UNIVERSIDAD TECNICA DE AMBATO

FACULTAD DE INGENIERIA EN SISTEMAS,
ELECTRONICA E INDUSTRIAL

CARRERA DE INGENIERÍA EN ELECTRÓNICA Y COMUNICACIONES

Seminario de Graduación “Proyectos de Conectividad y Redes de Comunicación, Administración de Redes y Servicios, Seguridad Industrial, Normativas de Calidad y Automatización Robótica (Mecatrónica)".

TEMA

SISTEMA DE SEGURIDAD Y MONITOREO BASADO EN INTERNET PARA CÁMARAS IP EN LA EMPRESA VIPDRIVE.

Proyecto de Graduación Modalidad Seminario, presentado como requisito previo a la obtención del título de Ingeniero en Electrónica y Comunicaciones.

AUTOR: DARWIN XAVIER ESTRADA MARTINEZ

TUTOR: ING. JAVIER SANCHEZ GUERRERO

Ambato - Ecuador

Septiembre/2009

APROBACIÓN DEL TUTOR

En mi calidad de tutor del trabajo de investigación sobre el tema:
Sistema de Seguridad y Monitoreo basado en Internet para Cámaras IP en la Empresa Vipdrive, de Darwin Xavier Estrada Martínez estudiante de la carrera de Ingeniería en Electrónica y comunicaciones de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial, de la Universidad Técnica de Ambato, considero que el informe investigativo reúne los requisitos suficientes para que continúe con los trámites y consiguiente aprobación de conformidad con el Art. 45 del Capítulo III Seminarios, del Reglamento de Graduación de Pregrado de la Universidad Técnica de Ambato..

Ambato septiembre, 2009

EL TUTOR

……

Ing. Javier Sánchez Guerrero

AUTORIA

El presente trabajo de investigación titulado: “Sistema de Seguridad y Monitoreo basado en Internet para Cámaras IP en la Empresa Vipdrive”. Es absolutamente original, auténtico y personal, en tal virtud, el contenido, efectos legales y académicos que se desprenden del mismo son de exclusiva responsabilidad del autor.

Ambato septiembre, 2009

Darwin Xavier Estrada Martínez
CC: 180388098-6

DEDICATORIA

A mis padres, a mi familia y amigos, porque gracias a su cariño, guía y apoyo he llegado a cumplir uno de mis mayores sueños, fruto de la inmensa ayuda, confianza y comprensión constante e incondicional para forjar dentro de mí, el deseo y las ganas de superación y así incentivarme y llegar a la culminación de este proyecto.

Darwin Xavier Estrada Martínez

AGRADECIMIENTO

Al termino de esta labor que me fue posible con llevar gracias a Dios, a la Universidad Técnica de Ambato, que a través de sus maestros quienes, compartieron su sabiduría, experiencia, valores morales y formación profesional, en especial al ingeniero Javier Sánchez tutor del presente proyecto.

Darwin Xavier Estrada Martínez

INDICE DE CONTENIDOS

A. PÁGINAS PRELIMINARES

B. TEXTO

CAPITULO I

EL PROBLEMA

CAPITULO II

MARCO TEORICO

CAPITULO III

METODOLOGÍA

CAPITULO IV

ANÁLISIS E INTERPRETACIÓN DE RESULTADOS

CAPITULO V

CONCLUSIONES Y RECOMENDACIONES

CAPITULO VI

PROPUESTA

C. MATERIALES DE REFERENCIA

INDICE DE CUADROS Y GRAFICOS

CAPITULO II

MARCO TEORICO

CAPITULO VI

PROPUESTA

Resumen Ejecutivo

El presente trabajo está enfocado en el diseño e implementación de un Sistema de Seguridad y Monitoreo basado en internet para cámaras IP en la empresa Vipdrive.

La Empresa Vipdrive, nace en el mes de agosto del 2008, en la ciudad de Ambato, con la finalidad de prestar sus servicios como escuela de conducción a toda la ciudadanía del centro del país. Además siempre desde una perspectiva de crecimiento humanístico y concientizar a la ciudadanía para que ya no ocurrieren más accidentes y teñir de sangre las carreteras ecuatorianas.

La Empresa Vipdrive, se encuentra buscando tecnología de punta, que facilite su crecimiento y a través del Sistema de Seguridad y Monitoreo basado en internet para cámaras IP, puede realizar el control y supervisión de la misma a cualquier hora y lugar gracias al internet, ya que se puede observar con más frecuencia lo que suceda entre los diferentes departamentos para tener un mejor control y rendimiento de sus trabajadores.

El Sistema de Seguridad y Monitoreo basado en internet para cámaras IP beneficia tanto a la empresa como a sus estudiantes y trabajadores, ya que permite evitar los delitos o identificar a los autores de un robo o de una conducta indebida.

Los principales beneficios que tendrá la empresa serán:

- Estar acorde con la tecnología.
- Contar con seguridad las 24 horas del día.
- Las grabaciones de video pueden guardarse y analizarse con facilidad.
- La video vigilancia tiene capacidad de proporcionar otras funciones y servicios, siendo una tecnología con continuo desarrollo.
- Rápida y fácil instalación de la red.
- Permiten la movilidad y tienen menos costo de mantenimiento.
- Flexibilidad en la red para aumentar numero de dispositivos.

El diseño de un Sistema de Seguridad y Monitoreo basado en internet para cámaras IP está planteado de la siguiente manera:

1. Estudio de planos existentes.
2. Análisis de áreas criticas.
3. Definir áreas a proteger.
4. Análisis de tecnología a utilizar.
5. Costos
6. Ubicación del PC que hace de servidor.
7. Diseño del cableado.
8. Diseño del sistema de seguridad.

Los dispositivos a utilizar son los siguientes:

LA CÁMARA DE VIGILANCIA IP DCS-910 DE D-LINK

Esta cámara proporciona una solución de vigilancia versátil y única tanto para la pequeña oficina como el hogar y tener acceso a cualquier hora desde el internet.

LA CÁMARA DCS-910 INCLUYE EL SOFTWARE DE VIGILANCIA IP D-VIEWCAM 2.0

El sistema de vigilancia está diseñado para administrar de manera centralizada y simultánea hasta 32 cámaras IP para usuarios en el hogar.

CPU INTEL PENTIUM DUAL CORE E2160 A 3.0GHZ

Este CPU debe tener un disco duro de 500GB, con el objetivo de tener suficiente espacio para la grabación de las imágenes.

SWITCH

Este dispositivo permite la conexión entre los elementos de la red y el internet.

SISTEMA DE ALARMA

Este sistema esta también dirigido a la seguridad de la empresa y esta conformado por: unidad central o cerebro con caja, teclado, sirena con caja, detectores de movimiento, detector lineal, batería, adaptador.

CABLE MULTIPAR DE 2 Y 6 PARES

Este cable es utilizado para conectar los diferentes dispositivos del sistema de alarma.

CABLE UTP CATEGORIA 5E

Este cable es utilizado para conectar las cámaras con el switch.

CONECTORES RJ45

Los conectores son conectados a los extremos del cable UTP.

JACK

Es un adaptador que facilita la adaptación de las cámaras al cable que se utiliza.

CANALETAS

Son elementos que contribuyen a una mejor organización de los cables, así como a dar una buena imagen del sitio donde son conectadas.

CAPITULO I

EL PROBLEMA

1.1 TEMA:

Sistema de Seguridad y Monitoreo basado en internet para cámaras IP en la empresa Vipdrive.

1.2 PLANTEAMIENTO DEL PROBLEMA

1.2.1 CONTEXTUALIZACION

Los medios de comunicación a medida que pasa el tiempo van evolucionando día a día y surge la necesidad de aplicar la tecnología de video vigilancia IP por internet para asegurar y prevenir pérdidas. Las empresas y sus trabajadores están continuamente expuestos a robos y atracos. Por otro lado, la supervisión del trabajo, el buen funcionamiento y el control son otra de las preocupaciones constantes. El sistema de video vigilancia proporciona gran seguridad y control.

Mundialmente la revolución tecnológica en los últimos tiempos ha crecido evidentemente y por ende es conveniente ser parte de ello para poder acceder a nuevas tecnologías que den tranquilidad al personal de las empresas y control sobre el mismo. Las cámaras IP en nuestro país y provincia ha sobresalido considerablemente y en este momento podemos observar varias empresas e instituciones que están

implementando o en proceso sistemas de seguridad usando video vigilancia IP por internet, alarmas, etc. El riesgo que implica el despliegue de un sistema de seguridad vía internet consiste en que la información viaja en un medio que no es limitable a un espacio determinado.

El diseño de dicho sistema beneficia tanto a la empresa como a sus supervisores, pues observar y controlar lo que esta ocurriendo, tan solo con conectarse a internet, la tranquilidad y seguridad cuando no se encuentre en la empresa es posible, ya que permite identificar a los autores de un robo o de alguna conducta indebida.

Por ende uno de los mayores problemas con el que se está encontrando dicha empresa es la seguridad, control y supervisión de la misma, por esto es necesario un sistema de seguridad basado en internet para cámaras IP.

1.2.2 ANALISIS CRÍTICO

La inseguridad es un factor que ha crecido mucho en los últimos años en todas las sociedades, las causas de este crecimiento son muy complicadas de entender y muchas veces se encuentran interrelacionadas; algunas personas asumen que aspectos como bajos recursos o marginación social son la causa principal de la gesta de la inseguridad, pero esta idea no es del todo acertada.

El desconocimiento de los avances en los sistemas de seguridad junto al desarrollo de nuevos estándares y tecnologías que van revolucionando el mundo de las comunicaciones ha causado que el país camine hacia un peligroso retraso tecnológico y para las empresas que prestan este tipo de servicio los ingresos económicos no sean los esperados de acuerdo a las estadísticas y proyecciones realizadas.

Una restricción para la implementación de este tipo de sistemas es el factor económico ya que la mayor parte de proveedores de los equipos son internacionales

con marcas aprobadas por las instituciones de seguridad y monitoreo los mismos que son muy costosos, también la evolución de la tecnología hace que en poco tiempo se requiera actualizar este tipo de sistemas y la inversión realizada no está acorde con este desarrollo tecnológico.

1.2.3 PROGNOSIS

De continuar esta situación la empresa y sus trabajadores están continuamente expuestos a robos y atracos, la video vigilancia permite la visualización remota de las cámaras en cualquier momento, disponiendo de la mayor gama de soluciones profesionales de vídeo para vigilar y controlar su negocio tanto local como remotamente desde internet. Los sistemas de vídeo vigilancia le permiten ver las cámaras de su negocio en cualquier momento y desde cualquier parte del mundo con solo una conexión de internet.

Sin embargo para evitar todos los problemas antes mencionados es necesario un sistema de seguridad y monitoreo basado en internet para cámaras IP.

1.2.4 FORMULACIÓN DEL PROBLEMA

¿Qué incidencia tiene un sistema de seguridad y monitoreo basado en internet para cámaras IP en la empresa Vipdrive?

1.2.5 PREGUNTAS DIRECTRICES

1.2.5.1 ¿Cuál es la situación actual de la empresa Vipdrive?

1.2.5.2 ¿En que situación se encuentran los sistemas de seguridad y monitoreo en nuestro país?

1.2.5.3 ¿Es necesario un sistema de seguridad y monitoreo basado en internet para cámaras IP en la empresa Vipdrive?

1.2.5.4 ¿Qué beneficios se obtendrían con un sistema de seguridad?

1.2.5.5 ¿Qué beneficios se obtendrían con un sistema de monitoreo?

1.2.6 DELIMITACIÓN

Este proyecto está enfocado en un sistema de seguridad y monitoreo basado en internet para cámaras IP en la empresa Vipdrive, con una duración de cinco meses, desde el diez de noviembre del 2008 al treinta de marzo del 2009 y se trabajará con una población comprendida de ocho docentes.

1.3 JUSTIFICACIÓN

Actualmente la seguridad está ocupando una amplia área en el sector comercial o en el ámbito personal, mediante los sistemas de seguridad es posible realizar todo tipo de vigilancia y control o simplemente estar en contacto con los trabajadores pero la evolución tecnológica hace que sea necesario realizar un estudio de dichos sistemas con los nuevos estándares y tecnologías, de esta forma solucionar los problemas existentes como la inseguridad, vigilancia y control.

El vigente proyecto resolverá los problemas de seguridad existentes en la empresa, y con el apropiado control y la utilización de tecnología de los últimos tiempos como es video vigilancia IP por Internet.

El desarrollo de la tecnología ha permitido que la humanidad día a día realice su trabajo con menos esfuerzo y en el menor tiempo, motivo por el cual el sistema de seguridad a más de prestar vigilancia y control, permitirá una comunicación

inmediata con trabajadores de dicha empresa.

El presente proyecto permitirá poner en práctica los conocimientos obtenidos durante la carrera de Electrónica y Comunicaciones, logrando dar solución a los problemas como es la falta de vigilancia y seguridad en la empresa Vipdrive y será un aporte tecnológico que beneficiara tanto al propietario como a sus empleados y estudiantes, por ende mientras se tenga un buen servicio se mantendrá el prestigio de la empresa.

1.4 OBJETIVOS

1.4.1 OBJETIVO GENERAL

1.4.1.1 Desarrollar un sistema de seguridad y monitoreo basado en internet para cámaras IP en la empresa Vipdrive.

1.4.2 OBJETIVOS ESPECÍFICOS

1.4.2.1 Realizar un análisis de la situación actual de la empresa Vipdrive.

1.4.2.2 Realizar un análisis de la situación actual de los sistemas de seguridad y monitoreo en nuestro país.

1.4.2.3 Conocer las diferentes utilidades para un sistema de seguridad y monitoreo basado en internet para cámaras IP en la empresa Vipdrive.

1.4.2.4 Realizar un estudio acerca de los beneficios que se obtendría con un sistema de seguridad.

1.4.2.5 Realizar un estudio acerca de los beneficios que se obtendría con un sistema de monitoreo.

CAPITULO II

MARCO TEÓRICO

2.1. ANTECEDENTES INVESTIGATIVOS

Previa la investigación realizada en los archivos de la biblioteca de la Facultad de Ingeniería en Sistemas, Electrónica e industrial de la Universidad Técnica de Ambato, existe un proyecto de pasantía desarrollado por la ingeniera Cecilia Elizabeth Izurieta Pazmiño en el periodo Mayo-Septiembre del 2006, la cual lleva por titulo "DISEÑO DE UN SISTEMA DE SEGURIDAD MEDIANTE CAMARAS IP PARA LA EMPRESA PROALPI DE LA CIUDAD DE PILLARO"; cuyas conclusiones se refieren a:

Al realizar el análisis dentro de las áreas críticas de la empresa se pudo determinar los lugares que requerirán de mayor vigilancia , así como el mejoramiento en el desempeño de los empleados y una mejor utilización y optimización de los materiales para la elaboración de los productos; además se pudo determinar que no es necesario la presencia física para la vigilancia del personal solo recurrir a los avances tecnológicos como es la utilización de cámaras IP. El proyecto ayudo a mantener una mejor comunicación entre empleados y subalternos asimismo ayudo a que exista orden y mayor responsabilidad de los empleados en la realización de actividades.

El uso de software y la grabación de video en el computador son de fácil reproducción y grabación; también se puede visualizar a distancia lo que sucede en la

fabrica, mediante el uso de internet por medio del cual se puede tener manipulación sobre las cámaras y emitir ordenes desde cualquier lugar del planeta; por ultimo el sistema de seguridad brinda mayor protección a la fabrica.

Las conclusiones a las que se ha llegado en este trabajo serán considerados en el presente trabajo investigativo.

2.2 FUNDAMENTACIÓN LEGAL

Leyes que rigen las Telecomunicaciones en el Ecuador.

Ley No. 184

Ámbito de la Ley.- La presente Ley Especial de Telecomunicaciones tiene por objeto normar en el territorio nacional la instalación, operación, utilización y desarrollo de toda transmisión, emisión o recepción de signos, señales, imágenes, sonidos e información de cualquier naturaleza por hilo, radioelectricidad, medios ópticos u otros sistemas electromagnéticos.

Ley de reforma al código penal N° 99-38 mediante la cual se reforma el artículo 422, publicada en el registro oficial N° 253 del doce de Agosto de 1999.

2.3 CATEGORÍAS FUNDAMENTALES

VARIABLE INDEPENDIENTE

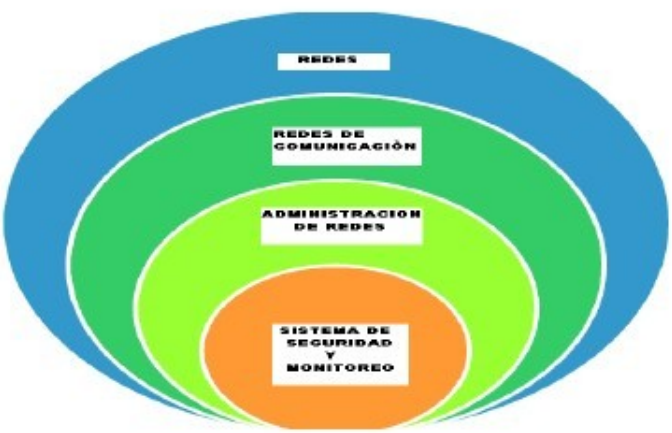


Figura 1.

