UNIVERSIDAD NACIONAL TECNOLÓGICA DE LIMA SUR

FACULTAD DE INGENIERÍA MECÁNICA Y ELÉCTRICA, ELECTRÓNICA Y AMBIENTAL

CARRERA PROFESIONAL DE INGENIERÍA ELECTRÓNICA Y TELECOMUNICACIONES

DISEÑO DE RED DE VIGILANCIA REMOTA PARA EL MEJORAMIENTO EN EL CONTROL DEL FUNCIONAMIENTO DE LOS NODOS DE COMUNICACIÓN EN LA PROVINCIA DE PICUSH – PASCO - PERU

TEMA DE INVESTIGACIÓN PARA OPTAR EL TÍTULO DE INGENIERO ELECTRÓNICO Y TELECOMUNICACIONES

PRESENTADO POR EL BACHILLER

SILVERIO FLORES SILVIO EDGAR

LIMA – PERÚ

2015

Dedico este trabajo a mi abuelo Rafael Silverio y Eladio flores que me habría encantado que me acompañaran en esta etapa de mi vida, pero ahora se encuentran en el cielo observando y guiando mi camino, sé que me protegen y guían.

Edgar Silverio

Agradezco en primer lugar a mis padres que debido a ellos no hubiera conseguido nada, también a mi familia que siempre me apoyaron y aconsejaron, y como olvidar a los docentes que formaron parte de mi formación profesional ya que debido a ellos he podido afrontar las adversidades que se me presentan en el camino es por ello que mis más sincero agradecimiento a todos aquello que formaron parte de mi formación profesional.

Edgar Silverio

ÍNDICE

INTRODUCCIÓN

En la actualidad la tecnología ha dado grandes pasos con respecto a la video vigilancia e incluso se puede visualizar en los Smartphone, por ello con tan solo tener acceso a la NUBE se puede tener acceso desde cualquier parte del mundo por ello se optó por este sistema ya que con el adecuado ancho de banda y correcta comprensión de los archivos se puede visualizar desde cualquier punto remoto y con la gran variedad de cámaras se puede alternar entre distintos modelos, por ello lo que genera es que se muestre diversidad de tomas de filmación y grandes aplicaciones es debido a eso que es una solución rentable fiable y sobre todo que es visible desde cualquier punto remoto esto genera que se ponga una central de monitoreo con al cual se puede observar daño o hurto de los equipos de telecomunicaciones. La estructura que hemos seguido en este proyecto se compone de 3 capítulos. El primer capítulo comprende el planteamiento del problema, el segundo capítulo el desarrollo del marco teórico y el tercer capítulo corresponde al desarrollo del proyecto de video vigilancia remota.

CAPITULO I
PLANTEAMIENTO DE PROBLEMA

1.1 DESCRIPCIÓN DE LA REALIDAD PROBLEMÁTICA

En la actualidad si bien estamos viviendo un gran auge tecnológico gracias a los avances tecnológicos a nivel mundial, la comunicación de datos atreves de los teléfonos móviles se están volviendo indispensables, ya que con ellos se puede transmitir fotos, videos y mantenerse al corriente de cualquier cosa que ocurra en el mundo atreves de las redes sociales YouTube, twiter, Facebook, etc., es por ello que las empresas de telecomunicaciones buscan llegar a todo rincón del país y del mundo, y muchas veces para llegar a lugares recónditos le toca instalar una BTS y NODOB en lugares aislados de la civilización por lo cual no se cuenta con una vigilancia o fácil acceso a estos puntos de trasmisión , y debido a su aislamiento se vuelven blanco fáciles de los delincuentes y en estos SITE se cuentan con equipos de transmisión muy valiosos, se propone la instalación de un equipo de vigilancia con tecnología IP y cámaras con visión panorámicas.

1.2 JUSTIFICACIÓN DEL PROBLEMA

En la actualidad con el crecimiento de la tecnología se busca expandir las redes de comunicaciones hasta los lugares más recónditos del país, con el fin de que la tecnología y la información ya sea voz o data esté al alcance de todos se ubican puntos de trasmisión y comunicación, pero estos nodos se encuentran muchas veces en lugares alejados a hora del pueblo más cercano, por lo que son vulnerable a robos o fallas climáticas que no se pueden prevenir que se necesite debido a que no se sabe el origen del problema por ello se vio la posibilidad de implementar un sistema de video vigilancia remota y así poder dar pronta solución a problemas de transmisión que se presenten debido a que la empresa de telecomunicaciones puede recibir una fuerte multa por caída de señal en las comunicaciones.

1.3 DELIMITACIÓN DEL PROYECTO

1.3.1 ESPACIAL

La estación se encuentra ubicada en el centro poblado de Maral, distrito de Paucar, Provincia de Yanahuanca, departamento de Pasco.

1.3.2 TEMPORAL

Comprende el periodo enero – marzo 2015

1.4 FORMULACIÓN DEL PROBLEMA

¿Se puede diseñar un sistema de vigilancia remota para diseño de red vigilancia remota para el mejoramiento en el control del funcionamiento de los nodos de comunicación en la provincia de Picush – Pasco – Perú.

1.5 OBJETIVOS:

1.5.1 Objetivo general

DISEÑO DE RED DE VIGILANCIA REMOTA PARA EL MEJORAMIENTO EN EL CONTROL DEL FUNCIONAMIENTO DE LOS NODOS DE COMUNICACIÓN EN LA PROVINCIA DE PICUSH – PASCO - PERU

CAPITULO II
MARCO TEÓRICO

2.1 ANTECEDENTES

El presente proyecto de investigación toma como punto de partida el Diseño de una red de vigilancia local y remota con la utilización de tecnología IP para la vigilancia de los nodos de comunicación, para lo cual se ha investigado si existen proyectos similares o relacionados al tema y se han encontrado los siguientes:

- DISEÑO DE SISTEMA DE MONITOREO CCTV CON CAMARAS IP INALAMBRICAS Y ALARMAS PARA LA SEGURIDAD DE LOS PUNTOS MAS CRITICOS DE EL DISTRITO DE VILLA EL SALVADOR

  Ahora, el foco de esta investigación, se centra en el Distrito de Villa el Salvador (puntos más vulnerables), donde el problema de la seguridad es casi nulo, por una parte no se cuenta con personal de vigilancia ni con equipos de monitoreo especializados que ayuden a solventar este problema, lo que ha provocado que la delincuencia, el robo, pandillaje en otras cosas crezca más en este distrito y todo esto debido a las faltas de gestión y no prevención de la entidad a cargo de la seguridad.

- RED DE VIDEO VIGILANCIA UTILIZANDO CÁMARAS IP PARA EL MONITOREO DEL PROCESO DE PRODUCCIÓN EN LA EMPRESA AGROCUEROS S.A., elaborado por Medina Medina, Tannia Leonela en el 2011, Biblioteca de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial en la universidad técnica de Ambato.

  Conclusión: "Supervisar y proteger, de forma local y remota su planta de producción, en tiempo real tan solo con conectarse a internet, para organizar la producción y controlar el tiempo trabajado por el operario.

- "ANÁLISIS Y DISEÑO DE UN PROYECTO DE VIDEO VIGILANCIA INALÁMBRICA EN LOS LABORATORIOS DEL BLOQUE "A" Y PARQUEADERO NORTE DEL CAMPUS PEÑAS" Zambrano Oscar en el 2009, Biblioteca de la Espol

  Conclusión: "El proyecto de Video Vigilancia consiste en el Diseño de una red inalámbrica capaz de transmitir imágenes y video en tiempo real, a través de la tecnología Wi-Fi bajo el estándar 802.11a en la frecuencia de 5 GHz, Considerando el Internet como un medio de acceso remoto por parte de los usuarios Finales, y la utilización de herramientas para la notificación por correo electrónico y Grabación de video como medio de respaldo." Los mismos que servirán como soporte para desarrollar la presente investigación.

2.2 BASE TEÓRICA

2.2.1 Redes y Servicios IP

2.2.1.1 Redes De Datos

Las redes de datos son utilizadas para compartir recursos, equipos, información y programas que se encuentran almacenados localmente o dispersos geográficamente; el objetivo de una red de datos es dar confiabilidad a la información que se está transmitiendo entre usuarios cercanos o distantes de la manera más rápida y eficiente posible.

2.2.2 Clasificación de las redes de datos.

a) LAN (Local Área Networks)

Son redes privadas que se encuentran instaladas dentro de un mismo edificio, Oficina, la distancia máxima es de 5 Km; el objetivo principal es compartir recursos Como impresoras, archivos, discos, etc.

b) MAN (Metropolitan Area Network)

Son redes con cobertura urbana concebidas inicialmente para vincular distintas Redes LAN entre ellas, formando lo que se denomina un internet.

Transportan señales a velocidades de 100 Mbps, prestan servicios de transporte para interconectar redes, como por ejemplo telefonía con PBX. Pueden ser de conmutación de paquetes o de circuitos con servicios orientados o no a la conexión.

c) WAN (Wi de Area Networks)

Estas redes también son llamadas de área extendida o área extensa, y en la práctica son de cobertura ilimitada, ya que encadenan diferentes redes de cobertura menor. Para poder hacerlo, se valen generalmente de redes públicas y privadas, utilizando todo tipo de vínculos: no tangibles, como satélites y radio enlaces, y tangibles como el cable de par de cobre, coaxiales y fibras ópticas. Son necesariamente utilizadas para poder comunicarse más allá de un edificio, cuando no existe una MAN, o más allá del alcance de la MAN.

2.2.3 La vigilancia IP inalámbrica

“La vigilancia IP inalámbrica comprende dos tecnologías probadas, la de transmisión inalámbrica en exteriores y la de video vigilancia en red que, combinadas crean una potente solución que representa una solución alternativa a la mayoría de los desafíos que actualmente a los usuarios

finales a la hora de instalar sistemas de seguridad y vigilancia: distancia, falta de infraestructura de red, condiciones climatológicas, precio y otras. La vigilancia IP inalámbrica representa un innovador avance.

