: Tiempo de Interrupcion + off - retardo (aprox. 1.5 seg.) Contacto de Capacidad: 30V AC/DC, 0.1° o menos		
Salida de ambiental	Contacto de relé seco: 1a o 1b (sobre interruptor) Contacto de operación: Salida cuando la condición ambiental empeora Contacto de capacidad: 30V AC/DC, 1° o menos		
Salida de Tamper	Relé de contacto seco: 1b Contacto de operación: Salida cuando se manipula la cubierta del receptor. Contacto de capacidad: 30V AC/DC, 0.1° o menos		
LED de alarma	LED rojo del receptor se ilumina cuando se inicia una alarma.		
LED Atenuación de Sensibilidad	LED rojo del receptor se ilumina cuando la recepción del haz es atenuado		
Funciones	Selección de frecuencia del haz modulado. Indicador de tono. Selección de potencia del haz. Indicación de memoria de alarma, AGC programado, Función de cierre de auto ganancia, Jack de Monitor		
Adjuste de HAZ	Horizontal: ±90°, Vertical: ±10°		
Temperatura Ambiente	- 13°F to +140°F (-25°C to + 60°C)		
Posición de instalación	Exterior		
Cableado	Terminales		
Peso	Transmisor : 1200 gramos Receptor : 1300 gramos		
Apariencia	Rojo vino - Resina PC		

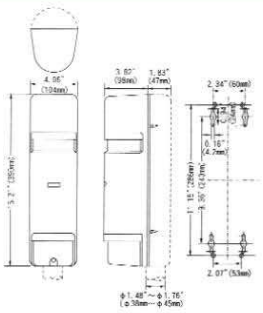
Debido a constantes mejoras, las especificaciones pueden cambiar sin previo aviso.

Cobertura



PB-IN-50HF : Exterior 50m
PB-IN-100HF : Exterior 100m
PB-IN-200HF : Exterior 200m

Dimensiones Externas



Cerramiento del haz

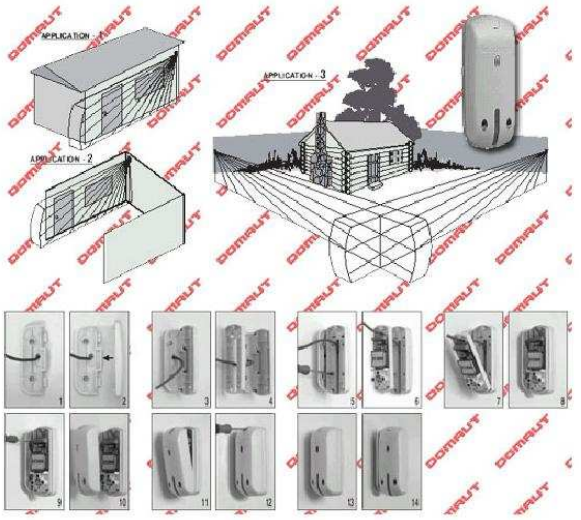
BT175
BT175W

Note : Este sensor está diseñado para la detección de intrusiones y para iniciar la alarma, no es un equipo para prevenios. PULNIX no es responsable de los daños o pérdidas causadas por accidente, robo, actos de Dios, (incluyendo descaducturas o rayos), abusos, maltratos, uso anormal, fallos de instalación o mantenimiento impropio.

TURSON, S.A.
C/ Corazón de María 5
28002 - Madrid (Spain)
Tel: +34 914152502
+34 934354608
Fax: +34 914134775
Email: turson@arrakis.es
Internet: www.turson.com

PB-IN-50HF DS-07 01

Detector de cortina



DESCRIPCIÓN:

Detector de movimiento tipo cortina cableado. Se combinan 3 tecnologías, microondas, infrarrojos pasivos e infrarrojos activos más detector de vibración, para asegurar la máxima seguridad y evitar posibles falsas alarmas. Es un producto tecnológicamente avanzado, 1 sensor PIR de cuatro elementos y microondas bajo una misma carcasa, sistema antimasking, microprocesador con algoritmos de movimiento humano, preparado para todo tipo de clima, lluvia directa, niebla, radiación solar, inmunidad animal, circuito anti RFI, rayos, etc. Contactos de Relé libres de potencial (NA) para señales de alarma, apertura de puertas, encendido de luces, activación de sistemas de grabación ... (Recuerde este detector no permite activar cargas directamente). Alimentación 12VDC y bajo consumo.

CARACTERÍSTICAS TÉCNICAS:

ü **Detector de exterior de cortina**.
ü Doble tecnología PIR + MICROONDAS y ANTI ENMASCARAMIENTO.
ü 1 SENSOR PIR de 4 elementos.
ü Tecnología MICROONDAS a 24,125Ghz.
ü Resistente a la lluvia (todo tipo de clima).
ü Análisis de señal **microprocesado**.
ü **Inmunidad animal.**
ü Protección contra intentos de ocultación de las ópticas PIR con aerosoles.
ü Infrarrojos activos contra intentos de ocultación del detector con objetos sólidos.
ü Compensación de temperatura adaptativa.
ü Sensibilidad MICROONDAS ajustable.
ü Posibilidad de combinar tecnologías: funciones OR/AND.
ü Área de detección 12 metros.
ü Campo de detección (3º).
ü Velocidad de detección movimiento: de 0,1m/s a 5m/s.
ü Alimentación: 9 a 14V.
ü Consumo en reposo: 20mA a 12V.
ü Consumo Máx. (Alarma): 30mA a 15V.
ü Impulso de alarma: 2 seg.
ü Salida de alarma: RELÉ N.C. (24VDC – 0,1A máx.)
ü TAMPER switch: N.C. (24VDC - 0,1A máx.)
ü Contacto anti-enmascaramiento: N.C (24VDC - 0,1A máx.)
ü Retraso alarma por enmascaramiento: 2 minutos.
ü Contacto TEMPER: N.C (0,1A/28VDC máx.)
ü TAMPER switch: N.C.
ü Alta inmunidad EMI y RFI: desde 20V/m, DC hasta 1GHz.
ü Protección frente a rayos.
ü Humedad de trabajo: 95% máx.
ü **Temperatura de trabajo: -37ºC a 70ºC**
ü Material chasis: ABS.
ü Dimensiones: tamaño súper reducido

Cámara IP fija

PIXORD-428 La cámara IP **PIXORD-428 es un modelo DÍA/NOCHE basado en un CCD 1/3" SONY INTERLACED con IRIS Mecanico** y una **luminosidad mínima de 0 LUX** gracias a sus potentes **Iluminadores de Infrarojo** que nos permiten alcanzar una distancia de **visión de entre 80 y 100 metros** en condiciones nulas de luminosidad. Incorpora un **lente de varifocal de 7,5 a 50 mm**. Esta **construida en Aluminio resistente** que le permite soportar la instalación en exteriores gracias a su **protección Ip66.** Los ajustes se realizan de manera sencilla gracias a su tapa de fácil apertura.

