# CAPITULO I
# EL PROBLEMA

## 1.1 Planteamiento del Problema

El Sistema desactualizado de vigilancia provoca inseguridad en las diferentes áreas del Servicio Ecuatoriano de Capacitación Profesional – Centro de Formación Industrial Ambato.

### 1.1.1 Contextualización

A nivel de Latinoamérica el avance de la tecnología crece cada vez más, dentro de ella las cámaras IP han ganado espacio como un método eficiente para realizar video vigilancia en hogares y oficinas. De igual modo, la nueva generación de estos dispositivos son usados cada vez más dentro de la industria, no sólo para tareas de vigilancia, sino también para aplicaciones de telepresencia y supervisión remota de procesos industriales.

En el Ecuador existe dependencias financieras, la cadena de centros comerciales, empresas e industrias se han visto en la necesidad de implementar en sus instalaciones el monitoreo mediante cámaras IP, el mismo que ha dado excelente resultado en cuanto a seguridad se refiere.

El Servicio Ecuatoriano de Capacitación Profesional – Centro de Formación Industria Ambato, no cuenta con un servicio de seguridad modernizado en comparación con los diferentes establecimientos en el Ecuador; que si cuentan con vigilancia IP.

Por lo dicho anteriormente es necesario realizar el diseño de un sistema de seguridad para el SECAP – CEFIA puesto que es una institución gubernamental y su equipamiento electrónico e industrial es de elevado costo.

### 1.1.2 Análisis Crítico

La Seguridad del Servicio Ecuatoriano de Capacitación Profesional – Centro de Formación Ambato; está a cargo del servicio de guardianía privado, los mismos que poseen casetas en las puertas de ingreso de la Institución.

Los guardias de esta Institución son los encargados de la seguridad de la misma, efectúan su vigilancia por turnos en la mañana, tarde y noche; pero, solamente controlan el ingreso y salida de personas, subestimando el cuidado y la seguridad de los bienes institucionales.

La situación actual del SECAP - CEFIA es vulnerable a cualquier efecto de inseguridad y sustracción de bienes; pues no cuenta con una vigilancia óptima de todos sus sectores en especial aquellos donde se encuentra maquinaria de alto costo.

SECAP – CEFIA siendo una Institución Pública de servicio a la Comunidad; necesita tener seguridades de última tecnología, para evitar pérdidas que afectarían a un presupuesto Institucional y de Estado.

### 1.1.3 Prognosis

Si no modernizamos el sistema de vigilancia en el SECAP - CEFIA, sus equipos electrónicos, industriales y miembros se verán expuestos a posibles riesgos: inseguridad del personal que trabaja ahí, hurto de equipos y maquinaria que pertenecen al establecimiento; no podemos descartar de que en el futuro se presenten pérdidas de costo elevado.

El Establecimiento continuaría sin tener en sus instalaciones un sistema de vigilancia digital acorde con los avances tecnológicos.

Al no tener un sistema de video vigilancia IP no se puede tener un control continuo de seguridad y no recopilara imágenes o sucesos que acontecieron en la Institución.

## 1.2 Formulación del Problema

¿Cómo diseñar el sistema de monitoreo por medio de Cámaras IP para el SECAP – CEFIA?

### 1.2.1 Preguntas Directrices

- ¿Cuál es la situación actual de vigilancia del SECAP – CEFIA?
- ¿Qué áreas son de prioridad para la seguridad dentro de la Institución?
- ¿Qué tecnología y equipos se requieren para poder bosquejar el sistema de video vigilancia IP?

### 1.2.2 Delimitación

El Diseño de Sistema de Video Vigilancia IP, en tiempo real, para control de seguridad del Servicio Ecuatoriano de Capacitación Profesional – Centro de Formación Industrial Ambato se efectuó, de abril a octubre 2010.

## 1.3 Justificación

El Diseño de un sistema de video vigilancia IP en el SECAP – CEFIA, ayuda al cuidado, control, observación en tiempo real; las 24 horas del día de todos los sitios que sean vulnerables a la inseguridad.

La seguridad debe ser óptima, visible y exclusivamente dedicada a evitar pérdidas de equipos y materiales que el establecimiento posee, con el presente estudio de supervisión mediante Cámaras IP se obtuvo la información necesaria para esbozar la vigilancia requerida para el SECAP – CEFIA.

Al proyectar un Sistema de Video Vigilancia IP se beneficio el SECAP – CEFIA, por tener una observación en tiempo real de todas las áreas dentro de la entidad mencionada.

El proyecto es factible para su desarrollo ya que se cuenta con la aprobación del Director de la Institución, la colaboración del Tutor de tesis, además de ello los conocimientos teóricos y prácticos adquiridos en la Universidad Técnica de Ambato – Facultad de Ingeniería en Sistemas, Electrónica e Industrial.

## 1.4 Objetivos de la Investigación

### 1.4.1 Objetivo General

- Diseñar un Sistema de Seguridad, en tiempo real, mediante Cámaras IP, para optimizar la vigilancia en el Servicio Ecuatoriano de Capacitación Profesional – Centro de Formación Industrial Ambato.

### 1.4.2 Objetivos Específicos

- Analizar científicamente los sistemas de seguridad mediante cámaras IP.
- Determinar las áreas importantes para la seguridad dentro de la Institución.
- Establecer la tecnología y equipos necesarios para el Sistema de Video Vigilancia IP en el SECAP – CEFIA.
- Diseñar el sistema de monitoreo por medio de Cámaras IP para el SECAP – CEFIA.

# CAPITULO II
# MARCO TEORICO

## 2.1 Antecedentes Investigativos

El proyecto de pasantía "Sistema de Video Vigilancia para la Brigada de Caballería Blindada número 11 Galápagos en la ciudad de Riobamba" realizado por Sr. Washington Daniel Ibarra Córdova; el número de la tesis es 370. Es un ejemplo de cómo las vigilancia por cámaras IP ayudan a la seguridad de los establecimientos, que implementan esta tecnología.

## 2.2 Fundamentación Legal

El Servicio Ecuatoriano de Capacitación Profesional – Centro de Formación Industrial Ambato; es una Institución perteneciente al Estado Ecuatoriano, está ubicado Av. Bolivariana y el Cóndor frente al Mercado Mayorista km. 3,5 vía a Baños de la Ciudad de Ambato.

"Creado el 3 de octubre de 1966, por Decreto 1207, tiene como objetivo principal Formar, Capacitar, Perfeccionar, Certificar y Titular a la población económicamente activa del país o en capacidad de integrarse a la misma, para satisfacer con efectividad las expectativas y exigencias de formación profesional integral para el trabajo."

**Visión**

" Ser la Institución oficial, líder de la Formación Profesional para el Trabajo, que desarrolla su gestión acorde a los cambios económico-sociales y tecnológicos, en relación directa con el plan de desarrollo y políticas de empleo nacionales."

## 2.3 Categorías Fundamentales

En esta página web *http://www.aytec.es/Camaras-IP-alarmas-videovigilancia:* se encuentra aplicaciones de ¿cómo? y ¿dónde? poder usar las Cámaras IP.

"Controle su hogar, oficina o negocio desde cualquier lugar que disponga de internet. La solución completa para la vigilancia y grabación en comercios, grupos de tiendas, oficinas, industrias, almacenes,....
Con las Cámaras IP se pueden ver y grabar las imágenes desde cualquier ordenador instalado en el propio local o en cualquier lugar del mundo a través de Internet"

### 2.3.1 Definición de Cámara IP

Las **cámaras IP**, son videocámaras de vigilancia que tienen la particularidad de enviar las señales de video (y en muchos casos audio), pudiendo estar conectadas directamente a un Router ADSL, o bien se conectan directamente a una conexión LAN (RJ45) de su instalación de internet o red doméstica y llevan incorporado un servidor Web.

O a través de cualquier equipo conectado a Internet (WAN) pudiendo estar situado en cualquier parte del mundo.

Son totalmente autónomas del ordenador, se les asigna una dirección IP interna, y se precede teclear esa dirección IP desde cualquier navegador para acceder a la cámara y disponer de los menús que permiten todo tipo de funciones; visionar, realizar grabaciones, escuchar, alarmas, etc.

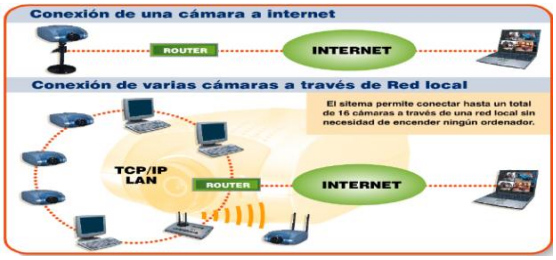



*Figura 2.1 Esquema de conexión de Cámaras IP Fuente: http://www.informaticajg.com/INTRODUCCION%20A%20CAMARA%20IP.pdf*

### 2.3.1.1 Router ADSL

El **router ADSL** es un dispositivo que permite conectar uno o varios equipos o incluso una red de área local (LAN)

Realmente se trata de varios componentes en uno. Realiza las funciones de:

- **Puerta de enlace:** ya que proporciona salida hacia el exterior a una red local.
- **Router:** cuando le llega un paquete procedente de Internet, lo dirige hacia la interfaz destino por el camino correspondiente, es decir, es capaz de encaminar paquetes IP.
- **Módem ADSL:** modula las señales enviadas desde la red local para que puedan transmitirse por la línea ADSL y demodula las señales recibidas por ésta para que los equipos de la LAN puedan interpretarlos.
- **Punto de acceso wireless:** algunos router ADSL permiten la comunicación vía Wireless (sin cables) con los equipos de la red local.

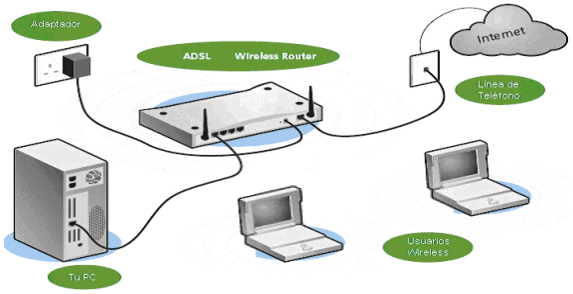



*Figura2.2 Aplicación de ROUTER ADSL*
*Fuente: http://lljyvll.blogspot.com/2010/03/router-adsl.html*

### 2.3.1.2 Red Inalámbrica:

**(Wireless**; su significado es sin cables) y se denomina así a los dispositivos que no utilizan cables para realizar el envío y la recepción de datos. **802.11 -** Estándar para redes inalámbricas con línea visual.

#### 2.3.1.2.1 Wi-Fi (IEEE 802.11)

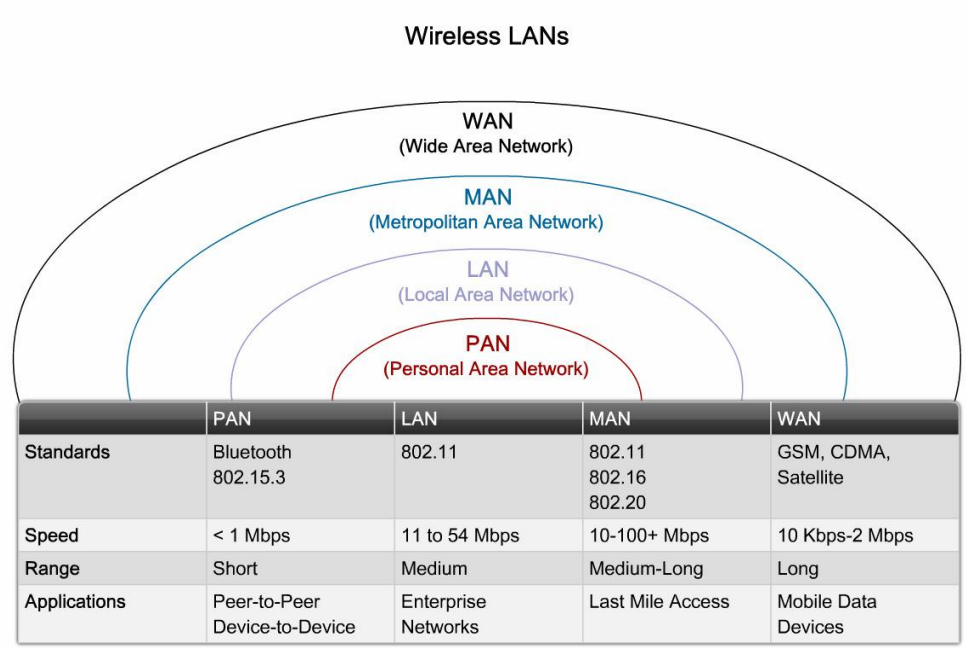
- *802.11a:* Utiliza OFDM, funciona en una banda de frecuencia de 5 GHz y proporciona una velocidad máxima de transmisión de 54 Mbps.
- *802.11b:* Funciona en la banda de frecuencia de 2.4 GHz, proporciona una velocidad máxima de transmisión de 11 Mbps y utiliza el espectro ensanchado de secuencia directa (DSSS).
- *802.11e:* Estándar encargado de diferenciar entre video-voz-datos. Su único inconveniente el encarecimiento de los equipos.
- *802.11g:* Funciona en una banda de frecuencia de 2.4 GHz, utiliza OFDM y proporciona una velocidad máxima de transmisión de 54 Mbps.
- *802.11i:* Conjunto de referencias en el que se apoyará el resto de los estándares, en especial el futuro 802.11a. El 802.11i supone la solución al problema de autenticación al nivel de la capa de acceso al medio, pues sin ésta, es posible crear ataques de denegación de servicio (DoS).
- *802.15:* Bluetooth
- *802.16:* WMan
- *802.11n:* hasta 600 Mps
- *OFDM (Orthogonal Frequency Division Multiplex):* es una técnica de comunicación que divide un canal, de frecuencia, en un número determinado de bandas de frecuencias equiespaciadas, en cada banda se transmite un subportadora que transporta una porción de la información del usuario. Cada subportadora es ortogonal al resto.
- **WiMAX (interoperabilidad mundial para acceso por microondas) y la norma IEEE 802.16**

  Para redes de área metropolitana (MAN).Su alcance es de 50 km y ofrece una velocidad de transmisión de 70 Mbps.Funciona en frecuencias que oscilan entre 2 y 11 GHz y, ahora, también permite la conexión entre dispositivos que no se encuentren en la misma línea de visión.Esta tecnología es compatible con usuarios móviles que viajen a velocidades de entre 20 y 100 km/h (e incluso a velocidades superiores).

  El estándar *802.16e* ofrecerá a los usuarios movilidad y portabilidad**.**

***802.20:*** Se trata de una tecnología de acceso inalámbrico de banda ancha móvil. Se espera una velocidad de transmisión máxima de 1 Mbps y opera en bandas inferiores a 3.5 GHz y que precisan de licencia.

### 2.3.1.3 Wireless LANs




| | PAN | LAN | MAN | WAN |
|---|---|---|---|---|
| Standards | Bluetooth 802.15.3 | 802.11 | 802.11 802.16 802.20 | GSM, CDMA, Satellite |
| Speed | < 1 Mbps | 11 to 54 Mbps | 10-100+ Mbps | 10 Kbps-2 Mbps |
| Range | Short | Medium | Medium-Long | Long |
| Applications | Peer-to-Peer Device-to-Device | Enterprise Networks | Last Mile Access | Mobile Data Devices |

*Figura 2.3 Medios de transmisión no guiados en redes*
*http://www.dsic.upv.es/~jsilva/uned/redes/Redes%20(sesion%205).ppt*

**a) Red Pan:**

Una red de área personal, es una colección de dispositivos de tecnología de la comunicación dentro del rango de una persona.

Cuando la comunicación entre estos dispositivos es inalámbrica, la sigla se convierte en WPAN, o la red inalámbrica de área personal; opera en un rango relativamente corto, por lo general hasta un máximo de treinta pies.

El método más común de conexión es a través de tecnología inalámbrica Bluetooth.