A) Ventajas de la vigilancia IP Inalámbrica

- **Despliegue rápido y sencillo** Se puede desplegar prácticamente en cualquier sitio. Menos tiempo de implementación
- **Viabilidad** Costo menor que el coste de Fibra Óptica
- **Alta capacidad** Tiene un alto espectro de capacidades de ancho de banda desde 11 a 826 Mbps.
- **Fiabilidad** Tiene el 99.999% permitiendo una seguridad sin prácticamente ninguna interrupción

B) Escalabilidad y Flexibilidad

Un sistema de video en red se puede ampliar añadiendo más cámaras de red. Es Indiferente que las nuevas cámaras se instalen en el mismo local que las anteriores, o en un emplazamiento nuevo con comunicación a través de Internet. Se puede ampliar el sistema en cualquier momento en que las necesidades crezcan. Se puede añadir fácilmente nuevas tecnologías, cámaras adicionales y capacidad de 13 almacenamiento adicional según precise, gracias a la estricta adhesión a los estándares de la industria**.**

C) Rentabilidad de la Inversión

Se puede ahorrar dinero y reduce el coste total de propiedad gracias a la estricta adhesión a los estándares de la industria. Basados en estándares abiertos, los productos profesionales de video en red funcionan en una red Ethernet. Al usar un hardware para servidores de PC estándar para grabar y guardar, en lugar de un equipo patentado como los DVR, reducirá enormemente

los costes de gestión y equipamiento, en particular en sistemas de gran tamaño, donde el almacenamiento y los servidores son una parte considerable del coste total de la solución. Un ahorro de costes adicional proviene de la infraestructura que se utiliza. Las redes basadas en IP como Internet, las redes LAN y los distintos métodos de conexión como la conectividad inalámbrica se pueden aprovechar para otras aplicaciones en la organización. Los productos de video en red son compatibles con diversas tecnologías avanzadas, como alimentación a través de Ethernet (PoE).

D) Inteligencia Distribuida

En los sistemas de video en red actuales, la inteligencia se ha integrado en la propia cámara. Las cámaras de red avanzadas pueden disponer de detección de movimiento integrada estándar y gestión de alarmas para que la cámara decida cuando enviar el video, aqué velocidad de imagen y resolución, y cuando alertar a un operador determinado para que supervise o reaccione ante la alarma. Los algoritmos más inteligentes, como reconocimiento facial, visión nocturna, giro de 360 grados, etc., están siendo integrados en las cámaras de red. Obtiene los datos en formatos más manejables y con mayores niveles de precisión. La inteligencia al nivel de la cámara implica un medio de vigilancia mucho más productivo e efectivo que el que es posible con un DVR u otro sistema centralizado.

2.2.4 Direccionamiento IP

IP es la abreviatura de Internet Protocolo, el protocolo de comunicaciones más común entre las redes informáticas e Internet.14 “Para el funcionamiento de una red, todos sus dispositivos requieren una dirección IP única: La dirección MAC .Las Direcciones IP están construidas de dos partes: el identificador de red (ID Network) y el identificador del dispositivo (ID host). El sistema de direccionamiento IP

consiste de números binarios de 32 bits. Estos números Binarios, para su compresión, están separados en 4 octetos (bytes) y se pueden representar también en forma decimal separados por puntos cada byte.”

A) Clases de direcciones IP

Existen tres tipos de direcciones: Clase A, Clase B y Clase C.

La principal diferencia entre estos tres tipos principales de dirección deriva en el número de octetos usados para identificar la red.

La Clase A

Utiliza sólo el primer octeto para identificar la red, dejando los 3 octetos (24 bits) restantes para identificar el host. La clase A es utilizada para grandes corporaciones internacionales.

se puede apreciar de mejor manera como se realiza la distribución de los octetos para la red y para los host.

Network Host Host Host

La Clase B

Utiliza los primeros dos octetos para identificar la red, dejando los 3 octetos (24 bits) restantes para identificar el host. La clase B es utilizada por grandes compañías que necesitan un gran número de nodo. Los 2 octetos le dan cabida a 16.384 redes supliendo todas ellas un total de 65.534 (216 - 2) direcciones IP para los hosts. En la tabla 2.3 se puede apreciar de mejor manera como se realiza la distribución de los octetos para la red y para los host.

La Clase C

Usa los primeros 3 octetos para el identificador de red, dejando los 8 bits restantes para el host. En la tabla 2.4 se

puede apreciar de mejor manera como se realiza la distribución de los octetos para la red y para los host.

Network Network Network Host

La clase C es utilizada por pequeñas redes, que suman un total de 2.097.152 redes con un máximo de 254 (28 - 2) hosts cada una.

Se le resta un 2 a la formula porque: 2n – 2= número de host/redes.

Donde n es el número de bits.

El 2 significa que se está reservando un lugar para la dirección de subred y el restante para la dirección de broadcast.

Siempre será la primera dirección IP para la subred y la última dirección IP para efectos de broadcast. La siguiente dirección IP seguida de la dirección de subred generalmente se asigna al enrutador o default Gateway.

B) Resumen de dirección IP según su clase

En la tabla 2.5 se tiene como resumen que: el rango del 1er. Octeto para la Dirección IP de Clase A comienza desde la IP 1 hasta la 126, no comienza desde 0 ya que esta es reservada para la dirección de red; 127 es reservada para la dirección del local host. Se tiene 127 redes, 16.777.214 host.

Network Network Host Host

De la misma manera para la dirección IP de la Clase B, el 1er. Octeto comenzará desde la IP 128 a 191, se amplía la red con 16.384 números de redes, disminuye el humero de host a 65.534.

En la dirección IP de clase C, el 1er. Octeto comenzará desde la IP 192 a 223, se aumenta el número de redes ya que tenemos 3

Octetos para la misma, y disminuye el número de host ya que solo tenemos un Octeto para el número de host y este será 254.

Clases
Rango del 1er. Octeto
Número de redes
Números de hosts
Ejemplo
A 1- 126
127 16.777.214
10.16.124.7
B 128 – 191
16.384 65.534
130.16.56.53
C 192 – 223
2.097.152 254
200.15.23.8

Mascaras de subred (SubnetMask)

“La subnetmask para una dirección IP en particular es utilizada por los enrutadores para resolver que parte de la dirección IP provee la dirección de red y que parte la dirección del host.

Clase Mascara de Subred
A 255.0.0.0
B 255.255.0.0
C 255.255.255.0

La red 127.x.x.x está reservada para pruebas de diagnósticos conocidas como loopback (ida y regreso), el cual permite a las computadoras enviarse a ellas mismas un paquete sin afectar el ancho de banda de la red.

También existen una clase D y una clase E. la clase D es usada para multicast de grupos de datos de una determinada aplicación o servicio de un servidor. La clase E está reservada para usos experimentales.

2.2.5 Puertos

Un número de puertos define un servicio o aplicación concretos para que el servidor receptor (por ejemplo una cámara de IP) sepa procesar los datos entrantes. Cuando un computador envía datos vinculados a una aplicación concreta, normalmente añade el número de puerto a una dirección IP sin que el usuario lo sepa. Los números de puerto pueden ir del 0 al 65535.

2.2.6 Reenvío de Puertos

“Para acceder a cámaras ubicadas en una LAN privada a través de Internet, la dirección IP pública del router se debería usar junto con el número de puerto correspondiente del codificador de video o la cámara de red en la red privada. Dado que un servicio web a través de HTTP normalmente se asigna al puerto 80, en un escenario con varios codificadores de video o cámaras de red que utilizan el puerto 80 para HTTP en una red privada ocurre lo siguiente: En lugar de cambiar el número de puerto HTTP predeterminado en cada producto de video en red, se puede configurar un router para asociar un único número de puerto HTTP al puerto HTTP predeterminado y a la dirección IP de un producto de video en red concreto. Este proceso se denomina reenvío de puertos; y funciona como se indica a continuación.

Los paquetes de datos entrantes llegan al router a través de su dirección IP pública (externa) y un número de puerto específico. El router está configurado para reenviar los datos que entran por un número de puerto predefinido a un dispositivo específico de la parte del router correspondiente a la red privada.

A continuación, el router sustituye la dirección del emisor por propia dirección IP privada (interna). Para el cliente receptor, el router es el

origen de los paquetes. Con los paquetes de datos salientes ocurre lo contrario. Elrouter sustituye la dirección IP privada del dispositivo origen por la IP pública del propio router antes de enviar los datos a través de internet.”

2.2.7 NAT (Network AddressTranslation)

Traducción de dirección de red, para que un dispositivo de red con una dirección IP privada pueda enviar información a través de internet, debe utilizar un router compatible con NAT. Con esta técnica, el router puede traducir una dirección IP privada en una pública sin el conocimiento del host que realiza el envío.

2.3 VIGILANCIA LOCAL Y REMOTA CON TECNOLOGÍA IP

2.3.1 Vigilancia remota

Se encarga de localizar el acceso tanto a las imágenes,video en vivo cualquier lugar del mundo solo con tener acceso a Internet. Los productos de video red proporcionan una manera sencilla de capturar y distribuir imágenes de video de gran calidad a través de cualquier tipo de red IP o de Internet. Esto significa que incluso las empresas con oficinas en distintas partes del mundo pueden hacer un uso efectivo de una solución de video en red para fines de vigilancia de seguridad y de supervisión a distancia.

2.3.2 Vigilancia local

La vigilancia local se hace desde el mismo sitio donde se encuentran el sistema de vigilancia es decir se puede conectar a la red LAN, WLAN, o simplemente Internet; para poder visualizar lo que está sucediendo en vivo y en directo.

2.3.3 Cámaras IP

“Las cámaras IP, son vídeo cámaras de vigilancia que tienen la particularidad de enviar las señales de video (y en muchos casos audio),

pudiendo estar conectadas 19 directamente a un Router ADSL, o bien a un concentrador de una Red Local, para poder visualizar en directo las imágenes bien dentro de una red local (LAN), o a través de cualquier equipo conectado a Internet (WAN) pudiendo estar situado en cualquier parte del mundo.” Las Cámaras IP poseen un computador es decir que cuenta con su propia dirección IP y se puede conectar a la red como cualquier otro dispositivo como por ejemplo un teléfono IP.

a) Componentes de una cámara IP

Lente: es el encargado de enfocar la imagen en el sensor (CCD/CMOS).

Sensores de imagen: a medida que la luz a traviesa un objeto ésta se enfoca en el sensor de imagen de la cámara. Un sensor de imagen está compuesto de muchos foto sitos y cada foto sito corresponde a un elemento de la imagen, comúnmente conocido como pixel, en un sensor de imagen. Cada pixel de un sensor de imagen registra la cantidad de luz a la que expone y la convierte en un número de electrones correspondientes. Cuanto más brillantes es la luz, más electrones se genera.

CCD: dispositivo de acoplamiento de carga, estos sensores ofrecen una sensibilidad lumínica ligeramente superior y producen menos ruido. Con esta mayor sensibilidad lumínica se traduce en mejores imágenes en condiciones de poca luz. Este sensor puede consumir hasta 100 veces más energía que un sensor CMOS equivalente.