VARIABLE DEPENDIENTE

Figura 2.

2.3.1 Redes

La industria de ordenadores ha mostrado un progreso espectacular en muy corto tiempo. El viejo modelo de tener un solo ordenador para satisfacer todas las necesidades de cálculo de una organización se está reemplazando con rapidez por otro que considera un número grande de ordenadores separados, pero interconectados, que efectúan el mismo trabajo. Estos sistemas, se conocen con el nombre de redes de ordenadores. Estas nos dan a entender una colección interconectada de ordenadores autónomos. Se dice que los ordenadores están interconectados, si son capaces de intercambiar información. La conexión no necesita hacerse a través de un hilo de cobre, el uso de láser, microondas y satélites de comunicaciones. Al indicar que los ordenadores son autónomos, excluimos los sistemas en los que un ordenador pueda forzosamente arrancar, parar o controlar a otro, éstos no se consideran autónomos.

2.3.1.1 Estructura de una Red

En toda red existe una colección de máquinas para correr programas de usuario (aplicaciones). Seguiremos la terminología de una de las primeras redes, denominada

ARPANET, y llamaremos hostales a las máquinas antes mencionadas. También, en algunas ocasiones se utiliza el término sistema terminal o sistema final. Los hostales están conectados mediante una subred de comunicación, o simplemente subred. El trabajo de la subred consiste en enviar mensajes entre hostales, de la misma manera como el sistema telefónico envía palabras entre la persona que habla y la que escucha. El diseño completo de la red simplifica notablemente cuando se separan los aspectos puros de comunicación de la red (la subred), de los aspectos de aplicación (los hostales).

Una subred en la mayor parte de las redes de área extendida consiste de dos componentes diferentes: los elementos de conmutación y las líneas de transmisión (conocidas como circuitos, canales o troncales), se encargan de mover bits entre máquinas, los elementos de conmutación son ordenadores especializados que se utilizan para conectar dos o más líneas de transmisión. Cuando los datos llegan por una línea de entrada, el elemento de conmutación deberá seleccionar una línea de salida para reexpedirlos

2.3.1.2 Redes de comunicación:

La posibilidad de compartir con carácter universal la información entre grupos de computadoras y sus usuarios; un componente vital de la era de la información. La generalización de la computadora personal (PC) y de la red de área local (LAN) durante la década de los ochenta ha dado lugar a la posibilidad de acceder a información en bases de datos remotas; cargar aplicaciones desde puntos de ultramar; enviar mensajes a otros países y compartir ficheros, todo ello desde una computadora personal; las redes que permiten todo esto son equipos avanzados y complejos. Su eficacia se basa en la confluencia de muy diversos componentes. El diseño e implantación de una red mundial de ordenadores es uno de los grandes milagros tecnológicos de las últimas décadas.

- Redes de área local (LAN).- Red de área local (Local Area Network). Tiene como alcance 10 metros a 1 kilómetro.

- Redes de área extensa (WAN).- Cuando se llega a un cierto punto deja de ser poco práctico seguir ampliando una LAN. A veces esto viene impuesto por limitaciones físicas, aunque suele haber formas más adecuadas o económicas de ampliar una red de computadoras. Dos de los componentes importantes de cualquier red son la red de teléfono y la de datos. Son enlaces para grandes distancias que amplían la LAN hasta convertirla en una red de área extensa (WAN). Casi todos los operadores de redes nacionales (como DBP en Alemania o British Telecom en Inglaterra) ofrecen servicios para interconectar redes de computadoras, que van desde los enlaces de datos sencillos y a baja velocidad que funcionan basándose en la red pública de telefonía hasta los complejos servicios de alta velocidad (como frame relay y SMDS-Synchronous Multimegabit Data Service) adecuados para la interconexión de las LAN. Estos servicios de datos a alta velocidad suelen denominarse conexiones de banda ancha. Se prevé que proporcionen los enlaces necesarios entre LAN para hacer posible lo que han dado en llamarse autopistas de la información.

Para la construcción de una red es necesario la utilización de medios de transmisión que a continuación los vamos a detallar.

2.3.2 Medios De Transmisión

2.3.2.1 Medios guiados

- Los medios de transmisión son un componente básico de todo sistema de comunicaciones. Existen diferentes tipos de medios guiados.

- Cada medio de transmisión tiene sus ventajas e inconvenientes; no existe un tipo ideal.

- Las principales diferencias entre los distintos tipos de medios guiados radican en el ancho de banda permitido y por tanto en la velocidad máxima de transmisión, su grado de inmunidad a interferencias electromagnéticas y la relación entre la atenuación de la señal versus la distancia del enlace.

Existen básicamente tres tipos de medios de transmisión físicos guiados:

Par de cobre,
Cable Coaxial y
Fibra Óptica

2.3.2.2 Alambre de cobre

Las líneas de alambre abierto (sin aislar) fueron muy usadas en el siglo pasado con la aparición del telégrafo.

La composición de los alambres fue al principio de hierro (acero) y después fue desplazado por el cobre.

-La resistencia al flujo de corriente eléctrica de los alambres abiertos varía grandemente con las condiciones climáticas, y es por esta razón que fue adoptado el cable par trenzado.

- Hoy en día los cables vienen protegidos con algún material aislante.

- Los conductores pueden ser de dos tipos sólidos (solid) e hilados (stranded).

- El grosor de los cables es medido de diversas maneras, el método más común es el American Wire Gauge Standard (AWG).

- Los grosores típicos de los conductores utilizados en cables eléctricos para uso residencial son del 10-14 AWG.

- Los calibres más usados en cables telefónicos son AWG 22, 24 y 26.

- Los conductores más utilizados en cables para aplicaciones de redes de área local son el AWG 24 y 26.

Figura 3. Medidas de Conductores

2.3.2.3 Cable UTP

- Existen dos tipos de cable par trenzado, el UTP (Unshielded Twisted Pair Cabling), o cable par trenzado sin blindaje y el cable STP (Shielded Twisted Pair Cabling), o cable par trenzado blindado.

- El UTP se utiliza comúnmente para aplicaciones de redes de área local Ethernet.

- El término UTP generalmente se refiere a los cables categoría 3, 4 y 5, 5e y 6 especificados por los estándares TIA/EIA 568-A, y TIA/EIA-568-B.2-1.

- El cable UTP comúnmente incluye 4 pares de conductores. 10Base-T, 10Base-T, 100Base-TX, y 100Base-T2 sólo utilizan 2 pares de conductores, mientras que 100Base-T4 y 1000Base-T requieren los 4 pares.

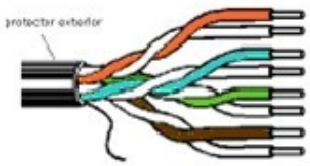


Figura 4. Cable UTP (4 pares)

Categoría 1: Voz solamente (Cable Telefónico).

Categoría 2: Datos 4 Mbps (LocalTalk [Apple]).

Categoría 3: UTP con impedancia de 100 ohmios y características eléctricas que soportan frecuencias de transmisión de hasta 16 MHz.
Definido por la especificación TIA/EIA 568-A. Puede ser usado con Ethernet 10Base-T, 100Base-T4, y 100Base-T2.

Categoría 4: UTP con impedancia de 100 ohms y características eléctricas que soportan frecuencias de transmisión de hasta 20 MHz.

Categoría 5: UTP con 100 ohm de impedancia y características eléctricas que soportan frecuencias de transmisión de hasta 100 MHz. Definida en TIA/EIA 568-A. Puede ser usado con 10Base-T, 100Base-T4, 100Base-T2, y 100Base-TX. (Fast Ethernet).

Categoría 6 (TIA/EIA-568-B.2-1) ("Cat 6" balanced twistedpair cabling) standard for telecommunications cabling: Category 6 standard specifies requirements for 100-ohm balanced twisted-pair cables, connecting hardware, patch cords, channels, and permanent links and provides test procedures for laboratory and field performance verification over the frequency range of 1 to 250 MHz, backward compatible with Categories 3, 5 and 5e. When different category components are mixed with Category 6 components, the resultant

cabling will satisfy the category transmission requirements of the lower performing component.

Figura 5. Cable de Red CAT6 de 0.9m y 2.1m

2.3.2.4 Cable Coaxial

- Este tipo de cable esta compuesto de un hilo conductor central de cobre rodeado por una malla de hilos de cobre. El espacio entre el hilo y la malla lo ocupa un conducto de plástico que separa los dos conductores y mantiene las propiedades eléctricas. Todo el cable está cubierto por un aislamiento de protección para reducir las emisiones eléctricas.

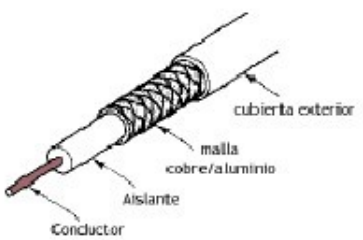


Figura 6. Partes del Cable Coaxial

Presenta propiedades mucho más favorables frente a interferencias y a la longitud de la línea de datos, de modo que el ancho de banda puede ser mayor. Esto permite una mayor concentración de las transmisiones analógicas o más capacidad de las transmisiones digitales.

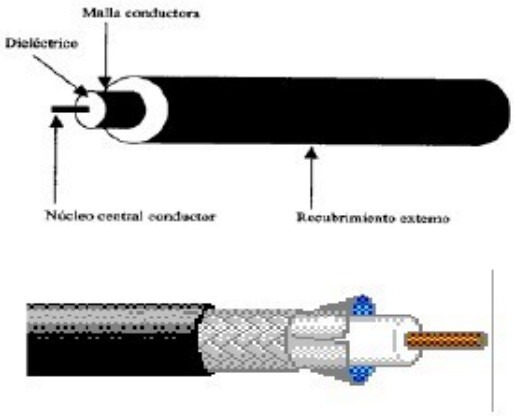


Figura 7. Forma Física del Cable Coaxial

2.3.2.4.1 Sección de un cable coaxial.

Su estructura es la de un cable formado por un conductor central macizo o compuesto por múltiples fibras al que rodea un aislante dieléctrico de mayor diámetro Figura siguiente. Una malla exterior aísla de interferencias al conductor central. Por último, utiliza un material aislante para recubrir y proteger todo el conjunto. Presenta condiciones eléctricas más favorables. En redes de área local se utilizan dos tipos de cable coaxial: fino y grueso.

Es capaz de llegar a anchos de banda comprendidos entre los 80 Mhz y los 400 Mhz (dependiendo de si es fino o grueso). Esto quiere decir que en transmisión de señal analógica seríamos capaces de tener, como mínimo. del orden de 10.000 circuitos de voz.

Figura 8. Cable Coaxial RG-58 con conector BNC

Figura 9. Cable Coaxial RG-6 con conector tipo **F** (Ej: TV Cable)

2.3.2.4.2 Ejemplo uso coaxial

50 ohm RG-8/RG-11 usado en 10Base5 (Thicknet) conector tipo T:

Tasa de transmisión: 10 Mbps

Longitud máxima: 500 metros por segmento

Diámetro del conductor: 2.17 mm

Nodos por segmento: 100

Longitud máxima (con repetidores): 1500 metros.

50 ohm, RG58 (thin coax) usado en 10Base2 conector BNC

Tasa de transmisión: 10 Mbps

Longitud máxima: 180 metros por segmento

Diámetro del conductor: 0.9 mm

Nodos por segmento: 30

Longitud máxima (con repetidores): 1500 metros.

2.3.2.5 Fibra óptica

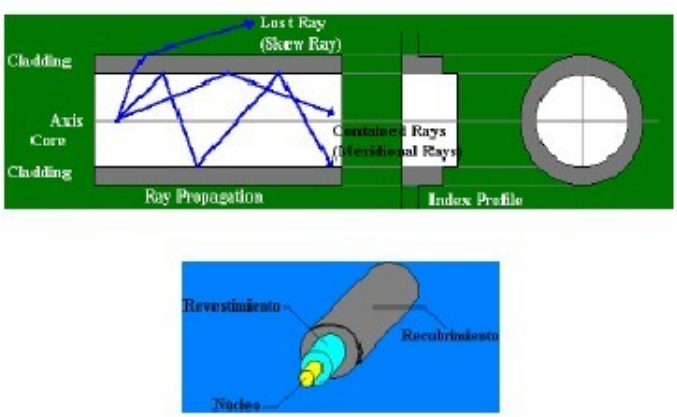


Figura 10. Estructura de una Fibra Óptica

- Una fibra óptica es un conductor altamente transparente. El cual constituye un excelente camino para la conducción de la luz.

- Luz: ondas con l comprendida entre los 0.4 y los 10 μm (luz visible e infrarrojo).

Ejemplo:

Figura 11. Radio de Fibra Óptica según color

Tipos de Instalación:

- aérea,
- ductos bajo tierra
- enterrada directamente en la tierra

2.3.2.6 Principio de transmisión

- El principio de transmisión con el cual la fibra óptica logra encaminar la luz se denomina reflexión total interna.

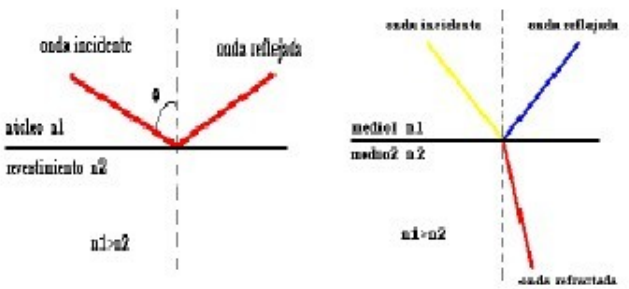


Figura 12. Gráfico de Transmisión

2.3.2.6.1 Clasificación

- Modo de propagación: monomodo y multimodo.
- Perfil de índice: índice abrupto e índice gradual (menor dispersión).

- Material de Fabricación: plásticas y de aleaciones de silicio y vidrio.

2.3.2.7 Causas de atenuación y pérdidas

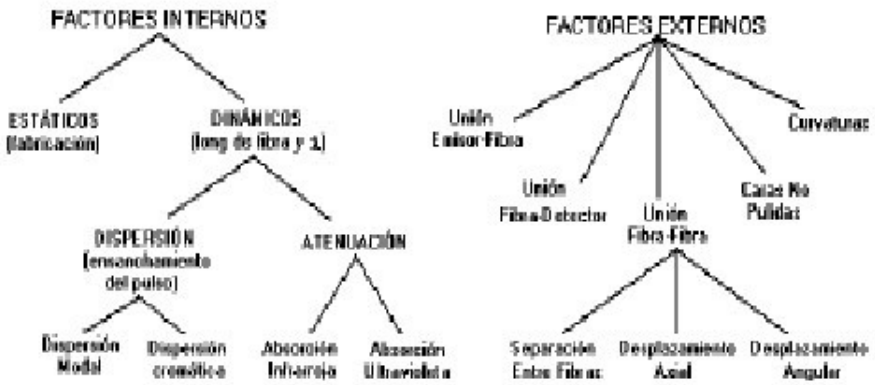


Figura 13. Factores Internos y Externos de la Atenuación

2.3.2.7.1 Atenuación

- $$\alpha = 10\frac{\ln(P_{in}/P_{out})}{L} \quad [\text{dB/km}]$$

$$P_{out}/P_{in} = \exp^{-\alpha L/10}$$

- Los detalles del proceso de fabricación tienen un profundo efecto en el diagrama de pérdidas vs longitud de onda.

- Para obtener bajas pérdidas se necesita alta pureza.

2.3.3 Administración de redes.

La Administración de Redes es un conjunto de técnicas tendientes a mantener una red operativa, eficiente, segura, constantemente monitoreada y con una planeación adecuada y propiamente documentada.

Sus objetivos son:

Mejorar la continuidad en la operación de la red con mecanismos adecuados de control y monitoreo, de resolución de problemas y de suministro de recursos.

Hacer uso eficiente de la red y utilizar mejor los recursos, como por ejemplo, el ancho de banda.

Reducir costos por medio del control de gastos y de mejores mecanismos de cobro.

Hacer la red más segura, protegiéndola contra el acceso no autorizado, haciendo imposible que personas ajenas puedan entender la información que circula en ella.

Controlar cambios y actualizaciones en la red de modo que ocasionen las menos interrupciones posibles, en el servicio a los usuarios.

La administración de la red se vuelve más importante y difícil si se considera que las redes actuales comprendan lo siguiente:

Mezclas de diversas señales, como voz, datos, imagen y gráficas.

Interconexión de varios tipos de redes, como WAN, LAN y MAN.

El uso de múltiples medios de comunicación, como par trenzado, cable coaxial, fibra óptica, satélite, láser, infrarrojo y microondas.