Sensor CCD	SONY 1/3" INTERLACED	**Luminosidad**	0 LUX IR ON
Compresión	MPEG-4 / MJPEG dual streaming	**Maxima resolución en red**	720x576 pixels D1
Resolución	más de 500 TV	**Lente**	Varifocal 7,5 a 50mm
Iris	Mecánico	**Iluminadores**	LED de gran distancia
Protección carcasa	IP66	**Interface de Red**	Ethernet 10/ 100 Base-T
Alimentación	DC 12V	**Consumo**	1A
Dimensiones	135X85x40mm	**Peso**	570 grms.

Domo IP

Infinova

Domo IP: Cámara Domo PTZ con Servidor de Video Integrado.

* **Zoom 18 x 12, 22 x 12, 23 x 12, 26 x 12, 35 x 12**
* **Servidor de video sobre IP incorporado, no se requiere ningún equipo adicional.**
* **Compresión de video MPGE-4 ó MJPEG para óptima calidad de imagen y velocidad de transmisión.**
* **Hasta 128 presets.**

* Véa y controle cámaras desde cualquier punto usando un navegador de internet estándar.
* Autoiris, autofoco, y compensación de luz trasera.
* Velocidad de shutter ajustable (White Dynamic Range).
* Alta velocidad proporcional para Pant y Tilt y giro automático avanzado CCD DSP 1/4".
* Protección de contraseña.
* 3 Patrones programables.
* Posición automática de casa.
* Driver y receptor de multi-protocolos interno

* Datos de PTZ incluidos Manchester, RS-422 y RS-485
* 4 entradas de alarma con salidas de relevadores programables
* Protector de descargas de alto voltaje interconstruido
* Opciones para exteriores incluyen: Antiniebla, calentador incorporado y sistema de circulación de aire
* Excede especificaciones de IP 66 y NEMA 4X
* Menu multilenguaje.

Incluye:
* Software de monitoreo unitario a través del navegador de internet. (Descargar)

Información Técnica :
Domos IP y Sistema Inalámbrico AIRAYA

Servidor de vídeo 4 canales

SERVIDOR AUDIO Y VIDEO WEB 4 C FLEXWATCH 3450 S130703

CARACTERISTICAS TECNICAS

Hardware:	CPU integrado de 32 bit
	Flash de 8 Mbytes/SDRAM: 64 Mbytes
	Hardware MJPEG & MPEG4
	Sistema de funcionamiento Lynux versión 2.4 xx
Requerimientos del Sistema (tiempo real y grabado)	Windows XP, 2000, NT4.0
	Internet Explorer 6.x o posterior
	PC H/W Pentium III 500Mhz o superior
	RAM: 64 MB o superior
Protocolos del Sistemas:	HTTP, TCP/IP,ICMP,SMTP,Telnet, DHCP, ARP, NTP, PPPoE
Vídeo:	4 CIF- 704 x 576 (PAL)
	2 CIF- 704 x 288 (PAL)
	CIF - 352 x 288 (PAL)
	QCIF- 176 x 144 (PAL)
	NTSC/ PAL sensor de vídeo automático
	Calidad de la imagen: 6 niveles de calidad
	MJPEG: Tasa de imagen controlable
	MPEG4: Ancho de banda controlable (tasa de imagen constante y variable)
Transmisión:	Transmisión: 60fps (NTSC)/60 fps (PAL)
Interface:	4 entradas de vídeo y 1 salida quad compuesta
	4 entradas optocopladas o 4 entradas digitales
	4 salidas rele
	Dos puertos serie para consolas, modem (PSTN &GSM), dispositivo serie de entrada/ salida,PTZ, Kit de voz.
	Cada puerto puede ser configurado como un RS-232
	RS-485 o RS-422 (max 115kbit/s)
	Botón de reseteo para configuración de fallo de fabrica
	4 canales de entradas de audio y 1 canal de salida, compresión IMA ADPCM, 4 formato de bit, tasa de muestra de 8 KHz
Características de Seguridad:	Canal con protección de acceso a las cámaras multi usuarios, PTZ, Entrada y salida de alarma, Voz
Servicios Avanzados:	Superior a 24 M de memoria para buffer de pre y post alarma
	Detección de movimiento integrada (más de 144 bloques)

	e-mail, FTP, Buffer de alarma por evento o programada
	Notificación de Ip, Notificación de alarma a el e-mail, ruta CGI por eventos y programados
Control PTZ & UART:	Dispositivo de protocolo PTZ integrado con más de 30 protocolos diferentes de Pelco, Vicon, Kalatel, Sony, Panasonic, Canon, Honeywell
	Comando de control para controlar el dispositivo UART
	Dispositivos de control de X10 para controlar dispositivos conectados a la corriente
Otros:	Detección de perdida de vídeos
	Dial vía PSTN entrada/ salida o moden GSM
	Fecha estampada en el vídeo
	Entrada serie de transmisión de datos con vídeo
	Notificación de IP por e-mail
Soporte desarroyado:	Provee HTTP CGI API
	Kit de desarrollo de control ActiveX
Administración:	Configuración serie, web o telnet
	Sistema de actualización remota via telnet, FTP o navegador web.
Alimentación de la corriente:	12 voltio,4.3 Am, SMPS
Dimensiones:	140mm x 44mm x 155mm
Peso:	1 kg
Temperatura de trabajo:	32º-125ºF (0º-50ºC)
Homologación:	FCC
	CE
	RoHS
Accesorio:	Cable de la consola para sistemas de configuración
	Cable de test LAN
	CD para manual de usuario, Asistente de instalación e Información técnica
	Guia de Instalación rápida
Miscelaneo:	Kit de Voz (FW-V10s)
	Servidor grabador NVR para grabar vídeo de multiples servidores NVR
	Herramienta de conversión AVI compatible con el FW- voyager
	Trabaja con FW-Manager NDVR S/W
	Soporta IP dinámica através de la AOIP

Servidor de vídeo 1 canal (IP PIXORD 1000)

Descripción:

El servidor de vídeo IP PIXORD 1000 permite conectar 1 cámara analógica a una misma dirección IP a través de una red Ethernet. Incorpora un Servidor Web por lo que únicamente hemos de conectarnos a la dirección IP correspondiente desde un Navegador de Internet y tendremos la visualización de la cámara . Sin ningún tipo de software adicional, el servidor de vídeo IP PIXORD 1000 hace fácil la visualización de imágenes a través de Internet y aun más, se puede realizar una grabación de video en local o remotamente asi como enviarnos un email cuando se produzca un alarma predefinida. El servidor de vídeo IP PIXORD 1000 dispone de 1 entradas de vídeo que le permite poder enviar vídeo a través de una Intranet o de Internet usando la conexión Ethernet. Dispone un chipset que le habilita para poder enviar ese vídeo comprimido en tiempo real usando los algoritmos de compresión JPEG y MJPEG. La asignación de la dirección IP para poder acceder a ella es muy sencilla; bien a través de un software de localización denominado IP Installer que se suministra o bien mediante la utilidad ARP. La página Web del servidor de vídeo IP PIXORD 1000 esta basada en JAVA lo que le asegura la máxima compatibilidad con todas las plataformas. Asimismo soporta la ejecución de comandos de control Active-X con el fin de ofrecer el máximo rendimiento con Internet Explorer. El servido de vídeo IP PIXORD 1000 dispone de Detección de Movimiento incorporado, asi como de 4 entradas de alarmas opto acopladas y un rele de salida. Una vez producida la alarma esta se puede comunicar mediante e-mail, FTP, activación de algún dispositivo externo gracias al relé de salida de que dispone o almacenar imágenes en el buffer interno. El servidor de vídeo IP PIXORD 1000 puede ser programada mediante un sencillo Script (instrucciones de programación) que nos permitirá hacer que una vez se produzca una alarma realice unas determinada acciones. Asimismo para usuario más avanzados que deseen realizar aplicaciones más específicas el servidor de vídeo IP PIXORD 1000 dispone de un listado de comandos CGI que nos posibilita un control total del producto. Aunque la opción más recomendable para este tipo de servidores de vídeo IP es utilizar una dirección IP fija en Internet puede soportar direcciones IP dinámicas. Gracias a su especial y cuidado diseño no necesita ventilador para su correcto funcionamiento disponiendo además de un sistema que hace que la cámara se reinicialize cuando detecta un error (Wacthdog). Con el fin de permitir el acceso solo a los usuarios autorizados el servidor de vídeo IP PIXORD 1000 dispone de tres niveles de acceso mediante password. PIXORD es un fabricante reconocido en servidores de vídeo IP y continuamente realiza actualizaciones para sus dispositivos mejorando su rendimiento, estas actualizaciones las podemos incorporar en nuestro servidor de vídeo IP PIXORD 1000 mediante la utilidad FTP, asegurándonos que siempre tendremos nuestra cámara con las últimas novedades y en su máximo rendimiento.

Especificaciones técnicas:

BNC: 1 Entrada de video
CPU: Procesador RISC de 32 Bits
Flash ROM: 2 Mb de memoria
SDRAM: 16 Mb de memoria
RS-232: para control externo desde consola
RS-485: para control de cámaras PTZ
Alarmas: 4 Entradas y 1 relé de salida
RED : Ethernet (10/100 Base-T)
Compresión: JPEG; Motion JPEG
Ajuste de vides: Brillo, Contraste, Matiz, Saturación
Protocolos: TCP/IP, UDP, ARP, ICMP, HTTP, FTP, Telnet, SMTP, DHCP
Res máxima: VGA 704x576
- SIF:320x240
RED: hasta 800Kbytes/seg
Conexiones: 30 simultaneas
Envio de video: Hasta 25 fps modo 1 cámara
Eventos programables: mediante Script con una sencilla guía
Activación por: Tiempo (frecuencia)
- Entrada por GPIO
- Detección de movimiento
- video
- Conexión de Red
- CGI

Acciones: Imágenes mediante FPT a un sitio remoto
- Envio de imágenes mediante E-mail a una cuenta específica
- Salida de relé para activación de dispositivos externos

Asignación de dirección IP: mediante ARP y Ping o usando el software suministrado IP-Installer
Actualización de Software: Local o Remote mediante el uso de FTP
Personalización WEB: mediante FTP y Telnet
Requerimientos del sistema: Navegador estándar Microsoft IE4x/5x o superior
- Netscape 7x ejecutandose sobre Win95/98/NT/2000/XP
- Linux

Protección: mediante tres niveles de Password
Accesorios: CD con software y manuales, guía de instalación rápida
- Cable Ethernet
- Fuente de alimentación
- Soporte para montaje de la cámara
- Cable para convertir el MiniDin a Dsub para conectar puerto Com o GPIO

Switch Gigabit 8 puertos

SWITCH 8 PUERTOS 10/100/1000 GIGABIT RACK CON WEBVIEW Y SNMP

Linksys 8-port 10/100/1000 Managed Gigabit Switch with WebView SRW2008 - Conmutador - 8 puertos - EN, Fast EN, Gigabit EN - 10Base-T, 100Base-TX, 1000Base-T + 2 x SFP compartido (vacías) - 1U

Linksys es el líder en la industria de soluciones de conectividad y banda ancha para pequeñas y mediana empresas (PyMEs). Cada producto **Linksys** ha sido diseñado para darle la mayor velocidad, el menor precio, la simplicidad para conectar y operar, y la mejor compatibilidad con la mayoría de los sistemas operativos de red. Las soluciones de **Linksys** se diseñan para empresas que desean el mayor rendimiento de red posible.

GENERAL	*Tipo de dispositivo:* **Conmutador** *Tipo incluido:* **Externo - 1U** *Anchura:* **43 cm** *Profundidad:* **35 cm** *Altura:* **4.4 cm** *Peso:* **3.3 kg**
CONEXIÓN DE REDES	*Cantidad de puertos:* **16 x Ethernet 10Base-T, Ethernet 100Base-TX, Ethernet 1000Base-T** *Velocidad de transferencia de datos:* **1 Gbps** *Protocolo de interconexión de datos:* **Ethernet, Fast Ethernet, Gigabit Ethernet** *Tecnología de conectividad:* **Cableado** *Modo comunicación:* **Semidúplex, dúplex pleno** *Protocolo de conmutación:* **Ethernet** *Indicadores de estado:* **Estado puerto, actividad de enlace, sistema** *Características:* **Control de flujo, auto-sensor por dispositivo, negociación automática, señal ascendente automática (MDI/MDI-X automático)** *Cumplimiento de normas:* **IEEE 802.3, IEEE 802.3u, IEEE 802.1Q, IEEE 802.3ab, IEEE 802.1p, IEEE 802.3x, IEEE 802.1x**
EXPANSIÓN / CONECTIVIDAD	*Total ranuras de expansión (libres):* **2 (2) x SFP (mini-GBIC)** *Interfaces:* **16 x red - Ethernet 10Base-T/100Base-TX/1000Base-T - RJ-45** **1 x gestión**
DIVERSO	*Cumplimiento de normas:* **CE, CSA, EN 60950, UL 1950**
ALIMENTACIÓN	*Dispositivo de alimentación:* **Fuente de alimentación - interna** *Voltaje necesario:* **CA 120/230 V**
PARÁMETROS DE ENTORNO	*Temperatura mínima de funcionamiento:* **0 °C** *Temperatura máxima de funcionamiento:* **50 °C** *Ámbito de humedad de funcionamiento:* **20 - 95%**