CMOS: semiconductor de óxido metálico complementario, estos sensores permiten mayor posibilidades de integración y más funciones, tienen un tiempo menor de lectura lo que resulta una ventaja cuando se requieren imágenes de alta resolución, una

disipación de energía menor a nivel del chip, un menor tamaño en el sistema.

b) **Filtro óptico,** realiza la tarea de remover cualquier luz infrarroja (IR), para que los colores sean mostrados correctamente. En cámaras infrarrojas, este filtro es removible para que se puedan proporcionar imágenes de alta calidad en blanco y negro en condiciones de poca luz.

c) **Procesador,** realiza las funciones de administración y control de la exposición (niveles de luz), balance de blancos (ajuste de colores), brillo de imagen y 20 otros aspectos relacionados con la calidad de la imagen, también este procesador incluye un componente de compresión el cual comprime las imágenes digitales a un formato que contiene menos datos y que puede ser transmitido por la red de forma eficiente.

d) **Puerto de red Ethernet,** el cual se encarga de conectar por medio de cable UTP a internet, computador, switch, router, servidor, con el fin de compartir los datos enviados por el CCD.

e) Funcionamiento de una cámara IP

En la figura 2.4 se puede visualizar el funcionamiento interno de una cámara IP, el cual la luz de la imagen pasa por la lente, esta se refleja en un filtro RGB (Red-Green-Blue), el cuál descompone la luz en tres colores básicos: rojo, verde y azul. Esta división de rayos se concentra en un chip sensible a la luz denominado CCD/CMOS, el cual asigna valores binarios a cada pixel y envía los datos digitales para su codificación en video y posterior envío a través de internet hasta el dispositivo al cual se desee, desde el cual el interesado necesita ver las acciones en tiempo real.

f) Tipos de cámaras IP

Los tipos de cámaras IP se pueden clasificar en función de su utilización tanto para exteriores como para interiores. Pueden observar los tipos de cámaras que se detallan a continuación.

❖ **Cámaras fijas**

Una cámara de red fija, que puede entregarse con un objetivo fijo, es una cámara que dispone de un campo de vista fijo una vez montada.

❖ **Domos fijos**

También conocida como mini domo, consta básicamente de una cámara fija preinstalada en una pequeña carcasa domo. La cámara puede enfocar el punto seleccionado en cualquier dirección. La ventaja radica en su discreto y disimulado diseño, así como en la dificultad de ver hacia qué dirección apunta la cámara. Es resistente a manipulaciones.

❖ **Cámaras PTZ y Domos PTZ**

Las cámaras PTZ o Domos PTZ pueden moverse horizontalmente, verticalmente y acercarse o alejarse de un área o un objeto manual o automática.

❖ **Cámaras IP con visión día/noche**

Las cámaras de red a color con visión diurna y nocturna proporcionan imágenes a color a lo largo del día cuando la luz disminuye bajo un nivel determinado, la cámara puede cambiar automáticamente al modo nocturno para utilizar la luz prácticamente infrarroja (IR) para proporcionar imágenes de alta calidad en blanco y negro. Resultan útiles en entornos que restringen el uso de luz, vigilancia oculta y aplicaciones del tránsito en la que las luces brillantes podrían entorpecer la conducción nocturna.

❖ **Cámara Ojo de Pez.**

Cama con visión de 180° y 360° y con la tecnología digital son imágenes filtradas y reacomodas para una mejor visualisacion.

2.4 VIGILANCIA IP

Es aquella tecnología en que las imágenes y audio son capturados por las cámaras IP y micrófonos, se comprimen y transmiten por una red de datos esta puede ser de LAN, WLAN, WAN y pueden ser accesados desde uno o varios puntos en cualquier lugar del mundo mediante computadoras convencionales. Las ventajas de un sistema de video IP que utiliza servidores son las siguientes.

- ✓ Utilización de red estándar y hardware de servidor de PC para la grabación y gestión de video.
- ✓ El sistema escalable permitiendo añadir cámaras con facilidad.
- ✓ Es posible la grabación fuera de las instalaciones
- ✓ Crecimiento a futuro, facilidad de incorporación de cámaras IP.
- ✓ Un sistema de video IP que utiliza cámaras IP añade las ventajas siguientes.
- ✓ Cámaras de alta resolución en orden de los Mega píxel
- ✓ Calidad de imagen constante
- ✓ Alimentación eléctrica a través de Ethernet y funcionalidad inalámbrica
- ✓ Flexibilidad y escalabilidad completa.

2.4.1 Sistemas de seguridad

Un sistema de seguridad no es un servicio aislado es una combinación de elementos físicos y electrónicos. Es muy difícil de conseguir seguridad total, entonces podemos hablar de fiabilidad o probabilidad de que un sistema se comporte tal y como se espera. Más que de seguridad, se habla de sistemas fiables en lugar de hacerlos de sistemas seguros. A grandes rasgos se entiende que mantener un sistema fiable consiste básicamente en garantizar tres aspectos:

- Confidencialidad
- Integridad
- Disponibilidad

Tipos de Seguridad

- **Física o medios técnicos:** Medidas de protección civil y respaldo electrónico.
- **Lógica:** Con fines estadísticos y de seguimiento de atención de incidencias.
- **Desarrollo y aplicaciones:** Registro de expedientes entregados por los empleados y recursos humanos del organismo.
- **Comunicaciones y Redes:** Sistema de Comunicación interna y externa para acceder a la información depositada en el sistema los usuarios tienen su propia clave y contraseña.
- **Seguridad Física o medios técnicos**

  En estos medios están enfocados a disuadir, detener o al menos, retardar o canalizar la progresión de la amenaza. El incremento del tiempo que estos elementos imponen a la acción agresora para alcanzar su objetivo resulta, en la mayoría de las ocasiones, imprescindibles para que se produzca en tiempo adecuado la alarmareacción. El conjunto de medios pasivos constituye lo que se denomina seguridad física, que está formada por:
- **Elementos de carácter estático y permanente**

  "Protegen y suponen el primer obstáculo que se presenta para la penetración de intrusos formando por la protección perimetral (vallas, cercados, setos de jardín, etc.), protección periférica (puertas, rejas, cristales, etc.) y protección del bien, que está constituido por recintos cerrados (cajas fuertes, cámaras acorazadas, etc.)." Tomado de: Sistemas de Seguridad Integral inteligente para una vivienda Aislada,
- **Medios técnicos Activos**

  La función de los medios activos es la de alertar local o remotamente de un intento de violación o sabotaje de las medidas de seguridad física establecidas. El conjunto de medios activos constituye lo que se denomina seguridad electrónica; pueden utilizarse de forma oculta o visible. Sus principales funciones son:
  - Detección de intrusos en el interior y en el exterior.

- Control de accesos y tráfico de personas, paquetes, correspondencia y vehículos.
- Vigilancia óptica por fotografía o circuito cerrado de televisión.
- Protección de las comunicaciones.

2.4.2 Seguridad Ciudadana

Desde hace más de una década, el concepto de la seguridad ciudadana domina el debate sobre la lucha contra violencia y delincuencia en América Latina. La expresión está conectada con un enfoque preventivo y, hasta cierto grado, liberal a los problemas de violencia y delincuencia. El término pone énfasis en la protección delos ciudadanos y contrasta con el concepto de la seguridad nacional que dominaba el discurso público en décadas pasadas y que enfocaba más en la protección y la defensa del Estado. Existen múltiples conceptos y nociones del término "seguridad ciudadana" y su contenido concreto puede variar considerablemente dependiendo del actor o autor quien lo utilice. Por ejemplo, no hay un consenso si la seguridad ciudadana se refiere también a riesgos o amenazas de tipo no intencional (accidentes de tránsito, desastres naturales) o de tipo económico y social. Un punto en que sí concuerdan la gran mayoría de autores es que el término referencia a dos niveles de la realidad: Primero, se refiere a una condición o un estado de un conjunto de seres humanos a la ausencia de amenazas que ponen en peligro la seguridad de un conjunto De individuos. En este sentido, el término tiene un significado normativo. Describe una situación ideal que probablemente es inexistente en cualquier lugar del mundo pero que funciona: “como un objetivo a perseguir” por ejemplo, define la seguridad ciudadana como "la condición personal, objetiva y subjetiva, de encontrarse libre de violencia o amenaza de violencia o despojo intencional por parte de otros".

Segundo, se refiere a políticas públicas encaminadas a acercar la situación real a la situación ideal, es decir, se refiere a políticas que apuntan hacia la eliminación de las amenazas de seguridad o hacia la

protección de la población ante esas amenazas. En ese sentido, el término se refiere a prácticas sociales empíricamente existentes.

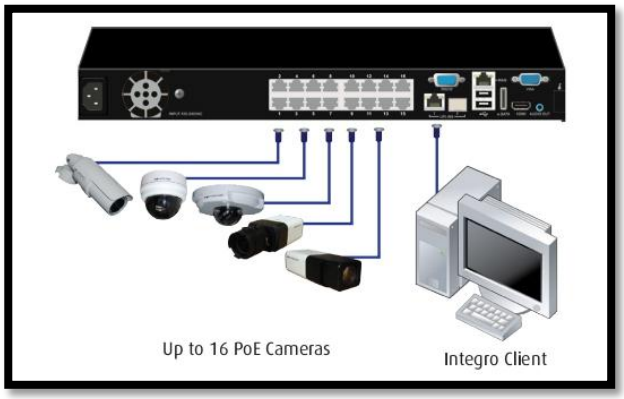
2.4.3 Seguridad Electrónica

Es un área que presta herramientas de última tecnología para ayudar a completar las otras áreas de seguridad. La importancia de los sistemas de seguridad electrónica radica en que se sustenta en el uso de alta tecnología aplicada a la seguridad y soportada en un adecuado diseño, instalación e interconexión, de modo que obtener una alerta temprana de los eventos generados en las instalaciones, en el momento en que están siendo vulneradas.

2.4.3.1 NVR

Network video recorder, es un dispositivo de almacenamiento en red dedicado para el almacenamiento activo de grabaciones de cámaras de red. El dispositivo graba video en forma digital a una unidad de disco, flash USB o en otro tipo dispositivo de almacenamiento masivo desde diferentes cámaras IP situadas en lugares locales o remotos.

Disponen de interfaces amigables para las tareas de grabación y gestión, de la monitorización de eventos y gestión del sistema, y todas las ventajas propias del software de vigilancia que integran.



2.4.3.2 CCTV

El circuito cerrado de televisión o Closed Circuit Television, se denomina circuito cerrado ya que todos sus componentes están enlazados; el circuito puede estar compuesto, por una o más cámaras de vigilancia conectadas a uno o más monitores o televisores, que reproducen las imágenes capturadas por las cámaras. Es un sistema pensado para un número limitado de espectadores.

2.4.3.3 Monitoreo

Es el seguimiento rutinario de la información prioritaria de un programa, su objetivo principal es observar continuamente para identificar cambios de lo que se está observando. El monitoreo debe ser relevante, transparente, sistemático y continuo.

2.4.3.4 Software de Monitoreo

Cada cámara IP cuenta con su software de monitoreo solo basta con instalarlo en su servidor y en los hosts que van hacer vistas las cámaras IP. Hoy en día con la actualización de la tecnología se ha creado múltiples software de reconocimiento de todo tipo de cámaras.