Diversos protocolos de comunicación, incluyendo TCP/IP, SPX/IPX, SNA, OSI.

El empleo de muchos sistemas operativos, como DOS, Netware, Windows NT, UNÍS, OS/2.

Diversas arquitecturas de red, incluyendo Ethernet 10 base T, Fast Ethernet, Token Ring, FDDI, 100vg-Any Lan y Fiber channel.

Varios métodos de compresión, códigos de línea, etc...

El sistema de administración de red opera bajo los siguientes pasos básicos:

1.- Colección de información acerca del estado de la red y componentes del sistema. La información recolectada de los recursos debe incluir: eventos, atributos y acciones operativas.

2.- Transformación de la información para presentarla en formatos apropiados para el entendimiento del administrador.

3.- Transportación de la información del equipo monitoreado al centro de control.

4.- Almacenamiento de los datos coleccionados en el centro de control.

5.- Análisis de parámetros para obtener conclusiones que permitan deducir rápidamente lo que pasa en la red.

6.- Actuación para generar acciones rápidas y automáticas en respuesta a una falla mayor.

La característica fundamental de un sistemas de administración de red moderno es la de ser un sistema abierto, capaz de manejar varios protocolos y lidiar con varias arquitecturas de red. Esto quiere decir: soporte para los protocolos de red más importantes.

2.3.3.1 Elementos involucrados en la administración de red

- Objetos: son los elementos de más bajo nivel y constituyen los aparatos administrados.

- Agentes: un programa o conjunto de programas que colecciona información de administración del sistema en un nodo o elemento de la red. El agente genera el grado

de administración apropiado para ese nivel y transmite información al administrador central de la red acerca de:

Notificación de problemas.

Datos de diagnóstico.

Identificador del nodo.

Características del nodo.

- Administrador del sistema: Es un conjunto de programas ubicados en un punto central al cual se dirigen los mensajes que requieren acción o que contienen información solicitada por el administrador al agente.

2.3.3.2 Seguridad.

La estructura administrativa de la red debe proveer mecanismos de seguridad apropiados para lo siguiente:

Identificación y autentificación del usuario, una clave de acceso y un password.

Autorización de acceso a los recursos, es decir, solo personal autorizado.

Confidencialidad. Para asegurar la confidencialidad en el medio de comunicación y en los medios de almacenamiento, se utilizan medios de criptografía, tanto simétrica como asimétrica.

Un administrador de redes en general, se encarga principalmente de asegurar la correcta operación de la red, tomando acciones remotas o localmente. Se encarga de administrar cualquier equipo de telecomunicaciones de voz, datos y video, así como de administración remota de fallas, configuración rendimiento, seguridad e inventarios.

2.3.3.3 Protocolo de administración de red tcp/ip.

El sistema de administración de red de TCP/IP se basa en el protocolo SNMP (Simple Network Management Protocol), que ha llegado a ser un estándar de ipso en la industria de comunicación de datos para la administración de redes de computadora, ya que ha sido instalado por múltiples fabricantes de puentes, repetidores, ruteadores, servidores y otros componentes de red.

Para facilitar la transición de SNMP a CMOT (Common Management Information Services and Protocol Over TCP/IP), los dos protocolos emplean la misma base de administración de objetos MIB (Management information Base).

Para hacer más eficiente la administración de la red, la comunidad de TCP/IP divide las actividades en dos partes:

- Monitoreo, o proceso de observar el comportamiento de la red y de sus componentes, para detectar problemas y mejorar su funcionamiento.

- Control, o proceso de cambiar el comportamiento de la red en tiempo real ajustando parámetros, mientras la red está en operación, para mejorar el funcionamiento y repara fallas.

2.3.3.4 Esquema De Administración.

Como se observa, el agente y la MIB residen dentro del aparato que es monitoreado y controlado. La estación administradora contiene software que opera los protocolos usados para intercambiar datos con los agentes, y software de aplicación de administración de red que provee la interfaz de usuario para a fin de habilitar a un operador para saber el estado de la red , analizar los datos recopilados e invocar funciones de administración.

2.3.4 Sistemas De Seguridad

Desarrollar un sistema de seguridad significa: “planear, organizar coordinar dirigir y controlar las actividades relacionadas a mantener y garantizar la integridad física de los recursos implicados en las diferentes aplicaciones existentes, así como el resguardo de los activos de la empresa

Para dotar de medios necesarios para elaborar su sistema de seguridad se debe considerar los siguientes puntos:

Sensibilizar a los ejecutivos de la organización en torno al tema de seguridad.

Se debe realizar un diagnóstico de la situación de riesgo y seguridad de la información en la organización a nivel software, hardware, recursos humanos, y ambientales.

Elaborar un plan para un programa de seguridad.

Desde que el hombre ha habitado esta tierra se siente en la necesidad de obtener seguridad, desde que las primeras sociedades se asentaron una de las principales funciones del estado fue administrar justicia y proveer seguridad; es por esto que no es extraño que los usuarios opten por sistemas de seguridad para sus hogares.

Para aquellos que pretenden una definición técnica del concepto “sistema de seguridad” decimos que es un conjunto de dispositivos colocados estratégicamente en el perímetro de un sitio específico para detectar las presencia, irrupción, o invasión de un desconocido o de un individuo que no posea un acceso permitido.

La inseguridad es un factor que ha crecido mucho en los últimos años en todas las sociedades, las causas de este crecimiento son muy complicadas de entender y muchas veces se encuentran interrelacionadas; algunas personas asumen que aspectos como bajos recursos o marginación social son la causa principal de la gesta de la inseguridad, pero esta idea no es del todo acertada.

2.3.4.1 Sistema de Seguridad Electrónica

Figura 14. Sistema de Seguridad Electrónica

Cuando hacemos referencia a un sistema de seguridad no estamos hablando únicamente de sensores, cámaras y alarmas, sino también de puertas blindadas, persianas protegidas y rejas de seguridad. Podemos decir que la elección de un tipo de sistema u otro dependerá de las necesidades de cada familia o individuo, esta necesidad varía de acuerdo a la cultura del entorno, el estándar de vida y los factores psicológicos directos e indirectos. El sistema de monitoreo profesional, por ejemplo, tiene dos funciones fundamentales: minimizar las falsas alarmas y asegurar el efectivo funcionamiento del sistema en todo momento; para que ambas acciones se cumplan es fundamental que los proyectos o instalaciones y procedimientos se lleven a cabo mediante normas. Por lo general, un sistema de seguridad no es un servicio aislado sino una combinación de elementos físicos y electrónicos o una combinación de ambos.

2.3.5 Monitoreo

Existen varias clases diferentes de herramientas de monitoreo, cada una le muestra un aspecto diferente de lo que "está pasando", desde la interacción física del radio a las formas en que las aplicaciones de los usuarios interactúan entre ellas. Al observar el desempeño de la red a través del tiempo se puede tener una idea de lo que es "normal" para ella, y ser notificado automáticamente cuando las cosas están fuera de orden.

2.3.6 Circuito Cerrado de Televisión.

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. Además, a diferencia de la televisión convencional, este es un sistema pensado para un número limitado de espectadores.

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

Se encuentran fijas en un lugar determinado. En un sistema moderno las cámaras que se utilizan pueden estar controladas remotamente desde una sala de control, donde se puede configurar su panorámica, enfoque, inclinación y zoom.

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.

A continuación se enunciara varios de los dispositivos con sus respectivos fundamentos necesarios para el desarrollo de un Circuito Cerrado de Televisión.

2.3.6.1 Cámaras de T.V. en circuito cerrado

Constituyen el elemento base del sistema, ya que transforman una imagen óptica en una señal eléctrica fácilmente transmitible.

Figura 15. Cámaras de T.V. en circuito cerrado

2.3.6.1.1 El dispositivo captador de imagen.

El desarrollo de los captadores de estado sólido (CCD), con centenares de miles de elementos de imagen que actúan por transferencia de línea, desbancó a los captadores de tubo, de igual forma que los circuitos integrados sustituyeron a las válvulas electrónicas.

Se fueron estandarizado sucesivamente tres formatos, cada uno de ellos con la mitad de superficie sensible que el anterior, pero manteniendo la relación en sus lados de 4/3 (anchura/altura):

Captador CCD de 2/3"

Captador CCD de 1/2"

Captador CCD de 1/3"

En general todos dan una buena resolución, con retículas de más de 500 x 500 elementos captadores de imagen (pixels), por lo que se está imponiendo el formato pequeño, incluso para cámaras de alta resolución; su duración se considera prácticamente ilimitada, su sensibilidad es muy alta, superior a la de los antiguos tubos Ultricón, y algunas versiones permiten, como ellos, ver con luz infrarroja.

Con esta misma tecnología CCD aparecieron también cámaras en color para aplicaciones en CCTV, con sensibilidades muy altas para ser de color (menos de 2 lux en la escena, cuando las de tubo precisaban más de 200), que solucionan problemas específicos en casinos, centros comerciales, vigilancia de procesos industriales en que interviene el color, etc.

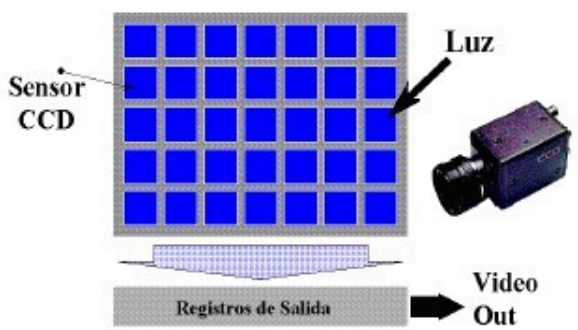


Figura 16. Arreglos del Sensor CCD

Los circuitos electrónicos, conjuntamente con el dispositivo captador, determinan la calidad de la imagen, la cual es explorada electrónicamente de izquierda a derecha y de arriba a abajo mediante unos impulsos eléctricos denominados sincronismos (horizontal y vertical).

A medida que se realiza la exploración de la imagen formada en el dispositivo captador la señal obtenida varía en función de la iluminación de cada punto, obteniéndose unas ondas eléctricas denominadas señal de vídeo.

Así pues, la señal eléctrica suministrada por una cámara de T.V. en circuito cerrado está compuesta por la superposición de tres diferentes:

Señal de vídeo
Señal de sincronismo horizontal
Señal de sincronismo vertical

En Europa se emplea la norma CCIR, que implica trazar la imagen con 625 líneas y 25 veces por segundo; para color se usa el sistema PAL, con la misma base, de forma que es compatible (pueden verse imágenes en blanco y negro provenientes de cámaras en color).

2.3.6.2 Elementos reproductores de imagen

Los elementos de un circuito cerrado de T.V. que nos permiten reproducir las imágenes captadas por las cámaras son los monitores.

Un monitor de T.V. en circuito cerrado es básicamente similar a un televisor doméstico, si bien carece de los circuitos de radiofrecuencia y dispone de selector de impedancia para la señal de entrada; también está diseñado para soportar un funcionamiento continuo.

Existen varios tamaños de la pantalla reproductora (tubo de rayos catódicos); habitualmente, en seguridad y para blanco y negro se emplean los de 9 ó 12 pulgadas (tamaño de la diagonal de la pantalla), pero pueden emplearse otros tamaños superiores para Salas de Control en que los monitores estén muy alejados del vigilante. Para color las pantallas más usuales son de 10 y 14 pulgadas.

2.3.6.3 Elementos grabadores de imagen

La señal proveniente de una cámara de T.V. en circuito cerrado, que como hemos visto es la resultante de tres tipos diferentes de impulsos eléctricos, es susceptible de ser grabada, por medio de los dispositivos adecuados.
Los dispositivos grabadores de imágenes en movimiento, que utilizan cintas magnéticas, pueden ser de dos tipos:

a) Magnetoscopios
b) Videocassettes o videograbadores

2.3.6.4 Los magnetoscopios.

También llamados grabadores de bobina abierta, prácticamente han desaparecido del mercado del CCTV, quedando solamente versiones de alto precio para estudios profesionales.

Los videocassettes son los más empleados para vigilancia, sobre todo los que utilizan cassettes VHS con cinta magnética para 3 ó 4 horas (el doble a media velocidad) y proporcionan una resolución horizontal de 240 líneas (en color) ó 300 líneas (en blanco y negro), ampliable a 400 líneas en las versiones con S-VHS.

Son recomendables los videograbadores específicamente preparados para vigilancia, con insertador de fecha y hora incorporado y entrada para señales de alarma, que prolongan una cinta de 3 horas hasta las 24 horas sin necesidad de detener el motor de arrastre; hay versiones más completas, que permiten grabaciones de hasta 960 horas, denominadas "time lapse" o intervalométricas.

Para grabar más de una cámara simultáneamente pueden emplearse los insertadores (2 cámaras) los generadores digitales de cuadrantes (4 cámaras) y los multiplexores (hasta 16 cámaras), tanto en modelos de blanco y negro como en color.

2.3.6.5 Señal de Vídeo

La señal de vídeo que genera la cámara incluye un pulso de sincronización vertical (VSYNC) que identifica el comienzo de un campo ("field") y un pulso de sincronización horizontal (HSYNC) que identifica el comienzo de una línea.

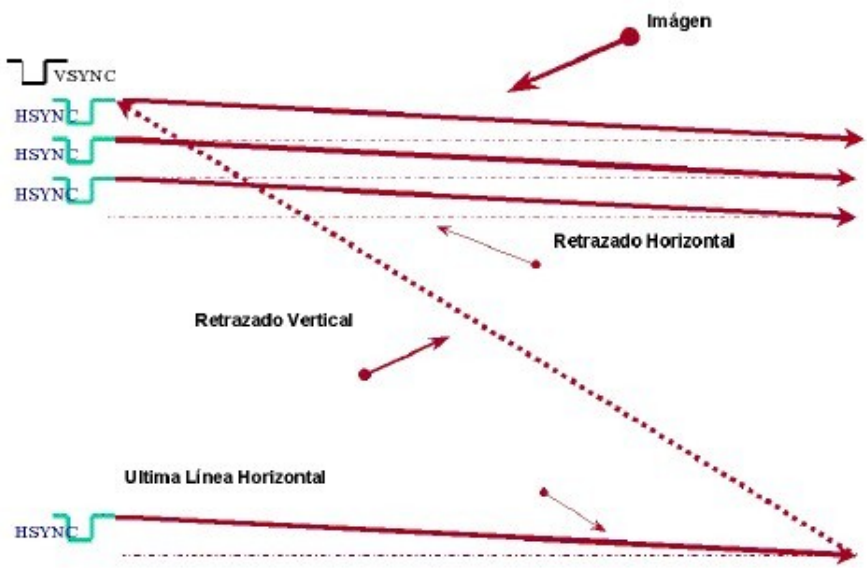


Figura 17. Barrido (despliegue de una señal de vídeo)

Por ejemplo, las cámaras que cumplen con el estándar EIA (Electronic Industries Association) RS-170, actualizan la imágen de vídeo a una tasa de 30 cuadros por segundo (30 frames/sec). Los campos (fields) son entrelazados para aumentar la tasa de actualización o refrescamiento percibido de la imagen.

2.3.7 Sistema de video vigilancia

Los sistemas garantes basados en la tecnología referida a las CÁMARAS DE SEGURIDAD, han venido actualmente en brindar un fuerte apoyo al tema de la seguridad integral, aludiendo entre sus virtudes ejercer una VIGILANCIA PREVENTIVA, mediante el registro visual de sucesos. Su incorporación y aplicación en el mercado, va dirigida a asegurar un amplio espectro de ambientes y lugares, que van desde: Empresas de diversas rubros; Centros Comerciales; Supermercados; Aeropuertos; Condominios y Viviendas particulares; Vías Públicas; Centros de Eventos; Trasporte Público; Gran Minería y Establecimientos Educacionales, entre otros. A modo de conocimiento respecto de la evolución que han experimentado estos sistemas durante el transcurso de los últimos años, podríamos catalogarlas en dos grandes eras: La ANÁLOGA y la DIGITAL.

Figura 18. Cámara de un Sistema Digital

No obstante contar actualmente el mercado con los dos tipos de sistemas, la mayoría de las empresas e instituciones de variada índole aun cuentan con sistemas de seguridad basados en cámaras de vigilancia ANÁLOGA (en muchos casos obsoletos). Sin embargo, dada la rápida evolución de las técnicas delictuales es recomendable reemplazar a la brevedad los sistemas análogos por los llamados digitales, (DVR). Introduciéndolos y para obtener una mayor comprensión acerca de la evolución de los llamados SISTEMAS DIGITALES, con relación a sus virtudes y a las ventajas que para su seguridad representan a continuación exponemos una breve reseña de sus progresos.

2.3.8 Cámaras IP

Una Cámara IP (también conocidas como cámaras Web o de Red) son videocámaras especialmente diseñadas para enviar las señales (video, y en algunos casos audio) a través de Internet desde un explorador (por ejemplo el Internet Explorer) o a través de concentrador (un HUB o un SWITCH) en una Red Local (LAN).