Switch Gigabit 16 puertos

SWITCH GESTIONABLE 16 PUERTOS 10/100/1000 + 2 PUERTOS EXPANSION MINI GBIC. GESTION WEB SMART Y RACK

16 puertos 10/100/1000 Gigabit con WebView. Este nuevo conmutador de montaje en soporte **Linksys** permite una conmutación a velocidad de cable y sin bloqueos, además de ofrecer diversas opciones para la conexión a la red troncal. Los 16 puertos 10/100/1000 aumentan la velocidad de las estaciones de trabajo. Además, los dos puertos mini-GBIC permiten la expansión en el futuro a otros medios de transmisión alternativos, como la fibra óptica. Incluye monitorización WebView y configuración mediante explorador Web, lo que facilita la administración de 64 redes VLAN y hasta 8 grupos de sistemas de radiotelefonía cerrados (trunking). O, si lo prefiere, puede utilizar el puerto consola integrado para configurar el conmutador.
Apto para montaje en RACK

GENERAL	*Tipo de dispositivo*: **Conmutador** *Tipo incluido*: **Externo - 1U** *Anchura*: **43 cm** *Profundidad*: **35 cm** *Altura*: **4.4 cm** *Peso*: **3.3 kg**
CONEXIÓN DE REDES	*Cantidad de puertos*: **16 x Ethernet 10Base-T, Ethernet 100Base-TX, Ethernet 1000Base-T** *Velocidad de transferencia de datos*: **1 Gbps** *Protocolo de interconexión de datos*: **Ethernet, Fast Ethernet, Gigabit Ethernet** *Tecnología de conectividad*: **Cableado** *Modo comunicación*: **Semidúplex, dúplex pleno** *Protocolo de conmutación*: **Ethernet** *Indicadores de estado*: **Estado puerto, actividad de enlace, sistema** *Características*: **Control de flujo, auto-sensor por dispositivo, negociación automática, señal ascendente automática (MDI/MDI-X automático)** *Cumplimiento de normas*: **IEEE 802.3, IEEE 802.3u, IEEE 802.1Q, IEEE 802.3ab, IEEE 802.1p, IEEE 802.3x, IEEE 802.1x**
EXPANSIÓN / CONECTIVIDAD	*Total ranuras de expansión (libres)*: **2 (2) x SFP (mini-GBIC)** *Interfaces*: **16 x red - Ethernet 10Base-T/100Base-TX/1000Base-T - RJ-45** **1 x gestión**
DIVERSO	*Cumplimiento de normas*: **CE, CSA, EN 60950, UL 1950**
ALIMENTACIÓN	*Dispositivo de alimentación*: **Fuente de alimentación - interna** *Voltaje necesario*: **CA 120/230 V**
PARÁMETROS DE ENTORNO	*Temperatura mínima de funcionamiento*: **0 °C** *Temperatura máxima de funcionamiento*: **50 °C** *Ámbito de humedad de funcionamiento*: **20 - 95%**

Adaptador switch FO

LINKSYS MGBLH1

Funciones del Producto

Gigabit Ethernet SX Mini-GBIC SFP Transceiver

- easy-to-install
- can achieve distances up to 220 or 550 meters

Descripción de producto

This easy-to-install Mini-GBIC (or SFP) module provides a simple way to add Gigabit functionality to your Linksys switch. Gigabit fiber is often used to connect two switches together. The technology used depends on the distance between the two switches.

The SX module uses 850 nanometer wavelength light in multimode fiber optic cables, and can achieve distances up to 220 or 550 meters, depending on the fiber used:

- 62.5/125um MMF @ 160 MHz/km, up to 220m
- 62.5/125um MMF @ 200 MHz/km, up to 275m
- 50/125um MMF @ 400 MHz/km, up to 500m
- 50/125um MMF @ 500 MHz/km, up to 550m

For other options, see the 1000Base-T (MGBT1) and LH (MGBLH1) modules.

Más información

» Imágenes de productos

» Imágenes de productos (alta resolución)

» Instalación Rápida pdf

» Legislación sobre los WEEE

» ROHS Compliance

Fibra Óptica

POL. IND. MAS ROGER. C/ BENJAMÍN FRANKLIN, S/N. 08397 PINEDA DE MAR (BARCELONA) SPAIN TEL +34-937 625 553 FAX +34-937 625 831

OPTRAL

MM50

FIBRA ÓPTICA MULTIMODO 50/125

Fibras ópticas multimodo de 50/125 micras de indice gradual. Estas fibras están diseñadas para ser utilizadas en 850 y 1300 nm. Adecuadas para su uso en aplicaciones de cableado como las Redes de Área Local (LAN) con video, datos y voz, utilizando LED, VCSEL o Laser Fabry Perot.

Estas fibras cumplen con IEC 60793-2-10 A1a.1 y A1a.2.

PROPIEDADES GEOMÉTRICAS / MECÁNICAS	VALOR
Diámetro núcleo	50 ± 2.5 µm
No circularidad núcleo	≤ 6 %
Error concentricidad núcleo / revestimiento	≤ 1.5 µm
Diámetro revestimiento	125 ± 2 µm
No circularidad revestimiento	≤ 1 %
Diámetro recubrimiento primario	245 ± 10 µm
No circularidad recubrimiento primario	≤ 6 %
Error concentricidad recubrimiento primario	≤ 12.5 µm
Proof Test	≥ 8.8 N / ≥ 1 % / ≥ 100 Kpsi

Propiedades geométricas conforme a CEI 60793-2-10.

PROPIEDADES ÓPTICAS		OM1	OM2	OM2 XL	OM3 SL	OM3	OM3 XL	Giga
Coeficiente Atenuación (dB/Km)	850 nm	≤ 2.5	≤ 2.5	≤ 2.5	≤ 2.5	≤ 2.5	≤ 2.5	≤ 2.5
	1300 nm	≤ 0.7	≤ 0.7	≤ 0.7	≤ 0.7	≤ 0.7	≤ 0.7	≤ 0.7
Ancho de Banda (MHz x Km)	850 nm	≥ 200	≥ 500	≥ 600	≥ 700	≥ 1500	≥ 3500	≥ 600
	1300 nm	≥ 500	≥ 500	≥ 1200	≥ 500	≥ 500	≥ 500	≥ 1200
Distancia Enlace (m)	1000Base-SX	275	550	550	800	900	1100	750
	1000Base-LX	550	550	550	550	550	550	2000
	10GBASE-SX	33	82	82	150	300	550	110
Apertura Numérica		0.200 ± 0.015						
Índice de Refracción	850 nm	1.482						
	1300 nm	1.477						