2.4.3.5 Almacenamiento y compresión del video

"El almacenamiento de video se puede realizar en una computadora que haga de servidor o propiamente en un servidor adecuado. Ahora en día los Software´s gestionan la grabación del video utilizando el sistema de ficheros de Windows estándar el almacenamiento del mismo, pero existen Software libre que también puede guardar la grabación del video y lo mejor puede gestionar el video creando niveles de almacenamiento." Existen normas de compresión de video y algoritmos de compresión para ayudar a asegurar transmisiones de alta calidad. "Existe un conflicto entre la tasa de transferencia de paquetes y la calidad de la imagen JPEG, JPEG2000, MPEG-1,2,4, Wavelet.MPEG Y JPEG son normas ISO/IEC que permiten transmisiones de video de alta calidad." En la figura 2.6 se puede observar como es el Posicionamiento de algoritmos el cual se detalla a continuación.

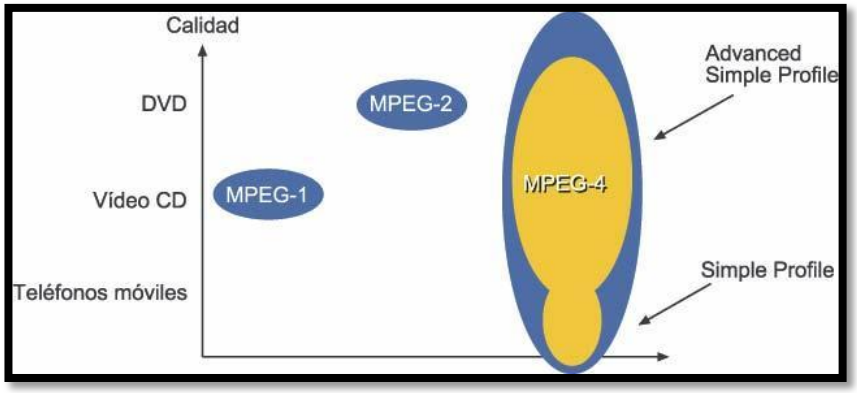
MPEG-1, fue desarrollado para video digital en CD-ROOM.

MPEG-2, fue desarrollado con el DVD y la televisión de alta definición;de excelente calidad pero muybajo nivel de compresión.

MPEG-4, es apropiado para aplicaciones de animación o para teléfonos móviles.

MPEG4 Layer 2, de buena calidad y buen nivel de compresión, es el más utilizado a nivel mundial.

MPEG4 Layer 10, mejor conocido como H.264, de buena calidad y excelente nivel de compresión.



Finalmente, no interesa que formato se use; lo importante es comprimir a su máxima expresión un video sin sacrificar mucho la calidad que el ojo humano puede apreciar. Tomado de: Algoritmos de Compresión de Video Teoría y Estándares.

2.4.4 Servidores

Es equipo informático que es similar a un computador corriente pero se diferencia por ser de forma robusta para soportar trabajo pesado y dar la posibilidad de proveer servicios a otras computadoras denominadas clientes.

Tipos de servidores

- **Servidor de archivo,** es el que almacena varios tipos de archivos y los distribuye a otros clientes en la red.
- **Servidor de impresiones,** controla una o más impresoras y acepta trabajos de impresión de otros clientes de la red.
- **Servidor de correo,** almacena, envía, recibe, en ruta y realiza otras operaciones relacionadas con email para los clientes de la red.
- **Servidor de Fax,** almacena, envía, recibe, en ruta, y realiza otras funciones necesarias para la transmisión, la recepción y la distribución apropiadas de los fax.
- **Servidor de telefonía,** realiza funciones relacionadas con la telefonía, como es la de contestador automático, realizando las

funciones de un sistema interactivo para la respuesta de la voz, almacenando los mensajes de voz, encaminando las llamadas.

- **Servidor proxy,** permite administrar el acceso a internet en una red de computadoras permitiendo o negando el acceso a diferentes sitios Web.
- **Servidor de acceso remoto (RAS),** controla las líneas de módem de los monitores u otros canales de comunicación de la red para que las peticiones conecten con la red de una posición remota, responde llamadas telefónicas entrantes o reconoce la petición de la red y realiza la autentificación necesaria y otros procedimientos necesarios para registrar a un usuario en la red.
- **Servidor de uso,** realiza la parte lógica de la informática o del negocio de un uso del cliente, aceptando las instrucciones para que se realicen las operaciones de un sitio de trabajo.
- **Servidor web,** almacena documentos HTML, imágenes, archivos de texto, escrituras, y demás material Web compuesto por datos (conocidos colectivamente como contenido) y distribuye este contenido a clientes que la piden en la red.
- **Servidor de Base de Datos,** provee servicios de base de datos a otros programas y computadoras, como es definido por el modelo cliente- servidor. También puede hacer referencia a aquellas computadoras (servidores)dedicadas a ejecutar esos programas, prestando el servicio.
- **Servidor de reserva,** tiene el software de reserva de la red instalado y tiene cantidades grandes de almacenamiento de la red en discos duros u otras formas de almacenamiento (cinta, etc.)disponibles para que se utilice con el fin de asegurarse de que la pérdida de un servidor principal no afecte a la red. Esta técnica también es denominada clustering.
- **Servidor de impresión,** muchas impresiones son capaces de actuar como parte de una red de ordenadores sin ningún otro dispositivo, tal como un “print server”, a actuar como intermediario entre la impresora y el dispositivo que está

solicitando que se termine un trabajo de impresión.

- **Servidor de video,** son dispositivos creados para permitir la transición tecnológica entre los sistemas análogos de vigilancia conocidos como CCTV y las nuevas formas de vigilancia conocidas como vigilancia IP.

2.4.5 Detección de Movimiento (WMD)

La detección de movimiento en videopor IP, es una función ya integrada en cámaras IP, ofrece grandes ventajas respecto al caso de un DVR ya que es este caso es un proceso intensivo de la CPU y ejecutar la detección de movimiento en vide o en muchos canales que implica un esfuerzo excesivo en el sistema DVR; en IP la detección de movimiento se procesa en la cámara de red o en propio servidor de video, lo que reduce la carga de trabajo para cualquier dispositivo de grabación en el sistema y permite la vigilancia condicionada a los eventos.

En la figura 2.7 se puede ver las áreas de color verde y rojo las cuales han sido distribuidas por zonas para proceder mediante la detección de movimiento.

Detección de Movimiento

La VMD también puede residir en el software de aplicación de video, proporcionando así la funcionalidad VMD a las cámaras de red que originalmente no incorporan esta característica.

VENTAJAS DEL VDM

Mantiene el ancho de Banda.

Reduce la carga de trabajo de la CPU en el servidor de grabación.
Ahorra espacio de almacenamiento.

La cámara puede interactuar con otros sistemas que I/O utilizan puertos

Como las de activar alarmas, encendido de luces eléctricas.

2.5 MEDIOS DE TRANSMISIÓN

2.5.1 Medio de transmisión Guiados

2.5.1.1 Par trenzados

El par trenzado se constituye en dos cables de cobre recubiertos de un aislante, entrecruzados en forma de espiral. Cada par de cables constituye solo un enlace de comunicación. Es el medio guiado más utilizado por su bajo coste.

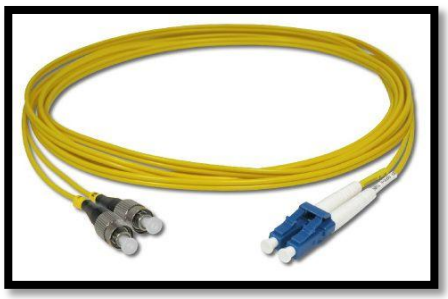
2.5.1.2 Cable coaxial

"El cable coaxial tiene dos conductores pero está construido de forma diferente para que pueda operar sobre un rango mayor de frecuencias, este cable coaxial es el medio más versátil para la transmisión, el cable coaxial tiene una mejor respuesta que el cable de par trenzado, lo cual permite mayores frecuencias y

velocidades de transmisión. El inconveniente del cable coaxial es su atenuación, el ruido térmico."

2.5.1.3 Fibra óptica

"El cable de fibra óptica es un medio flexible y fino, tiene una forma cilíndrica y está formado por tres secciones concéntricas: el núcleo, el revestimiento, y la cubierta. El núcleo está constituido por una o varias hebras o fibras muy finas de cristal o plástico. El cable de fibra óptica soporta mayor capacidad de ancho de banda, y por lo tanto la velocidad de transmisión es mayor que los anteriores cables mencionados, tiene menor tamaño y peso su atenuación es mínima, tiene aislamiento electromagnético, se puede usar para la transmisión a mayores distancias por consecuencia existe una mayor separación entre repetidores." "Tomado del libro de Comunicaciones y redes de Computadores de William Stallings, de las páginas 103-119".



2.6 SISTEMA DE RESPALDO DE ENERGÍA

El objetivo principal es mantener la seguridad dentro de un edificio, casa, etc cuando falla el suministro de energía eléctrica de la red externa; como también garantizar el funcionamiento del sistema de monitoreo.

2.6.1 Generador eléctrico

Un generador es una maquina eléctrica que realiza el proceso de transformación de energía mecánica en energía eléctrica.

2.6.2 Inversores

También se lo llama ondulador es un circuito utilizado para convertir corriente continua en corriente alterna. El objetivo principal es cambiar un voltaje de entrada de corriente directa a un voltaje simétrico de salida de corriente alterna, con la magnitud y frecuencia deseada por el usuario.

Los inversores también son utilizados para convertir la corriente continua generada por los paneles solares fotovoltaicos, acumuladores o baterías, etc, en corriente alterna.

2.6.3 Sistema de alimentación ininterrumpida (UPS)

Es un dispositivo que contiene baterías en su interior, este puede proporcionar energía eléctrica tras un corte de energía eléctrica de la red externa a todos los dispositivos que tenga conectados y un convertidor de corriente que transforma la energía continua en alterna.

UPS Offline o Standby

Es un equipo que se ocupa para computadores personales. El interruptor de transferencia está configurado para utilizar la entrada CA filtrada como fuente de alimentación principal y cambiar a la batería como suministro de reserva si falla el principal.

En la figura 2.12 se muestra el diagrama de UPS offline.