La tecnología Bluetooth tiene varias ventajas a través de Wi-Fi en la facilidad de uso, ya que no es necesario configurar cada componente y requiere considerablemente menos energía para funcionar.

Un Bluetooth red personal inalámbrica, también conocida como una piconet, puede conectarse de forma inalámbrica un mínimo de dos y un máximo de ocho dispositivos.

b) **Red Lan:**

Se denomina redes **LAN** (*Local Area Network*) a aquéllas que tienen cerca las computadoras: en la misma habitación, en diferentes pisos de un edificio o en edificios muy cercanos.

Las redes de área local proveen una excelente velocidad de transferencia, que va desde los 10 hasta los 1.000 Mbps. Esto se debe a la corta distancia existente entre las computadoras, lo cual evita las interferencias.

**WLAN** (*Wireless Local Area Network*, o red de área local inalámbrica) una WLAN es un tipo de red de área local (LAN) que utiliza ondas de radio de alta frecuencia en lugar de cables para comunicar y transmitir datos.

**c) Red Man:**

(**MAN**, por metropolitan area network) abarcan el área geográfica de una ciudad y generalmente interconectan redes LAN. Por lo tanto su cobertura es de $10^3$ metros.

**d) Red Wan:**

(**WAN**, por wide area network) 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 satélite y radio enlace, y tangibles, como pares de cobre, coaxiales y fibras.

### 2.3.1.4 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 del protocolo TCP/IP.

Dirección IP se puede cambiar; esta dirección puede cambiar 2 ó 3 veces al día; y a esta forma de asignación de dirección IP se denomina una *dirección IP dinámica*.

Los sitios de Internet que por su naturaleza necesitan estar permanentemente conectados, generalmente tienen una *dirección IP fija* (comúnmente, *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.

### 2.3.1.5 Definición de IPv4 e IPv6

**Internet Protocolo Versión 4 (IPv4):**

Es la cuarta versión del Protocolo de Internet y es la primera versión del protocolo que fue mundialmente desplegada.
IPv4 usa direcciones de 32 bits, limitándola a $2^{32}$ = 4.294.967.296 direcciones únicas, muchas de las cuales están dedicadas a redes locales (LANs). Por el crecimiento enorme que ha tenido del Internet, combinado con el hecho de que se desperdician direcciones en muchos casos, ya hace varios años se vio que escaseaban las direcciones de la versión 4.

**Internet Protocolo Versión 6 (IPv6):**

Es la nueva versión del Protocolo Internet, diseñado como el sucesor de IP versión 4 (IPv4). IPv6 está destinado a sustituir al IPv4, IPv6 es un sistema de numeración más nuevo que, entre otras ventajas, brinda un espacio de direcciones mucho mayor que IPv4. Se lanzó en 1999 y se supone que satisfará ampliamente las necesidades futuras de direcciones IP del mundo.

**Cuáles son las diferencias más importantes:**

La principal diferencia entre IPv4 e IPv6 reside en la cantidad de direcciones IP. Hay algo más de 4.000.000.000 de direcciones IPv4. En cambio, existen más de 340.000.000.000.000.000.00 0.000.000.000.000.000.000 de direcciones IPv6.
El funcionamiento técnico de Internet es el mismo con ambas versiones, y es probable que ambas sigan operando simultáneamente en las redes por mucho tiempo más. En la actualidad, la mayoría de las redes que usan IPv6 admiten tanto direcciones IPv4 como IPv6 en sus redes.

*Tabla2.1Diferencias entre IPv4 e IPv6*

| **Descripción** | **IPv4** | **IPv6** |
|---|---|---|
| **Tamaño de las direcciones** | Número de 32 bits | Número de 128 bits |
| **Formato de las direcciones** | Notación decimal con puntos: 192.149.252.76 | Notación hexadecimal: 3FFE:F200:0234:AB00: 0 123:4567:8901:ABCD |
| **Notación de prefijos** | 192.149.0.0/24 | 3FFE:F200:0234::/48 |
| **Cantidad de direcciones** | 232 = ~4,000,000,000 | 2128 = ~340,000,000, 000,000,000,000,000, 000,000,000,000,000 |

*Fuente: https://www.arin.net/knowledge/ipv4_ipv6_sp.pdf*

### 2.3.2 Estructura Interna de las Cámaras IP

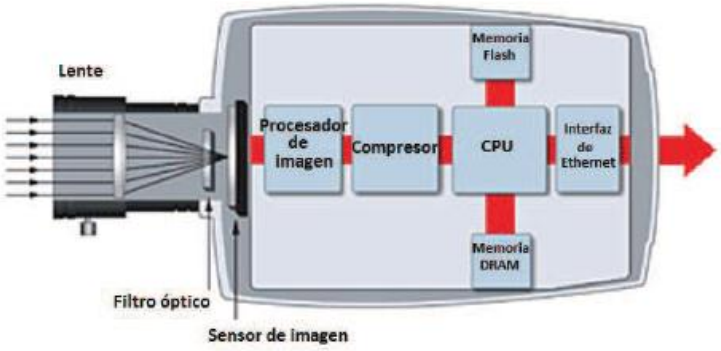



*Figura2.4 Estructura Interna de Cámara IP*
*Fuente: http://bibliodigital.epn.edu.ec.bitstream/15000/2162/CD-2919.pdf*

Las **cámaras IP** internamente están constituidas por la "***cámara***" de Vídeo propiamente dicha (Lentes, sensor de imagen, procesador digital de señal), por un "***motor***" de compresión de imagen (Chip encargado de comprimir al máximo la información contenida en las imágenes) y por un "***ordenador***" en miniatura (CPU, FLASH, DRAM, y módulo ETHERNET/ WIFI) encargado en exclusiva de gestionar procesos propios, tales como la compresión de las imágenes, el envío de imágenes, la gestión de alarmas y avisos, la gestión de las autorizaciones para visualizar imágenes.

#### 2.3.2.1 Funcionamiento técnico de la cámara de red.

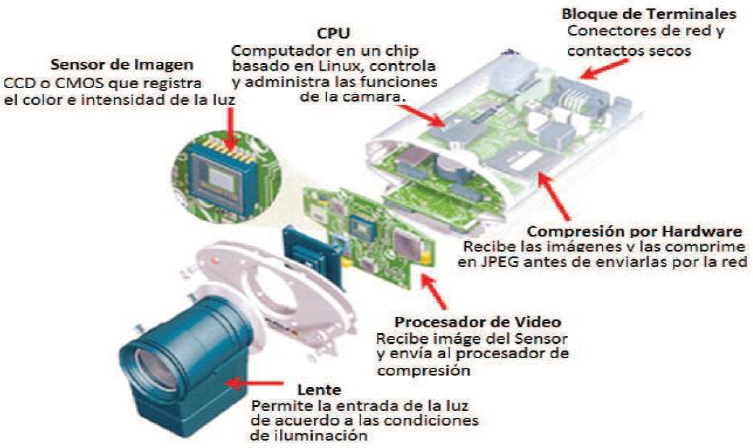



*Figura2.5 Funcionamiento técnico de la cámara de Red*
*Fuente: http://litenet.tech.officelive.com/camaraipdesc.aspx*

La lente de la cámara enfoca la imagen en el sensor de imagen (CCD). Antes de llegar al sensor la imagen pasa por el filtro óptico que elimina cualquier luz infrarroja de forma que se muestren los colores correctos. El sensor de imagen convierte la imagen, que está compuesta por información lumínica, en señales eléctricas. Estas señales eléctricas se encuentran ya en un formato que puede ser comprimido y transferido a través de redes.

Las funciones de cámara gestionan la exposición (el nivel de luz de la imagen), el equilibrio de blancos (el ajuste de los niveles de color), la nitidez de la imagen y otros aspectos de la calidad de la imagen. Estas funciones las llevan a cabo el controlador de cámara y el chip de compresión de vídeo; esto es desarrollado y determinado por los fabricantes.

La imagen digital se comprime en una imagen que contiene menos datos para permitir una transferencia más eficiente a través de la red.

La conexión Ethernet de la cámara la proporciona el chip, una solución optimizada para la conexión de periféricos a la red. El chip incluye una CPU de 32 bits, conectividad Ethernet 10/100 MBps, funcionalidad de Acceso Directo a Memoria (DMA) y una amplia variedad de interfaces de entrada y salida. La CPU, y la memoria flash y DRAM representan los “cerebros” o funciones de ordenador de la cámara y están específicamente diseñados para su aplicación en redes.

Juntos, gestionan la comunicación con la red y el servidor Web.

#### 2.3.2.2 Técnicas de compresión y resolución de imagen

La resolución de las imágenes digitales se mide en píxeles. La imagen más detallada es la que tiene más datos y por tanto mayor número de píxeles. Las imágenes con más detalles ocupan más espacio en los discos duros y precisan mayor ancho de banda para su transmisión.

Para almacenar y transmitir imágenes a través de una red los datos deben estar comprimidos o consumirán mucho espacio en disco o mucho ancho de banda.

Si el ancho de banda está limitado la cantidad de información que se envía debe ser reducida rebajando el número de frames por segundo o aceptando un nivel de calidad inferior.

Existen múltiples estándares de compresión que resuelven los problemas de número de frames por segundo y calidad de imagen de diferentes formas. De los estándares más comunes tanto el JPEG como el MPEG transmiten vídeo de alta

calidad, mientras que los estándares-H, usados normalmente en videoconferencia, no generan imágenes claras de objetos que se mueven a gran velocidad.

#### 2.3.2.3 Requerimientos de luz de las cámaras

La razón más habitual de una calidad de imagen pobre es la insuficiencia de luz. Con un nivel de luz muy bajo el nivel de los colores será sombrío y las imágenes borrosas. El nivel de luz se mide en Lux.

La luz solar fuerte tiene aproximadamente 100.000 Lux, la luz diurna tiene aproximadamente 10.000 Lux.

Habitualmente se precisan al menos 200 Lux para capturar imágenes de buena calidad. Las áreas brillantes deben ser evitadas dado que las imágenes pueden resultar sobre-expuestas y que los objetos aparezcan muy oscuros.

Este problema ocurre igualmente cuando se intenta capturar un objeto con luz negra. Una cámara ajusta la exposición para conseguir una buena media de nivel de luz para la imagen, pero el contraste de color entre el objeto y el fondo influye en la exposición.

Para evitar este problema los objetos oscuros pequeños deberían disponerse delante de un fondo oscuro para conseguir el color y el contraste correctos.

#### 2.3.2.4 Almacenar la información

Habitualmente en un único disco duro pueden almacenarse millones de imágenes. Cuando el disco duro está lleno, el ordenador puede programarse para borrar

automáticamente las imágenes más antiguas y liberar espacio para otras nuevas. Existen muchos sistemas de seguridad profesionales que gestionan las completas aplicaciones de seguridad disponibles actualmente en el mercado.

#### 2.3.2.5 Software especifico para el acceso a las cámaras IPG

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, mediante el mismo tendremos acceso a la dirección propia de la Cámara de Red, 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 se adjunta un software de visualización de hasta 4 cámaras, permitiendo la visualización simultánea 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.

### 2.3.3 Aplicaciones específicas de las cámaras de red

La tecnología de la cámara de red puede emplearse en literalmente miles de aplicaciones de valor añadido, y no necesariamente en aspectos de seguridad. Los usos pueden variar en las oficinas, los establecimientos comerciales y los casinos, o ampliarse a la monitorización de procesos de producción y atracción web. A continuación se describen algunas de las aplicaciones más productivas y económicas de las cámaras de red:

#### 2.3.3.1 Seguridad y Vigilancia

Las cámaras de red se usan en sistemas de seguridad profesionales y permiten vídeo en directo para que sea visualizado por personal autorizado. Las cámaras de red se integran fácilmente en sistemas mayores y más complejos, pero también

pueden funcionar como soluciones aisladas en aplicaciones de vigilancia de bajo nivel.

- Las cámaras de red pueden usarse para vigilar áreas sensibles como pueden ser edificios, casinos, bancos y tiendas. Las imágenes en vídeo de estas áreas pueden ser monitorizadas desde salas de control, dependencias policiales y/o por directores de seguridad desde diferentes localizaciones.
- Las cámaras de red han mostrado igualmente ser efectivos sustitutos de las cámaras analógicas en aplicaciones tradicionales de refuerzo a las fuerzas de seguridad, como por ejemplo para mantener seguros determinados lugares públicos.
- Las cámaras de red pueden igualmente emplearse para el control de accesos. Las personas, al igual que los vehículos, pueden grabarse junto con la información de la fecha y la hora de entrada de forma que sea sencilla su revisión y localización. Las imágenes pueden almacenarse en un lugar remoto, imposibilitando el robo de esta valiosa información.

#### 2.3.3.2 Monitorización Remota

Las cámaras de red se conectan fácilmente a las redes IP existentes y permiten actualizaciones en tiempo real de vídeo de alta calidad para que resulte accesible desde cada uno de los ordenadores de una red. Las áreas sensibles como son la sala de servidores, la recepción o cualquier lugar remoto pueden ser monitorizadas detalladamente de una forma única y económica, a través de la red de área local o de Internet.

- Las cámaras de red mejoran la monitorización de un establecimiento comercial para asegurar que todo está en orden.
- Una cámara de red es una herramienta útil en la oficina. Áreas como la recepción y las salas de conferencias pueden estar monitorizadas para controlar su actividad. Además los usuarios pueden hacer seguimiento de quién ha entrado en la sala de informática, por ejemplo, y tomar las acciones pertinentes cuando haya problemas.

- Las cámaras de red son herramientas útiles en la industria de la fabricación. Monitorizar robots, u otras máquinas, y las líneas de producción desde la oficina o desde casa y permitir a los ingenieros de servicio acceder a las cámaras remotamente.

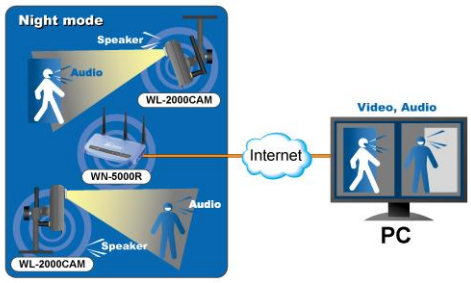



*Figura2.6 Monitorización de las Cámaras de Red*
*Fuente: http://litenet.tech.officelive.com/camaraipdesc.aspx*

## 2.4 Hipótesis

El Diseño de un Sistema de Vigilancia, en tiempo real, mediante Cámaras IP, permitirá optimizar la seguridad del Servicio Ecuatoriano de Capacitación Profesional – Centro de Formación Industrial Ambato.

## 2.5 Señalamiento de Variables:

### 2.5.1 Variable Independiente:

- Sistema de Vigilancia, en tiempo real, mediante Cámaras IP.

### 2.5.2 Variable Dependiente:

- Optimizara la seguridad del Servicio Ecuatoriano de Capacitación Profesional – Centro de Formación Industrial Ambato.

# CAPITULO III
# METODOLOGÍA

## 3.1 Enfoque

El presente estudio tiene un enfoque cuali-cuantitativo debido a que benefició a la población involucrada en el problema y al investigador a aplicar los conocimientos científicos y técnicos adquiridos.

## 3.2 Investigación de Campo

Se realizó un estudio sistemático en el lugar que se produce el problema, en este caso las instalaciones del SECAP – CEFIA, se obteniendo los datos de la fuente como es el Sr. Director, los Señores Profesores, Señoritas Secretarias y los Señores Guardias de la Institución.

### 3.2.1 Investigación Documental - Bibliográfica

El trabajo estuvo enmarcado dentro de la modalidad de investigación documental debido a que los temas fueron consultados en Internet y a la vez bibliográfica ya que se utilizó diversos libros para sustentar el tema.

### 3.2.2 Proyecto Factible

El proyecto es factible debido a que se cuenta con los dispositivos necesarios, como son las cámaras IP disponibles en el mercado y el conocimiento

indispensable para la realización pertinente del diseño de seguridad, mediante Cámaras IP, para el SECAP – CEFIA.