2.3.8.1 Dirección IP

Es la dirección única en la red donde se encuentra nuestro dispositivo y servirá de identificador del dispositivo. Veamos que nos dice Wikipedia sobre lo que es una dirección IP. Cuando nos encontremos con un "tecnicismo" o un término tecnológico que no sabemos lo que significa, podemos ir al diccionario Wikipedia en Internet: Es como la clásica enciclopedia de toda la vida, pero en Internet. Pedimos que nos busque "Dirección IP" y obtenemos esto: Una dirección IP es un número que identifica de manera lógica y jerárquica a una interfaz de un dispositivo (habitualmente una computadora) dentro de una red que utilice el protocolo IP (Internet Protocol), que corresponde al nivel de red o nivel 3 del modelo de referencia OSI. Dicho número no se ha de confundir con la dirección MAC que es un número hexadecimal fijo que es asignado a la tarjeta o dispositivo de red por el fabricante, mientras que la dirección IP se puede cambiar.

Es habitual que un usuario que se conecta desde su hogar a Internet utilice una dirección IP.

Esta dirección puede cambiar al reconectar; y a esta forma de asignación de dirección IP se denomina una dirección IP dinámica (normalmente se abrevia como IP dinámica). Los sitios de Internet que por su naturaleza necesitan estar permanentemente conectados, generalmente tienen una dirección IP fija (se aplica la misma reducción por IP fija o IP estática), es decir, no cambia con el tiempo. Los servidores de correo, DNS, FTP públicos, y servidores de páginas web necesariamente deben contar con una dirección IP fija o estática, ya que de esta forma se permite su localización en la red. A través de Internet, los ordenadores se

conectan entre sí mediante sus respectivas direcciones IP. Sin embargo, a los seres humanos nos es más cómodo utilizar otra notación más fácil de recordar y utilizar, como los nombres de dominio; la traducción entre unos y otros se resuelve mediante los servidores de nombres de dominio DNS. Existe un protocolo para asignar direcciones IP dinámicas llamado DHCP (Dynamic Host Configuration Protocol).

2.4 HIPÓTESIS

Un sistema de seguridad y monitoreo basado en internet para cámaras IP permitirá un mejor control de la empresa disminuyendo el posible número de robos.

2.5 VARIABLES

2.5.1 VARIABLE INDEPENDIENTE

Sistema de seguridad y monitoreo

2.5.2 VARIABLE DEPENDIENTE

Cámaras IP

CAPITULO III

METODOLOGIA

3.1 Enfoque

La presente investigación estará enmarcada dentro del paradigma crítico propositivo por lo tanto tendré un enfoque cuali-cuantitativo porque se efectuará una investigación que permitirá obtener información que servirá de referencia para interpretarla con el sustento científico y profesional, con lo que se pretende solucionar el problema.

La parte cualitativa estará enmarcada en un análisis de resultados de calidad en base al marco teórico consultado y que servirá de base para la toma de decisiones.

3.2 Modalidad básica de la investigación

3.2.1 Investigación Bibliográfica - Documental

Se realizó una investigación bibliográfica - documental para poder obtener información más profunda con respecto a problemas similares, de esta manera recopilar información valiosa que sirvió de apoyo en la realización del proyecto.

3.3 Nivel o tipo de Investigación

3.3.1 Exploratorio

Es exploratorio porque fue necesario realizar el estudio del problema, para poder establecer el origen del mismo, además de investigar las causas del problema, y el porqué se dio el mismo.

3.3.2 Descriptivo

Es descriptivo porque analizó al problema, cuales son las causas, consecuencias y dificultades por lo que está atravesando el problema.

3.4 Población y muestra

3.4.1 Población

Para la elaboración del presente proyecto se trabajo con toda la población ya que la población es pequeña por que consta de seis Ingenieros.

3.5 Recolección de información

3.5.1 Plan de Recolección de Información

Las personas que proporcionaron información fueron los Ingenieros encargados de los diferentes módulos quienes asesoraron en la parte científica y de las experiencias obtenidas por los dueños de empresas.

3.6 Procesamiento y análisis de la Información

3.6.1 Plan que se empleará para procesar la información recogida.

Procesamiento de la información, una vez aplicados los instrumentos y analizada la validez de la información se procedió a la tabulación de los datos, los cuales se presentaron en gráficos en términos de porcentaje para facilitar la interpretación.

3.6.2 Plan de análisis e interpretación de resultados

Se realizó el análisis integral en base a juicios críticos desprendidos del marco teórico, objetivos y variables de la investigación. A continuación se estructuro las conclusiones y recomendaciones que organizadas secuencialmente permitieron dar solución al problema planteado.

CAPITULO IV

ANÁLISIS E INTERPRETACIÓN DE RESULTADOS

4.1 Análisis de resultados

Que impacto causará en el personal los sistemas de seguridad y monitoreo basado en internet para cámaras IP: Con los sistemas inteligentes de captación de cámaras IP no se busca sólo detectar la infracción de seguridad, o el hurto, sino una vez analizados los datos que se graban online, detectar pautas de comportamiento para corregirlas y evitarlas. La eficacia esta cambiando a raíz de los acontecimientos, cuando no sirve para prevenir, las cámaras IP pueden servir para identificar y capturar a los culpables de los hechos, o encontrar elementos de su organización.

La empresa y sus trabajadores están continuamente expuestos a robos y atracos. Por otro lado, la supervisión del trabajo, el buen funcionamiento y el control del personal son otra de las preocupaciones constantes e mediante dicho sistema tendremos mayor seguridad y eficiencia. El sistema de video vigilancia proporciona gran seguridad y control.

Por medio de este sistema no necesita estar presente para saber lo que sucede, desde la comodidad de su hogar o de cualquier lugar del mundo con una computadora conectada a internet podemos observar las imágenes de las cámaras instaladas en la empresa.

CAPITULO V

CONCLUSIONES Y RECOMENDACIONES

5.1 CONCLUSIONES

La video vigilancia por cámaras IP es uno de los sistemas más prácticos y rentables en materia de seguridad. Como soporte técnico ofrece una excelente calidad y además si se instala adecuadamente, los costos de mantenimiento prácticamente no existe.

Muchas empresas, locales comerciales y hogares no son aun consientes de que hay caminos para transformar los actuales sistemas de seguridad analógicos a la tecnología de video digital.

La mayoría de los usuarios finales aun no tienen conocimiento de los beneficios y posibilidades de los sistemas de vigilancia digitales basados en redes, incluso una sola cámara conectada a un servidor de video proporcionara al usuario final todo el rango de beneficios que vienen asociados a la

vigilancia digital en red por lo tanto, la video vigilancia en red es lo mejor en este momento.

La video vigilancia por cámaras IP va más allá del control y grabación de seguridad conocido hasta ahora. Con el sistema desarrollado, se puede observar desde cualquier parte del mundo, en tiempo real, lo que sucede en la empresa, así mismo, con la grabación digital basada en el movimiento y la comprensión de imágenes se incrementa de forma significativa el tiempo de grabación disponible.

El sistema de alarma es una tecnología digital que va ayudar considerablemente al sistema de video vigilancia ya que por medio de sus sensores podemos saber en el instante que se esta suscitando un robo ya que este sistema también cuenta con monitoreo y en ese momento conectarnos al internet y observar que esta sucediendo.

5.2 RECOMENDACIONES

Cuando se de implementación del sistema de video vigilancia con cámaras IP y el sistema de alarma se debe capacitar al personal con el funcionamiento de los equipos.

Los beneficios de la tecnología video digital se deben dar a conocer a las empresas mediante conferencias, a los locales comerciales y residencias mediante promociones.

Revisar la funcionalidad, la nitidez en la resolución de los videos e imágenes, la facilidad de conexión, la movilidad de las cámaras y en fin las innumerables ventajas que el sistema de video vigilancia con cámaras IP ofrece desde el mismo instante en que empieza a trabajar.

El sistema de video vigilancia y seguridad que el presente trabajo de investigación planteamos cumple con vigilancia en áreas estratégicas, así como también esta en un nivel superior de acuerdo a las exigencias que los propietarios de la empresa demandan, eso quiere decir que satisface todas las necesidades en cuanto a vigilancia, control y seguridad se refiere.

El sistema de alarma se recomienda junto al sistema de video vigilancia IP ya que trabajando los dos en forma simultánea vamos a tener mucha más seguridad en dicha empresa.

CAPITULO VI

PROPUESTA

6.1 Datos Informativos

Tema:

Sistema de Seguridad y Monitoreo basado en internet para cámaras IP en la empresa Vipdrive.

Autor:

Darwin Xavier Estrada Martínez

Tutor:

Ing. Javier Sánchez Guerrero.

Fecha Duración:

06/11/08 – 06/04/09

6.2 Antecedentes de la propuesta

Desde que el hombre ha habitado esta tierra se siente en la necesidad de obtener seguridad, desde que las primeras sociedades se asentaron una de las principales funciones del estado fue administrar justicia y proveer seguridad; es por esto que no es extraño que los usuarios opten por sistemas de seguridad para sus hogares.

Para aquellos que pretenden una definición técnica del concepto “sistema de seguridad” decimos que es un conjunto de dispositivos colocados estratégicamente en el perímetro de un sitio específico para detectar las presencia, irrupción, o invasión de un desconocido o de un individuo que no posea un acceso permitido.

La evolución en las comunicaciones en el mundo hace que día a día nos quedemos atrás, por esta razón es necesario que apliquemos la tecnología de video vigilancia para prevenir y controlar pérdidas; aseguramiento a personas; planes de protección ambiental; proyectos de prevención de incendios como también la protección de la estructura física de las empresas, y otros servicios que le darán la clave para sentirse seguro y protegido integralmente en todo momento.

Entre las distintas cámaras y la imagen a presentar al operador se proponen una variedad de posibilidades dependiendo de la arquitectura del edificio, de la zonificación del mismo y de las posibilidades de control. Estos últimos equipamientos incluyen: mecanismos de control de posición de cámara (pon-tild), controles de aproximación (zoom), controladores de señal (switches), grabadores de

señal, particionadores de imagen (quad), etc. Todos estos procesos se pueden hoy controlar mediante el software aplicado, e incluso utilizar las redes instaladas más comunes como las Ethernet, fibras ópticas e incluso la red telefónica del edificio para transmitir las señales de vídeo.

El sistema de seguridad electrónica puede estar conectado a una central de vigilancia privada para que al cabo de pocos minutos personal policial se haga presente en nuestra ayuda. La inseguridad es un factor que ha crecido mucho en los últimos años en todas las sociedades, las causas de este crecimiento son muy complicadas de entender y muchas veces se encuentran interrelacionadas; algunas personas asumen que aspectos como bajos recursos o marginación social son la causa principal de la gesta de la inseguridad, pero esta idea no es del todo acertada.

6.3 Justificación

La empresa Vipdrive necesita trabajar con seguridad y control, ser capaces de adaptar las funciones a las nuevas necesidades o introducirse rápidamente en nuevos mercados para responder a las nuevas demandas. Pues bien, en los últimos años, tenemos que se ha potenciado el desarrollo de la tecnología de cámaras IP (Internet Protocol), alternativa que ha venido en resolver la totalidad de los problemas presentados por dicha empresa.

Estos nuevos sistemas están principalmente basados en una plataforma computacional que permite la visualización/grabación de grupos de cámaras (en formatos de 4, 8, 16,32 cámaras como estándar) durante las 24 horas del día, manteniendo como característica relevante el almacenamiento digital de las imágenes obtenidas desde las cámaras en discos duros, de la misma forma en que un archivo se guarda en un PC.

Esta función permite, entre otros beneficios, obtener una mayor calidad de las imágenes grabadas sin deterioro en el tiempo, grabación circular sin necesidad de reemplazar cintas (esto es, que dependiendo de la capacidad de los discos duros, se

pueden almacenar varios días continuos de grabación que se van renovando en forma automática), y entre otros una fácil búsqueda automatizada de las imágenes grabadas sobre la base de fechas, horas, número de cámara, sistemas de alarmas, etc.

6.4 Objetivos

6.4.1 Objetivo General

6.4.1.1 Instalar Cámaras IP y Sistema de Seguridad Electrónico.

6.4.2 Objetivos Específicos

6.4.2.1 Estudio de Planos de la Empresa Vipdrive.

6.4.2.2 Configurar Cámaras IP.

6.4.2.3 Instalar Software.

6.4.2.4 Configurar Switch.

6.4.2.5 Programación del Sistema de Seguridad Electrónico.

6.5 Análisis de Factibilidad

6.5.1 Factibilidad tecnológica

El presente estudio contempla la posibilidad de realizar el proyecto, se realizó un análisis de la propuesta a desarrollar y las características de hardware y software de

dicho proyecto son totalmente accesibles, se tiene las capacidades técnicas requeridas por cada alternativa del diseño que se esté considerando.

6.5.2 Factibilidad Económica

La Empresa Vipdrive cuenta con el presupuesto necesario para poder realizarlo. Los costos de implementación incluyen comúnmente el costo de la investigación del sistema, los costos de hardware y software, los costos de operación del sistema para su vida útil esperada, y los costos de mano de obra, material, energía, reparaciones y mantenimiento.

6.5.3 Factibilidad Operativa

El proyecto es operativo, ya que es posible conectar un conjunto de computadoras mediante la red de área local de la empresa y comunicarnos al sistema mediante internet.

6.6 Fundamentación Teórica

6.6.1 La Comunicación

La comunicación es un fenómeno de carácter social que comprende todos los actos mediante los cuales los seres vivos se comunican con sus semejantes para transmitir o intercambiar información. Comunicar significa poner en común e implica compartir.

La comunicación inicia con el surgimiento de la vida en nuestro planeta y su desarrollo ha sido simultáneo al progreso de la humanidad. Se manifestó primero a través de un lenguaje no verbal.

Todos los días los seres vivos se comunican de diferentes maneras, pero sólo los seres humanos podemos hacerlo racionalmente; llevando a cabo infinidad de actividades, tales como: conversar, reír, llorar, leer, ver televisión entre otras; por ello se dice que la comunicación humana es un proceso:

- Dinámico: porque está en continuo movimiento.
- Inevitable: porque se requiere para la transmisión de significados.
- Irreversible: porque una vez realizada, no puede regresar, borrarse o ignorarse.
- Bidireccional: porque existe una respuesta en ambas direcciones.
- Verbal y no verbal: porque implica la utilización de ambos lenguajes.

Desde un punto de vista técnico se entiende por comunicación el hecho que un determinado mensaje originado en el punto A llegue a otro punto determinado B, distante del anterior en el espacio o en el tiempo. La comunicación implica la transmisión de una determinada información. La información como la comunicación supone un proceso; los elementos que aparecen en el mismo son:

- El código es un sistema de signos y reglas para combinarlos, que por un lado es arbitrario y por otra parte debe de estar organizado de antemano.
- El proceso de comunicación que emplea ese código precisa de un canal para la transmisión de las señales. El Canal sería el medio físico a través del cual se transmite la comunicación.

6.6.2 Redes de área local (LAN)

Uno de los sucesos más críticos para la conexión en red lo constituye la aparición y la rápida difusión de la red de área local (LAN) como forma de normalizar las conexiones entre las máquinas que se utilizan como sistemas ofimáticos. Como su propio nombre indica, constituye una forma de interconectar una serie de equipos informáticos. A su nivel más elemental, una LAN no es más que un medio compartido (como un cable coaxial al que se conectan todas las computadoras y las impresoras) junto con una serie de reglas que rigen el acceso a dicho medio. La LAN más difundida, la Ethernet, utiliza un mecanismo denominado Call Sense Multiple Access-Collision Detect (CSMS-CD). Esto significa que cada equipo conectado sólo puede utilizar el cable cuando ningún otro equipo lo está utilizando. Si hay algún conflicto, el equipo que está intentando establecer la conexión la anula y efectúa un nuevo intento más adelante. La Ethernet transfiere datos a 10 Mbits/seg, lo suficientemente rápido como para hacer inapreciable la distancia entre los diversos equipos y dar la impresión de que están conectados directamente a su destino.

Ethernet y CSMA-CD son dos ejemplos de LAN. Hay tipologías muy diversas (bus, estrella, anillo) y diferentes protocolos de acceso. A pesar de esta diversidad, todas las LAN comparten la característica de poseer un alcance limitado (normalmente abarcan un edificio) y de tener una velocidad suficiente para que la red de conexión resulte invisible para los equipos que la utilizan.

Además de proporcionar un acceso compartido, las LAN modernas también proporcionan al usuario multitud de funciones avanzadas. Hay paquetes de software de gestión para controlar la configuración de los equipos en la LAN, la administración de los usuarios, y el control de los recursos de la red. Una estructura muy utilizada consiste en varios servidores a disposición de distintos (con frecuencia, muchos) usuarios. Los primeros, por lo general máquinas más potentes, proporcionan servicios como control de impresión, ficheros compartidos y correo a los últimos, por lo general computadoras personales.