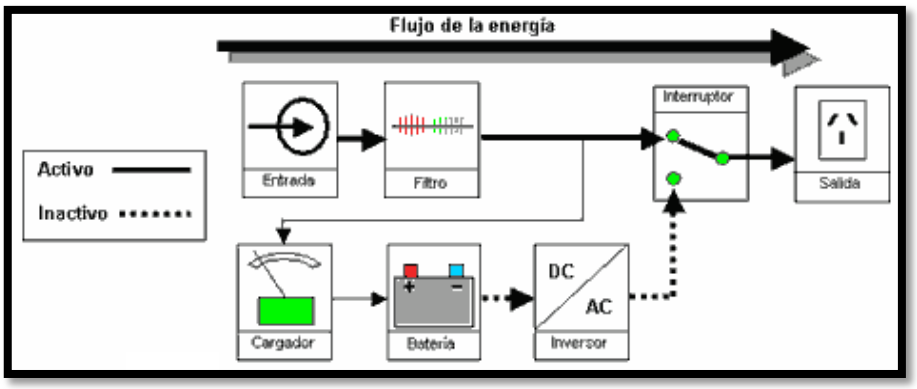


Figura 2.12. UPS Offline

Funcionamiento

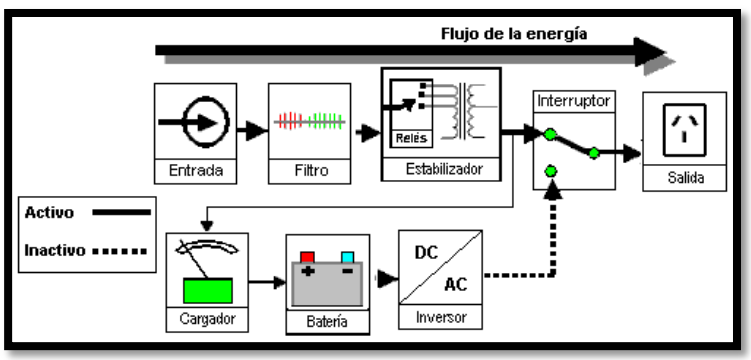
UPS Interactivo

Es el más utilizado en empresas pequeñas, Internet y para respaldo de servidores. En este tipo de UPS el inversor de corriente de batería a CA esta siempre conectado a la salida del UPS. Cuando la alimentación de CA de entrada es normal se activa el inversor al revés haciendo que se carga la batería.

Esta tecnología permite mayor estabilidad de la tensión para la carga, aumentando el rango de tensión admisible en la entrada del UPS.

Las principales ventajas de este modelo es su gran eficacia, tamaño reducido, bajo costo, confiabilidad y su capacidad de manejo de tensión baja o alta.

Un UPS interactivo trabaja mayoritariamente en la gama de potencia de 0.5-5 kVa. En la figura 2.13 se muestra el diagrama de un UPS interactivo.



UPS Interactivo-Funcionamiento

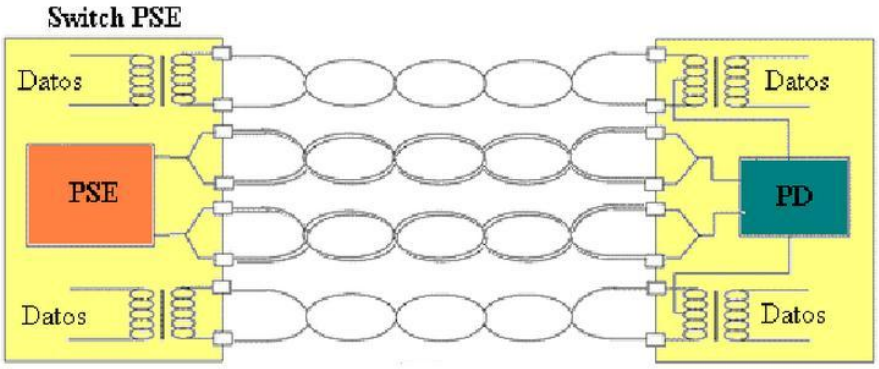
2.6.4 Tecnología PoE.

Es un sistema para transferir de forma segura potencia eléctrica junto con datos, permite que la alimentación eléctrica se suministre al dispositivo de red, como por ejemplo, un teléfono IP o una cámara IP, usando el mismo cable que se utiliza para una conexión de red. Elimina la necesidad de utilizar tomas de corriente en las ubicaciones de la cámara y permite una aplicación más sencilla de los sistemas de alimentación ininterrumpida para garantizar un funcionamiento las 24 horas del día, 7 días a la semana.

PowerOver Ethernet está regulado en la norma IEEE 802.3af, y está diseñado de manera que no haga disminuir el rendimiento de comunicación de los datos en la red. La corriente suministrada a través de la infraestructura LAN se activa de forma automática cuando se identifica un terminal compatible y se bloquea ante dispositivos preexistentes que no sean compatibles.

Esta norma utiliza cables estándares categoría 5 o superiores y asegura que la transferencia de datos no se vea afectada. “En dicho estándar al dispositivo que proporciona la energía se le conoce como equipo de suministro eléctrico (PSE). El dispositivo que recibe la energía se conoce como dispositivo alimentado (PD).”

En la figura 2.14 se muestra un gráfico del funcionamiento de un POE.



Funcionamiento POE

La norma 802.3af establece que un PSE proporciona un voltaje de 48 VCC con una potencia máxima de 15,4 W por puerto; pero debido a las pérdidas que se producen en un cable de par trenzado sólo se garantiza 12.95 W.

En el diseño la tecnología PoE permitirá un ahorro de costos en fuentes de alimentación y cableado. Además, ayuda a la administración de la red permitiendo a los administradores monitorear y manejar los dispositivos remotamente.

Ventajas de PoE

- Cableado más barato: un cableado es más barato que los repetidores USB y se elimina la necesidad de colocar el cableado eléctrico para AC.
- Poder colocar 48 V. DC desde arreglos de baterías permite manejar mejor las interrupciones del fluido eléctrico.
- Los dispositivos se instalan fácilmente donde pueda colocarse un cable LAN, y no existentes las limitaciones debidas a la proximidad de una base de alimentación (Dependiendo la longitud del cable se deberá utilizar una fuente de alimentación de mayor voltaje debido a la caída del mismo, a mayor longitud mayor pérdida de voltaje, superando los 25 metros de cableado aproximadamente).
- PoE también permite conseguir una localización óptima de las cámaras a fin de maximizar la cobertura, esto significa que los instaladores de cámaras de red no son ilimitados por la localización de las fuentes de alimentación existentes.

CAPITULO III
DESARROLLO DE LA METODOLOGIA

3.1 DESCRIPCIÓN DE PROYECTO

Los sistemas de vigilancia basados en red IP proporcionan soluciones rentables, flexibles y escalables, con un sinfín de aplicaciones. En este caso, la aplicación será la vigilancia en nodos de comunicación picush-pasco. Lo que se plantea realizar en el diseño es dividir en redes LAN (Local Área Network) independientes que luego se interconectaran para de ese modo cubrir todas las zonas, formando una red MAN (Metropolitan Area Network).

En primer lugar se realizará el diseño para la primera área, la cual se pondrá como base para el diseño de las otras áreas. Se tomará en cuenta las consideraciones y parámetros vistos anteriormente para todos los elementos que conforman el sistema de vigilancia.

segundo punto, se hará el estudio de cómo deben estar distribuidos los mismos elementos para un despliegue efectivo. Esta distribución debe cubrir zonas con la adecuada distribución de las cámaras, puntos de accesos inalámbricos, routers en cada área y también los elementos que permitirán la interconexión entre las demás áreas.

El tercer paso es obtener un plano con la distribución y escoger los elementos con los parámetros deseados buscando la alternativa más conveniente (no necesariamente el mejor modelo con todas las prestaciones) entre las diferentes marcas que desarrollan estos elementos para la vigilancia y seguridad.

El último paso es validar el diseño el cual corroborará si el diseño es correcto, rentable y cumple con los objetivos planteados.

3.2 UBICACIÓN DEL PROYECTO:

ESTACION DE TDP : EBC PICUSH

Departamento : Pasco

Provincia : Yanahuanca

Distrito : Paucar

DESCRIPCION	DATOS
Tipo de Estación	EBC
Tipo de torre	AUTOSOPORTADA
Altura de torre	50 m.
Altura de antena a instalarse	35 m.
Latitud de la Estación	10°20'54.0"S
Longitud de la Estación	76° 25'26.8"O
Altitud msnm de la Estación	3794.77 msnm

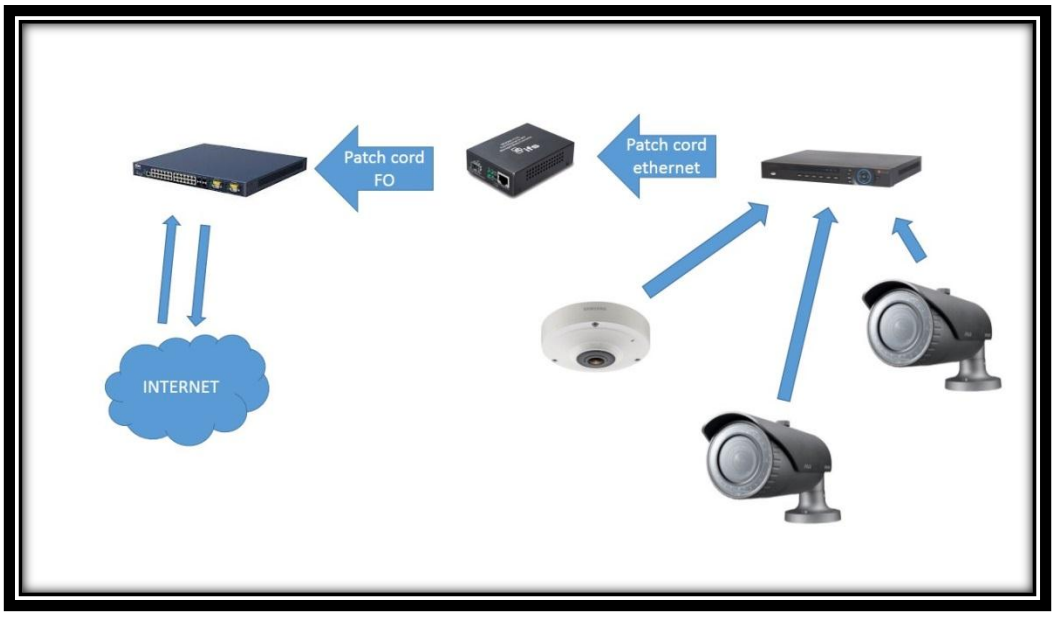
En la actualidad está protegida con cercado eléctrico

3.3 ESTRUCTURA DEL SISTEMA DE VIDEO VIGILANCIA:

Las cámaras que se utilizarán serán del tipo PTZ (pan, tilt, zoom), es decir, de movimiento horizontal y vertical. Según la distribución, habrá tres cámaras para la zona y así respectivamente según el área y su extensión.

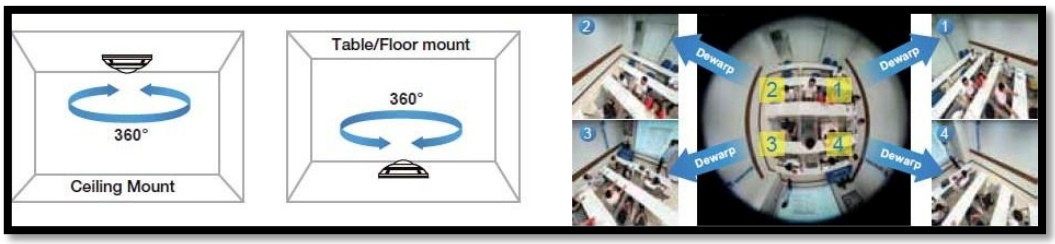
Definimos la posición de las cámaras y sus parámetros. Al tratarse de un demo del programa VideoCAD los parámetros del lente, tamaño de sensor (1/3") y longitud focal (4mm), se encuentran establecidos y no se puede cambiar el valor. Por tal motivo, se realizará el esquema con estos valores predeterminados que de igual forma son coherentes con los valores comerciales que se mostró anteriormente.