### 3.3 Nivel o Tipo de Investigación

La investigación obtuvo los siguientes niveles, en primera instancia el nivel exploratorio por que la recopilación de la información, ayudó a tener bases para desarrollarar el nivel descriptivo, debido a que busco las propiedades del problema se analizo los requerimientos, con el nivel correlacional se comparó los diferentes dispositivos de seguridad mediante cámaras IP y por último en el nivel explicativo se desglosó la propuesta para la solución del problema.

### 3.4 Población y Muestra

#### 3.4.1 Población

<table>
<tr><th>Área</th><th colspan="3">Miembros</th></tr>
<tr><td>Dirección</td><td>1 Director</td><td>1 Secretaria</td><td></td></tr>
<tr><td rowspan="10">Gestión de Recursos Humanos</td><td>1 Líder</td><td>1 Secretaria</td><td>1 Bibliotecario</td></tr>
<tr><td>1 Responsable de Mantenimiento</td><td>1 Bodeguero<br>1 Proveedor</td><td>1 Chofer</td></tr>
<tr><td colspan="3">1 Responsable de comercio y Servicios</td></tr>
<tr><td colspan="3">1 Responsable de Diseño Curricular</td></tr>
<tr><td colspan="3">1 Responsable de CNCF</td></tr>
<tr><td colspan="3">1 Responsable de Estadísticas</td></tr>
<tr><td colspan="3">1 Responsable de Certificación</td></tr>
<tr><td colspan="3">1 Responsable de GAB</td></tr>
<tr><td colspan="3">1 Promotora</td></tr>
<tr><td>Financiero</td><td colspan="3">1 Responsable y 1 Recaudadora</td></tr>
<tr><td>Instituto Técnico SECAP – CEFIA</td><td>1 Rector<br>1 Vicerrector</td><td colspan="2">1 Secretaria – 1 Asistente<br>1 Contador – 1 Promotora</td></tr>
<tr><td>Señores Instructores</td><td colspan="3">13</td></tr>
<tr><td>Estudiantes</td><td colspan="3">170</td></tr>
<tr><td>Señores Guardias</td><td colspan="3">2</td></tr>
<tr><td>Total Personas</td><td colspan="3">209</td></tr>
</table>

### 3.4.2 Muestra

Para la determinación de la muestra se aplicó la siguiente fórmula:

$$n = \frac{N}{(0.05)^2(N-1)+1}$$

Donde:

n = tamaño de la muestra = ?

N= población a investigarse = 209

E = índice de error máximo admisible = 0.05

$$n = \frac{209}{(0.05)^2(209-1)+1}$$

$$n = \frac{209}{0.0025(790)+1}$$

$$n = \frac{209}{1.52}$$

$$n = 137.5$$

La Muestra (n) = 138 personas

### 3.5 Recolección de Información

Mediante la observación, la entrevista y la encuesta que se realizo a las personas del muestreo se obtuvo la información que brindo una idea global de la seguridad actual en el SECAP – CEFIA; la misma que es analizada e interpretada de forma técnica en el siguiente capítulo.

| Concepto | Dimensiones | Indicadores | Items | Tec. – Inv. |
|---|---|---|---|---|
| **Variable Independiente:** Sistema de Vigilancia, en tiempo real, mediante Cámaras IP.- comprende dos tecnologías la de transmisión de datos de interiores y exteriores conjuntamente con la de Vídeo Vigilancia en red que, combinadas crean un potente sistema de seguridad. | 1.- Tipo de Cámaras IP<br><br>2.- Tecnologías para el manejo cámaras IP<br><br>3.- Conexión<br><br>4.- Servicios que ofrece | Alámbricas e Inalámbricas, movimiento, ocultas, exterior e interior.<br><br>Para una Red Alámbricas o Red Inalámbricas.<br><br>Medios guiados o no guiados, por la relación funcional.<br><br>Seguridad y grabación de imágenes. | 1.- ¿Cuáles son los tipos de cámaras IP?<br><br>2.- ¿Cuáles son las Tecnologías para el manejo de cámaras IP?<br><br>3.- ¿Cómo se realiza la conexión de las Cámaras IP?<br><br>4.- ¿Cuáles son los servicios que ofrecen los videos de vigilancia IP? | Bibliográfica<br><br>Bibliográfica<br><br>Bibliográfica<br><br>Bibliográfica |
| **Variable Dependiente:**<br><br>Optimizar la Seguridad del Servicio de Capacitación Profesional - Centro de Formación Industrial Ambato. | 1.- Áreas vulnerables a la Inseguridad.<br><br>2.-Diseño de las conexiones de las cámaras IP en la Institución | Personal que labora ahí.<br><br>Laboratorios del Establecimiento.<br><br>Estudio y Análisis de los Planos. | 1.- ¿La Institución necesita un sistema de seguridad actualizado?<br><br>2.- ¿Cuáles son los sectores vulnerables a la Inseguridad? | Entrevista<br><br>Encuesta, Observación y Planos. |

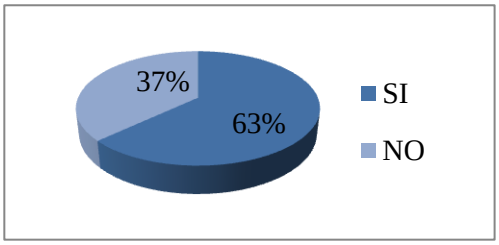
## CAPITULO IV

## ANALISIS E INTERPRETACION DE RESULTADOS

Con la encuesta realizada a 138 personas del Servicio Ecuatoriano de Capacitación Profesional – Centro de Formación Industrial Ambato; se obtuvo los siguientes resultados; además los análisis de cada pregunta se detallan a continuación:

- ¿Cree usted que el sistema de seguridad del SECAP – CEFIA está desactualizado?

| | CANTIDAD | PORCENTAJE |
|---|---|---|
| SI | 87 | 63,04% |
| NO | 51 | 36,96% |
| **TOTAL** | 138 | 100% |



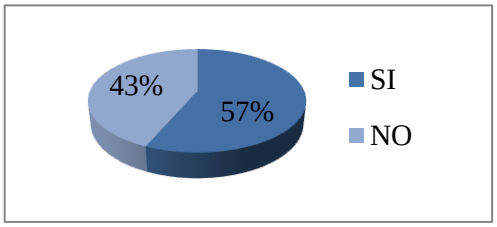

**Análisis:**

El 63% de personas del SECAP – CEFIA opinan que su sistema está desactualizado, además algunos de los interrogados mencionaron que no existe un sistema tecnológico de seguridad en la Institución; contando solamente con el servicio de guardianía tradicional.

El 37% piensa que no está desactualizado.

- ¿Conoce alguna situación en la que los equipos electrónicos e industriales o personal de la Institución se ha visto expuesta a riesgo de inseguridad?

| | CANTIDAD | PORCENTAJE |
|---|---|---|
| SI | 78 | 56,52% |
| NO | 60 | 43,48% |
| **TOTAL** | 138 | 100% |



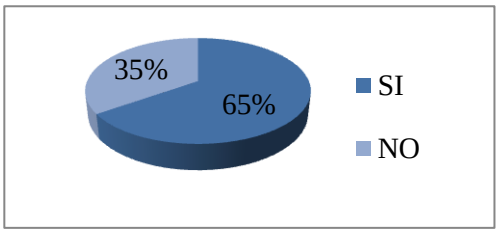

**Análisis:**

El 57% piensa que si están expuestos a riesgos de inseguridad los equipos electrónicos e industriales y personal de la Institución.

En cambio el 43% responde que no existe ningún riesgo de inseguridad.

- ¿Está de acuerdo con la implementación de un sistema de vigilancia por medio de cámaras de video en la Institución?

| | CANTIDAD | PORCENTAJE |
|---|---|---|
| SI | 90 | 65,22% |
| NO | 48 | 34,78% |
| **TOTAL** | 138 | 100% |

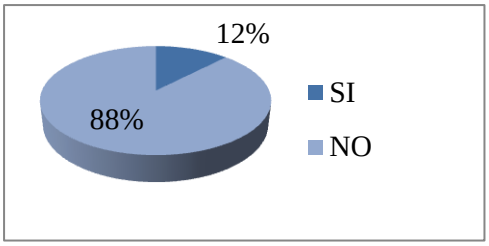



**Análisis:**

El 65% del personal del SECAP – CEFIA está de acuerdo con la implementación de cámaras de video. Porque esto mejoraría la seguridad, mientras que el 35% que no es necesario implementar.

- ¿Ha escuchado el término de Cámaras IP?

| | CANTIDAD | PORCENTAJE |
|---|---|---|
| SI | 17 | 12,32% |
| NO | 121 | 87,68% |
| **TOTAL** | 138 | 100% |

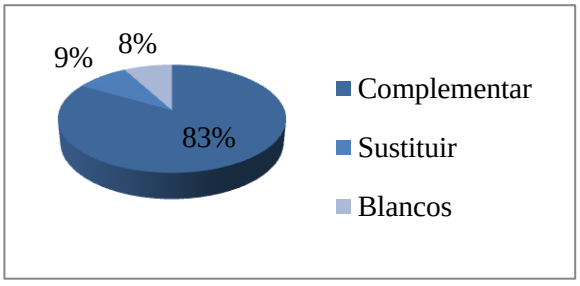



**Análisis:**

En la Institución el 88% no han escuchado el término de Cámaras IP mientras que el 12% si.

- Cree usted que el sistema de vigilancia mediante Cámaras IP debería:
  - Complementar la Seguridad del SECAP – CEFIA
  - Sustituir la Seguridad de SECAP – CEFIA

| | CANTIDAD | PORCENTAJE |
|---|---|---|
| Complementar | 115 | 83,33% |
| Sustituir | 12 | 8,70% |
| Blancos | 11 | 7,97% |
| **TOTAL** | 138 | 100% |



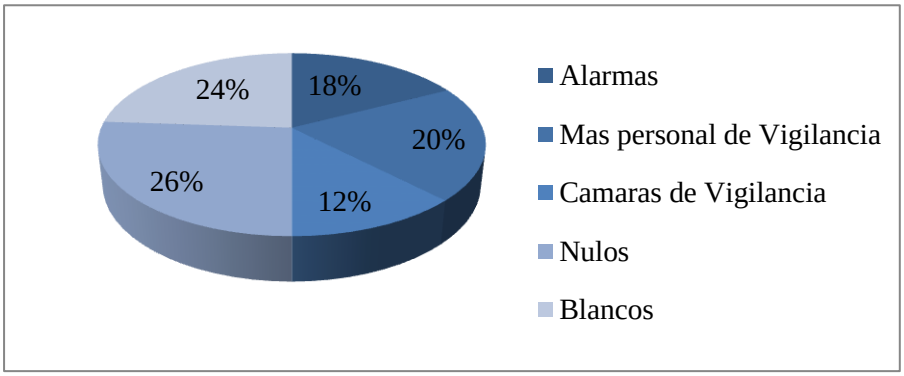
**Análisis:**

El 83% piensa que las Cámaras IP complementarían la seguridad en el SECAP – CEFIA; mientras que el 9% optó por señalar que debería sustituir el servicio que actualmente posee la Institución.

El 8% no opinó.

- ¿Qué otro tipo de Sistema de seguridad recomendaría usted para la Institución?

| | CANTIDAD | PORCENTAJE |
|---|---|---|
| Alarmas | 24 | 17,39% |
| Más personal de Vigilancia | 28 | 20,29% |
| Cámaras de Vigilancia | 17 | 12,32% |
| Nulos | 36 | 26,09% |
| Blancos | 33 | 23,91% |
| **TOTAL** | 138 | 100% |




**Análisis:**

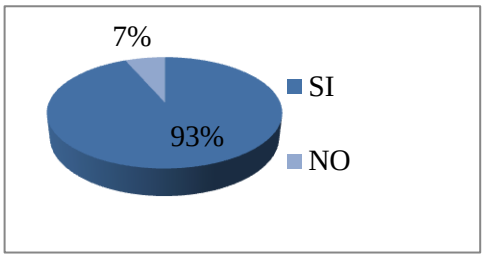
De acuerdo con lo que se presenta en la tabla de datos; las personas optarían por otro sistema el 18% las Alarmas, 20% Más personal de Vigilancia en cada sección, y el 12% Cámaras de Vigilancia.

Los Nulos que representan el 26% no dieron una opinión acorde con lo que se les preguntaba.

Los Blancos que es el 24% no dieron ninguna opinión.

- ¿Está de acuerdo que el SECAP – CEFIA implemente un sistema de Seguridad acorde con las tecnologías actuales?

| | CANTIDAD | PORCENTAJE |
|---|---|---|
| SI | 129 | 93,48 |
| NO | 9 | 6,52 |
| **TOTAL** | 138 | 100% |




**Análisis:**

El 93% está de acuerdo que la Institución cuente con un Sistema de Seguridad acorde con las tecnologías actuales. Mientras que el 7% piensa que no necesita vigilancia actualizada.

La Encuesta se realizó a las Autoridades y un grupo de Estudiantes completando el número de 138 personas cumpliendo con la muestra obtenida.

De acuerdo con los datos tabulados se puede observar en cada pregunta que la seguridad en el Servicio Ecuatoriano de Capacitación Profesional es vulnerable y que requiere de una vigilancia continua de sus instalaciones, de manera especial los talleres y laboratorios de la Institución.

**Análisis de la red en el SECAP – CEFIA**

El Proveedor de Servicio de Internet para SECAP – CEFIA es la CNT (Corporación Nacional de Telecomunicaciones) mismo que suministra al establecimiento dos bandas de Internet de 512Kbps. En la figura 4.1 muestra el diseño físico que actualmente funciona en la Institución.

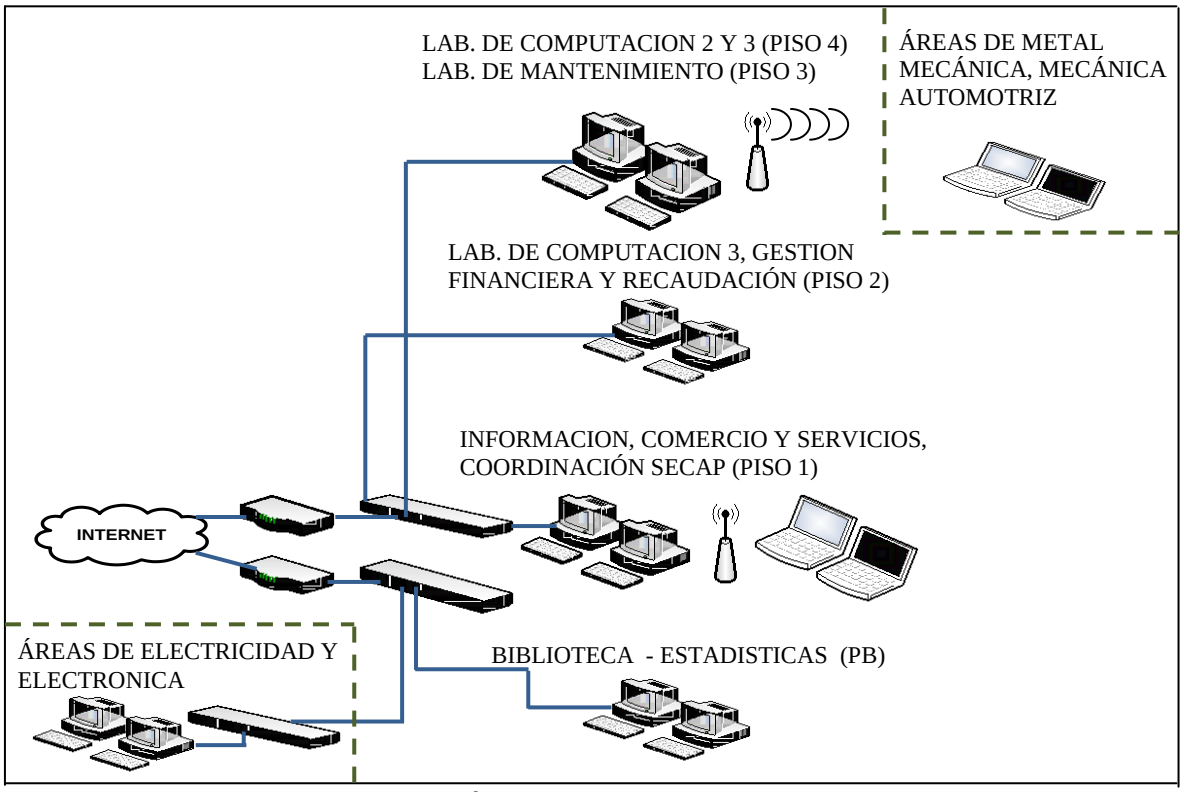



*Figura 4.1 Diseño Físico del SECAP – CEFIA*

La red del SECAP – CEFIA es utilizada para la parte administrativa, pedagógica y operativa. Luego de analizar se puede mencionar que:

- Las Áreas de Metal Mecánica, Mecánica Automotriz y Confecciones Industriales disponen de acceso a Internet inalámbrico para 2 máquinas portátiles.