6.6.2.1 Diseño de una LAN

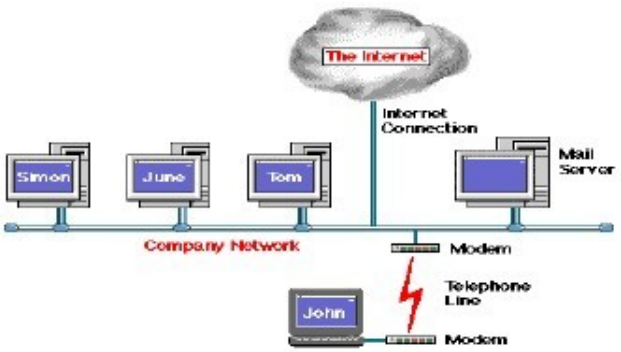


Figura 19. Diseño de una LAN

6.6.2.2 Topología:

Es simplemente visualizar el sistema de comunicación en una red es conveniente utilizar el concepto de topología, o estructura física de la red. Las topologías describen la red físicamente y también nos dan información acerca de el método de acceso que se usa (Ethernet, Token Ring, etc.). Entre las topologías conocidas tenemos.

6.6.2.3 Perdida de las Datos:

La pérdida de datos es producida por algún virus o por otro tipo de incidencia, los mas comunes son mal manejo por parte del usuario o personas inescrupulosas que acceden al sistema o mediante Internet, estos puede incidentes pueden evitarse de tal manera que en las estaciones de trabajo se instalan códigos para que así tengan acceso solo personal autorizado, en cuanto a Internet hay muchos software en el mercado mejor conocidos como Muros de fuego, que sirve para detener a los intrusos.

6.6.2.4 Caídas Continuas de la Red:

La caída continua en una Red se debe en la mayoría de los casos a una mala conexión Servidor > Concentrador o la conexión existente con el proveedor de Internet.

6.6.2.5 En el procesamiento de la información es muy lento:

Cuando el procesamiento de información de una Red es muy lento tenemos que tomar en cuenta el tipo de Equipos que elegimos, (Servidor, Cableado, Concentrador, Estaciones de Trabajo y otros, ya que si tomamos una decisión errónea perderemos tanto tiempo como dinero.

6.6.2.6 Protocolos a usar

6.6.2.6.1 TCP/IP:

Se refiere a los dos protocolos que trabajan juntos para transmitir datos: el Protocolo de Control de Transmisión (TCP) y el Protocolo Internet (IP). Cuando envías información a través de una Intranet, los datos se fragmentan en pequeños paquetes. Los paquetes llegan a su destino, se vuelven a fusionar en su forma original. El Protocolo de Control de Transmisión divide los datos en paquetes y los reagrupa cuando se reciben. El Protocolo Internet maneja el encaminamiento de los datos y asegura que se envían al destino exacto.

6.6.2.6.2 Norma EIA/TIA 568:

ANSI/TIA/EIA-568-A (Alambrado de Telecomunicaciones para Edificios Comerciales). Este estándar define un sistema genérico de alambrado de telecomunicaciones para edificios comerciales que puedan soportar un ambiente de productos y proveedores múltiples.

El propósito de este estándar es permitir el diseño e instalación del cableado de telecomunicaciones contando con poca información acerca de los productos de telecomunicaciones que posteriormente se instalarán. La instalación de los sistemas de cableado durante el proceso de instalación y/o remodelación son significativamente más baratos e implican menos interrupciones que después de ocupado el edificio.

El propósito de esta norma es permitir la planeación e instalación de cableado de edificios comerciales con muy poco conocimiento de los productos de telecomunicaciones que serán instalados con posterioridad. La instalación de sistemas de cableado durante la construcción o renovación de edificios es significativamente menos costosa y desorganizadora que cuando el edificio está ocupado.

6.6.2.7 Alcance

La norma EIA/TIA 568A específica los requerimientos mínimos para el cableado de establecimientos comerciales de oficinas. Se hacen recomendaciones para:

- Las topología
- La distancia máxima de los cables
- El rendimiento de los componentes
- Las tomas y los conectores de telecomunicaciones

Se pretende que el cableado de telecomunicaciones especificado soporte varios tipos de edificios y aplicaciones de usuario. Se asume que los edificios tienen las siguientes características:

- Una distancia entre ellos de hasta 3 Km.
- Un espacio de oficinas de hasta 1,000,000 m2

Una población de hasta 50,000 usuarios individuales

Las aplicaciones que emplean los sistemas de cableado de telecomunicaciones incluyen, pero no están limitadas a:

Voz , Datos, Texto, Video, Imágenes

La vida útil de los sistemas de cableado de telecomunicaciones especificados por esta norma debe ser mayor de 10 años.
Las normas EIA/TIA es una de las mejores Normas por sus Antecedentes que son: Vos, Dato, video, Control y CCTV

6.6.2.8 Utilidades y Funciones:

Un sistema de cableado genérico de comunicaciones para edificios comerciales. Medios, topología, puntos de terminación y conexión, así como administración, bien definidos. Un soporte para entornos multi proveedor multi protocolo. Instrucciones para el diseño de productos de comunicaciones para empresas comerciales. Capacidad de planificación e instalación del cableado de comunicaciones para un edificio sin otro conocimiento previo que los productos que van a conectarse.

Beneficios: Flexibilidad, Asegura compatibilidad de Tecnologías, Reduce Fallas, Traslado, adiciones y cambios rápidos

6.6.2.9 Plataforma a utilizar.

Microsoft Windows XP: Windows XP se utiliza porque es muy sencillo por la compatibilidad entre aplicaciones y hardware. Confiabilidad del sistema operativo y la Seguridad, incluida las actualizaciones más recientes que resuelven los problemas de seguridad detectados en Windows XP

6.6.2.10 Determinación de los Equipos a utilizar en una LAN.

6.6.2.10.1 Estaciones de Trabajo:

Dispositivo electrónico capaz de recibir un conjunto de instrucciones y ejecutarlas realizando cálculos sobre los datos numéricos, o bien compilando y correlacionando otros tipos de información. Estos permiten que los usuarios intercambien rápidamente información y en algunos casos, compartan una carga de trabajo.

Generalmente nos enfocamos en los ordenadores más costosos ya que posee la última tecnología, pero para el diseño de una Red de Área Local solamente necesitamos unas estaciones que cumpla con los requerimientos exigidos, tengamos cuidado de no equivocarnos ya que si damos fallo a un ordenador que no cumpla los requerimientos perderemos tiempo y dinero.

Switch o (HUB).- Es el dispositivo encargado de gestionar la distribución de la información del Servidor (HOST), a la Estaciones de Trabajo y/o viceversa. Las computadoras de Red envía la dirección del receptor y los datos al HUB.

MODEM.- Equipo utilizado para la comunicación de computadoras a través de líneas analógicas de transmisión de datos. El módem convierte las señales digitales del emisor en otras analógicas susceptibles de ser enviadas por teléfono. Cuando la señal llega a su destino, otro módem se encarga de reconstruir la señal digital primitiva, de cuyo proceso se encarga la computadora receptora. NOTA: El Fax Modem solo lo usaremos para el Servidor (HOST). Comúnmente se suele utilizar un Modem de 56K.

Tarjetas Ethernet (Red).- es aquella que se encarga de interconecta las estaciones de trabajo con el concentrador y a su vez con el Servidor (HOST).

6.6.3 Cable UTP Categoría 5E

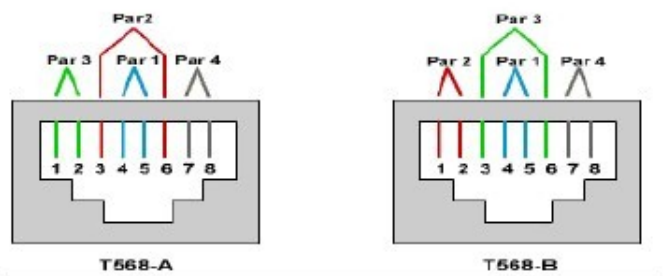
Las aplicaciones de telecomunicaciones que actualmente se desarrollan son cada día más demandantes de recursos, por lo que el sistema para transporte de información (anteriormente cableado estructurado) es uno de los factores más importantes dentro de las redes informáticas. Por lo tanto la solución que se instale deberá estar a la altura de estas aplicaciones y deberá ser la mejor opción en términos de costo-beneficio.

Es un cable de 8 hilos formado por 4 pares que se usa conjuntamente con conectores RJ45 en conexiones de red. Cada par viene enrroscado y diferenciados por colores.

Los 4 pares a su vez vienen enrroscados entre sí, para minimizar los efectos negativos entre ellos y el medio ambiente. Las diferentes categorías han ido surgiendo a medida que se mejoraron las técnicas de fabricación. Ya se está en la categoría 6.

De los 4 pares por ahora solo se usan dos, los otros dos se previeron para un aumento de uso en un futuro que quizás nunca se llegue a dar, pues posiblemente la técnica cambie antes, pero por ahora el cable nos cuesta más de lo necesario por eso mismo.

Algunos datos sobre el cableado Categoría 5: El cableado estructurado en categoría 5 es el tipo de cableado más solicitado hoy en día. El cable UTP (Unshielded Twisted Pair) posee 4 pares bien trenzados entre si.



- Par 1: Blanco/Azul * Azul ----------Contactos: 5 * 4
- Par 2: Blanco/Naranja * Naranja-----Contactos: 3 * 6
- Par 3: Blanco/Verde * Verde---------Contactos: 1 * 2
- Par 4: Blanco/Marrón * Marrón------Contactos: 7 * 8

Figura 20. Diagrama que muestra los colores de los cables T568-A y T568-B

Esta normalizado por los apéndices EIA/TIA TSB 36 (cables) y TSB 40 (conectores)

Es la más alta especificación en cuanto a niveles de ancho de banda y performance.

Es una especificación genérica para cualquier par o cualquier combinación de pares.

No se refiere a la posibilidad de transmitir 100 Mb/s para solo una sola combinación de pares elegida; El elemento que pasa la prueba lo debe hacer sobre "todos" los pares.

No es para garantizar el funcionamiento de una aplicación específica. Es el equipo que se le conecte el que puede usar o no todo el Bw permitido por el cable.

Los elementos certificados bajo esta categoría permiten mantener las especificaciones de los parámetros eléctricos dentro de los limites fijados por la norma hasta una frecuencia de 100 Mhz en todos sus pares.

Como comparación se detallan los anchos de banda (Bw) de las otras categorías:

Categoría 1y 2: No están especificadas

Categoría 3: hasta 16 Mhz

Categoría 4: hasta 20 Mhz

Categoría 5: hasta 100 Mhz

Los parámetros eléctricos que se miden son:

Atenuación en función de la frecuencia (db)

Impedancia característica del cable (Ohms)

Acoplamiento del punto mas cercano (NEXT- db)

Relación entre Atenuación y Crostalk (ACR- db)

Capacitancia (pf/m)

Resistencia en DC (Ohms/m)

Velocidad de propagación nominal (% en relación C)

Distancias permitidas:

El total de distancia especificado por norma es de 99 metros.

El límite para el cableado fijo es 90 m y no está permitido excederse de esta distancia, especulando con menores distancias de patch cords.

El limite para los patch cord en la patchera es 6 m. El limite para los patch cord en la conexión del terminal es de 3 m.

6.6.4 Conectores RJ45:

Es un acoplador utilizado para unir cables o para conectar un cable adecuado en este caso se Recomienda los conectores RJ45.

Figura 21. Conectores RJ45

6.6.4.1 Ponchado

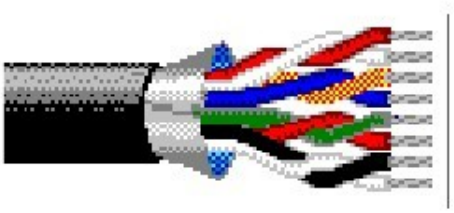


Figura 22. Cable UTP Categoría 5E

La relación de colores de los cuatro pares de hilos del cable UTP son:

Par 1: T1,R1 = AZUL

Par 2: T2,R2 = NARANJA

Par 3: T3,R3 = VERDE

Par 4: T4,R4 = CAFE

La tabla muestra la posición de los pares de hilos para el estandar EIA/TIA 568-A y la figura muestra las posiciones de un conector RJ45 (jack).

ESTANDAR EIA/TIA 568A

PIN COLOR/HILO

PAR 3 1 VERDE

PAR 3 2 BLANCO/VERDE

PAR 2 3 BLANCO/NARANJA

PAR 1 4 BLANCO/AZUL

PAR 1 5 AZUL

PAR 2 6 NARANJA

PAR 4 7 CAFÉ

PAR 4 8 BLANCO/CAFÉ

6.6.5 Switch

Figura 23. Switch

Es el dispositivo encargado de gestionar la distribución de la información del Servidor (HOST), a la Estaciones de Trabajo y/o viceversa. Las computadoras de Red envía la dirección del receptor y los datos al HUB, que conecta directamente los ordenadores emisor y receptor. Tengamos cuidado cuando elegimos un tipo de concentrador (HUB), esto lo decimos ya que se clasifican en 3 categorías. Solo se usaran concentradores dependiendo de las estaciones de trabajo que así lo requieran.

6.6.5.1 Switch para Grupos de Trabajo:

Un Switch para grupo de trabajo conecta un grupo de equipos dentro de su entorno inmediato.

6.6.5.2 Switchs Intermedios:

Se encuentra típicamente en el
Closet de comunicaciones de cada planta. Los cuales conectan
Los Concentradores de grupo de trabajo. (Ellos pueden ser
Opcionales)

6.6.5.3 Switch Corporativos:

Representa el punto de conexión
Central para los sistemas finales conectados los concentradores
Intermedio. (Concentradores de Tercera Generación).

6.6.6 Cámaras IP

Una cámara de red puede ser descrita como una cámara y un ordenador en una unidad inteligente. Captura y transmite imágenes digitales en vivo directamente a través de cualquier red IP (por ejemplo: LAN/Intranet/Internet), permitiendo a los usuarios ver

y/o manejar la cámara de forma remota a través de un servidor Web en cualquier lugar y en cualquier momento.

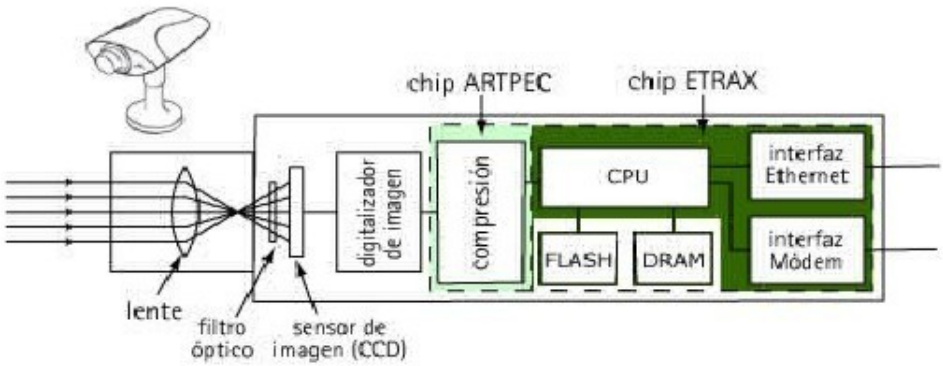


Figura 24. Estructura Interna de una Cámara IP

6.6.6.1 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 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.

El chip ARTPEC (Axis Real Time Picture EnCoder), desarrollado por Axis, es el que realiza 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. El chip ARTPEC también incluye un componente de compresión de vídeo que comprime la imagen digital a una imagen con la información reducida para su eficiente envío a través de la red.

La conexión Ethernet de la cámara se consigue gracias al chip ETRAX, una solución de sistema en un chip que permite conectar periféricos a la red. El ETRAX incluye una CPU de 32 bit, conectividad 10/100 Mb 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.

6.6.6.2 Ventajas de las Cámaras de Red

6.6.6.2.1 Transmisión de imagen universal y económica

Cualquier componente IT, tal como RALI, DSL, RDSI, GSM y Ethernet, se puede utilizar para transmitir imágenes de manera económica. Incluso se puede acceder a las cámaras desde cualquier parte del mundo a través de líneas especializadas o de Internet. No se requiere cableado analógico

especial. Como no es necesario adherirse rígidamente al video analógico estándar, ya no hay ninguna restricción en la resolución de la imagen. Por consiguiente, las primeras cámaras de seguridad con mega pixel están ahora disponibles.

6.6.6.2.2 Tecnología web libre de licencia

Se puede acceder a las imágenes de las cámaras de red a través de Internet utilizando el navegador web actual de cualquier PC (Explorer, Netscape). A pesar del sistema operativo y del número de usuarios de la cámara, no se requieren licencias de mantenimiento ni software.

6.6.6.2.3 Alta seguridad

A diferencia del cable de video analógico que puede sufrir interferencias relativamente fácil a través de medios electromagnéticos, las cámaras de red se pueden proteger de diferentes maneras. Junto con las tecnologías de codificación del software establecido como PGP (Pretty Good Privacy), también soportan enrutadores VPN seguros (Virtual Private Network) a través de Internet.