Propiedades ópticas conforme a CEI 60793-2, ISO/IEC 11801, EN 50173, TIA/EIA-492AAAC, EIA/TIA 568-B.

optral@optral.com - www.optral.com

Ref: ETW.04.001/01

Central de Alarmas Galaxy

ADEMCO International

DIVISION MICROTECH

galaxy500

Unidad de Control de 500 Zonas. Altas Prestaciones

CARACTERISTICAS GENERALES:

- Opción fin de semana.
- Apertura fuera de hora.
- Anulación de zonas de protección.
- Códigos de usuario temporales.
- Lectores de tarjetas integrados.
- Armados/Desarmados con sistemas MAX.
- Autodiagnosis.
- Teclas de función programables.
- Nombres de usuario.
- Descriptores de zona.
- Busqueda rápida adelante/atrás.
- Protección antisabotaje mecánica.
- Búsqueda registro de 500 eventos.
- 7 niveles de acceso.
- Servicio remoto.
- Menú usuario programable..
- Monitorización Resistencia alta/baja de zonas.
- Cambio automático horario verano/invierno.
- Impresora en línea.
- Polaridad de salidas reversible.
- Programación por teclado ó remota.
- Modo de salidas programable.
- Autoarmado independiente por grupo.
- Cancelación independiente por grupo.
- Ventanas de autoformato semanales.

PANEL DE CONTROL DE INTRUSIÓN Y ACCESOS

La central galaxy500 incorpora el más alto nivel de seguridad requerido por la banca y otras áreas de alto riesgo. Gracias a su versatibilidad, sin embargo, puede asegurar y proteger de forma flexible una amplia gama de establecimientos comerciales y residenciales. De sus multiples cualidades, destacan las siguientes:

- 16 Particiones con Auto- Armado.
- Funciones de seguridad controladas por tiempo.
- Lectores de control de accesos integrados.

FLEXIBILIDAD

Flexibilidad operacional gracias a su diseño innovador:

- Se puede programar para uso multi-funcional.
- Fácilmente expandible.

MANEJO SENCILLO

De fácil manejo y sin complicaciones:

- Fácil de programar.
- Necesita un mínimo de manipulación para operar.

ADEMCO microtech

GALAXY500-HT-R01 11/99

Módulo expansor de zonas

Honeywell

RIO/B

Módulo Expansor Multiplexado

Si necesita ampliar una instalación de sistemas galaxy, encontrará la respuesta en el módulo expansor rio. El módulo rio proporciona hasta 32 ZRF adicionales y 4 salidas lógicas programables.

Caracteristicas:

- Módulo expansor multiplexado de 8 zonas identificadas individualmente y con doble balanceamiento + 4 salidas lógicas programables, para ampliación de sistemas galaxy
- Se suministra en caja metálica auto protegida por tamper de dimensiones 175x155x25.

Honeywell Security & Custom Electronics
C/ Mijancas nº1, 3ª planta
Poligono Industrial Las Mercedes
28022 Madrid
España
Tel : +34 902 667 800
Fax : +34 902 932 503
Email : seguridad@honeywell.com
www.honeywell.com/security/es

HSCE-RIOB-02-ES(02/06)DS-C
Febrero 2006

SAI


Domésticos, Pymes y TPV
Redes y Cableado
Comunicaciones y Telefonía
Industriales y Automatismos
PLUS
GAMA DE SAI INTERACTIVOS. 500 a 2.000VA
Su Tecnología Interactiva entrega una alimentación estabilizada a su ordenador, además de brindar un amplio margen de entrada lo cual asegura una larga vida útil de las baterías.
Nuestra Insuperable Garantía se ejerce por teléfono o e-mail y durante los 3 primeros años de operación, los SAI defectuosos son reemplazados In Situ, sin gastos de portes ni de otra índole. Incluye las fallas de baterías
GARANTIA Reemplazo IN SITU
3 AÑOS
www.integra-eu.com
902.36.38.13
Con la función de Arranque en Frío podrá encender sus equipos informáticos aún en ausencia de electricidad y su SAI PLUS funcionará como un Generador Eléctrico.
Software de Control y cable de comunicación incluido para la eficiente gestión de todas las prestaciones del SAI. Además de impedir la pérdida de datos ante fallas prolongadas de la electricidad, permite notificar alarmas y eventos por e-mail, SMS o la red.
Gracias a los modelos de baterías de la gama PLUS, podrá disfrutar de una Autonomía Extendida y la tranquilidad necesaria para terminar sus trabajos críticos aunque falle la electricidad.
Para las aplicaciones más exigentes en las que deba ampliar la autonomía de la gama, están los modelos PLUS 1K Ex, 1.4K Ex y 2K Ex con Baterías Externas y toda la autonomía que necesite.
La Protección Total de los SAI PLUS, protege sus equipos informáticos contra Fluctuaciones de Voltaje, EMI / RFI y Picos Eléctricos en la Línea de CA, de Teléfono o Ethernet 10/100 Mb.
Integra
Moderna interfaz para supervisar el SAI
Conexión directa y sencilla de sus equipos informáticos
Protección para su conexión de Voz y Datos: Fax / Módem / ADSL / Ethernet 10/100 Mb, todo con el mismo puerto de conexión
Integra TECH
www.integra-eu.com

GAMA PLUS 500 A 2.000VA

En la gama PLUS, los usuarios de aplicaciones informáticas encuentran gran facilidad de instalación gracias a sus tomas de salida DIN y protección de la línea de voz y datos. De la misma manera, la eficiente gestión del SAI puede fácilmente optimizarse mediante el flexible y profesional software que incluyen: ***WinPower.***

Por otra parte, las capacidades de la gama cubren las necesidades de prácticamente cualquier instalación informática.

Todo esto nos permite afirmar que la gama PLUS es la alternativa perfecta en aplicaciones informáticas domésticas, oficina y redes pequeñas .