- Los Equipos del área Administrativa se indican en la tabla 4.1:

*Tabla 4.1 Equipos del área Administrativa*

| | | | |
|---|---|---|---|
| Piso 5 | Sala de Audiovisuales | 0 máquinas | |
| Piso 4 | Laboratorio Computación 2 | 16 máquinas | |
| | Laboratorio Computación 3 | 16 máquinas | |
| Piso 3 | Laboratorio de Mantenimiento | 3 máquinas | |
| | 3 Aulas | 0 máquinas | |
| Piso 2 | Laboratorio Computación 1 | 12 máquinas | |
| | Gestión Financiera | 2 máquinas | |
| | Recaudación | 2 máquinas | |
| | Oficina | 2 máquinas | |
| Piso 1 | Información Comercio y Servicios | 4 máquinas | |
| | Coordinación SECAP | 3 máquina | |
| Planta Baja | Biblioteca – Estadística | 4 máquina | |
| | BAR | 0 máquinas | |

- El Área de Electricidad y Electrónica

*Tabla 4.2 Equipos del área Electricidad y Electrónica*

| | | |
|---|---|---|
| **Planta Alta** | | |
| Rectorado – Secretaria | 2 máquinas | |
| Lab. Máquinas Eléctricas | 0 máquinas | |
| Lab. PLC | 4 máquinas | |
| Lab. Instalaciones Electricas | 0 máquinas | |
| **Planta Baja** | | |
| Lab. Computación | 16 máquinas | |
| Coordinación de Electricidad y Electrónica | 2 máquinas | |
| Taller de Cazado | 1 máquinas | |

En la tabla 4.3 se presenta la descripción de los equipos que actualmente funcionan en el SECAP – CEFIA

*Tabla 4.3 Descripción de Equipos*

| Equipo | Descripción |
|---|---|
| | 90 Computadoras |
| | CNSH-1600 16-Port Fast Ethernet Switch |
| | DGS-1224T 24-ports Gigabit Smart Switch |
| | DIR-600 wireless 150 router with 4-port10/100mbps switch |
| | DSL-500B **Router ADSL con puertos Ethernet** |
| | Router D-link Dsl-524b 4 Puertos Lan Adsl |
| | Conexión UTP |

**Análisis del Tráfico y Ancho de Banda que maneja actualmente a red del SECAP – CEFIA**

Con la ayuda del software CommView el cual permite el monitoreo de los paquetes que circulan por la red. Se analizó el tráfico presente en la misma.

CommView es un programa que monitorea la actividad de la red, y es capaz de capturar y analizar paquetes de información. Se recogió la información del flujo de datos en la red LAN del Establecimiento. Este programa permite observar las conexiones de la red, estadísticas IP esenciales, y examinar los paquetes.

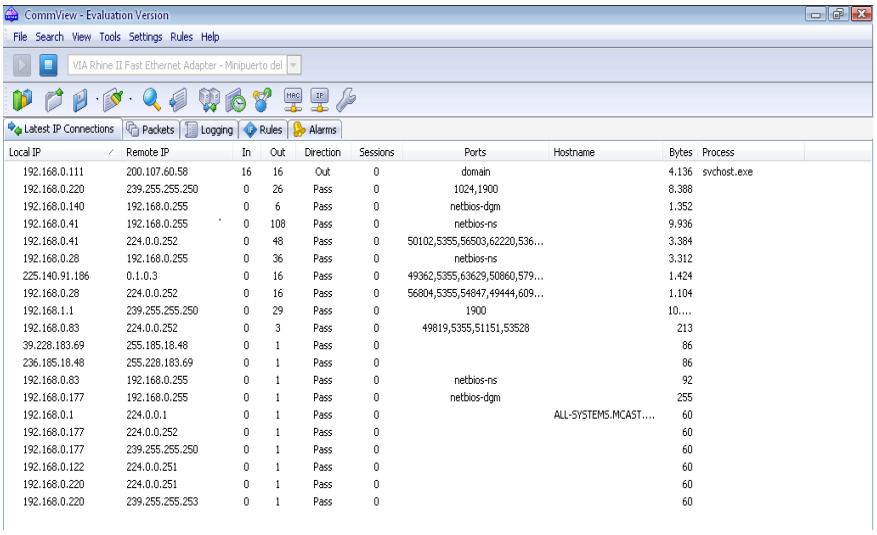



*Figura4.2Monitoreo con software CommView*

El software CommView determino el funcionamiento de la red en el SECAP – CEFIA, describiendo direcciones IP privadas de clase C: 192.168.0.1 a 92.168.0.254.

En las siguientes tablas se observan las mediciones realizadas en la red del SECAP – CEFIA se monitorio de Martes 3 a Sábado 7 de Agosto 2010 de 9:00 a 11:00 a.m.

*Tabla4.4 Martes 3 de Agosto 2010*

| Item \ Direction | Inbound | Outbound | Pass-through |
|---|---|---|---|
| **Packets** | 25 | 44 | 1.989 |
| **Bytes** | 3.704 | 5.376 | 261.670 |
| **Bytes per sec.** | 8 | 11 | 551 |

*Tabla4.5 Miércoles 4 de Agosto 2010*

| Item \ Direction | Inbound | Outbound | Pass-through |
|---|---|---|---|
| **Packets** | 26 | 46 | 2.075 |
| **Bytes** | 3.852 | 5.620 | 272.909 |
| **Bytes per sec.** | 8 | 12 | 580 |

*Tabla4.6 Jueves 5 de Agosto 2010*

| Item \ Direction | Inbound | Outbound | Pass-through |
|---|---|---|---|
| **Packets** | 28 | 47 | 2.162 |
| **Bytes** | 4.148 | 5.743 | 285.042 |
| **Bytes per sec.** | 9 | 12 | 609 |

*Tabla4.7 Viernes 6 de Agosto 2010*

| Item \ Direction | Inbound | Outbound | Pass-through |
|---|---|---|---|
| **Packets** | 28 | 47 | 2.162 |
| **Bytes** | 4.148 | 5.743 | 285.042 |
| **Bytes per sec.** | 9 | 12 | 609 |

*Tabla4.8 Sábado 7 de Agosto 2010*

| Item \ Direction | Inbound | Outbound | Pass-through |
|---|---|---|---|
| **Packets** | 23 | 40 | 1.8160 |
| **Bytes** | 3.407 | 4.8873 | 239.027 |
| **Bytes per sec.** | 7 | 10 | 493 |

En la figura 4.4 se presenta el total de bytes por día en la red del SECAP-CEFIA; determinando que el día con menos trafico es el Sábado.

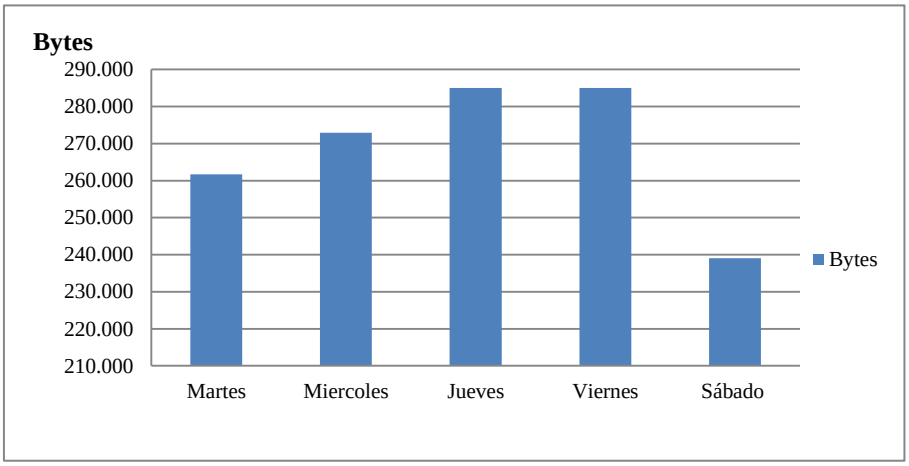



*Figura 4.3 Trafico de la red en Bytes*

En la figura 4.5 muestra el total de bytes/sec de cada día en la red del SECAP-CEFIA.

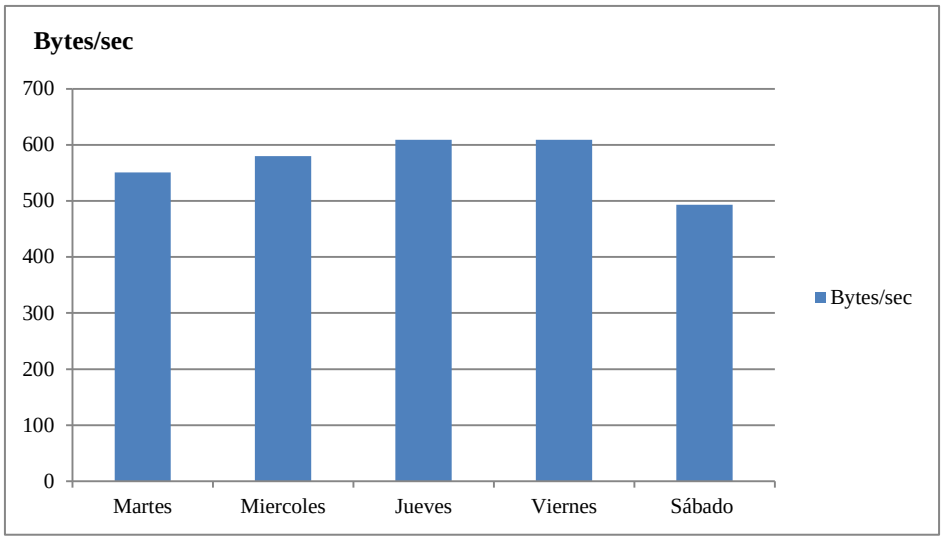



*Figura 4.4 Trafico de la red en Bytes/sec*

En la tabla 4.9 está calculado el tráfico promedio de la red de la Institución.

*Tabla 4.9 Promedio del tráfico de la red en el SECAP – CEFIA*

| **Día** | **Trafico** |
|---|---|
| Martes | 551 |
| Miércoles | 580 |
| Jueves | 609 |
| Viernes | 609 |
| Sábado | 493 |
| **Total** | **568.4** *Bytes/sec* |

# CAPITULO V
# CONCLUSIONES Y RECOMENDACIONES

## 5.1 Conclusiones:

- La seguridad actual del SECAP – CEFIA es desempeñada por el servicio de guardianía tradicional.
- La Institución no dispone de seguridad acorde con las tecnologías actuales.
- Las personas del Establecimiento declararon que se han visto expuestos a riesgos de inseguridad, los equipos, maquinaria eléctrica y electrónica.
- El Servicio Ecuatoriano de Capacitación Profesional – Centro de Formación Industrial Ambato posee áreas vulnerables a la inseguridad como laboratorios y talleres donde tienen máquinas de alto costo.
- Las personas que trabajan y estudian en el SECAP – CEFIA manifestaron estar de acuerdo, con la implementación de un sistema de vigilancia actualizado, para resguardar la seguridad de los bienes y personal del Establecimiento.
- La Red del SECAP-CEFIA es una red pequeña con direccionamiento Ip de clase C; posee dos accesos a internet 512 Kbps que le proporciona la CNT.
- El trafico de la red no sobre pasa los 100kbps; ya que la red se lo utiliza para la parte administrativa, operativa y enseñanza pedagógica.
- Los equipos que se encuentran conectados a la red no tienen una secuencia lógica en la asignación de las direcciones IP.
- No tienen una documentación detallada de las direcciones IP de cada uno de los equipos conectados a la red.

## 5.2 Recomendaciones

- El SECAP – CEFIA, siendo una Institución Pública es recomendable que tenga seguridades de última tecnología, para evitar pérdidas que afectarían a un presupuesto Institucional y de Estado.
- Determinar áreas susceptibles a inseguridad para brindar un mejor control de las mismas.
- Implementación de un sistema de vigilancia con tecnología; inalámbrica y alámbrica (hibrida), para complementar el servicio de seguridad que la Institución posee actualmente.
- Para tener un mejor aprovechamiento de la red y optimizar el transporte de información se debe realizar VLAN y además documentar la administración de la red.

# CAPITULO VI
# PROPUESTA

## 6.1 Datos Informativos

El Servicio Ecuatoriano de Capacitación Profesional – Centro de Formación Industrial Ambato; es una Institución perteneciente al Estado Ecuatoriano, está ubicado en la Av. Bolivariana y el Cóndor frente al Mercado Mayorista km. 3,5 vía a Baños de la Ciudad de Ambato.

## 6.2 Antecedentes de la Propuesta

El avance de la tecnología ha permitido ver cómo el mundo cambia rápidamente. El mercado tecnológico de seguridad es un sector que está en constante crecimiento y el mundo detrás de las cámaras de seguridad está en plena evolución. Las cámaras IP son una excelente alternativa para brindar seguridad; ya que la vigilancia lo realizan las 24 horas del día y el usuario puede acceder a información de cualquier cámara, mediante internet.

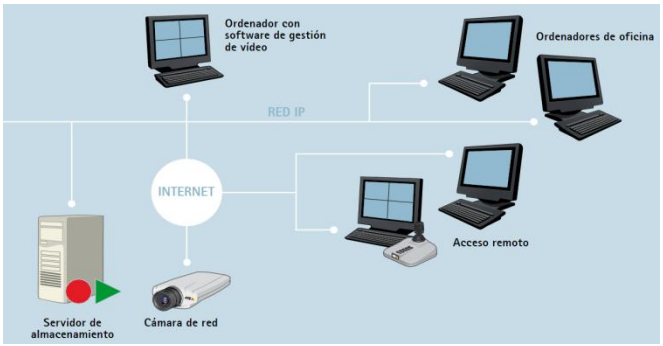



*Figura6.1 Esquema de red con cámara IP*
*https://www.axis.com/files/brochure/pg_video_36879_es_1002_lo.pdf*

Mediante la conexión directa a una red o un módem, los productos de vigilancia IP pueden distribuir secuencias de vídeo de alta calidad a través de cualquier red IP, ya sea una red local o Internet, tanto alámbrica como inalámbrica.

La flexibilidad de distribuir; datos de video, audio y otros se pueden transmitir sobre redes IP alámbricas e inalámbricas existentes, estás diversas opciones de transmisión

permiten controlar las cámaras; en cualquier momento que sea conveniente por medio del internet dentro y fuera del lugar vigilado.

Las cámaras IP, son usadas para vigilar áreas sensibles a la inseguridad; como por ejemplo: en edificios, casinos, bancos, establecimientos educativos e instituciones comerciales. Además son útiles en la industria de la fabricación, puesto que monitorean robots u otras máquinas; en los procesos de producción.

### 6.3 Justificación

El diseño de un sistema de vigilancia mediante cámaras IP para optimizar la seguridad del Servicio Ecuatoriano de Capacitación Profesional – Centro de Formación Industrial Ambato; se estructuro de forma técnica – metodológica , priorizando las necesidades de la Institución.

El sistema de vigilancia mediante cámaras IP; está sustentado con los equipos tecnológico. La estructura metodológica son los pasos ordenados para esquematizar el sistema de vigilancia por medio de cámaras IP.