6.6.6.2.4 Expansión ilimitada

Hay incontables ordenadores interconectados en empresas grandes, guardando la información céntricamente en el servidor de la empresa. Así mismo es posible interconectar cientos de cámaras exactamente de la misma manera. La estructura de red le permite al sistema de cámaras ampliarse sin ninguna dificultad. Si es necesario, esto también se puede

hacer sobre una base inalámbrica utilizando una WLAN (Wireless Local Área Network).

6.6.6.3 ¿Cómo se conecta una cámara IP a Internet? ¿Y a una red local (LAN)?

Figura 25. Conexión de una Cámara IP a Internet

6.6.6.4 ¿Qué necesito para ver una cámara IP desde una red externa?

Lo más importante para poder usar una cámara IP es disponer de una conexión a Internet si tenemos intención de poder las imágenes en una red externa, para ello conecto la cámara IP a un Router ADSL , XDSL, o Cable modem (o a un HUB) u otros sistemas de banda ancha.

No es necesario IP fija, ya que en el caso de IP dinámica podemos acudir a sitios como www.no-ip.com (algunas cámaras vienen con sitios de resolución dinámica de IP,s especiales) para la resolución DNS.

6.6.6.5 ¿Cómo es una cámara IP por dentro?

Básicamente una cámara IP se compone de:

- La " cámara " de video tradicional (lentes, sensores, procesador digital de imagen, etc) Un sistema de compresión de imagen (para poder comprimir las imágenes captadas por la cámara a formatos adecuados como MPEG4
- Un sistema de procesamiento (CPU, FLASH, DRAM y un módulo Wireless ETHERNET/WIFI). Este sistema de procesamiento se encarga de la gestión de las imágenes, del envío al modem. Del movimiento de la cámara (si dispone de motor), de la detección de movimiento.

Con todo esto únicamente necesitamos conectar la cámara al Router ADSL y a la alimentación eléctrica y no necesitamos nada más o si pensamos usar la cámara en una red local, lo conectamos a un HUB/SWITCH y pasa a ser un equipo más que se comunica con el resto de la LAN (y con el exterior si la LAN dispone de conexión a Internet)

6.6.6.6 ¿Qué puedo hacer con una cámara IP?

Las cámaras IP se utilizan mucho en entornos de vigilancia:

- En el hogar: para poder " vigilar " tu casa, negocio, empresa, a personas mayores, a niños o bebes, y hacerlo desde tu trabajo, desde tu lugar de vacaciones, desde cualquier lugar con una conexión Internet y un explorer.

- En el trabajo: puede utilizarse para controlar puntos de tu comercio a los que tu vista no alcanza y no quieres dejar sin vigilancia o para ver lo que ocurre en tu cadena de tiendas desde tu casa.

- Empresas: para vigilar almacenes, aparcamientos, obras, entradas.

- Hostelería: restaurantes, hoteles, o simplemente para promoción de estos.

 Zonas deportivas

Y no sólo para vigilancia: muchos organismos de turismo utilizan cámaras IP para que los futuros turistas o gente interesada puedan ver la ciudad que van a visitar o el tiempo que hace o algún monumento, y han decidido poner cámaras para que puedan verse por Internet.

Y también se utilizan en temas de marketing, en museos, para control de fauna, y un sin fin de aplicaciones.

6.6.6.7 ¿Con una cámara IP puedo accionar dispositivos de forma remota?

Si que es posible. (al menos con las cámaras que disponemos en Domodesk) Se puede conectar un relé que maneje por ejemplo el encendido de luces, o la apertura de una puerta. Las cámaras IP y los servidores de video disponen de una salida Abierto-Cerrado que se controla desde el software de visualización.

6.6.6.8 ¿Puedo poner las cámaras IP en el exterior?

Si que se puede, al igual que casi todas las cámaras de TV. Las cámaras IP están diseñadas para ser utilizadas en interiores (con unas condiciones de polvo, humedad, temperatura), pero para ser utilizadas en el exterior (o en interiores con condiciones especiales) es necesario el uso de carcasas de protección adecuadas al uso que se quiera dar a la cámara. Hay una amplia variedad de carcasas: estancas, con ventilación, con calefacción, metálicas, plásticas, domos según el uso que se le quiera dar a la cámara se aconseja uno u otro tipo de carcasa

6.6.6.9 El acceso a una cámara IP ¿Qué protección tiene?

Una cámara IP, al igual que los servidores de Vídeo, dispone de un software interno sobre el tema de seguridad, que nos permiten establecer varios niveles de seguridad sobre el acceso:

- Administrador: Para poder configurar el sistema. Nos pide un nombre de usuario y una contraseña

- Usuario: Para poder ver las imágenes, manejar la cámara y manejo del relé de salida. Nos pide un usuario y una contraseña.

- Demo: permite un acceso libre. No pide ningún tipo de identificación.

6.6.6.10 ¿Cuantas personas pueden conectarse simultáneamente a una cámara IP?

El número de usuarios que admite una cámara IP o un servidor de Vídeo depende del tipo de cámara, pero en general es de alrededor de 10 a 20. También se puede enviar " snapshots " automáticamente (con un periodo de refresco establecido (por ejemplo, unos segundos)) a una Web determinada, para que el público en general pueda ver esas imágenes.

6.6.6.11 Además de Vídeo, ¿se puede transmitir audio?

En general, la mayoría de cámaras IP disponen de micrófonos de alta sensibilidad incorporados en la propia cámara, con objeto de poder transmitir audio mediante el protocolo de conexión UDP. (Audio y Vídeo nos exigen conexiones con mayor ancho de banda)

6.6.6.12 ¿Qué sistemas de compresión utilizan las Cámaras IP?

El sistema de Compresión de Imagen de las cámaras IP sirve para hacer que la información obtenida de la cámara, que es mucha información y de gran tamaño, y que si no se comprime adecuadamente es imposible que se envíe por los cables de una red Local (LAN) o de las líneas telefónicas. Al comprimir pretendemos que ocupe lo menos posible, sin que las imágenes enviadas sufran pérdidas en la calidad o en la visualización.

Resumiendo, los sistemas de compresión tienen como objetivo ajustar la información captada por la cámara a los anchos de banda de los sistemas de transmisión como por ejemplo el ADSL. Los estándares de compresión actuales son el MJPEG y MPEG4, este último es el más reciente y muy potente, y la mayor parte de las cámaras comercializadas por Domodesk lo llevan.

6.6.6.13 Para el acceso a las Cámaras IP ¿Es necesario algún software específico?

Para la visualización de las Cámaras IP lo único que se necesita es que en el sistema operativo del PC se encuentre instalado el Microsoft Internet Explorer, gracias al cual tendremos acceso a la dirección propia de la cámara IP, que nos mostrará las imágenes de lo que en ese momento este sucediendo. Esto resulta extremadamente útil, ya que permitirá poder visualizar la cámara desde cualquier ordenador, en cualquier parte del mundo, sin necesidad de haber instalado un software especifico.

No obstante, con las Cámaras IP nuestras se adjunta un software de visualización de hasta 4/16 cámaras, permitiendo la visualización simultanea de las mismas, el control, la administración,... y por supuesto la reproducción de los videos que se hayan grabado mediante grabación programada, o como consecuencia de alarmas.

6.6.6.14 ¿Es posible configurar las Cámaras IP de forma remota?

Las cámaras IP y los servidores de Vídeo solamente necesitan conectarse directamente a un PC mediante un cable de red "cruzado" cuando se instalan por primera vez.

Una vez instalada, cualquier modificación de la configuración, de los ajustes de calidad de imagen, de las contraseñas de acceso,... se realizará de forma remota desde cualquier punto del mundo, bastará con conectarse a la cámara en modo "Administrador".

6.6.6.15 Puedo conectar sensores externos de alarma a una cámara IP?

También es posible. La mayoría de las cámaras y los servidores de video disponen de entradas para poder conectar sensores que no vengan integrados en la cámara , humo, fuego, por ejemplo sensores de movimiento convencionales , aunque estos últimos son innecesarios debido a que el mismo soft nos permite esa detección de movimientos.

Figura 26. Conexión de Sensores Externos de Alarma a una Cámara IP

Las cámaras IP y los servidores de video suelen disponer de un sistema de detección de movimiento (utilizando el análisis instantáneo y continuado de los cambios que se producen en los fotogramas registrados por el sensor óptico. Con este sistema de detección podemos graduar el nivel de detección de movimiento de las imágenes, y poder diferenciar si en el sistema ha entrado un coche o un peatón, incluso pudiendo diferenciar áreas dentro de una misma imagen en algunos modelos de cámaras y cada área con diferente sensibilidad de movimiento.

6.6.7 Sistema de Seguridad Electrónica

Figura 27. Sistema de Seguridad Electrónica

Cuando hacemos referencia a un sistema de seguridad no estamos hablando únicamente de sensores, cámaras y alarmas, sino también de puertas blindadas, persianas protegidas y rejas de seguridad. Podemos decir que la elección de un tipo de sistema u otro dependerá de las necesidades de cada familia o individuo, esta necesidad varía de acuerdo a la cultura del entorno, el estándar de vida y los factores psicológicos directos e indirectos. El sistema de monitoreo profesional, por ejemplo, tiene dos funciones fundamentales: minimizar las falsas alarmas y asegurar el efectivo funcionamiento del sistema en todo momento; para que ambas acciones se cumplan es fundamental que los proyectos o instalaciones y procedimientos se lleven a cabo mediante normas. Por lo general, un sistema de seguridad no es un servicio aislado sino una combinación de elementos físicos y electrónicos o una combinación de ambos.

Introducción

La necesidad de controlar el ingreso de personas no autorizadas en algún lugar determinado es la base de la existencia de estos equipos, los cuales mantienen la seguridad en comercios, oficinas, industrias, almacenes, áreas de diseño o desarrollo, laboratorios, etcétera.

La instalación de los sistemas de alarmas contra intrusos ha contribuido a reducir la cantidad de robos y hurtos producidos en los hogares de todo el mundo, presentando no sólo la ventaja directa de la seguridad que brinda a las personas y sus bienes, sinó también permitiendo reducir los montos de las primas de los seguros de las empresas, comercios y viviendas.

Los robos y hurtos también pueden causar diferentes trastornos psico-físicos sobre las víctimas de estos hechos delictivos, siendo las más afectadas las personas mayores y las que sufren problemas del corazón, las mujeres embarazadas, y sobre todo los niños, quienes pueden resultar muy traumatizados por la situación de peligro resultante.

Estos sistemas de alarmas pueden contener los siguientes elementos:

- Central de alarma
- Batería y cargador
- Consola de activación/desactivación
- Cableado o vinculación inalámbrica
- Alarma
- Avisador telefónico
- Pulsadores de pánico/asalto
- Detectores

En ciertos modelos comerciales, algunos de estos elementos se encuentran debidamente integrados dentro de la central de alarma. A continuación se presentan las características mas destacadas de cada tipo de elemento.

6.6.7.1 Unidad Central o Cerebro

Figura 28. Unidad Central o Cerebro

La central de alarma es la parte medular del equipamiento, ya que es el elemento que se encarga de controlar automáticamente el funcionamiento general del sistema de alarma, recogiendo información del estado de los distintos detectores y accionando eventualmente los sistemas de aviso de la presencia de intrusos en el área protegida.

La central en sí es una tarjeta electrónica con sus distintas entradas y salidas, que se encuentra resguardada en un gabinete con protección antidesarme, el que generalmente también incluye la batería y su cargador.

Las centrales se clasifican de acuerdo a la cantidad de zonas independientes a proteger, por lo que podemos encontrar productos de 2 zonas, 6 zonas, 16 zonas, etcétera.

Cada zona puede ser activada y desactivada en forma individual, lo que permite en hogares con muchas dependencias, proteger las áreas que no tienen presencia humana prevista y deshabilitar la protección en aquellas zonas ocupadas por los dueños de casa.

Asimismo, se suele incorporar un retardo de activación de la alarma en al menos una zona (zona temporizada), para dar tiempo a que pueda desactivarse el sistema, al ingresar los dueños al domicilio protegido.

Sin embargo, esto no es necesario en los casos en que se dispone de un control remoto por ondas de radio.

Batería y cargador

Figura 29. Batería y cargador

Estos elementos sirven para proveer un sistema de alimentación eléctrica ininterrumpida (UPS), de manera que ante una falta del suministro eléctrico de red (normal o provocado por un ladrón), el sistema de alarma contra intrusos continúe brindando protección en forma absolutamente normal.

6.6.7.2 Teclado

Figura 30. Teclado

Esta consola habitualmente contiene un teclado que permite programar todas las funciones del sistema. Esta interfase de control cuenta con teclas alfanuméricas, como así también otras funciones de señalización de estados, por lo que constituye una pieza importante para el usuario del sistema.

Existen señalizadores de dos tipos, los de led o luces, y también los de pantalla de cuarzo líquido. En ambos casos brindan información de cada una de las zonas que están conectadas (áreas de protección exterior, puertas, ventanas, áreas interiores, etcétera).

En algunos modelos, la consola de activación/desactivación se encuentra montada en el frente de la central de alarma, aunque esto tiende a caer en desuso.
También existen modelos en que se dispone un control remoto por ondas de radio codificadas, que permite la activación/desactivación de la central, y eventualmente puede accionar las sirenas y hacer llamados telefónicos en caso de asaltos.

6.6.7.3 Alarma

Figura 31. Sirena

El elemento de alarma está formado generalmente por una sirena (o campana) que advierte de la ocurrencia de una intrusión detectada por el sistema, mediante una señal sonora de alto nivel. En algunos casos, también puede incluir algún tipo de señalización visual, como balizas y destelladores (flash), para aquellas personas que tienen problemas de audición o cuando existe un alto nivel de ruido ambiente.
La sirena exterior se coloca dentro de un gabinete para su protección, y se instala en la fachada de la casa, comercio o industria a proteger. Además de su función de alertar en los casos en que se ha detectado un intruso, la sirena exterior es un elemento disuasivo de por sí, ya que advierte de la existencia de un sistema de alarma instalado en el domicilio.

Por otro lado, la sirena interior sirve para actuar como auxiliar de la exterior, de manera que las dos sirenas suenen al mismo tiempo. Si el intruso destruye la sirena exterior, queda funcionando la sirena interior dentro del lugar a proteger.

En todos los casos, estas sirenas emiten un sonido de unos 120 decibeles (equiparable al sonido de una ambulancia) y tienen una protección antidesarme que envía una señal a la central, en los casos en que se pretenda sabotear su correcto funcionamiento.

Para determinar el tipo de alarma a instalar debe tenerse en cuenta algunos factores como el nivel de ruido ambiental, el tipo y calidad del sonido ambiental, la duración de la señal requerida, el nivel acústico deseado y la alimentación eléctrica disponible.

Por ello, para su correcta instalación hay que tener en cuenta la presencia de fuentes de sonido en los locales a proteger, como por ejemplo equipos de aire acondicionado, sistemas estereofónicos, televisores, etcétera, que eventualmente impidan la audición de las sirenas de alarma.

Por otro lado, el entorno en el cual un señalizador luminoso debe ser instalado es lo que determina tanto el tipo de producto como la intensidad luminosa necesaria para cada aplicación. Por ello, un avisador luminoso diseñado para uso industrial, que incorpora una gran salida luminosa nunca podrá ser adecuado para un domicilio y viceversa.

6.6.7.4 Pulsadores de pánico/asalto

Estos dispositivos de seguridad contra asalto deben ser colocados estratégicamente y de manera oculta, cerca de cajas registradoras, mostradores, baños, cajas de seguridad, armarios, etcétera, de manera tal que al momento del asalto se puedan presionar los pulsadores correspondientes en forma disimulada, para enviar una señal a la central de alarma, que ordene una acción de respuesta silenciosa, como por ejemplo la ejecución de un llamado telefónico o la activación de una señal luminosa en el puesto central de vigilancia.

6.6.7.5 Detectores

Figura 32. Detector

Los detectores se fabrican con diversas técnicas que operan bajo principios de funcionamiento diferentes. Algunos de ellos han pasado a la obsolescencia por la gran cantidad de falsas alarmas que generan y por lo tanto no se describirán.

En la mayoría de los casos se dispone un elemento sensor que analiza la alteración de alguna magnitud física. Esta alteración es detectada por un circuito electrónico asociado que opera un contacto normalmente cerrado, que al abrirse envía la información de su estado a la central, la que acciona la alarma acústica y/o lumínica del sistema, para advertir la presencia de intrusos en el ambiente en que se halla instalado.
Estos detectores deben ser cuidadosamente seleccionados en función del tipo de alteración a identificar, para evitar falsas alarmas.

Por lo general, el detector está concebido para dar una rápida advertencia a un costo razonable, de manera de brindar un oportuno preaviso. Esta advertencia sólo es posible si el detector está correctamente localizado, instalado y mantenido.