PLUS 500-700VA

PLUS 1 / 1.4 / 2 K

1. Puerto USB
2. Puerto Serie
3. Protección de Voz/Datos
4. Entrada CA
5. Disyuntor de entrada
6. Salidas Protegidas

	Modelo	Plus 500	Plus 700	Plus 1K	Plus 1.4K	Plus 2K
Entrada	VA / Watts	500 / 300	700 / 420	1000 / 600	1400 / 840	2000 / 1080
	Voltaje (Vac)	230				
	Margen de Voltaje (Vac)	158 a 290				
Salida	Voltaje (Vac)	230				
	Frecuencia (Hz)	50 ± 1				
	Regulación en Modo Normal	± 10%				
	Tiempo de Transferencia (Típica, mSeg)	4				
	Forma de Onda	Sinusoidal Sintetizada				
Batería	Capacidad y Cantidad	12V/7AH x 1	12V/9AH x 1	12V/7AH x 2	12V/9AH x 2	
	Autonomía (Con un PC y Monitor TFT de 15")	25	30	50	60	60
	Tiempo de Recarga	8 Horas a 90%, luego de una descarga completa				
Indicadores Luminosos	Modo Normal	Piloto Verde Encendido		1er Piloto: Encendido; 2do al 5to Piloto: Nivel de Carga del SAI		
	Modo Inversor	Piloto Verde Parpadeando		1er Piloto: Intermitente; 2do a 5to Piloto: Nivel de Batería Restante		
	Falla de Batería	-------		Piloto Batería (Rojo): Encendido		
Alarmas audibles	Modo Inversor	1 Bip cada 10 Segundos				
	Batería Baja	1 Bip cada ½ Segundo		1 Bip cada Segundo		
	Sobrecarga	-------		2 Bips por Segundo		
	Batería Descargada	Sonido Continuo				
Protecciones	EMI / RFI	Cumple con Norma EN50081-1 ó FCC parte 15 Clase A				
	Picos Eléctricos	Cumple con Norma IEEE-587 Categoría A				
	Variaciones Eléctricas	Regulador de 3 pasos.				
	Corto Circuitos	Fusible (AC y DC) y límite de corriente				
	Línea de Voz y Datos	Para conexiones de: Módem / Fax / ADSL / Ethernet 10/100 Mb				
	Sobrecargas	Fusible, límite de corriente y corte del inversor				
Físicas	Dimensiones Largo x Ancho x Alto (mm)	330 x 100 x 140		370 X 140 X 180		
	Peso Neto (Kg.)	6	6,5	13,8	14,2	16
	Salidas	2 Tomas DIN (Schuko)		3 Tomas DIN (Schuko) (0)		
	Temp. De Operación (°C)	0-40				
	Humedad Relativa	0-90% (No condensante)				
	Ruido	<40 dB @ 1 mtr				
Com.	Interfaz	USB (1)		Puerto Serie DB-9. USB Opcional		
	Plataformas Soportadas	Windows (98, 2000, NT, XP), Novell, Linux (2), Mac OS X				

SOFTWARE

WinPower

El Software de Monitorización y Control de los SAI PLUS es el ***WinPower***, el cual se descarga desde nuestra página web. ***WinPower*** es la perfecta plataforma de gestión tanto para instalaciones mono PC como en red y permite realizar ***shutdowns*** a cualquier ordenador de la red así como enviar notificaciones de eventos o alarmas vía e-mail, SMS o a través de la red.

Las especificaciones pueden cambiar sin previo aviso.
Las marcas registradas y Logos pertenecen a sus propietarios
(0) El PLUS 1K Ex, tiene 2 Tomas DIN y 1 toma para Baterías Externas
(1) La interfaz del PLUS 700S es tipo Serie;
(2) El Linux solo es soportado por los modelos con Puerto Serie

Distribuidor Autorizado

Integra Products
C/ Solsonés 55-57
Pol. Ind. Pla de la Bruguera, 08211
Castellar del Vallés. Barcelona. España
Tel: 902.363.813 - 93 714.4401
Fax: 93 714.4628

Disco Duro

Western Digital MyBook G2NC20000E

Nº Art.: AELW03

494 €

Sea el primero en valorar este producto.

» Valorar este producto

Descripción:

La Western Digital MyBook World Edition II (G2NC20000E) es la solución, para desarrollar una red doméstica local a una capacidad de almacenamiento de 2.0 Terabyte. Después de una instalación sencilla y rápida podrá guardar y compartir inmediatamente música, vídeos, imágenes y otros ficheros a través de un navegador web, tanto desde un PC como de un Mac. Software de seguridad EMC Retrospect Express incluido, un software fácil para el usuario para conseguir protección en un tiempo determinado o medidas de seguridad según las necesidades particulares.

» Especificaciones

La imagen puede diferir del original.

» mostrar más imágenes

» Especificaciones » ocultar

Denominación	Western Digital MyBook G2NC20000E
Formato	USB 2.0
Conexiones	1 x RJ-45 (LAN) 1 x USB 2.0 1 x fuente de alimentación
Tasa de transferencia	LAN 10/100/1000 MBit/s
Capacidad	2 TB
LEDs	1 x LAN Link
Características	Compatible con UPnP, indicador de capacidad de memoria, protección de datos adicional con RAID 0 y 1.
Observaciones	Dos discos duros de 750 GB con 8,9 ms y 7200 rpm, conexión USB-A Host para conexión de otros dispositivos USB
Accesorios	Instrucciones, CD de sofware, cable RJ-45, fuente de alimentación,(12V/4A)con cable de red (D, GB)
Peso	1,9 kg
Medidas (AnxAlxPr)	104 mm x 174 mm x 159 mm

ANEXO C: NORMATIVA SOBRE INSTALACIONES CCTV

Normativa sobre instalaciones de cámaras de CCTV y videograbadores

En relación con la consulta formulada sobre la normativa que regula la instalación de cámaras y videograbadoras de imágenes, por motivos de seguridad, en un establecimiento público, se expone lo siguiente:

En el plano normativo que regula la seguridad privada, la Ley 23/92, de 30 de Julio, de Seguridad Privada, en su artículo 5 y el Reglamento de Seguridad Privada, aprobado por Real Decreto 2364/1994, de 9 de diciembre, en su articulo 1, atribuye exclusivamente a las empresas de seguridad "la instalación y mantenimiento de aparatos, dispositivos y sistemas de seguridad". El artículo 39 del Reglamento de Seguridad Privada, establece que *"únicamente podrán realizar las operaciones de instalación y mantenimiento de sistemas de seguridad electrónicos contra robo e intrusión y contra incendios las empresas autorizadas, no necesitando estar inscritas cuando se dediquen sólo a la prevención de la seguridad contra incendios"*.
Posteriormente, la Orden Ministerial de 23 de abril de 1997, por la que se concretan determinados aspectos en materia de empresas de seguridad, contribuyó a clarificar más la cuestión, al establecer en su apartado vigésimo cuarto que *"a los efectos de la normativa reguladora de la seguridad privada, se entenderá por sistema de seguridad, el conjunto de aparatos o dispositivos electrónicos contra robo e intrusión, cuya activación sea susceptible de producir intervención policial"*.
Continua este apartado vigésimo cuarto de la citada Orden Ministerial, estableciendo que : "su instalación deberá ser efectuada por una empresa de seguridad autorizada para dicha actividad y ajustarse a lo dispuesto en los artículos 40 (aprobación de material), 42 (certificado de instalación) y 43 (revisiones) del Reglamento de Seguridad Privada".
En consecuencia, y teniendo en cuenta que los circuitos cerrados de televisión o los equipos de video-vigilancia deben catalogarse como aparatos o dispositivos de seguridad electrónicos, su instalación deberá ser realizada obligatoriamente por empresas de seguridad, cuando concurran las siguientes circunstancias:

- Que se trate de aparatos o dispositivos electrónicos, por contraposición a medidas de protección física o de cualquier otro tipo.
- Que el objeto de su instalación sea la prevención contra el robo o la intrusión.
- Que la activación de tales aparatos o dispositivos sea susceptible de producir intervención policial, independientemente de que el sistema de seguridad se encuentre o no conectado a una central de alarmas .