El estudio se lo realizo tanto para una red alámbrica como inalámbrica. Una vez bosquejado y establecido la red, los dispositivos electrónicos; de manera teórica y económica se determino cual es más idónea para el SECAP – CEFIA. Dando como resultado un sistema de vigilancia Ip Hibrido. Combinando los beneficios de red alámbrica como inalámbrica.

## 6.4 Objetivos

### 6.4.1 Objetivo General

- Diseñar un sistema de vigilancia mediante cámaras IP para el control de seguridad del SECAP – CEFIA.

### 6.4.2 Objetivos Específicos

- Analizar definiciones técnicas sobre redes alámbrica e inalámbrica.
- Estudiar la factibilidad del sistema de vigilancia por medio de cámaras IP en red alámbrica y red inalámbrica.
- Diseñar el sistema de vigilancia IP en forma física y lógica, más eficiente para la seguridad del SECAP – CEFIA.

## 6.5 Fundamentación

**6.5.1 Evolución de los sistemas de vigilancia por vídeo:** existen desde hace 25 años. Empezaron siendo sistemas analógicos al 100% y paulatinamente se fueron digitalizando. En la actualidad, estos sistemas utilizan cámaras y servidores de PC para la grabación de vídeo en un sistema completamente digitalizado.

En la tabla 6.1 presenta como a evolucionado los sistemas de vigilancia.

*Tabla6.1 Evolución de sistema de vigilancia por video*

| | |
|---|---|
| **Todo Analógico:** | ➢ Sistemas de circuito cerrado de TV analógicos usando VCR |
| **Parte Analógica con Parte Digital:** | ➢ Sistemas de circuito cerrado de TV analógicos usando DVR<br>➢ Sistemas de circuito cerrado de TV analógicos usando DVR de red<br>➢ Sistemas de vídeo IP que utilizan servidores de vídeo |
| **Todo Digital:** | ➢ Sistemas de vídeo IP que utilizan cámaras IP |

### a) Todo Analógico

Los circuitos cerrados de televisión (CCTV, Closed Circuit Television Systems) son los primeros sistemas de video-vigilancia.

Sus características analógicas encarecen su precio y no proporcionan: flexibilidad, escalabilidad, redundancia y tolerancia a fallas.

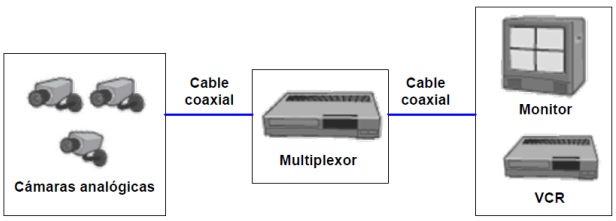



*Figura 6.2 Esquema de la plataforma de video-vigilancia analógica*
*Fuente: http://bieec.epn.edu.ec:8180/dspace/bitstream/CAP3.pdf*

**b) Parte Analogía con parte Digital**

**1) Sistemas de circuito cerrado de TV analógicos usando DVR**

Un sistema de circuito cerrado de TV (CCTV) analógico usando un DVR (grabador de vídeo digital) es un sistema analógico con grabación digital. En un DVR, la cinta de vídeo se sustituye por discos duros para la grabación de vídeo, y es necesario que el vídeo se digitalice y comprima para almacenar la máxima cantidad de imágenes posible de un día.

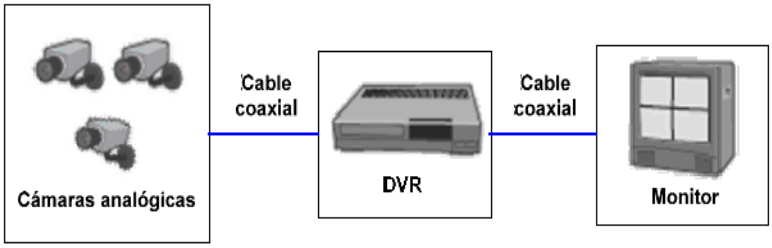



*Figura 6.3 Sistema analógico que incluye un DVR para grabar información digital*
*Fuente: http://bieec.epn.edu.ec:8180/dspace/bitstream/CAP3.pdf*

Con los primeros DVR, el espacio del disco duro era limitado, por tanto, la duración de la grabación era limitada, o debía usarse una velocidad de imagen inferior. El reciente desarrollo de los discos duros significa que el espacio deja de ser el principal problema. La mayoría de DVR disponen de varias entradas de vídeo, normalmente 4, 9 ó 16, lo que significa que también incluyen la funcionalidad de los quads y multiplexores.

El sistema DVR añade las siguientes ventajas:

- No es necesario cambiar las cintas
- Calidad de imagen constante

**2) Sistemas de circuito cerrado de TV analógicos usando DVR de red**

Un sistema de circuito cerrado de TV (CCTV) analógico usando un DVR IP es un sistema parcialmente digital que incluye un DVR IP equipado con un puerto Ethernet para conectividad de red. Como el vídeo se digitaliza y comprime en el DVR, se puede transmitir a través de una red informática para que se monitorice en un PC en una ubicación remota.

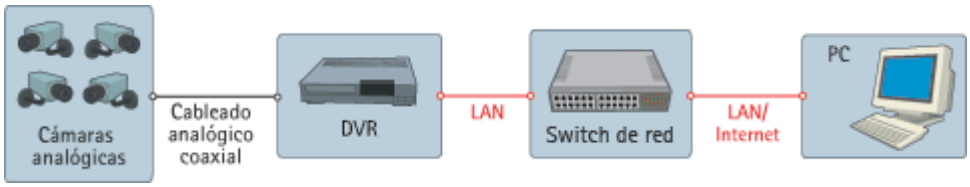



*Figura 6.4 Sistema analógico que incluye un DVR y dispositivos de Red*
*Fuente: http://bieec.epn.edu.ec:8180/dspace/bitstream/CAP3.pdf*

Algunos sistemas pueden monitorizar tanto vídeo grabado como en directo, mientras otros sólo pueden monitorizar el vídeo grabado. Además, algunos sistemas exigen un cliente Windows especial para monitorizar el vídeo, mientras que otros utilizan un navegador web estándar, lo que flexibiliza la monitorización remota.

El sistema DVR IP añade las siguientes ventajas:

- Monitorización remota de vídeo a través de un PC
- Funcionamiento remoto del sistema

**3) Sistemas de vídeo IP que utilizan servidores de vídeo**

Un sistema de vídeo IP que utiliza servidores de vídeo incluye un servidor de vídeo, un conmutador de red y un PC con software de gestión de vídeo. La cámara analógica se conecta al servidor de vídeo, el cual digitaliza y comprime el vídeo. A continuación, el servidor de vídeo se conecta a una red y transmite el vídeo a través

de un conmutador de red a un PC, donde se almacena en discos duros. Esto es un verdadero sistema de vídeo IP.

Un sistema de vídeo IP que utiliza servidores de vídeo añade las ventajas siguientes:

- Utilización de red estándar y hardware de servidor de PC para la grabación y gestión de vídeo.
- El sistema es escalable en ampliaciones de una cámara cada vez.
- Es posible la grabación fuera de las instalaciones.
- Preparado para el futuro, ya que este sistema puede ampliarse fácilmente incorporando cámaras IP.

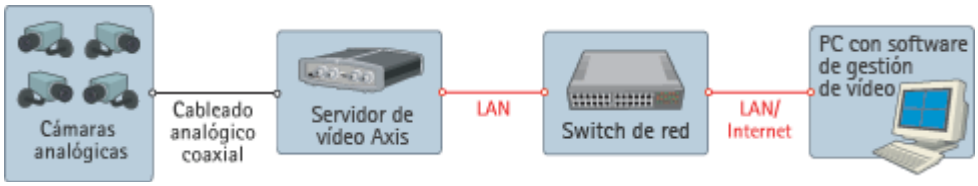



*Figura 6.5 Sistema analógico con transmisión digital*
*Fuente: http://bieec.epn.edu.ec:8180/dspace/bitstream/CAP3.pdf*

La información del vídeo se transmite de forma continúa a través de una red IP. Utiliza un servidor de vídeo como elemento clave para migrar el sistema analógico de seguridad a una solución de vídeo IP.

**c) Todo Digital**

- **Sistemas de vídeo IP que utilizan cámaras IP**

Una cámara IP combina una cámara y un ordenador en una unidad, lo que incluye la digitalización y la compresión del vídeo así como un conector de red. El vídeo se transmite a través de una red IP, mediante los conmutadores de red y se graba en un PC estándar con software de gestión de vídeo. Esto representa un verdadero sistema de vídeo IP donde no se utilizan componentes analógicos.

Un sistema de vídeo IP que utiliza cámaras IP añade las ventajas siguientes:

- Cámaras de alta resolución (megapíxel).
- Calidad de imagen constante.
- Alimentación eléctrica a través de Ethernet y funcionalidad inalámbrica.
- Funciones de Pan/tilt/zoom, audio, entradas y salidas digitales a través de IP, junto con el vídeo
- Flexibilidad y escalabilidad completas

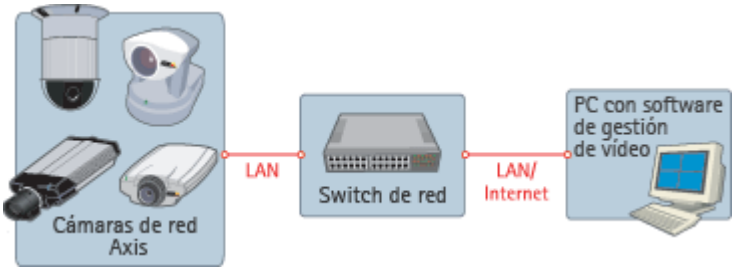



*Figura 6.6 Sistema de vigilancia Digital*
*Fuente: http://bieec.epn.edu.ec:8180/dspace/bitstream/CAP3.pdf*

Este diagrama muestra un verdadero sistema de vídeo IP, donde la información del vídeo se transmite de forma continua a través de una red IP, utilizando cámaras IP. Este sistema saca el máximo partido de la tecnología digital y proporciona una calidad de imagen constante desde la cámara hasta el visualizador, dondequiera que estén.

### 6.5.2 Tecnología PoE

La alimentación local y autónoma de un dispositivo resulta a menudo un problema cuando dicho elemento se pretende instalar en lugares poco accesibles o desprovistos de alimentación eléctrica; tal es el caso de las cámaras de vigilancia IP. Instalar alimentación eléctrica cerca de estos elementos puede resultar a veces muy dificultoso y caro.

Esta problemática se resuelve gracias a la tecnología PoE, diseñada para entregar a los dispositivos de red la alimentación que necesitan a través del propio cable de red.

En estándar IEEE 802.3af se establecen las características de los equipos y tecnología PoE, definiéndose la máxima potencia que puede ser entregada a los dispositivos utilizando formatos de transmisión 10BASE-T, 100BASE-T y 1000BASE-T.

Las ventajas de PoE son:

- Alimentación y comunicaciones de datos sobre el mismo cable
- Mayor control sobre el dispositivo
- Favorece la movilidad de los equipos (cambios de ubicación no requieren instalación de cableado eléctrico).
- Gestión de alimentación y monitorización vía SNMP
- No es necesaria la actualización del cableado (Cat5 o superior)

El estándar IEEE802.3af es capaz de entregar una potencia máxima de **15,4 Watt**, por puerto Ethernet, usando una tensión típica de **48 volt**. Se especifica una corriente alrededor de **350 mA** por conexión, que sobre 48 volt representan una potencia de **16W** por dispositivo.

Los dispositivos a alimentar pueden ser puntos de acceso inalámbricos, teléfonos IP, cámaras IP, lectores de tarjetas, impresoras.

IEEE 802.3af define dos principales piezas de hardware, el Dispositivo Alimentado (Powered Device – PD) y el Equipo de Alimentación (Power Sourcing Equipment – PSE).
Una cámara IP es un ejemplo de PD y un switch con PoE es un ejemplo de PSE.

**a) PSE- Power Sourcing Equipment** (*Equipo de Alimentación)*

El PSE tiene tres funciones primordiales:

- Detectar un PD (*Dispositivo Alimentado)* que acepte PoE
- Suministrar alimentación al PD
- Monitorizar y cortar la alimentación cuando sea necesario.

Dentro de la definición de PSE, existen dos tipos descritos: PSE Final y PSE Intermedio.
Un **PSE Final** es un **switch PoE** sobre el cual se conecta directamente el latiguillo de conexión del dispositivo PD.
Un **PSE intermedio** es un **adaptador** que tiene dos entradas (la alimentación y el cable de datos) y una sola salida RJ45 (datos y alimentación por cable de red).

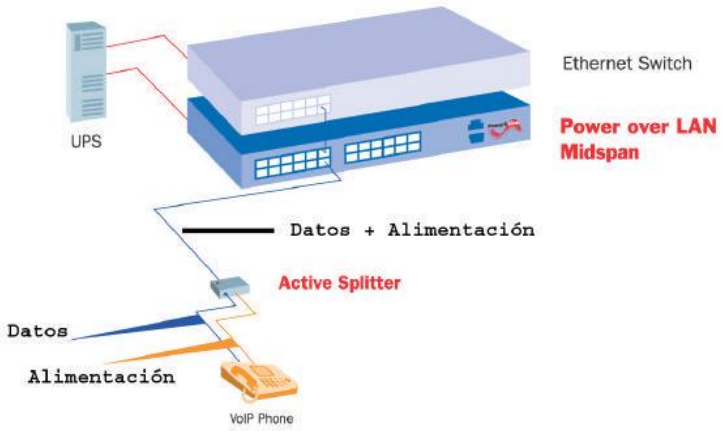



*Figura 6.7 Ejemplo de configuración con **PSE Final** (Switch PoE)*
*Fuente: http://www.imaginart.es/televigilancia/pdf/fundamentosPoE.pdf*

- **Switch PoE** : Equipo de red que distribuye el acceso a la red a los distintos equipos, directamente por un solo cable ethernet con los datos y la alimentación.
- **Midspan PoE**: Si el switch que dispone no cumple con PoE, existe este equipo, situado entre el switch normal y los equipos a los cuales hay que dotar de acceso a la red. De este equipo saldrán todas las conexiones con un solo cable (con datos y alimentación) a los diferentes equipos.
- **Splitter:** Elemento que separa la señal de datos de la alimentación para los equipos que no estén preparados para recibir las 2 señales en un solo cable ethernet.

La alimentación que entrega el PSE Final alcanza el PD usando los **pares de datos activos** (normalmente el naranja y el verde – pines 1,2 y 3,6)

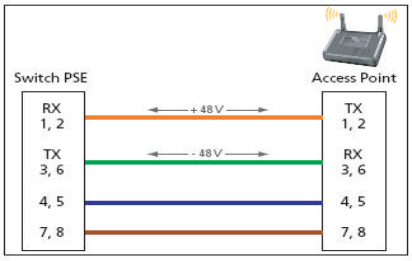



*Figura 6.8 ALTERNATIVA A: Pares activos*
*Fuente: http://www.imaginart.es/televigilancia/pdf/fundamentosPoE.pdf*

O **pares separados** (marrón y azul – pines 4,5 y 7,8).

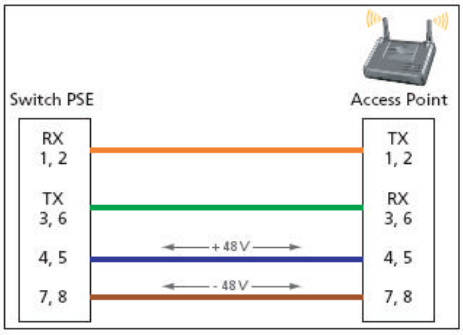



*Figura 6.9 ALTERNATIVA B: Pares separados*
*Fuente: http://www.imaginart.es/televigilancia/pdf/fundamentosPoE.pdf*

**b) *PD- Powered Device*(*Dispositivo Alimentado)***

Un PD que cumpla con el estándar IEEE 802.3af es capaz de ser alimentado de acuerdo con las dos alternativas, A y B.
El estándar define la posibilidad de que el PD (*Dispositivo Alimentado)* especifique al PSE (*Equipo de Alimentación)* la alimentación que requieren. Según estos requisitos, los PD se clasifican en distintas clases.