Los detectores no pueden dar aviso si el intruso no atraviesa el campo de acción de ellos. Por ello es aconsejable instalar detectores en cada cocina, dormitorio, pasillo, descanso y otros recintos cuyas puertas permanezcan cerradas normalmente.

Los detectores generalmente no deben colocarse directamente sobre una cocina o estufa, ni en las cercanías de extractores de aire , puertas o ventanas, ni en lugares con temperaturas elevadas.

Tampoco deben ubicarse en áreas sucias, con muchos insectos, o con atmósfera poluida, porque pueden dar origen a falsas alarmas.

Asimismo debe tenerse en cuenta la presencia de mascotas, como perros y gatos, que pueden producir innecesarios avisos, si no se toma en cuenta esta situación al ser instalados. Por este motivo, algunos detectores son inmunes a animales de 30 cm de altura.

Los detectores deben tener un mantenimiento regular, debiendo prestarse especial atención al estado de la zona de captación. Además hay que limpiarlos mensualmente para quitar el polvo o grasa que pueda perturbar su funcionamiento.

Hay detectores que funcionan en forma autónoma, pues poseen su propia sirena y batería, formando una pequeña central completa que brinda protección aún cuando se interrumpe el suministro de energía, siempre que la batería esté cargada y correctamente instalada.
En algunos casos, en vez de sirena se instala una luminaria incorporada, que al iluminar la zona en que detectó la anormalidad, alerta de la presencia de extraños en su campo de acción, ahuyentando posibles intrusos, animales, etcétera.

A continuación se presenta una síntesis de las características de los principales tipos de detectores que se emplean en la actualidad:

6.6.7.5.1 Pir O Sensor De Movimientos Infrarrojo Pasivo

Este sensor trabaja mediante la detección de la radiación infrarroja emitida por los cuerpos vivos ubicados dentro de su campo de acción. El mismo tiene una lente de forma especial que concentra los rayos infrarrojos en su foco, donde se instala el sensor propiamente dicho.

Dicha lente no enfoca todos los rayos que inciden en el sensor, presentando zonas (o mejor dicho ángulos) de sombra que se intercalan con zonas de detección. De esta manera, cuando un cuerpo caliente se mueve, se producirá un cambio en la distribución de zonas de sombra y detección de radiación, lo que produce una ligera modificación que es discriminada por el sensor infrarrojo, cuyo circuito asociado envía al control la señal de que una persona, u animal ha activando el sistema.

Hay que tener en cuenta que su funcionamiento se ve afectado por la distribución de temperaturas del lugar, por lo que no debe haber corrientes de aire bruscas que activen el sensor de movimientos. Esta limitación constituye un impedimento para su instalación en ciertos recintos.

El funcionamiento óptimo se produce cuando el cuerpo caliente se desplaza de forma transversal, atravesando el haz de ángulos de sombra y detección, y el menor índice de detección ocurre cuando el objeto se desplaza totalmente de frente hacia el detector, ya que de este modo no se modifica apreciablemente la distribución de haces y la detección se produce de forma más lenta.

Generalmente su alcance es de algo más de 10 m a lo largo y de 6 m a lo alto, con un ángulo de cobertura de unos 90º a 110º a lo ancho.

En algunos modelos pueden intercambiarse los lentes, para modificar su área de captación. Así hay lentes de largo alcance, apropiados para pasillos; hay lentes que no se enfocan a la zona mas baja del recinto, para mascotas; hay lentes tipo gran angular, etcétera.

Cabe señalar que los detectores de presencia por infrarrojos se están introduciendo cada vez más en el ámbito de la automatización de edificios y viviendas, así como en muchos otros entornos no relacionados con la seguridad, tanto domésticos como industriales. Este auge se debe no sólo a que resulten cómodos y prácticos para el encendido y temporización de luces y otras aplicaciones, sino también a la fiabilidad que han venido demostrando en los años que llevan en el mercado.

6.6.7.5.2 Sensor de Movimientos dual-tech (doble tecnología) Infrarrojo-Microonda

Este sensor de movimientos es uno de los más confiables que hay la actualidad, ya que a la acción de la detección infrarroja descripta anteriormente, se añade el uso de microondas.

La parte de microondas envía una señal desde el sensor hasta el final de su zona de alcance y luego el rebote de la señal permite confirmar que no hay intrusos.
Al ser interrumpida la señal por una persona u animal, la señal la regresa más rápido y el sensor detecta la anormalidad.
Sólo si la parte de microondas y la parte de infrarrojo detectan simultáneamente una anormalidad en su área de cobertura se activa el sistema, minimizándose así la ocurrencia de falsas alarmas.

Generalmente su alcance es de algo más de 10 m a lo largo y de 6 m a lo alto, con un ángulo de cobertura de unos 90º a lo ancho.

Su altura para instalación debe ser entre 1,80 a 2 m.

Algunos modelos más onerosos también incluyen un microprocesador, que almacena patrones de comportamiento típicos, para evitar falsas alarmas (triple tecnología).

6.6.7.5.3 Sensor de ultrasonido

Este sensor se basa en el efecto Doppler y resulta similar al componente de microondas descripto anteriormente, usándose en zonas al aire libre, donde no resultan efectivos otros tipos de detectores.

6.6.7.5.4 Sensor de rotura de cristal

Este sensor trabaja detectando las frecuencias del sonido característico que emite un cristal al ser quebrado, mediante el uso de un micrófono instalado en el interior del detector.

Este sensor se instala en lugares como ventanales, puertas corredizas de cristal, etcétera. El detector de rotura de cristal se coloca en el techo o en las paredes, siempre pensando en que el sensor esté frente al área a proteger. Habitualmente su cobertura es de algo más de 4 m^2.

6.6.7.5.5 Barrera infrarroja

Este sistema detector consta de un emisor y un receptor infrarrojo, colocados enfrentados a cierta distancia entre sí, de manera tal que la interposición de algún cuerpo en el trayecto entre ambos elementos produzca la desaparición de la señal recibida, activándose la correspondiente señal de alarma.

Este sistema resulta de bajo costo, pero necesita de un mayor cableado que en el caso del PIR, en virtud de que necesita una conexión para el emisor y otra para el receptor.

6.6.7.5.6 Contacto magnético

Este detector sirve para proteger todos los accesos de la casa que dan al exterior, como las puertas ó ventanas de uso normal, pudiendo ser instalados en distintos tipos de aberturas de metal o de madera, siempre y cuando las mismas no tengan movimiento con el viento.

Estos elementos se componen de dos partes; una que se instala en el marco de la abertura, que es la que contiene un reed-switch NC y está conectada al control central; y la otra que es un imán permanente que se coloca en la parte móvil de la abertura.

Si alguien intenta ingresar al domicilio abriendo alguna abertura, se aleja el imán, y la otra parte queda fuera del campo magnético que mantenía cerrado el reed-switch, lo que da lugar al envío de una señal al control para activar las sirenas.

Existen de dos tipos básicos: el normal y el oculto; su diferencia radica en que los contactos normales se instalan externamente y son visibles; y los ocultos son utilizados sólo en aberturas de madera y son empotrados dentro de la parte móvil y del marco.
Otra variante es el contacto "overhead", que maneja el mismo principio de los otros contactos pero resulta apropiado para cortinas de acero.

6.6.7.5.7 Detectores lineales

Figura 33. Detector lineal

Las barreras de infrarrojos están diseñadas para poder asegurar un perímetro tanto en el exterior como en el interior, la activación de dichas barreras podemos controlar señales de alarma, luces o poner en funcionamiento un grabador digital, activándose solo con la presencia de un intruso. El Kit esta compuesto de 2 unidades independientes: Emisor y receptor.

El emisor transmite unos rayos infrarrojos invisibles con cambios de frecuencias en el receptor. Estos cambios de frecuencias eliminan en gran medida las interferencias producidas por otros elementos. También ayudan a bajar el consumo del equipo ampliando la vida de los emisores. El alineamiento de las dos unidades se realiza de forma sencilla para una mayor precisión. Incorpora unos mandos rotativos que permitirán ajustar los haces tanto en horizontal (. 180 º- + 90 º) como en vertical (+ 10 º- + 5 º).. El ajuste puede ser controlado con un pequeño visor, con un voltímetro o en los modelos de 4 haces gracias a un smeter digital (10 LEDS) Para hacer el sistema mas preciso, eliminando falsas alarmas existen dispositivos de dos haces y cuatro haces. Están construidos con lentes asfericas, lo que ofrece una mayor precisión comparado con las barreras habituales de lentes fresnel. La carcasa esta construida con una cuidada estética además de poder resistir las inclemencias del tiempo, soportando altas temperaturas, golpes, polvo..etc. pudiendo así ser utilizadas tanto en interior como en exterior en las peores condiciones. Su difusor convexo y su electrónica están especialmente diseñados para evitar los efectos de la niebla, lluvia, tormentas de polvo, nieve, etc. Posee un circuito de AGC (control automático de Ganancia) que se autorregulara su sensibilidad dependiendo de las condiciones atmosféricas. Para evitar alarmas producidas por pequeños animales, posee además del ajuste por corte de haces, un ajuste por tiempo de corte, lo cual permitirá que detecte un intruso pero no salte cuando pase un gato o un pájaro.

6.6.7.6 Cableado o vinculación inalámbrica

Como su nombre lo indica, sirve para vincular los distintos componentes del sistema de alarma contra intrusos, ya sea por medio de cables o en forma inalámbrica. En el

caso de redes cableadas, generalmente se utilizan dos conductores para alimentación de 12 V y dos conductores para las señales (circuito serie de NC).

6.6.8 Cable multipar

Un cable de pares es el formado por grupos de 2 hilos (par) de material conductor, de grosores entre 0,3 y 3mm, recubiertos de plástico protector.

El cable multipar es aquel formado por un elevado número de pares de cobre, generalmente múltiplo de 25. Existen cables multipares normalizados con capacidad de 25, 50, 125, 250 y hasta 3600 pares en un único cable físico.

Los cables de pares son usados para la conexión física de equipos de telefonía, en redes de datos, como por ejemplo en redes LAN. En estas redes de datos se utilizan pares de cobre trenzados (UTP), donde los conductores se “trenzan” entre sí, y apantallados, es decir cubiertos de una pantalla o malla de material conductor. Estas mejoras permiten la transmisión de datos a capacidades altas y minimizan interferencias hacia/desde otros sistemas.

6.6.8.1 Código de colores en cables multipares

Las ICT que distribuyen más de 25 pares por vertical recurren a las llamadas mangueras o cables multipar. Estas pueden ser de 25, 50, 75 0 100 pares y en una distribución vertical se dan frecuentemente combinaciones entre ellas.

A la hora de realizar las conexiones con tanto par es necesario identificar cada uno de forma unívoca y por ello se emplea un código de colores universalmente reconocido. Este consiste en asignar a un conductor (a) un color de referencia y al otro conductor (b) un color de par que puede variar entre cinco opciones (azul, naranja, verde, marrón y gris).

Con un color de referencia podemos entonces identificar cinco pares, si aumentamos las variaciones para el conductor (a) tendremos por cada nuevo color cinco nuevas combinaciones. Esta estrategia se sigue hasta llegar a la identificación de 25 pares lo que se consigue haciendo que el conductor (a) adopte los colores (blanco, rojo, negro, amarillo y violeta).

¿Y como son los pares del 26 al 50 en un multipar de 50 pares?

Exactamente iguales, por lo que para no confundirlos los 25 primeros vienen rodeados de una cinta con los colores del par 1 (blanco, azul) y los 25 siguientes con los del par 2 (blanco, naranja). Con esta nueva técnica se pueden codificar hasta 600 pares.

6.7 Modelo Operativo

6.7.1 Configuración de una cámara IP

Nos vamos a basar en el modelo DLINK DCS-2100G, aunque casi todos los modelos y marcas tienen similares funcionalidades.

Una vez instalada la cámara, se puede acceder via web a la ip propia de la cámara (la suele indicar el fabricante en el manual, o suele llevar un programa de detección de IP).

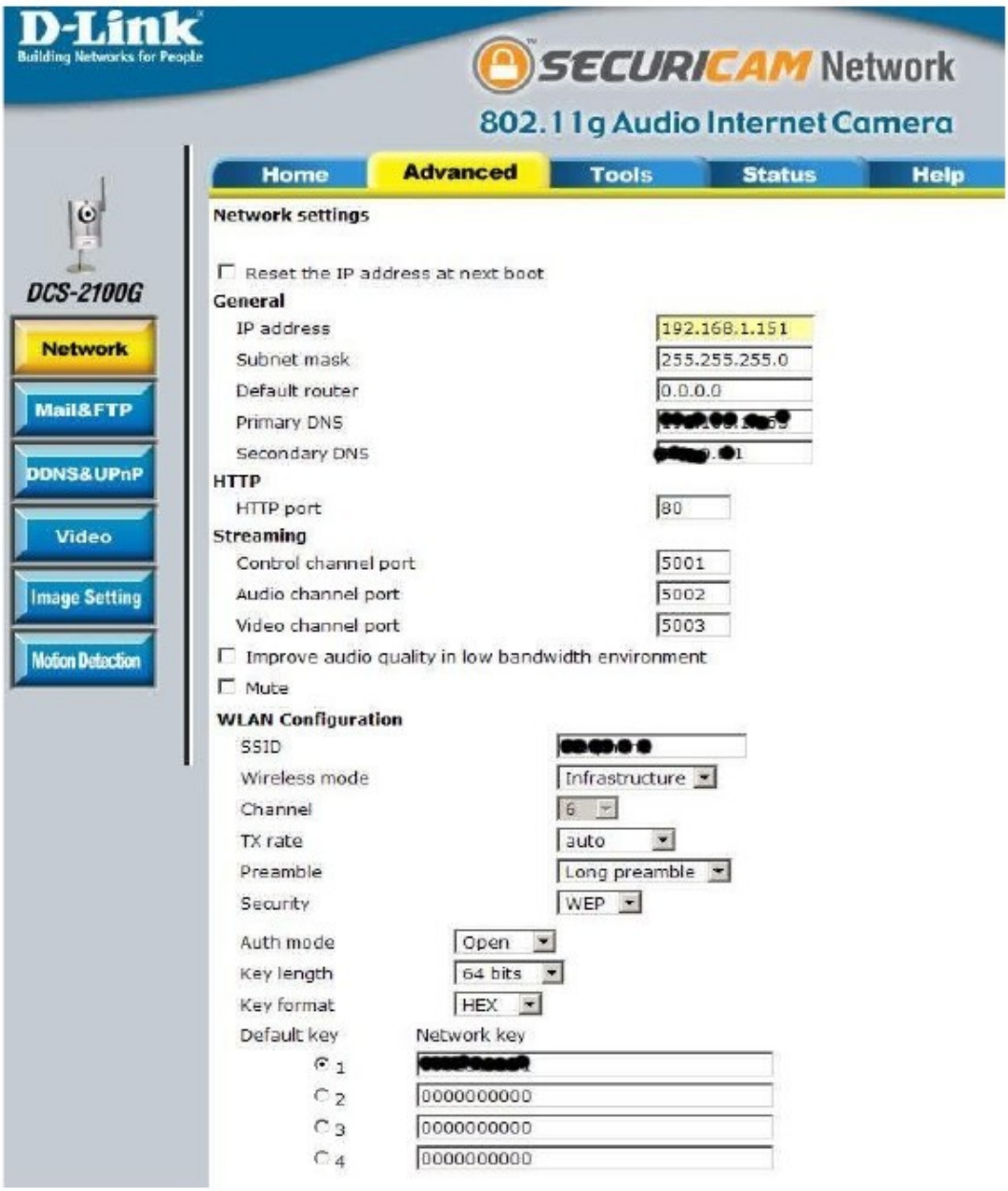


Figura 34. Configuración de la red

La pantalla anterior sirve para la configuración de red. Aqui los parámetros importantes son los siguientes:

- IP ADRESS: IP que queremos que tenga la cámara (deberá ser dentro del rango nuestro para poderla ver).

- La máscara de subred (SUBNET MASK) deberá ser la misma que la que tenga nuestra red, normalmente 255.255.255.0

- Los datos de ROUTER, y DNS, solamente serán necesarios si vamos a sacar la imagen a través de internet.

- El HTTP PORT es el puerto de acceso a la cámara, se puede cambiar si queremos que a través de internet la veamos por un puerto en concreto, lo mismo ocurre con los puertos de STREAMING.

Los parámetros de audio, recomiendo tenerlos deshabilitados, puesto que suelen incrementar el ancho de banda y aportan baja calidad al sonido. Si la cámara la estamos colocando en Wireless deberemos indicarle los datos de SSID, Canal, y tipo de encriptación (WEP, WPA). En este caso habrá que colocarle la clave correspondiente.