La siguiente gráfica muestra la configuración de la altura, ángulo de visión y rango de cobertura. Esta configuración es la misma para todas las cámaras, y solo varía el valor de la distancia de alcance, como se mencionó anteriormente. Se debe tener en cuenta que todas las medidas están dadas en metros.



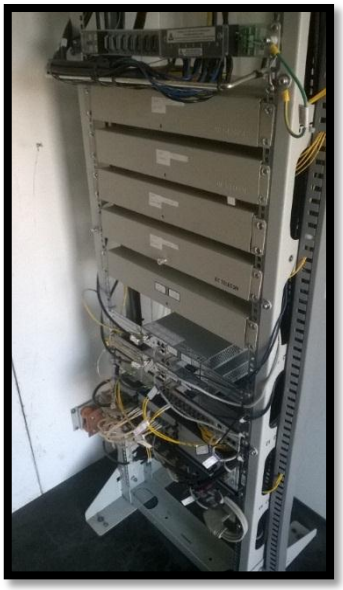
3.3.1 Distribución de cámaras

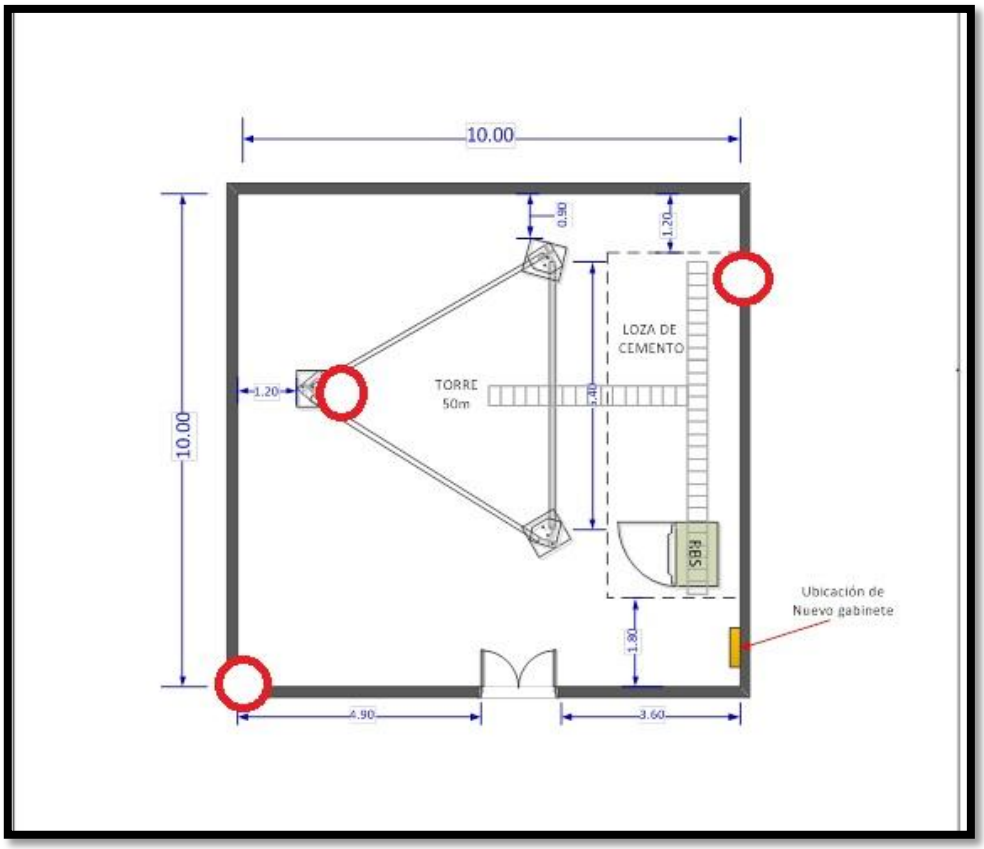
- **CÁMARA 1**: Vista desde la torre se ubicara la cámara ojo de pez para que pueda cubrir todo el perímetro y la imagen si bien se puede notar curva y talves un poco difícil de distinguir , pero con el software se puede filtrar y tener 4 área de cobertura o mas , de acuerdo a la elección.



- **CAMARA 2:** fija para cubrir la entrada al SITE y al shelter .

- **CAMARA 3:** fija cubrirán el área de los equipos dentro del shelter en los que se pueden encontrar BBU, SITE Router, baterías de 15000Ah , IDU ,…etc , de gran valor monetario y mucho más importante para el correcto funcionamiento del sistema de comunicación.




10.00
0.90
1.20
LOZA DE
CEMENTO
TORRE
50m
1.20
5.40
10.00
RBS
Ubicación de
Nuevo gabinete
1.80
4.90
3.60

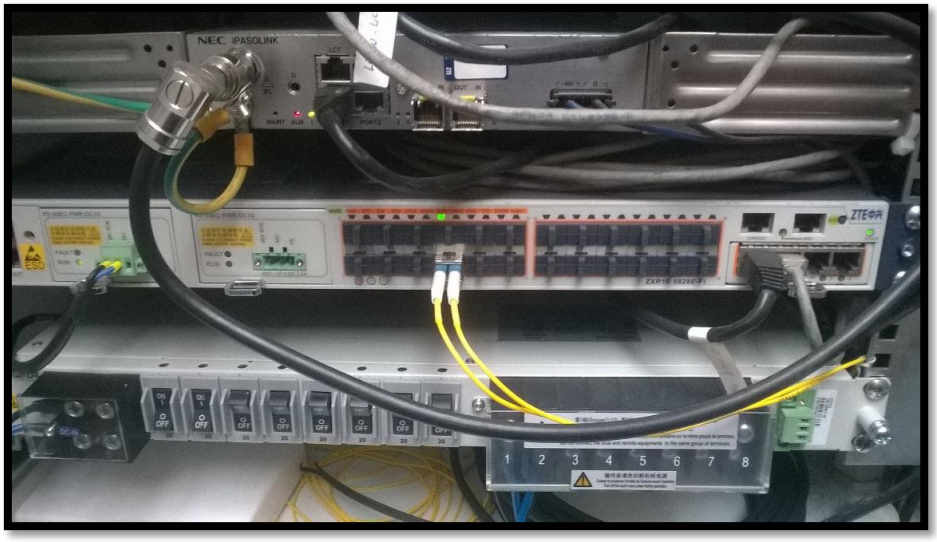
Se puede observar en el plano mostrado ubicaciones de las cámaras, las cuales se ubicaran en tres distintos lugares los cuales se indican con círculos de marco rojo y fondo blanco.

3.3.2 INSTALACIÓN DE EQUIPO

3.3.5.1.1.1 Selección de los elementos

Al igual que para el entorno del sistema, se debe escoger los equipos que cumplan con las especificaciones dadas y halladas para completar el sistema de vigilancia basado en la utilización de la red IP. Entre estos elementos tenemos los puntos de acceso (AP) encargados de transmitir la información de un grupo de cámaras hacia el equipo de distribución, el switch que se encarga de distribuir la información hacia la red, y finalmente el router que se encarga de en rutar la información, por medio de internet, a estaciones de trabajo lejanas.

Puesto que este equipo se encuentra en situ ya habilitado y en red , no se necesita una configuración en especial , simplemente comunicación con la central de monitoreo de red para que habiliten un puerto del router en el cual nos conectaremos a la red.



El router en situ es el ZXR10 5928e – FI el cual cuenta con 24 puertos ópticos los cuales están distribuidos de la siguiente forma:

- 1-6 para equipos te radio(RRU , RRH ,etc).
- 7-18 para puntos de venta de la empresa de telefonía.
- 19-24 para centro de emergencias o monitoreo de equipos del site.

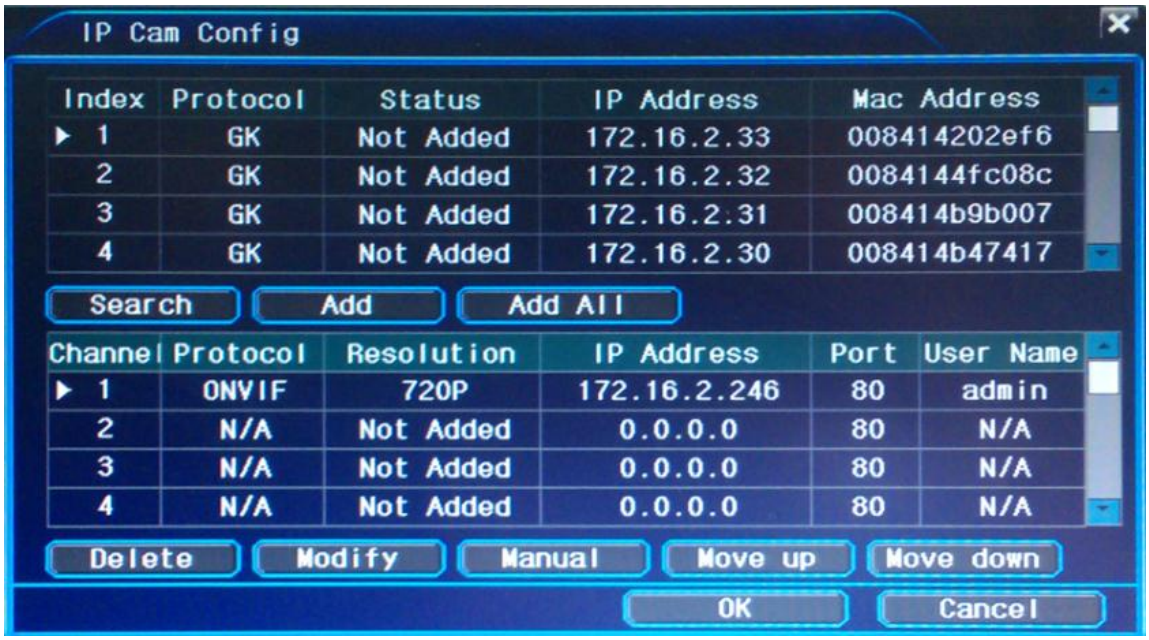
3.3.5.1.1.2 Selección del punto de acceso (AP)

El access point (AP) o punto de acceso es la estación que permite la comunicación entre los diferentes dispositivos conectados a la red y puede cumplir la función de puente entre red cableada y red de camaras. Este equipo es capaz de recibir información de un grupo de cámaras y retransmitirla a la red, previa configuración del equipo con los SSID (service set identifier) de cada cámara para que puedan ser identificados como parte de la red.