Estas clasificaciones son las siguientes:

- Clase 0: Desde 0,44 a 12,95 Watt
- Clase 1: Desde 0,44 a 3,84 Watt
- Clase 2: Desde 3,84 a 6,49 Watt
- Clase 3: Desde 6,49 a 12,95 Watt

**6.5.2.1Cámara Ip con Tecnología PoE:**

Permite a las cámaras IP **conectarse a la corriente eléctrica utilizando el mismo cable de red.** La ventaja inmediata al utilizar el mismo cable de red tanto para datos de video como para la alimentación eléctrica de la cámara es que **se elimina la necesidad de conectar al toma corriente cercana** o la necesidad de tener que **lidiar con cables eléctricos**.

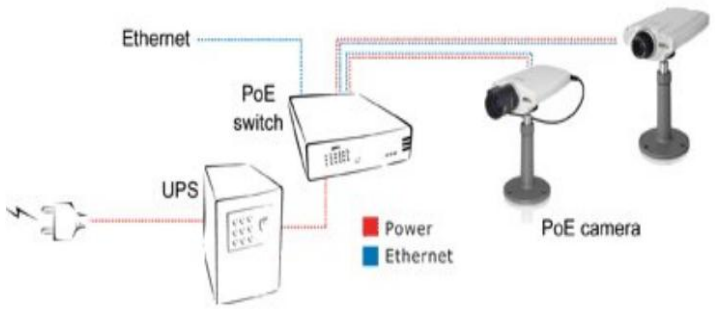



*Figura 6.10 PoE, un sólo UPS respalda a todo un sistema de video vigilancia IP*
*Fuente: http://www.condor.com.ni/blog/documentacion-y-guias/beneficio-2-de-las-camaras-ip-alimentacion-por-poe/*

**UPS:** Una UPS (Uninterruptible Power System) es un sistema que provee energía eléctrica ininterrumpida a una carga eléctrica determinada, para realizar esta función dispone de tres elementos claves:

- Una reserva de energía, que de alguna manera se convertirá en energía eléctrica y será entregada a la carga.
- Un elemento capaz de reponer la energía perdida cuando por algún motivo se utilizo total o parcialmente la reserva.

El eliminar toma corrientes en las ubicaciones de las cámaras brinda la posibilidad de centralizar la alimentación de las cámaras.
Sólo con utilizar PoE en las instalaciones de cámaras obtenemos:

- **Fácil instalación:** Para poner a funcionar las cámaras no requerimos tener que buscar toma corrientes cercanos, montar cableado eléctrico o trabajar con paneles eléctricos.
- **Ahorro en costos de instalación:** Se reducen los costos al no utilizar cableado adicional.
- **Respaldo eléctrico**: Todo desde un mismo sitio. No necesitamos buscar como respaldar cada cámara por individual. El sistema se vuelve más fiable.

#### 6.5.2.2 Dirección IP:

Es un número que identifica un ordenador dentro de una red que utilice el **protocolo IP**.

**a) Dirección MAC:**

Es un número asignado a la tarjeta de red del propio ordenador (viene impuesta por el fabricante de la tarjeta). Cualquier dispositivo que quiera comunicarse con otros dispositivos a través de Internet debe tener una dirección IP única y

adecuada. Las direcciones IP sirven para identificar a los dispositivos emisores y receptores.

**b) Dirección IP Dinámica:**

Es una IP asignada mediante un servidor DHCP (Dynamic Host Configuration Protocol) al usuario. La IP que se obtiene tiene una duración máxima determinada. El servidor DHCP provee parámetros de configuración específicos para cada cliente que desee participar en la red IP. Entre estos parámetros se encuentra la dirección IP del cliente.

***Asignación de direcciones IP***

Dependiendo de la implementación concreta, el servidor DHCP tiene tres métodos para asignar las direcciones IP:

- **Manualmente**: cuando el servidor tiene a su disposición una tabla que empareja direcciones MAC con direcciones IP, creada manualmente por el administrador de la red. Sólo clientes con una dirección MAC válida recibirán una dirección IP del servidor.
- **Automáticamente**: donde el servidor DHCP asigna permanentemente una dirección IP libre, tomada de un rango prefijado por el administrador, a cualquier cliente que solicite una.
- **Dinámicamente**: el único método que permite la reutilización de direcciones IP. El administrador de la red asigna un rango de direcciones IP para el DHCP y cada ordenador cliente de la LAN tiene su software de comunicación TCP/IP configurado para solicitar una dirección IP del servidor DHCP cuando su tarjeta de interfaz de red se inicie. El proceso es transparente para el usuario y tiene un periodo de validez limitado.

**c) Dirección IP fija:**

Es una IP asignada por el usuario de manera manual. Los sitios de Internet que por su naturaleza necesitan estar permanentemente conectados (servidores de correo, FTP públicos, etc.), generalmente tienen una dirección IP fija, es decir, no cambia con el tiempo.

**d) Dirección IP Local o Privada:**

La dirección IP local es la que corresponde a la red local de una casa u oficina (suele ser del tipo 172.26.0.1 ó 192.168.1.1). Se utiliza para acceder localmente a equipos instalados en su red local.

**e) Dirección IP Remota o Pública:**

Puede ser fija o dinámica, (suele ser del tipo 217.127.3.11 ó 81.32.123.14). Se utiliza para acceder remotamente a través de Internet a equipos instalados en una red local.

**f) Puertos:**

Un número de puerto define un servicio o aplicación concretos para que el servidor receptor (por ej. una cámara de red) sepa cómo procesar los datos entrantes. Cuando un ordenador 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. Algunas aplicaciones utilizan los números de puerto que les ha preasignado la Autoridad de Números Asignados de Internet (IANA). Por ejemplo, un servicio web vía http se suele asignar al puerto 80 de una cámara de red.

**g) Protocolos de transporte de datos para vídeo en red:**

El Protocolo de control de transmisión (TCP, Transmission Control Protocol) y el Protocolo de datagramas de usuario (UDP, User Datagram Protocol) son los protocolos basados en IP que se utilizan para enviar datos. Estos protocolos de transporte actúan como portadores para muchos otros protocolos. Por ejemplo, HTTP (Hyper Text Transfer Protocol), que se utiliza para visualizar páginas web en servidores de todo el mundo a través de Internet, se realiza en TCP.

TCP proporciona un canal de transmisión fiable basado en la conexión. Gestiona el proceso de división de grandes bloques de datos en paquetes más pequeños y garantiza que los datos enviados desde un extremo se reciban en el otro.

UDP es un protocolo sin conexión que no garantiza la entrega de los datos enviados, dejando así todo el mecanismo de control y comprobación de errores a cargo de la propia aplicación. No proporciona transmisiones de pérdida de datos, por lo que no provoca retrasos adicionales.

*Tabla6.2 Protocolos y puertos TCP/IP habituales utilizados para el vídeo en red.*

| **Protocolo** | **Protocolo de transporte** | **Puerto** | **Uso habitual** | **Uso de vídeo en red** |
|---|---|---|---|---|
| FTP (Protocolo de transferencia de ficheros) | TCP | 21 | Transferencia de archivos a través de Internet/intranets | Transferencia de imágenes o vídeo desde un codificador de vídeo/cámara de red a un servidor FTP o a una aplicación |
| SMTP (Protocolo simple de transferencia de correo) | TCP | 25 | Envío de mensajes de correo electrónico | Un codificador de vídeo/cámara de red puede enviar imágenes o notificaciones de alarma utilizando su cliente de correo electrónico integrado |
| HTTP (Protocolo de transferencia de hipertexto) | TCP | 80 | Se utiliza para navegar por la red, por ejemplo, para recuperar páginas web de servidores | Es el modo más habitual para transferir vídeo de un codificador de vídeo/cámara de red, en el que el dispositivo de vídeo en red funciona básicamente como servidor web que pone el vídeo a disposición del usuario o del servidor de aplicaciones que lo solicita |

| Protocolo | Protocolo de transporte | Puerto | Uso habitual | Uso de vídeo en red |
|---|---|---|---|---|
| HTTPS (Protocolo de transferencia de hipertexto sobre capa de sockets seguros) | TCP | 443 | Acceso seguro a páginas web con tecnología de cifrado | Transmisión segura de vídeo procedente de codificadores de vídeo/cámaras de red |
| RTP (Real Time Protocol) | UDP/TCP | No definido | Formato de paquete RTP estandarizado para la entrega de audio y de vídeo a través de Internet (a menudo utilizado en sistemas de transmisión multimedia o videoconferencia) | Un modo habitual de transmitir vídeo en red basado en H.264/MPEG y de sincronizar vídeo y audio, ya que RTP proporciona la numeración y la datación secuencial de paquetes de datos, lo que permite volver a unirlos en el orden correcto. La transmisión se puede realizar mediante unidifusión o multidifusión |
| RTSP (Protocolo de transmisión en tiempo real) | TCP | 554 | Utilizado para configurar y controlar sesiones multimedia a través de RTP | |

*Fuente: http://www.axis.com/es/products/video/about_networkvideo/internet.htm*

**h) NAT (Network address translation – 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 enrutador compatible con NAT. Con esta técnica, el enrutador puede traducir una dirección IP privada en una pública sin el conocimiento del host que realiza el envío.

**i) Reenvío de puertos:**

Para acceder a cámaras ubicadas en una LAN privada a través de Internet, la dirección IP pública del enrutador se debería usar junto con el número de puerto correspondiente del codificador de vídeo o la cámara de red en la red privada.

Los paquetes de datos entrantes llegan al enrutador a través de su dirección IP pública (externa) y un número de puerto específico. El enrutador está configurado para reenviar los datos que entran por un número de puerto predefinido a un dispositivo específico de la parte del enrutador correspondiente a la red privada. A continuación, el enrutador sustituye la dirección del emisor por su propia dirección IP privada (interna). Para el cliente receptor, el enrutador es el origen de los paquetes. Con los paquetes de datos salientes ocurre lo contrario. El enrutador sustituye la dirección IP privada del dispositivo origen por la IP pública del propio enrutador antes de enviar los datos a través de Internet.

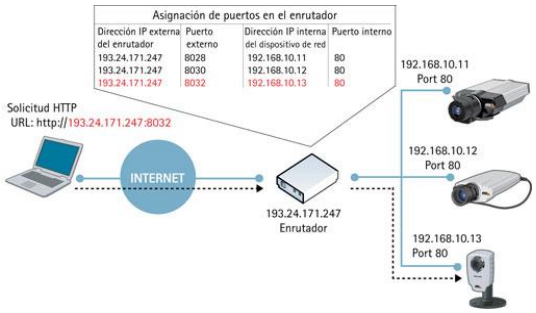



*Figura 6.11 Ejemplo de direccionamiento lógico en cámaras IP*
*Fuente: http://www.axis.com/es/products/video/about_networkvideo/internet.htm*

### 6.5.3 Ventaja de una vigilancia mediante Cámaras IP

**a) Accesibilidad Remota:**

Puede acceder al vídeo en tiempo real en cualquier momento desde cualquier ordenador, esté donde esté. El vídeo puede almacenarse en ubicaciones remotas, por motivos de comodidad o seguridad, y la información puede transmitirse a través de la red LAN o de Internet. Esto significa que incluso las empresas con establecimientos pequeños y dispersos pueden hacer un uso eficaz de la solución de vigilancia IP en aplicaciones de seguridad o supervisión a distancia.

**b) Flexibilidad:**

Las cámaras pueden colocarse prácticamente en cualquier lugar; pueden conectarse a una conexión LAN, xDSL, módem o inalámbrica o a un teléfono móvil.

**c) Escalabilidad:**

Para ampliar una solución de vídeo sobre red basta con añadir las cámaras una a una. El proceso es rápido; normalmente se conecta y empeza a enviar imágenes a través de la red. El sistema más grande instalado hasta la fecha emplea más de 2.000 cámaras.

**d) Rentabilidad:**

El vídeo sobre red es muy rentable, por muchos motivos: la infraestructura de cable existente y los equipos informáticos normales pueden reutilizarse, por lo que la inversión inicial es reducida. Además, al disminuir el número de equipos necesarios, se recorta el coste de mantenimiento. En una solución de vídeo sobre red, hay menos equipos que mantener que en un sistema analógico tradicional y,

por tanto, menos componentes susceptibles de desgaste. Las imágenes se almacenan en discos duros informáticos, que son una solución más práctica y económica que las cintas de vídeo.

**e) Integración y funcionalidad actualizable:**

La tecnología digital está cada día más extendida, y sustituye progresivamente a las soluciones analógicas.

### 6.5.4 Vigilancia IP Inalámbrica para Aplicaciones de Seguridad

La Vigilancia IP Inalámbrica comprende dos tecnologías la de transmisión inalámbrica en exteriores y la de Vídeo Vigilancia en red que, combinadas crean un potente sistema de seguridad.

IP es la abreviatura de Internet Protocol, el protocolo de comunicaciones más común entre redes informáticas e Internet. Una aplicación de Vigilancia IP crea secuencias de vídeo digitalizado que se transfieren a través de una red informática permitiendo la monitorización remota allá donde llegue la red así como la visualización de imágenes y la monitorización desde cualquier localización remota a través de Internet.

Los sistemas Ethernet inalámbricos proporcionan una solución sencilla. Las cámaras modernas de seguridad y vídeo vigilancia pueden convertir las imágenes en paquetes de protocolo IP que pueden ser transmitidos fácilmente usando sistemas multipunto y punto a multipunto. Las cámaras en múltiples localizaciones se conectan fácilmente a los bridges inalámbricos (Unidades de suscriptor), que envían los datos a una Unidad de Estación Base inalámbrica localizada generalmente en un comando de seguridad de la organización y en el centro de control.

Si es preciso, las soluciones punto a punto pueden ser usadas para conectar a un lugar remoto bajo vigilancia de hasta 70 kilómetros de distancia del centro de comandos.
El vídeo de alta resolución recogido de todas las localizaciones puede descargarse a una pantalla de visualización del centro de comando y control.

#### 6.5.4.1 Funcionamiento de la Vigilancia IP Inalámbrica

La Vigilancia IP inalámbrica puede separarse en dos funciones principales: monitorización y vigilancia.

- *La monitorización*, se implementa cuando el usuario final quiere visualizar la acción en áreas cubiertas por las cámaras.
- *La función de vigilancia* se usa cuando la investigación post evento u otros requerimientos precisan almacenamiento de datos.

**a) La Cámara de red:**

La tecnología de la cámara de red hace posible tener una cámara en una localización y visualizar vídeo en directo desde otra localización a través de la red/Internet. Si un edificio está equipado con una red IP, entonces la infraestructura necesaria para incorporar cámaras ya existe.

Cuando también hay ordenadores en el edificio no se requiere equipamiento adicional para visualizar las imágenes que proporciona la cámara.

Las imágenes pueden visualizarse de la forma más simple a través de un navegador web desde el monitor del ordenador y en forma de solución de seguridad más compleja con la ayuda de un software dedicado.

En los casos en los que ya existen cámaras analógicas instaladas, se pueden emplear servidores de vídeo para digitalizar la señal analógica, y entonces se pueden incorporar esas cámaras al sistema de Vigilancia IP Inalámbrica y permitir que estas imágenes estén disponibles en cualquier lugar que sea necesario.

Una cámara de red moderna generalmente incluye una lente, un filtro óptico, un sensor de imágenes, un digitalizador de imágenes, un compresor de imágenes y un servidor web así como interfaces de red y de conexión telefónica vía modem.

Las cámaras más avanzadas incluyen además muchas otras atractivas funciones como detección de movimiento, entradas y salidas de alarma y soporte al correo electrónico.

**b) La tecnología de redes inalámbricas:**

Las redes inalámbricas ofrecen mayores capacidades a un coste significativamente inferior al de las redes de datos con cables. Fiables y fáciles de desplegar, presentan dos variedades principales: los sistemas punto a punto y los sistemas punto a multipunto.