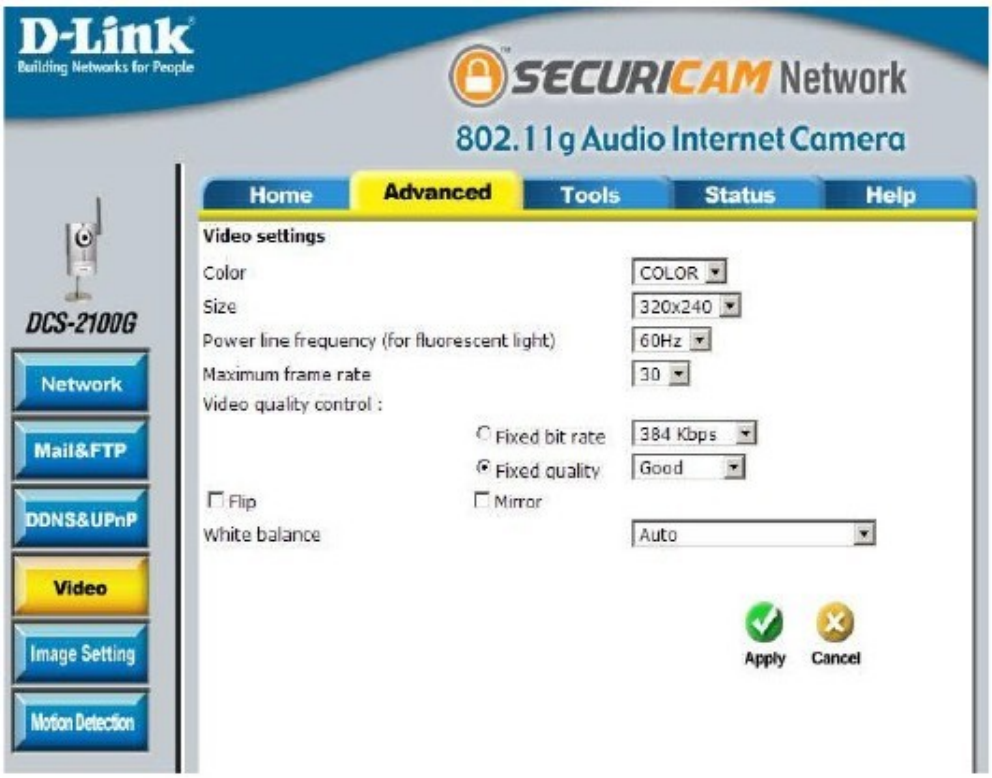


Figura 35. Configuración del video

En la pantalla de configuración de Video podemos configurar lo siguiente:
Color o blanco y negro para la imagen.

SIZE: Indica el tamaño de la imagen, cuanto mas pequeño, menor incremento de ancho de banda.

POWER LINE FREQUENCY: Si notamos que la luz de fluorescentes hace que la imagen parpadee, podemos cambiar la frecuencia.

MAXIMUN FRAME RATE: Son el número máximo de frames por segundo que puede emitir la cámara. A partir de 20 casi es tiempo real, por lo que podemos ajustarlo como creamos mas conveniente. Naturalmente también es un parámetro que puede incrementar seriamente el tráfico de la red.

El VIDEO QUALITY CONTROL: es lo que determina la calidad de la imagen. Se puede fijar con un tráfico fijo (desde 64k a 1200k), o bien por calidad (desde Medium a Excellent).

Estos parámetros que he comentado son los que en definitiva van a poder conseguir que nuestra red se pueda resentir de mucho tráfico o no.

Lo recomendable es buscar la calidad sin entorpecer la tasa de transferencia, y hay mas factores con los que se puede jugar (número de cámaras, clientes que se conectan simultáneamente, etc.). Siempre es mejor empezar con poca calidad y poco a poco ir aumentando los parámetros hasta que quede optimizado.

FLIP: Permite dar una vuelta de la imagen verticalmente, y MIRROR la gira horizontalmente.

El WHITE BALANCE: es un parámetro para configurar cámaras de interior o exterior, para que la propia cámara gestione la luz en función a su lugar de trabajo.

Figura 36. Configuración de la imagen

La tercera pestaña que comentamos hoy es la de IMAGE SETTING, es de las mas sencillas, y permite cambiar el brillo, contraste, saturación y matiz de la imagen para dejarla lo mas real posible.

Naturalmente todos estos parámetros se podrán cambiar tantas veces como se considere necesario.

6.7.2 Instalación de Software

- Escogemos Lenguaje a hacemos click en OK

Figura 37. Instalación de Software

- Hacemos click en Next para que continúe

Figura 38. Instalación de Software

- Hacemos click en Next para que el software de instalación se guarde en la carpeta asignada sino queremos que se guarde en esa carpeta presionamos browse para escoger en que carpeta queremos guardar.

Figura 39. Instalación de Software

- Hacemos click en Next para que empiece la instalación

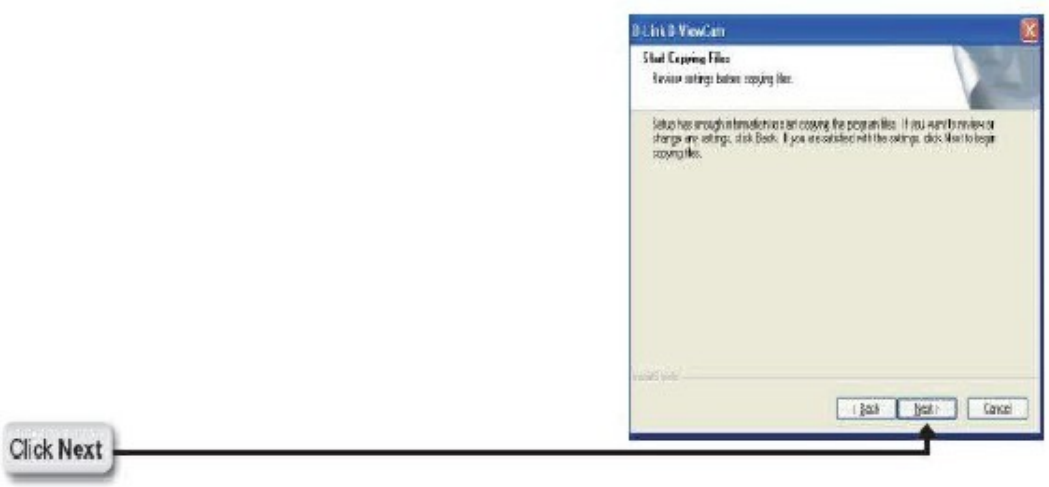


Figura 40. Instalación de Software

- Hacemos click en Next para que la instalación se complete.

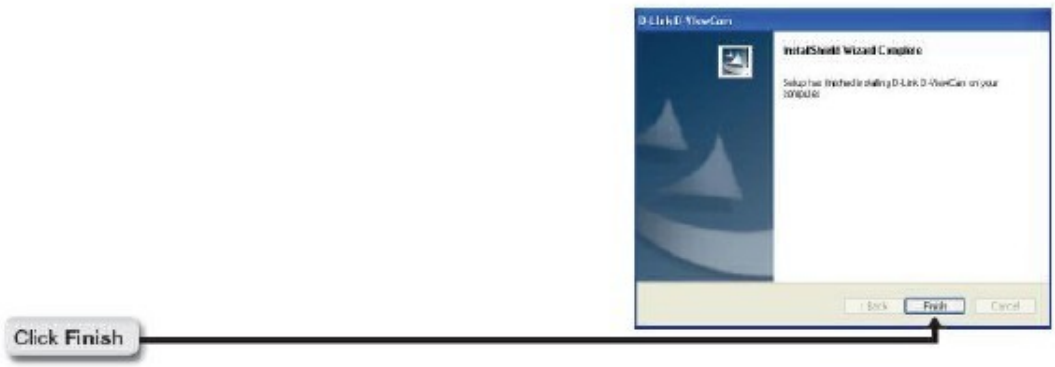


Figura 41. Instalación de Software

C. MATERIALES DE REFERENCIA

Bibliografía:

Referencias bibliográficas

RANDALL K. NICHOLS – PANOS C. LEKKAS. Seguridad para Comunicaciones Inalámbricas.
Este libro contiene el tema WLAN: Redes Inalámbricas de Área Local

"Redes de comunicación", Enciclopedia Microsoft(R) Encarta(R) 98. (c) 1993-1997 Microsoft Corporation. Reservados todos los derechos.

“Vigilante de seguridad” – Área técnico-profesional/Editorial CPD/Madrid, 1999.
Este libro contiene temas sobre Sistemas de Seguridad.

Directores de Seguridad-Seguridad y Protección /Editorial CPD/Madrid, 1999.

Este libro contiene temas sobre Sistemas de Seguridad.

Referencias bibliográficas de Internet

http://www.monografias.com/trabajos/introredes/introredes.shtml

http://www.rvcseguridad.com

http://www.monografias.com/trabajos43/seguridad-redes/seguridad-redes2.shtml

http://www.monografias.com/trabajos6/sicox/sicox.shtml

http://www.lukor.com/ordenadores/05062902.htm

http://laurel.datsi.fi.upm.es/~ssoo/DSCD/

https://upcommons.upc.edu/pfc/bitstream/2099.1/3330/5/34059-5.pdf

http://www.ab.com/catalogs/safety/es/pdf/prodtype/ch8/8-2_8-5.pdf

http://www.intercron.com/

http://www.ciscor.com/es/aplicaciones/seguridad_del_control_y_supervision_industrial.html

http://www.jocoya.cl/alarm03.htm

ANEXOS

Computadora

Caja: ATX Negro

Procesador: Intel Pentium Dual Core E2160 a 3.0Ghz (Allendale) - Doble Núcleo, FSB 800Mhz, 1MB L2 Cache, XD Bit de desactivación de ejecución, EMT64, Socket 775

Memoria RAM: 1GB DDR2 PC2-5400 667Mhz (ambas ranuras pueden estar ocupados)

Disco Duro: 500GB 7200rpm SATA

Tarjeta de Video: 2D/3D hasta 128MB Memoria compartido

Tarjeta de Red: 10/100Mbps Fast Ethernet integrado

Tarjeta de Sonido: 6 canales integrado

Unidad Optico: Quemador de DVD 20x Multiformato con Dople Capa

Unidad de Disquetes: no incluido

Lector de Tarjetas de Memoria:

Lector de Tarjetas de Memoria Todo-En-Uno (SD, CF, MS, MS Pro Duo entre otras)

Sistema Operativo: Windows XP

USB: 6 puertos USB 2.0/1.1 (4 traseros / 2 delanteros)

Conector de Video: 1x

Conector de Teclado: 1x PS/2

Conector de Mouse: 1x PS/2

Conectores Red: 1x RJ 45

Conectores Sata: 2x Serial ATA

Conectores de Sonido: Entrada, Salida, Micrófono

CAMARAS IP

CARACTERÍSTICAS PRINCIPALES

• Detección de movimiento para activar la grabación y alarmas por e-mail

• Sensor Megapixel CMOS (1280x1024)

• 0.5 lux de sensibilidad a la luz. Captura de video con iluminación mínima

• Soporte de vigilancia móvil 3GPP

• Ranura para tarjetas SD de almacenamiento

• Incluye D-ViewCam 2.0 para monitoreo y administración de hasta 32 cámaras

• 2-Way Audio, para captar y emitir sonido a través de la cámara

SWITCH

CARACTERÍSTICAS PRINCIPALES

• 16 puertos 10/100Mbps

• 2 Slots para Módulos opcionales

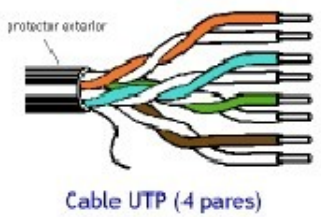
• Control de Bandwidth y tormenta de Broadcast

• Colas de prioridad (QoS basado en 802.1p)

• Spanning Tree / Rapid Spanning Tree

• VLAN (802.1Q)

CABLE UTP CATEGORIA 5E



Cable UTP Cat. 5e 100 omhs 24 AWG, LSZH, 4 pares.

No. de Parte	Descripción
VOL-5EUL4-305R	Cable Cat 5e, 100 ohms, Sólido, 24 AWG, UTP LSZH 4 Pares, Color Verde, Reelex 305 mts

Características

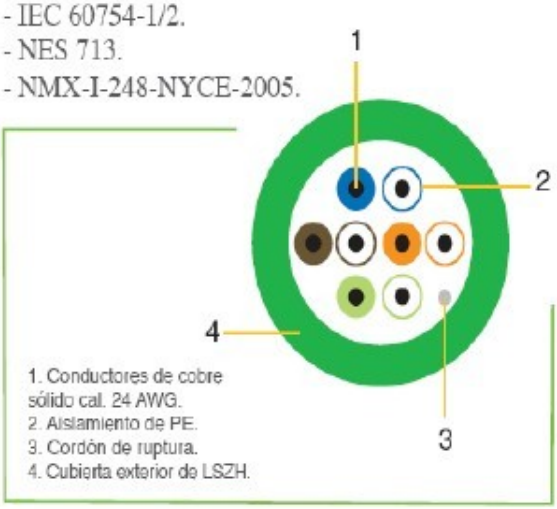
- Calibre del conductor: 24 AWG.
- Tipo de aislamiento: polietileno sin halógenos.
- Tipo de ensamble: 4 pares.
- Tipo de cubierta LSZH: con propiedades de baja emisión de humos sin halógenos.
- Para conexiones y aplicaciones IP.
- Conductor de cobre sólido de 0.51 mm.
- Diámetro exterior 5 mm.
- Desempeño probado hasta 200 Mhz.
- Impedancia: 100 Ω.

Aplicaciones

- 1.2 Gbps ATM.
- 622 Mbps ATM.
- 100 Base T.
- 100 Mbps TP-PMD.
- 100 BASE VG ANYLAN.
- 1000 Base T.

Normas Aplicables

- ANSI/TIA/EIA 568B.
- ANSI/ICEA S-90-661.
- ISO/IEC 11801 (2a edición, clase D).
- NEMA WC63.1.
- EN 50173-1.
- UL.
- IEC 60332-1 (parte 1).
- IEC 60332-3 C.
- IEC 1034 1/2.
- IEC 60754-1/2.
- NES 713.
- NMX-I-248-NYCE-2005.



Tensión máxima de instalación (N)	Rango de Temperatura (°C)	Peso aproximado (kg/km)
90	Instalación 0 a 50 Operación -20 a 60	35

Conector RJ45

Conector RJ 45 Keystone

No. de Parte	Descripción
VOL-OCK5E-U-W8	Conector RJ45 Cat.5e tipo Keystone, configuración A/B, con cubre polvo abatible, Color Blanco, paquete de 8 pzas
VOL-OCK5E-U-AL8	Conector RJ45 Cat.5e tipo Keystone, configuración A/B, con cubre polvo abatible, Color Marfil, paquete de 8 pzas
VOL-OCK5E-U-BL8	Conector RJ45 Cat.5e tipo Keystone, configuración A/B, con cubre polvo abatible, Color Azul, paquete de 8 pzas
VOL-OCK5E-U-GR8	Conector RJ45 Cat.5e tipo Keystone, configuración A/B, con cubre polvo abatible, Color Verde, paquete de 8 pzas
VOL-OCK5E-U-R8	Conector RJ45 Cat.5e tipo Keystone, configuración A/B, con cubre polvo abatible, Color Rojo, paquete de 8 pzas
VOL-OCK5E-U-Y8	Conector RJ45 Cat.5e tipo Keystone, configuración A/B, con cubre polvo abatible, Color Amarillo, paquete de 8 pzas
VOL-OCK5E-U-BK8	Conector RJ45 Cat.5e tipo Keystone, configuración A/B, con cubre polvo abatible, Color Negro, paquete de 8 pzas
VOL-OCK5E-U-O8	Conector RJ45 Cat.5e tipo Keystone, configuración A/B, con cubre polvo abatible, Color Naranja, paquete de 8 pzas

Características

- Desempeño superior a 150 Mhz.
- Guía de hilos en policarbonato, llegada de los cables por arriba y por abajo.
- Conexión sin herramienta (autoponchable o autoinsertable).
- Etiqueta de identifi cación de contactos y código de color T 568 A y B.
- Para montaje sobre placas de pared, cajas superfi ciales y paneles de parcheo modulares de 24 y 48 puertos tipo Keystone.
- Los conectores RJ-45 K5e, cumplen con las normas ISO/IEC 11801, EIA/TIA 568 B, EN 50173, UL y NMX-I-NYCE-248-2005.
- Cubrepolvos abatible.
- Categoría marcada en el cubrepolvo (quintado C5e).

TECLADO

CEREBRO O TARJETA MADRE

DETECTOR DE MOVIMIENTO

Descripción:

- Excepcional sensibilidad a elevadas temperaturas
- Diseño de Viga Vertical (VBS) brinda un mecanismo de anti-activación por animales domésticos de hasta 27 Kg (60 Lb)
- Ajuste de sensibilidad

DETECTOR LINEAL

Perimetral 190'/60mts

Código: SEC E960D190

- 190 ft. (60m) exterior, 390 ft. (120m) interior