Así pues, los titulares de establecimientos o instalaciones que deseen voluntariamente, o que por sus características vengan obligados a instalar dichos sistemas de seguridad, deberán contratar la instalación y mantenimiento de los mismos con empresas de seguridad autorizadas para la prestación de tales servicios.

Respecto de la utilización de videocámaras en el ámbito de la seguridad privada, actualmente no se ha desarrollado la normativa prevista en la Disposición Adicional Novena de la Ley Orgánica 4/1997 de 4 de agosto, que regula la utilización de vídeo cámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos.
Sin embargo, es necesario tener presente la Ley Orgánica 1/1982, de 5 de mayo, de Protección Civil del Derecho al Honor, a la Intimidad Personal y Familiar y a la propia Imagen, con objeto de conocer las responsabilidades en las que se puede incurrir, cuando la utilización de las vídeo cámaras tenga la consideración de intromisión ilegítima en el ámbito de protección de dicha Ley.
Finalmente, sería necesario tener en cuenta lo regulado por la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, para el supuesto de que las imágenes grabadas tengan la consideración de dato personal y pudieran ser incorporadas a un fichero.
Así pues y en contestación a la consulta planteada, cabe hacer las siguientes consideraciones:

1. La instalación y mantenimiento de las cámaras de seguridad deberá contratarse con empresa de seguridad autorizada e inscrita para la prestación de tales servicios.
2. Actualmente no existe una regulación de la utilización de vídeo cámaras en el ámbito de la seguridad privada.
3. Puede generar responsabilidades en el supuesto de que su utilización sea considerada una intromisión ilegítima en el ámbito del derecho al honor, a la intimidad personal y familiar y a la propia imagen.
4. En el caso de que las imágenes pudieran ser consideradas como dato personal y tratarse en un fichero, el tratamiento de los mismos requeriría consentimiento del afectado.

ANEXO D: PRESUPUESTO

1) Ejecución Material

- Compra de ordenador personal (Software incluido)..... 2.000,00 €
- Alquiler de impresora láser durante 6 meses..... 50,00 €
- Material de oficina..... 150,00 €
- Total de ejecución material..... 2.200,00 €

2) Gastos generales

- 16 % sobre Ejecución Material..... 352,00 €

3) Beneficio Industrial

- 6 % sobre Ejecución Material..... 132,00 €

4) Honorarios Proyecto

- 700 horas a 15 € / hora..... 10.500,00 €

5) Material fungible

- Gastos de impresión..... 60,00 €
- Encuadernación..... 200,00 €

6) Subtotal del presupuesto

- Subtotal Presupuesto..... 12.960,00 €

7) I.V.A. aplicable

- 16% Subtotal Presupuesto ..... 2.073,60 €

8) Total presupuesto

- Total Presupuesto ..... 15.033,60 €

Madrid, Mayo de 2008

El Ingeniero Jefe de Proyecto

Fdo.: Marta Naranjo Rico
Ingeniero Superior de Telecomunicación

ANEXO E: PLIEGO DE CONDICIONES

Este documento contiene las condiciones legales que guiarán la realización, en este proyecto, de "Solución Integral en materia de Seguridad Electrónica". En lo que sigue, se supondrá que el proyecto ha sido encargado por una empresa cliente a una empresa consultora con la finalidad de realizar dicho sistema. Dicha empresa ha debido desarrollar una línea de investigación con objeto de elaborar el proyecto. Esta línea de investigación, junto con el posterior desarrollo de los programas está amparada por las condiciones particulares del siguiente pliego.

Supuesto que la utilización industrial de los métodos recogidos en el presente proyecto ha sido decidida por parte de la empresa cliente o de otras, la obra a realizar se regulará por las siguientes:

Condiciones generales

1. La modalidad de contratación será el concurso. La adjudicación se hará, por tanto, a la proposición más favorable sin atender exclusivamente al valor económico, dependiendo de las mayores garantías ofrecidas. La empresa que somete el proyecto a concurso se reserva el derecho a declararlo desierto.

2. El montaje y mecanización completa de los equipos que intervengan será realizado totalmente por la empresa licitadora.

3. En la oferta, se hará constar el precio total por el que se compromete a realizar la obra y el tanto por ciento de baja que supone este precio en relación con un importe límite si este se hubiera fijado.

4. La obra se realizará bajo la dirección técnica de un Ingeniero Superior de Telecomunicación, auxiliado por el número de Ingenieros Técnicos y Programadores que se estime preciso para el desarrollo de la misma.

5. Aparte del Ingeniero Director, el contratista tendrá derecho a contratar al resto del personal, pudiendo ceder esta prerrogativa a favor del Ingeniero Director, quien no estará obligado a aceptarla.

6. El contratista tiene derecho a sacar copias a su costa de los planos, pliego de condiciones y presupuestos. El Ingeniero autor del proyecto autorizará con su firma las copias solicitadas por el contratista después de confrontarlas.

7. Se abonará al contratista la obra que realmente ejecute con sujeción al proyecto que sirvió de base para la contratación, a las modificaciones autorizadas por la superioridad o a las órdenes que con arreglo a sus facultades le hayan comunicado por escrito al Ingeniero Director de obras siempre que dicha obra se haya ajustado a los preceptos de los pliegos de condiciones, con arreglo a los cuales, se harán las modificaciones y la valoración de las diversas unidades sin que el importe total pueda exceder de los presupuestos aprobados. Por consiguiente, el número de unidades que se

consignan en el proyecto o en el presupuesto, no podrá servirle de fundamento para entablar reclamaciones de ninguna clase, salvo en los casos de rescisión.

8. Tanto en las certificaciones de obras como en la liquidación final, se abonarán los trabajos realizados por el contratista a los precios de ejecución material que figuran en el presupuesto para cada unidad de la obra.

9. Si excepcionalmente se hubiera ejecutado algún trabajo que no se ajustase a las condiciones de la contrata pero que sin embargo es admisible a juicio del Ingeniero Director de obras, se dará conocimiento a la Dirección, proponiendo a la vez la rebaja de precios que el Ingeniero estime justa y si la Dirección resolviera aceptar la obra, quedará el contratista obligado a conformarse con la rebaja acordada.