Este modelo de NVR SRN- 472S nos provee 4 puertos esto quiere decir que tenemos 4 puntos en donde colocar nuestras cámara, pero en este caso solo necesitaremos 3 puertos debido a que es lo que se requiere de acuerdo a diseño.

3.3.3 CONFIGURACIÓN DEL EQUIPO

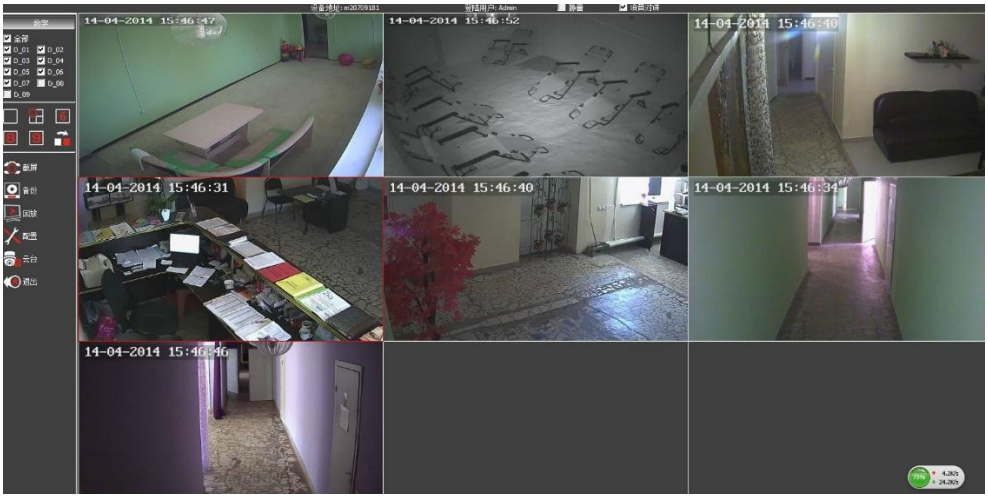
1) designación de IP



2) Elija “Onvif”

3) Detección de movimiento

4) Software central de la gestión de NVR



3.3.4 Selección equipos adicionales

Los equipos adicionales pueden ser diversos para un sistema de vigilancia, pero en este caso solo estamos tomando en cuenta los monitores y el teclado o joystick para controlar las cámaras y también necesitaremos un intermediario entre el site router y NVR debido a que el router cuenta con puertos ópticos mientras que el NVR no cuenta con tal puerto, debido a eso usaremos un media converter de fibra óptica – Ethernet para poder lograr la comunicación entre ambos y también un modul transceiver de 1km en este caso , pero se podría usar de menor distancia debido a que la distancia entre router y NVR es solo de 5mts.

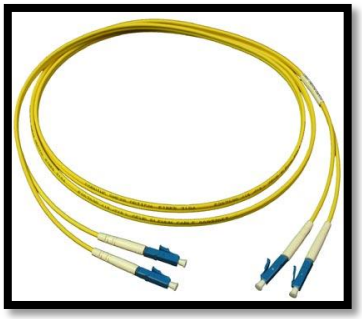
Media Converter

transceiver

En el caso de los monitores se plantea utilizar tres de la marca Samsung de 19" que se situaran en el local de vigilancia. Para la selección de los monitores se tomó en cuenta, básicamente, la garantía de las marcas y el precio debido a que para el caso de los monitores no se necesita características adicionales.

Asimismo, para el caso del teclado/joystick seleccionado es de la marca Axis 295 por ser un equipo que es compatible con los equipos que conforman el sistema y además por la garantía de la marca.

Se usara patch cord de 5mts lc/lc para la conexión del Media Converter y Router



3.3.5 CRONOGRAMA DE TRABAJO:

- Adquisición de equipos (planificación y ejecución):

  Teniendo el tamaño del área que se cubrirá se pueden ir adquiriendo los equipos de video vigilancia

- Montaje (planificación y ejecución):

Esto se realizará teniendo en cuenta el área de barrido de las cámaras para poder cubrir toda el área.

- Pruebas y control de Calidad (ejecución):

Luego de a ver realizado el montaje de las cámaras se procederá a realizar las pruebas de control y de barrido para su correcta funcionalidad.

CONCLUSIONES:

- Una vez finalizado el diseño de la red de vigilancia remota con tecnología IP, se concluye que es posible la implementación total de dicho proyecto de investigación, considerando q los equipos a utilizar existen en el mercado, dicha red permite mejorar considerablemente la cantidad de personal humano a movilizar, y funcionamiento y seguridad en los nodos de comunicación.
- La tecnología IP tiene ventajas hoy en día como la gestión centralizada de todas las cámaras del sistema de seguridad desde cualquier computador en cualquier lugar del mundo y la interacción remota con todo el sistema en tiempo real.
- Utilizando la red IP mejoran la calidad del servicio que un sistema analógico o un sistema DVR en aspecto como la calidad de imagen al utilizarse cámaras de red digitales, en el almacenamiento al usar servidores en contraste con las cintas de video las imágenes digítales que son de más fácil procesamiento.
- Finalmente, con los equipos propuestos en este tema de estudio, utilizando una red ampliamente difundida, se logra la implementación de un sistema moderno y factible de ser monitoreado a distancia. Es decir, se garantiza un medio de acceso seguro y los equipos pueden ser maniobrados y configurados desde cualquier parte del mundo, teniendo la autorización de la empresa por ello es muy recomendable y eficiente.

RECOMENDACIONES

- Para un correcto funcionamiento y supervisión se sugiere que la manipulación de los equipos estén a cargo del gerente y cuando se dese acceder a los bancos de memoria sea el quien autorice y supervise la información dentro de la memoria para que no se generen perdías de información por manipulación errónea o maliciosas.
- En caso falla de equipos no manipular la información de los bancos de memoria llamar a un técnico especializado de preferencia que pertenezca al mismo equipo de trabajo que realizo la instalación del mismo para que revise los equipos defectuosos

BIBLIOGRAFIA:

- REISZ F, Carlos: Manual y Tecnología CCTV. Segunda edición (2002)

- INGENIERIA DE SISTEMAS, REDES Y COMUNICACIONES RALCO NETWORKS (www.ralco-networks.com/noticias/torino.htm)

- UNIVERSIDAD TÉCNICA DE AMBATO FACULTAD DE INGENIERÍA EN SISTEMAS ELECTRÓNICA E INDUSTRIAL (http://repo.uta.edu.ec/handle/123456789/3130)
- PROYECTO DE ENLACE MICROONDAS ENTE PICUSH - YANAHUACCA

LINKOGRAFIA:

- Introducción a los Sistemas de Vigilancia IP. Consultado el 9 de Abril del 2012. http://www.midisec.com/index.php?option=com_content&view=article&id=64:in troduccion-a-sistemas-vigilancia-ip&catid=42:introduccion-a-las- tecnologias&Itemid=67.

- Martínez Evelio. Direccionamiento IPv4. Publicado el 21 de Julio del 2007.http://www.eveliux.com/mx/direccionamiento-ipv4.php.

- Tomado de Axis Communications http://www.casadomo.com/casadomo/biblioteca/axis_vigilancia_ip_inalambrica.pdf
- Sistema de Vigilancia. http://www.casadomo.com/casadomo/biblioteca/axis_vigilancia_ip_inalambrica.pdf"

- Cámaras IP
  http://www.informaticamoderna.com/Camara_IP.htm

- "Tomado de: Video vigilancia Y Seguridad De Cyoarte Y Cámaras De Red/Cámaras IP de Rnds".
  http://www.axis.com/es/products/video/about_networkvideo/internet.htm.
- SAMSUNG
  www.samsung-segurity.com

- Tomado de: Uso del Espectro Radioeléctrico,http://bibing.us.es/proyectos/abreproy/11677/fichero/Volumen+1%252F4

- Video vigilancia y Seguridad.
  http://www.cyoarte.com/descargas/VIDEOVIGILANCIA_SEGURIDAD.pdf

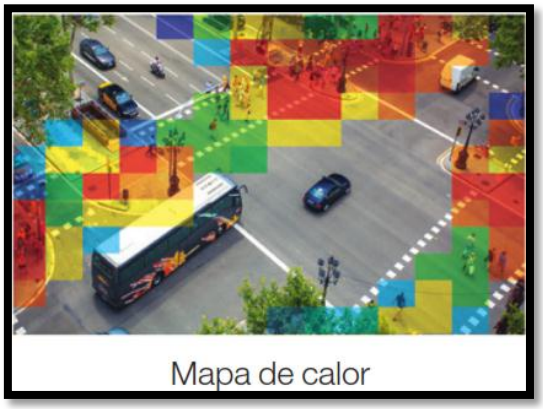
- Como elegir una cámara IP de seguridad.
  http://www.sitiosargentina.com.ar/notas/2009/junio/camara-ip.htm

- Serie de cámaras de red AXIS.
  .http://www.axis.com/es/products/p33_series/

- Vivotek
  http://www.vivotek.com/web/Product/ProductDetail.aspx?Model=IP8362,

ANEXO

Opciones en la configuración de cámaras de vigilancia



Seguimiento automático

La cámara puede detectar movimientos al enfocar un local predefinido para acompañar automáticamente un intruso. Recursos inteligentes incluyen aproximación de imágenes y dimensionamiento de blancos, área de activación de monitoreo y programación de tiempo.