Para aplicaciones de seguridad y vigilancia los sistemas punto a multipunto son las más relevantes, aunque los sistemas punto a punto también pueden ser usados para largas distancias y anchos de banda mayores.

**c) Sistemas Inalámbricos Punto a multipunto:**

Usando transmisores de radio de paquetes IP, interfaces Ethernet estándar y un diseño fácil de desplegar, estos sistemas permiten conexiones de red de alta

velocidad a múltiples switches Ethernet, routers, o PC's desde una única localización.

El sistema consiste en múltiples bridges inalámbricos, denominadas unidades de suscriptor (Subscriber Units, SU), que comunican con una Unidad de Estación Base (Base Suscriber Unit, BSU) inalámbrica.

Las cámaras de red pueden conectarse a una SU, que puede estar convenientemente localizada allá donde se precise. Las Unidades Suscriptoras transmiten los datos digitales a una BSU localizada centralmente.

Las capacidades de transmisión varían desde los 11 a los 60Megabites por segundo y las distancias que pueden cubrir van desde unos 5 a 20 Kilómetros.

**d) Bridges Ethernet Inalámbricos Punto a Punto:**

Mientras que los sistemas punto a multipunto proporcionan conectividad de una a múltiples localizaciones, los bridges punto a punto conectan dos localizaciones. Estos sistemas ofrecen mayores capacidades a distancias más largas que los sistemas punto a multipunto.

Cuando se usan para vigilancia y seguridad, son ideales para transmitir datos de vídeo desde el sitio central local donde se localiza una Estación Base a un comando central y centro de control que está localizado en una posición lejana.

También son ideales para conectar con un lugar remoto bajo vigilancia situado hasta a 70 kilómetros de distancia del centro. Los sistemas punto a punto están disponibles en capacidades que van de los 11 a los 430 Mbps.

**e) Servidores de PC's y software:**

Aunque las imágenes JPEG generadas por un sistema de vigilancia IP son nativas para la mayoría de los navegadores web estándar, el verdadero valor de los productos de Vigilancia IP se aprecia mejor cuando se utiliza software de grabación y monitorización profesional, lo que convierte al servidor de PC's de una red en un grabador de vídeo en red (Network Video Recorder, NVR).

Mientras que el vídeo de la Vigilancia IP puede visualizarse directamente desde un navegador web sin necesidad de software dedicado, el uso de una aplicación de software en combinación con las cámaras es recomendable.
El software proporciona al usuario opciones de visualización más flexibles y, más importante, la capacidad de almacenar y gestionar el vídeo con un NVR.

El software dedicado se instala en los PC's para monitorización, almacenado, visualización y convenientemente la gestión de las imágenes de vídeo para crear una sinergia que ofrece un nivel superior de funcionalidad del sistema al de cualquier sistema analógico actual.

El software puede ser una aplicación autónoma para un único PC o una aplicación más avanzada basada en cliente/servidor que proporcione soporte a múltiples usuarios. Cualquier sistema desde una a miles de cámaras puede desplegarse y escalarse en incrementos de una cámara. En algunos casos, el usuario final puede seleccionar software para implementar soporte a múltiples sistemas como control de accesos y vídeo.

**f) Seguridad*:***

Aunque se usa principalmente como información de dominio público, Internet puede también ser usada para transferir todos los tipos de información sensibles.

Pese a esto, la Vigilancia IP incorpora medidas correctas de seguridad como firewalls y protección por contraseña.

**g) Ancho de Banda**

- ✓ **Vigilancia IP:** Actualmente la mayoría de las redes son Ethernet a 100 Mbps. En la práctica esto significa que el máximo ancho de banda disponible es aproximadamente 50 Mbps. Consecuentemente, una cámara de red, transmitiendo imágenes a la máxima resolución y al mayor ratio de imágenes por segundo (30 imágenes por segundo) puede consumir potencialmente 5 Mbps.

### 6.5.4.2 Ventajas de la Vigilancia IP Inalámbrica

***Las ventajas de la tecnología Inalámbrica***

A la hora de proporcionar protección de seguridad en exteriores las organizaciones a menudo se enfrentan a costes elevados y problemas de instalación. Para un creciente número de organizaciones sensibles a los temas de seguridad las redes inalámbricas ofrecen una solución de redes de vigilancia fiable que puede proporcionar seguridad al entorno externo más exigente.

**a) Despliegue rápido y sencillo:**

La tecnología inalámbrica, puede desplegarse prácticamente en cualquier sitio, incluyendo contenedores de agua, terrenos escarpados y localizaciones remotas. La instalación de redes inalámbricas lleva menos tiempo que instalaciones por cable.

**b) Viabilidad:**

Los costes de la fibra óptica son superiores a los de un sistema inalámbrico. Sólo unos kilómetros de fibra pueden costar cientos de miles de euros.

**c) Flexibilidad:**

Las soluciones inalámbricas proporcionan una flexibilidad nunca vista. Dado que la red de seguridad es inalámbrica las cámaras no tienen porque estar en una localización fija. Si es preciso las cámaras y las unidades de suscripción pueden moverse a una nueva localización sin problemas y pueden volver a estar reconectadas en pocos minutos.

**d) Alta capacidad:**

Las redes inalámbricas están disponibles en un amplio espectro de capacidades de ancho de banda desde 11 a 826 Mbps (Megabites por segundo). El sistema asegura la transmisión de vídeo de alta resolución en tiempo real que es necesaria para los sistemas de vigilancia.

**e) Fiabilidad:**

Los sistemas inalámbricos de gama alta aseguran una fiabilidad del 99,999%, permitiendo una seguridad sin prácticamente ninguna interrupción.

**f) Diseño para exteriores:**

Las redes inalámbricas para exteriores se confunden a menudo con la tecnología inalámbrica no apta para su uso en exteriores. Basadas en un protocolo especial, que permite la escalabilidad del sistema y la gestión necesaria para despliegues en exteriores, las redes inalámbricas para exteriores (o Wireless WAN's) son potentes

y versátiles al usarlas en aplicaciones de vigilancia y seguridad. Es importante que los usuarios finales distingan entre la tecnología para interiores y las tecnologías diseñadas para las demandas de los sistemas exteriores.

**g) La accesibilidad remota ahorra costes:**

Cualquier secuencia de vídeo, en directo o grabada puede ser visualizada desde cualquier lugar del mundo con conexión a Internet a través de redes inalámbricas o con cables. El acceso mejorado a través de una Intranet o de Internet proporciona un acceso más rápido e inmediato a las imágenes, a la vez que reduce sustancialmente los costes en desplazamientos y los tiempos empleados en ir desde o hacia las localizaciones de monitorización. Las imágenes también pueden almacenarse automáticamente en lugares externos para mejorar la seguridad.

**h) Escalabilidad:**

Permite aumentar el ratio de imágenes por segundo y la capacidad de almacenamiento incorporando discos duros y servidores de aplicaciones a la red. No hay limitaciones, cualquier ratio de imágenes por segundo es posible, para cualquier cámara y en cualquier momento.

**i) Convergencia de redes:**

Un único tipo de red (IP) gestiona la compañía para datos, vídeo, voz, etc. haciendo que la gestión sea más económica y efectiva.

**j) Menores costes de sistema:**

En muchas instalaciones, el sistema de Vigilancia IP ha demostrado ser una alternativa más económica. Redes abiertas y basadas en estándares, equipamiento de almacenamiento y servidores permiten elecciones más económicas.

**k) Mayor fiabilidad:**

El transporte de datos basado en IP permite el almacenamiento externo y la posibilidad de utilizar infraestructura redundante de servidores y almacenamiento. El software de gestión proporciona datos sobre el estado de los mismos en tiempo real así como información sobre medidas preventivas para mantener el sistema funcionando en los momentos de mayor rendimiento.

**l) Abierto e interoperable:**

La Vigilancia IP está basada en estándares abiertos y permite el uso de productos como switches, routers servidores y software de aplicación de diferentes fabricantes. Por esto se ofrecen opciones de mayor rendimiento y menor coste.

### 6.5.5 ANCHO DE BANDA NECESARIO PARA VISUALIZACIÓN Y GRABACIÓN DE CÁMARAS IP

**a) Ancho de banda:**

En conexiones a Internet el ancho de banda es la cantidad de información o de datos que se puede enviar a través de una conexión de red en un período de tiempo dado.

El ancho de banda se indica generalmente en bits por segundo (BPS), kilobites por segundo (kbps), o megabites por segundo (mps).

En las redes de ordenadores, el ancho de banda a menudo se utiliza como sinónimo para la tasa de transferencia de datos - la cantidad de datos que se puedan llevar de un punto a otro en un período dado (generalmente un segundo). Esta clase de ancho de banda se expresa generalmente en bits (de datos) por segundo (bps). En ocasiones, se expresa como bytes por segundo (Bps).

**b) Sistemas De Vigilancia Y Ancho De Banda:**

Para un perfecto funcionamiento imagen del sistema IP se debe tener en cuenta las siguientes características:

- El tamaño de la imagen: Cada sistema de visualización ofrece distintos tamaños para visualizar las cámara, a mayor tamaño mayor consumo de ancho de banda.
- La Frame por segundo: FPS es el número de fotogramas por segundo que envía el sistema. El mínimo número de fotogramas para ver video en Internet es de 15 FPS por segundo por cada cámara.

- Cada sistema de monitoreo tiene un numero de FPS determinado, si se instalan varias cámaras se debe dividir este por el numero de cámaras.

EJ: sistema de vigilancia con 30 FPS.

Si se tiene una cámara se tiene 30 FPS. Si se tiene 2 cámaras se tienen 15 FPS para cada cámara. Si se tiene 3 cámaras se tienen 10 FPS para cada cámara. Si se tiene 4 cámaras se tienen 7.5 FPS para cada cámara.

Mientras más cámaras tenga activas en modo de visualización es menor así como la velocidad de visualización viéndose lento y pausado.

- En un sistema de vigilancia reducido compuesto de 8 a 10 cámaras, se puede utilizar un conmutador de red básico de 100 Megabits (Mbit) sin tener que considerar limitaciones de ancho de banda. La mayoría de las empresas pueden implementar un sistema de vigilancia de este tamaño utilizando la red que ya tienen.

Cuando se implementan 10 o más cámaras, la carga de red se puede calcular con algunas reglas generales:

- Una cámara configurada para ofrecer imágenes de alta calidad a altas frecuencias de imagen utilizará aproximadamente de 2 a 3 Mbit/s del ancho de banda disponible de la red.
- De 12 a 15 cámaras, con una red troncal de un gigabit. Si se utiliza un conmutador compatible con un gigabit, el servidor que ejecuta el software de gestión de vídeo debería tener un adaptador para redes de un gigabit instalado.

**c) Calcular requisitos de almacenamiento:**

El tipo de compresión de vídeo utilizado es uno de los factores que afectan a los requisitos de almacenamiento. El formato de compresión H.264 es de lejos la técnica de compresión de vídeo más eficiente que existe actualmente. Sin asegurar calidad de imagen, un codificador H.264 puede reducir el tamaño de

un archivo de vídeo digital en más de un 80% comparado con el formato Motion JPEG y en más de un 50% con el estándar MPEG-4.

Esto significa que se necesita mucho menos ancho de banda de red y espacio de almacenamiento para un archivo de vídeo H.264.

- **Cálculo en H.264:**

*Tabla 6.3 Cálculo en H.264*
*Fuente:http://www.axis.com/es/products/video/about_networkvideo/bandwidth*

| *Cámara* | *Resolución* | *Velocidad binaria aprox. (kbps)* | *Imágenes por segundo* | *MB/hora* | *Horas de funciona-miento* | *GB/día* |
|---|---|---|---|---|---|---|
| No. 1 | CIF | 110 | 5 | 49.5 | 8 | 0.4 |
| No. 2 | CIF | 250 | 15 | 112.5 | 8 | 0.9 |
| No. 3 | 4CIF | 600 | 15 | 270 | 12 | 3.2 |
| *Capacidad total para las 3 cámaras y 30 días de almacenamiento = 135 GB* | | | | | | |

Velocidad binaria aprox./8 (bits en un byte) x 3.600s = KB por hora/1.000 = MB por hora MB por hora x horas de funcionamiento diarias/1.000 = GB por día GB por día por periodo de almacenamiento solicitado = Necesidades de almacenamiento.

- **Cálculo en MPEG-4:**

  Velocidad binaria aprox./8 (bits en un byte) x 3.600s = KB por hora/1.000 = MB por hora
  MB por hora x horas de funcionamiento diarias/1.000 = GB por día
  GB por día x periodo de almacenamiento solicitado = Necesidades de almacenamiento.

*Tabla 6.4 Cálculo en MPEG-4*
*Fuente:http://www.axis.com/es/products/video/about_networkvideo/bandwidth*

| *Cámara* | *Resolución* | *Velocidad binaria aprox. (kbps)* | *Imágenes por segundo* | *MB/hora* | *Horas de funciona-miento* | *GB/día* |
|---|---|---|---|---|---|---|
| No. 1 | CIF | 170 | 5 | 76.5 | 8 | 0.6 |
| No. 2 | CIF | 400 | 15 | 180 | 8 | 1.4 |
| No. 3 | 4CIF | 880 | 15 | 396 | 12 | 5 |
| *Capacidad total para las 3 cámaras y 30 días de almacenamiento = 204 GB* | | | | | | |

- **Cálculo en Motion JPEG:**

  Tamaño de imagen x imágenes por segundo x 3.600s = kilobyte (KB) por hora/1.000 = megabyte (MB)
  MB por hora x horas de funcionamiento diarias/1.000 = gigabyte (GB) por día
  GB por día x periodo de almacenamiento solicitado = Necesidades de almacenamiento.

  *Tabla 6.5 Cálculo en Motion JPEG*
  *Fuente:http://www.axis.com/es/products/video/about_networkvideo/bandwidt*

| *Cámara* | *Resolución* | *Velocidad binaria aprox. (kbps)* | *Imágenes por segundo* | *MB/hora* | *Horas de funciona-miento* | *GB/día* |
|---|---|---|---|---|---|---|
| No. 1 | CIF | 13 | 5 | 234 | 8 | 1.9 |
| No. 2 | CIF | 13 | 15 | 702 | 8 | 5.6 |
| No. 3 | 4CIF | 40 | 15 | 2160 | 12 | 26 |
| *Capacidad total para las 3 cámaras y 30 días de almacenamiento = 1.002 GB* | | | | | | |

### 6.5.6 EJEMPLOS DE CONFIGURACIONES DE SISTEMA DE VIGILANCIA POR MEDIO DE CAMARAS IP

**a) Sistema pequeño (1 a 30 cámaras)**

Un sistema pequeño suele estar formado por un servidor que ejecuta una aplicación de vigilancia que graba el vídeo a un disco duro local. Un mismo servidor visualiza y gestiona el vídeo. Aunque la mayor parte de la visualización y gestión se realizará en el servidor, un cliente (local o remoto) puede conectarse con el mismo objetivo.


*Figura 6.12 Sistema pequeño*
*Fuente:http://www.axis.com/es/products/video/about_networkvideo/bandwidth*

**b) Sistema mediano (25 a 100 cámaras)**

Una instalación típica de tamaño mediano tiene un servidor con almacenamiento adicional conectado a él. El almacenamiento suele estar configurado con RAID con el fin de aumentar el rendimiento y la fiabilidad. El vídeo normalmente se visualiza y gestiona desde un cliente, más que desde el mismo servidor de grabación.


*Figura 6.13 Sistema mediano*
*Fuente:http://www.axis.com/es/products/video/about_networkvideo/bandwidth*

**c) Sistema grande centralizado (de 50 hasta +1.000 cámaras):**

Una instalación de gran tamaño requiere un alto rendimiento y fiabilidad para gestionar la gran cantidad de datos y el ancho de banda. Esto requiere múltiples servidores con tareas asignadas. Un servidor maestro controla el sistema y decide qué tipo de vídeo se almacena y en qué servidor de almacenamiento. Al haber servidores de almacenamiento con tareas asignadas, se puede equilibrar la carga. En una configuración de estas características, también es posible escalar el sistema añadiendo más servidores de almacenamiento cuando se necesite y efectuar mantenimiento sin cerrar todo el sistema.