10. Cuando se juzgue necesario emplear materiales o ejecutar obras que no figuren en el presupuesto de la contrata, se evaluará su importe a los precios asignados a otras obras o materiales análogos si los hubiere y cuando no, se discutirán entre el Ingeniero Director y el contratista, sometiéndolos a la aprobación de la Dirección. Los nuevos precios convenidos por uno u otro procedimiento, se sujetarán siempre al establecido en el punto anterior.

11. Cuando el contratista, con autorización del Ingeniero Director de obras, emplee materiales de calidad más elevada o de mayores dimensiones de lo estipulado en el proyecto, o sustituya una clase de fabricación por otra que tenga asignado mayor precio o ejecute con mayores dimensiones cualquier otra parte de las obras, o en general, introduzca en ellas cualquier modificación que sea beneficiosa a juicio del Ingeniero Director de obras, no tendrá derecho sin embargo, sino a lo que le correspondería si hubiera realizado la obra con estricta sujeción a lo proyectado y contratado.

12. Las cantidades calculadas para obras accesorias, aunque figuren por partida alzada en el presupuesto final (general), no serán abonadas sino a los precios de la contrata, según las condiciones de la misma y los proyectos particulares que para ellas se formen, o en su defecto, por lo que resulte de su medición final.

13. El contratista queda obligado a abonar al Ingeniero autor del proyecto y director de obras así como a los Ingenieros Técnicos, el importe de sus respectivos honorarios facultativos por formación del proyecto, dirección técnica y administración en su caso, con arreglo a las tarifas y honorarios vigentes.

14. Concluida la ejecución de la obra, será reconocida por el Ingeniero Director que a tal efecto designe la empresa.

15. La garantía definitiva será del 4% del presupuesto y la provisional del 2%.

16. La forma de pago será por certificaciones mensuales de la obra ejecutada, de acuerdo con los precios del presupuesto, deducida la baja si la hubiera.

17. La fecha de comienzo de las obras será a partir de los 15 días naturales del replanteo oficial de las mismas y la definitiva, al año de haber ejecutado la provisional, procediéndose si no existe reclamación alguna, a la reclamación de la fianza.

18. Si el contratista al efectuar el replanteo, observase algún error en el proyecto, deberá comunicarlo en el plazo de quince días al Ingeniero Director de obras, pues transcurrido ese plazo será responsable de la exactitud del proyecto.

19. El contratista está obligado a designar una persona responsable que se entenderá con el Ingeniero Director de obras, o con el delegado que éste designe, para todo relacionado con ella. Al ser el Ingeniero Director de obras el que interpreta el proyecto, el contratista deberá consultarle cualquier duda que surja en su realización.

20. Durante la realización de la obra, se girarán visitas de inspección por personal facultativo de la empresa cliente, para hacer las comprobaciones que se crean oportunas. Es obligación del contratista, la conservación de la obra ya ejecutada hasta la recepción de la misma, por lo que el deterioro parcial o total de ella, aunque sea por agentes atmosféricos u otras causas, deberá ser reparado o reconstruido por su cuenta.

21. El contratista, deberá realizar la obra en el plazo mencionado a partir de la fecha del contrato, incurriendo en multa, por retraso de la ejecución siempre que éste no sea debido a causas de fuerza mayor. A la terminación de la obra, se hará una recepción provisional previo reconocimiento y examen por la dirección técnica, el depositario de efectos, el interventor y el jefe de servicio o un representante, estampando su conformidad el contratista.

22. Hecha la recepción provisional, se certificará al contratista el resto de la obra, reservándose la administración el importe de los gastos de conservación de la misma hasta su recepción definitiva y la fianza durante el tiempo señalado como plazo de garantía. La recepción definitiva se hará en las mismas condiciones que la provisional, extendiéndose el acta correspondiente. El Director Técnico propondrá a la Junta Económica la devolución de la fianza al contratista de acuerdo con las condiciones económicas legales establecidas.

23. Las tarifas para la determinación de honorarios, reguladas por orden de la Presidencia del Gobierno el 19 de Octubre de 1961, se aplicarán sobre el denominado en la actualidad “Presupuesto de Ejecución de Contrata” y anteriormente llamado ”Presupuesto de Ejecución Material” que hoy designa otro concepto.

Condiciones particulares

La empresa consultora, que ha desarrollado el presente proyecto, lo entregará a la empresa cliente bajo las condiciones generales ya formuladas, debiendo añadirse las siguientes condiciones particulares:

1. La propiedad intelectual de los procesos descritos y analizados en el presente trabajo, pertenece por entero a la empresa consultora representada por el Ingeniero Director del Proyecto.

2. La empresa consultora se reserva el derecho a la utilización total o parcial de los resultados de la investigación realizada para desarrollar el siguiente proyecto, bien para su

publicación o bien para su uso en trabajos o proyectos posteriores, para la misma empresa cliente o para otra.

3. Cualquier tipo de reproducción aparte de las reseñadas en las condiciones generales, bien sea para uso particular de la empresa cliente, o para cualquier otra aplicación, contará con autorización expresa y por escrito del Ingeniero Director del Proyecto, que actuará en representación de la empresa consultora.

4. En la autorización se ha de hacer constar la aplicación a que se destinan sus reproducciones así como su cantidad.

5. En todas las reproducciones se indicará su procedencia, explicitando el nombre del proyecto, nombre del Ingeniero Director y de la empresa consultora.

6. Si el proyecto pasa la etapa de desarrollo, cualquier modificación que se realice sobre él, deberá ser notificada al Ingeniero Director del Proyecto y a criterio de éste, la empresa consultora decidirá aceptar o no la modificación propuesta.

7. Si la modificación se acepta, la empresa consultora se hará responsable al mismo nivel que el proyecto inicial del que resulta el añadirla.

8. Si la modificación no es aceptada, por el contrario, la empresa consultora declinará toda responsabilidad que se derive de la aplicación o influencia de la misma.

9. Si la empresa cliente decide desarrollar industrialmente uno o varios productos en los que resulte parcial o totalmente aplicable el estudio de este proyecto, deberá comunicarlo a la empresa consultora.

10. La empresa consultora no se responsabiliza de los efectos laterales que se puedan producir en el momento en que se utilice la herramienta objeto del presente proyecto para la realización de otras aplicaciones.

11. La empresa consultora tendrá prioridad respecto a otras en la elaboración de los proyectos auxiliares que fuese necesario desarrollar para dicha aplicación industrial, siempre que no haga explícita renuncia a este hecho. En este caso, deberá autorizar expresamente los proyectos presentados por otros.

12. El Ingeniero Director del presente proyecto, será el responsable de la dirección de la aplicación industrial siempre que la empresa consultora lo estime oportuno. En caso contrario, la persona designada deberá contar con la autorización del mismo, quien delegará en él las responsabilidades que ostente.