VISION DE CAMARA OJO DE PEZ


SAMSUNG


180° panorama
180° panorama
180° panorama
full image
180° panorama
panorama focus

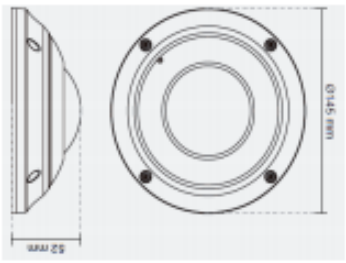
ESPECIFICACIONESTECNICAS

Lente	Tipo tarjeta, Fijo, F= 1.27mm @F2.8 Filtro IR Removible para función Día/Noche
Angulo de Visión	180°
Velocidad de obturador	1/5 ~ 1/32,000 sec
Sensor de imagen	1/2" CMOS en Resolución 2048x1536
Iluminación mínima	1.17 Lux @ F2.8 (Color)
	0.02 Lux @ F2.8 (B/N)
Video	Compresión: H.264, MPEG-4 & MJPEG Streaming: Múltiples streams simultáneos H.264 streaming over UDP, TCP, HTTP or HTTPS H.264/MPEG-4 multicast streaming MPEG-4 streaming over UDP, TCP, HTTP or HTTPS MJPEG streaming over HTTP or HTTPS Suporta streaming adaptable a la actividad para control de velocidad de cuadros dinámico Soporta eficiencia de datos ePTZ Soporta vigilancia móvil 3GPP Velocidad de cuadro: H.264: hasta 15 fps a 1536x1536 MPEG-4: hasta 15 fps a 1536x1536 MJPEG: hasta 15 fps a 1536x1536
Configuración de imagen	Imagen ajustable en tamaño, calidad, velocidad, bit rate Time stamp and text caption overlay Flip & mirror Configurable brillo, contraste, saturación, nitidez, balance blanco y exposición AGC AWB AES WDR avanzado Modo automático, manual o por horarios en mode día & noche Suporta máscaras privadas BLC (Backlight compensation)
Audio	Compresión GSM-AMR speech encoding, bit rate: 4.75 kbpsa 12.2 kbps MPEG-4 AAC codificación de audio, bit rate: 16 kbps a 128 kbps G.711 audio encoding, bit rate: 64 kbps, μ-Law or A-Law Interface: Micrófono incorporado Entrada de micrófono Externo Salida de audio Soporta audio de 2 vias Soporta audio mute

VIVOTEK

Networking	10/100/1000 Mbps Ethernet, RJ-45 / Soporta ONVIF Protocols: IPv4, IPv6, TCP/IP, HTTP, HTTPS, UPnP, RTSP/RTP/RTCP, IGMP, SMTP, FTP, DHCP, NTP, DNS, DDNS, PPPoE, CoS, QoS, SNMP and 802.1X
Manejo de Alarmas y Eventos	Detección de movimiento de Quintuples ventanas Detección de sabotaje 1 entrada D/I & 1 D/O para sensor externo y alarmas Notificación de eventos usando HTTP, SMTP, o FTP Grabación local en archivos MP4
Almacenamiento local	Slot para tarjeta SD/SDHC/SDXC Almacena fotos y clips de video
Seguridad	Multi-niveles de usuario acceso con clave de protección Filtrado de direcciones IP Transmisón de datos con encriptación HTTPS Autenticación de puerto basado en 802.1X con protección en Red
Usuarios	10 clients on-line monitoreados al mismo tiempo
Dimensiones	Ø: 145mm x 52 mm (H)
Peso	Neto: 556 g
Indicadores LED	Indicador de Estado y Encendido Indicadores de actividad del sistema y enlace de red
Cubierta	Certificación que brinda nivel de portección IK10 antivandálico Cubierta a prueba de intemperie IP66
Alimentación	12VDC Consumo: Máximo 3.84W 802.3at compatible con Power-over-Ethernet (Clase 2)
Aprobaciones	CE C-Tick FCC LVD VCCI, EN50155
Temperatura	Temperatura: -25°C ~ 50°C Humedad: 90% RH
Requerimientos de sistema para visualización	OS: Microsoft Windows 2000/XP/Vista/7 Navegador: Mozilla Firefox, Internet Explorer 6.x o superior Celular: 3GPP player Real Player: 10.5 o superior Quick Time: 6.5 o superior
Instalación, gerenciamiento	Instalación Wizard 2 Software de Gerenciamiento central libre de 32-CH Soporta actualización de firmware
Aplicaciones	SDK disponible para desarrollo de apliaciones e integración de sistemas

DIMENSIONES



VIVOTEK

TRANCEVER:

Fiber SFPs for devices that support Fast Ethernet, SONET OC-3 and SDH STM-1 network protocols. Compatible with a variety of Omnitron products, including *iConverter* xFF, T1, T3, X21 and Unmanaged T1/E1 Mux.

Model	Fiber Type	Spec. Distance (km)	Wavelength (nm)	Loss (db/km)	Min. Tx Power (dBm)	Max. Tx Power (dBm)	Min. Rx Sense (dBm)	Max. Rx Power (dBm)	Min. Attenuation (dBm)	Link Budget (dBm)
7006-0	MM/DF	5	1310	1	-20	-14	-31	-14	-	11
7007-1	SM/DF	30	1310	0.38	-15	-8	-32	-8	-	17
7007-2	SM/DF	60	1310	0.38	-5	0	-35	-3	3	30
7007-3	SM/DF	120	1550	0.2	-5	0	-35	-3	3	30
7014-1	SM/SF	30	1310 / 1550	0.38	-14	-8	-32	-3	-	18
7015-1	SM/SF	30	1550 / 1310	0.38	-14	-8	-32	-3	-	18
7014-2	SM/SF	50	1310 / 1550	0.38	-8	0	-34	-3	3	26
7015-2	SM/SF	50	1550 / 1310	0.38	-8	0	-34	-3	3	26
7014-3	SM/SF	80	1310 / 1550	0.38	0	5	-34	-3	8	34
7015-3	SM/SF	80	1550 / 1310	0.36	0	5	-34	-3	8	34

Fiber SFPs for devices that support Gigabit Ethernet, Fibre Channel x1, SONET OC-12 and SDH STM-4 network protocols. Compatible with a variety of Omnitron products, including *iConverter* xFF and Managed T1/E1 Mux.

Model	Fiber Type	Spec. Distance (km)	Wavelength (nm)	Loss (db/km)	Min. Tx Power (dBm)	Max. Tx Power (dBm)	Min. Rx Sense (dBm)	Max. Rx Power (dBm)	Min. Attenuation (dBm)	Link Budget (dBm)
7206-0	MM/DF	0.22 / 0.55	850	2.6	-9.5	-4	-17	-3	-	7.5
7206-6	MM/DF	2	1310	1.0	-9.5	-3	-19.5	-3	-	10
7207-1	SM/DF	15	1310	0.38	-9.5	-3	-21	-3	-	11.5
7207-2	SM/DF	34	1310	0.38	-5	0	-24	-3	3	19
7207-3	SM/DF	80	1550	0.2	-4	1	-24	-3	4	20
7207-4	SM/DF	110	1550	0.2	0	5	-24	-3	8	24
7207-5	SM/DF	140	1550	0.2	2	5	-30	-8	13	32
7207-6	SM/DF	160	1550	0.2	1	5	-33	-8	13	34
7214-1	SM/SF	20	1310 / 1550	0.38	-9	-3	-21	-3	-	12
7215-1	SM/SF	20	1550 / 1310	0.38	-9	-3	-21	-3	-	12
7214-2	SM/SF	40	1310 / 1550	0.38	-3	2	-23	-3	5	20
7215-2	SM/SF	40	1550 / 1310	0.38	-3	2	-23	-3	5	20
7214-3	SM/SF	60	1310 / 1550	0.38	0	5	-24	-1	6	24
7215-3	SM/SF	60	1550 / 1310	0.38	-2	4	-25	-1	5	23
7216-1	SM/SF	20	1310 / 1490	0.38	-9	-3	-21	-3	-	12
7217-1	SM/SF	20	1490 / 1310	0.38	-9	-3	-21	-3	-	12

MEDIA CONVER:

85xxN-x-xx

<Blank>	Standard Operating Temperature Range Model
W	Wide Operating Temperature Range Model

<Blank>	Plug-in Module
D	Standalone with integrated mounting brackets and External US AC Power Supply
E	Standalone with integrated mounting brackets and External Universal AC Power Supply
F	Standalone with integrated mounting brackets and DC Terminal Power

Fiber Type	Distance	Connector Type			Tx / Rx Wavelength [nm]	Min. Tx Power (dBm)	Max. Tx Power (dBm)	Min. Rx Sensitivity (dBm)	Max. Rx Sensitivity (dBm)	Min. Attenuation (dB)	Optical Power Budget
		ST	SC	SFP							
-	-	-	-	**8539N-0**	-	-	-	-	-	-	-
MM	220 / 550m[1]	**8520N-0**	**8522N-0**	-	850	-10	-4	-17	-3	-	7
MM	2km	**8520N-6**	**8522N-6**	-	1310	-9.5	-3	-19.5	-3	-	10
SM	12km	**8521N-1**	**8523N-1**	-	1310	-9.5	-3	-19.5	-3	-	10
SM	34km	-	**8523N-2**	-	1310	-5	0	-23	-3	3	18
SM	80km	-	**8523N-3**	-	1550	-5	0	-23	-3	3	18
SM	110km	-	**8523N-4**	-	1550	0	5	-24	-3	8	24
SM	140km	-	**8523N-5**	-	1550	2	5	-28	-8	13	30
SM-SF [2]	20km	-	**8530N-1**	-	1310/1550	-9.5	-3	-20	-3	-	10.5
SM-SF [2]	20km	-	**8531N-1**	-	1550/1310	-9.5	-3	-20	-3	-	10.5
SM-SF [2]	40km	-	**8530N-2**	-	1310/1550	-3	0	-20	-3	3	17
SM-SF [2]	40km	-	**8531N-2**	-	1550/1310	-3	0	-20	-3	3	17

Contact Omnitron for other fiber options and temperature ranges.
[1] = 62.5/125µm, 100/140µm multimode fiber up to 220m. 50/125µm multimode fiber up to 550m. Refer to the fiber cable manufacturer for multimode distance specifications.
[2] Single-Fiber converters must be used in pairs. The Tx wavelength on one end has to match the Rx wavelength on the other.

Model Type	GX/T2	
Protocols	10BASE-T, 100BASE-TX, 1000BASE-T, 100BASE-FX, 1000BASE-X	
Frame Size	10,240 bytes maximum frame size	
UTP Cable	RJ-45, Category 5 and higher	
Fiber Cables	Multimode: 50/125, 62.5/125, 100/140µm Single-mode: 9/125µm	
UTP Connectors	RJ-45	
Fiber Connectors	ST, SC and SFP	
DIP-Switches	Fiber: 100/1000 UTP: Auto/Man, 10/100/1000, FDX/HDX BP Enable, LS/LP, Pause, MAC Learning	
LED Displays	Power, FO 10/100/1000, FO FDX, SFP Stat, UTP Auto/Man, UTP 10/100/1000, UTP FDX/HDX	
Compliance	UL, CE, FCC Class A	
Plug-in Power Requirements	Typical: 1.4A @ 3.3VDC	
Standalone Power Requirements	DC Power Input Connector:	2.5mm Barrel Connector or 2-Pin Terminal Connector
	DC Power:	7 - 60VDC 0.7A max
	AC Power Adapter (US) via 2.5mm Barrel Connector	100 - 120VAC/60Hz 0.06A @ 120VAC
	AC Power Adapter (Univ) via 2.5mm Barrel Connector:	100- 240VAC/50 - 60Hz 0.06A @ 120VAC
Dimensions	Plug-in: Standalone:	W: 0.85" x D: 4.5" x H: 2.8" W: 3.8" x D: 4.8" x H: 1.0"
Weight	Plug-in: Standalone w/o PS: Standalone w PS:	8 oz. 1.0 lb. 1.5 lbs.
Temperature	Standard: Wide: Storage:	0 to 50° C -40 to 60° C -40 to 80° C
Humidity	5 to 95% (non-condensing)	
Altitude	-100m to 4000m	