*Figura 6.14 Sistema amplio centralizado*
*Fuente:http://www.axis.com/es/products/video/about_networkvideo/bandwidth*

**d) Sistema grande distribuido (de 25 hasta +1.000 cámaras):**

Cuando varias ubicaciones requieren vigilancia con una gestión centralizada, se pueden utilizar sistemas de grabación distribuidos. Cada ubicación graba y almacena el vídeo procedente de las cámaras locales. El controlador maestro puede visualizar y gestionar las grabaciones en cada ubicación.

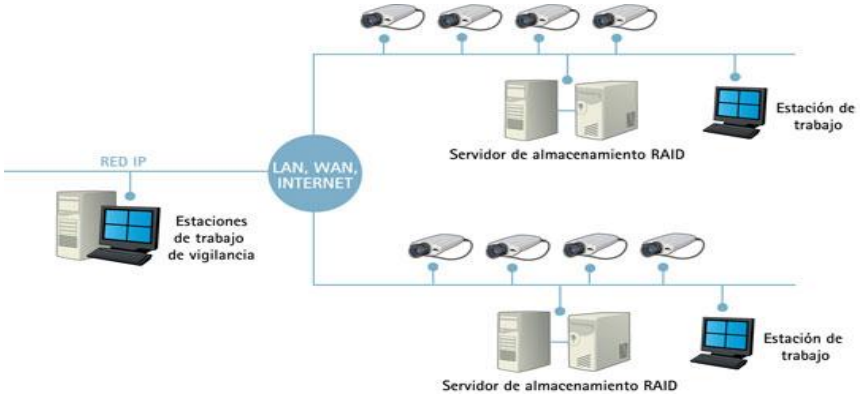



*Figura 6.15 Sistema grande distribuido*
*Fuente:http://www.axis.com/es/products/video/about_networkvideo/bandwidth*

## 6.6 Sistema de Vigilancia Ip para el SECAP – CEFIA

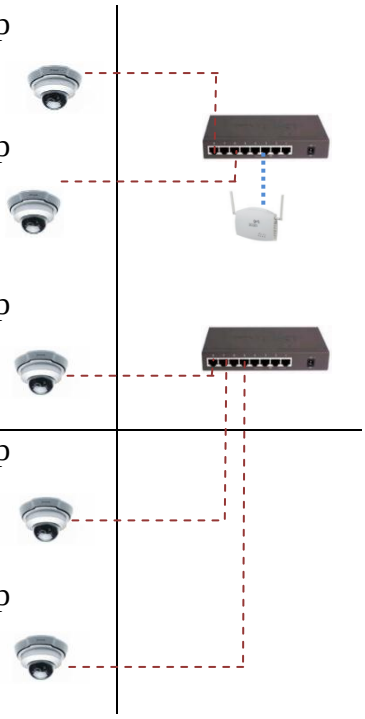
### 6.6.1 Análisis Técnico – Físico

***Topología física***: es la distribución física del cableado y los elementos físicos, y su forma de interconexión.
En las tablas 6.6, 6.7 y 6.8 se describe la distribución por áreas de los equipos del sistema de vigilancia Ip para el SECAP – CEFIA

- Las Áreas de Metal Mecánica, Mecánica Automotriz y Confecciones Industriales.

*Tabla 6.6 Distribución de Cámaras IP*

| | | |
|---|---|---|
| Área de Metal Mecánica | Taller de Soldadura | 2 cámaras Ip |
| | Maquinas Industriales | 1 cámaras Ip |
| Área de Mecánica Automotriz | Automóviles | 1 cámaras Ip |
| Área de Confecciones Industriales | Bodega | 2 cámaras Ip |
| | Maquinas de Confeccionar Ropa | 1 cámaras Ip |



- El Área Administrativa se desglosa de la siguiente forma:

*Tabla 6.7 Distribución de Cámaras IP*

| | | | |
|---|---|---|---|
| Piso 5 | Sala de Audiovisuales | 0 máquinas | |
| Piso 4 | Laboratorio Computación 2 | 16 máquinas | |
| | Laboratorio Computación 3 | 16 máquinas | |
| Piso 3 | Laboratorio de Mantenimiento | 3 máquinas | |
| | 3 Aulas | 0 máquinas | |
| Piso 2 | Laboratorio Computación 1 | 12 máquinas | |
| | G. Financiera | 2 máquinas | |
| | Recaudación | 2 máquinas | |
| | Oficina | 2 máquinas | |
| Piso 1 | Información Comercio y Servicios | 4 máquinas | |
| | Coordinación SECAP | 3 máquina | |
| Planta Baja | Biblioteca – Estadística | 4 máquina | |
| | BAR | 0 máquinas | |

- El Área de Electricidad y Electrónica

*Tabla 6.8 Distribución de Cámaras IP*

| | | |
|---|---|---|
| **Planta Alta** | | |
| Rectorado – Secretaria | 2 máquinas | |
| Lab. Máquinas Eléctricas | 0 máquinas<br>1 cámara Ip | |
| Lab. PLC | 4 máquinas<br>1 cámara Ip | |
| Lab. Instalaciones Electricas | 0 máquinas<br>1 cámara Ip | |
| **Planta Baja** | | |
| Lab. Computación | 16 máquinas<br>1 cámara Ip | |
| Coordinación de Electricidad y Electrónica | 2 máquinas | |
| Taller de Cazado | 1 máquinas<br>1 cámara Ip | |

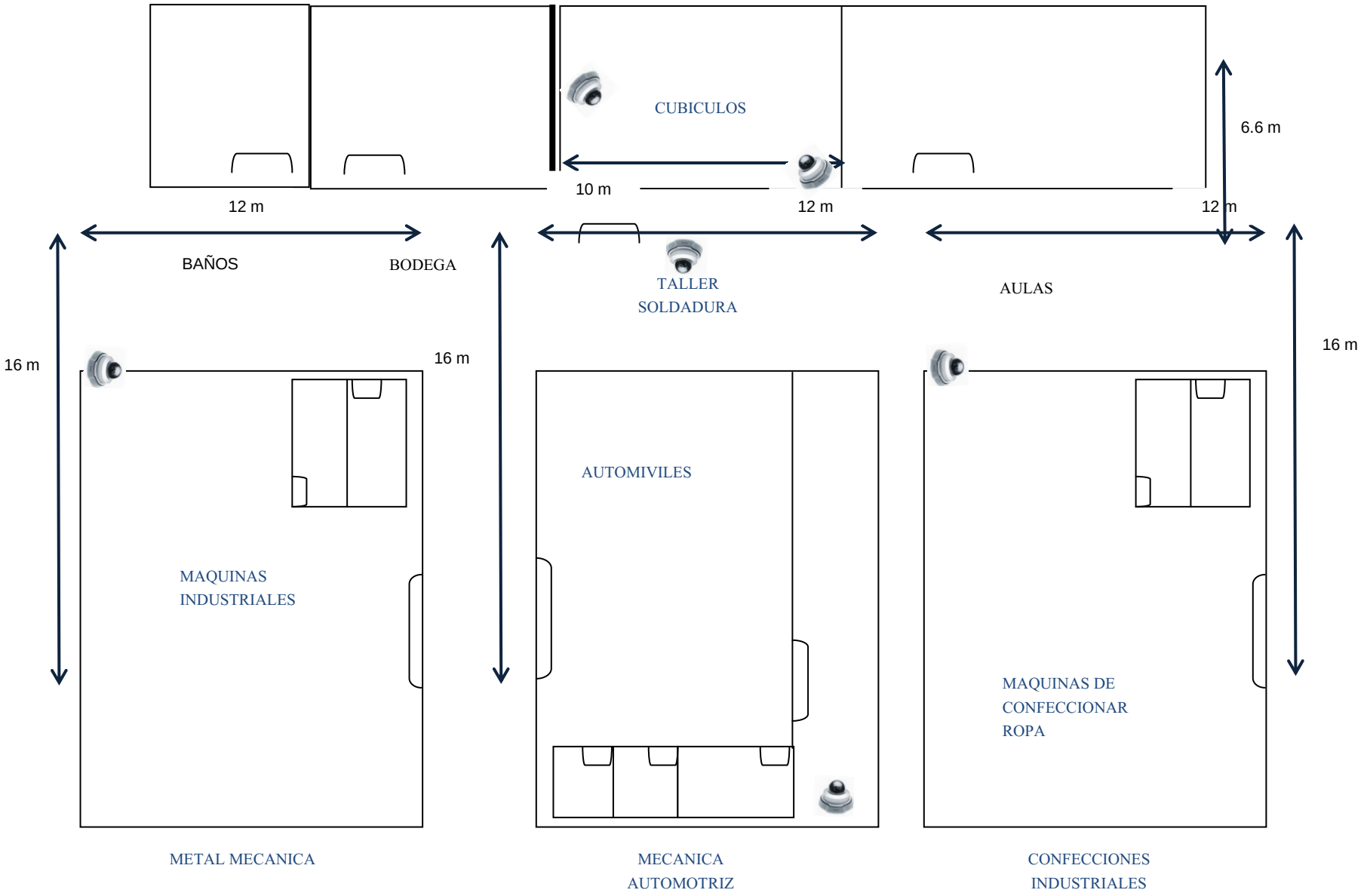
En la tabla 6.9 se identifican los equipos que actualmente posee la red, con los equipos que se requiere para la Vigilancia IP.

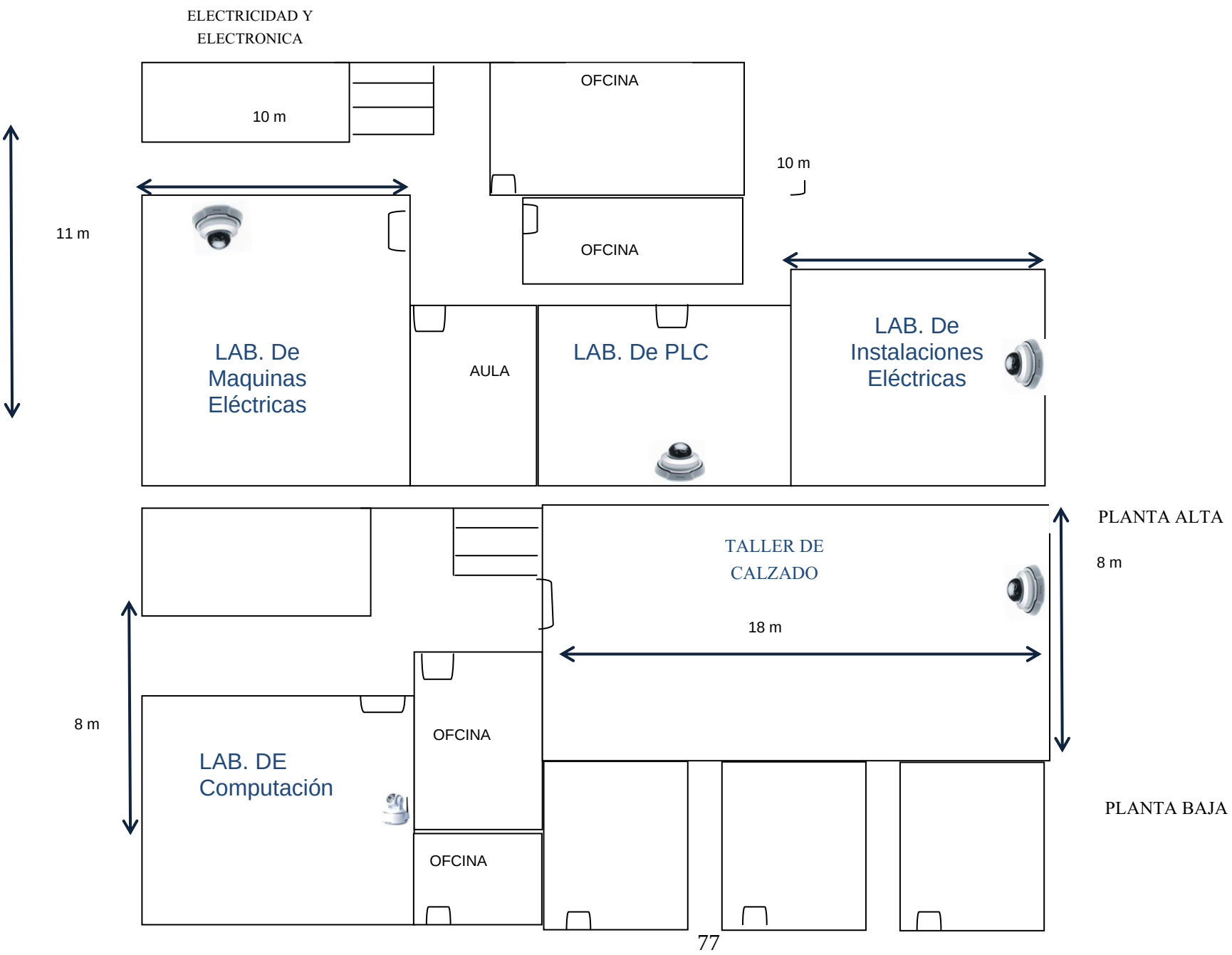
*Tabla 6.9 Descripción de equipos actuales y de vigilancia Ip*

| **Equipos Actuales del SECAP- CEFIA** | **Descripción** | **Equipos para Sistemas de Vigilancia Ip** | **Descripción** |
|---|---|---|---|
|  | 90 Computadoras |  | Cámara Ip Domo |
|  | CNSH-1600 16-Port Fast Ethernet Switch |  | Cámara Ip Inalámbrica |
|  | DGS-1224T 24-ports Gigabit Smart Switch |  | Switch de 8 Puertos/ 4PoE |
|  | DIR-600 wireless 150 router with 4-port10/100mbps switch |  | Access Point 3Com |
|  | DSL-500B **Router ADSL con puertos Ethernet** | | |
|  | Router D-link Dsl-524b 4 Puertos Lan Adsl | | |
| ..... | Conexión UTP | ---------- | Conexión PoE |

En la figura 6.16 se esquematiza la vigilancia con cámaras Ip para la Institución.

*Figura 6.16 Diagrama de Vigilancia Ip*




ELECTRICIDAD Y
ELECTRONICA
10 m
OFCINA
10 m
11 m
OFCINA
LAB. De
Maquinas
Eléctricas
AULA
LAB. De PLC
LAB. De
Instalaciones
Eléctricas
PLANTA ALTA
TALLER DE
CALZADO
8 m
18 m
8 m
OFCINA
LAB. DE
Computación
OFCINA
PLANTA BAJA

### 6.6.2 Análisis Lógico

**a) Subnetting:**

Es el proceso de descomposición de una red IP en pequeñas subredes. Las subredes son una serie de redes contenidas en una red; creadas por subdivisiones del campo de direcciones de hosts originándose así un campo de subredes.

- *Subredes Clase C:* Bits son robados del campo de hosts. Esto crea un campo de subred en la dirección IP.

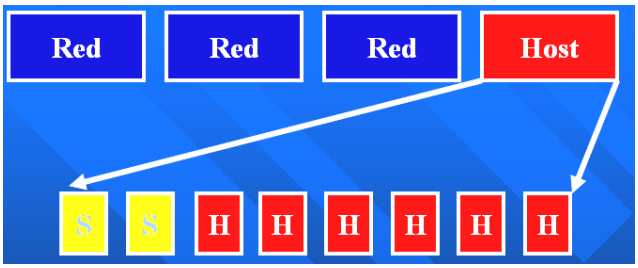



*Figura 6.17 Subnetting Clase C*
*Fuente: ubv2006.galeon.com/Programas/Subnetting.ppt*

Dos bits robados del campo de hosts para formar una tercera capa de jerarquía (*Un campo de subred*).

Dos bits mínimo y hasta un máximo de seis pueden ser robados de una red clase C.

El número de subredes "utilizables" creadas es calculado usando la siguiente fórmula:

$$\textbf{\# Subredes u. creadas} = 2^{\textbf{\# bits robados}} - 2$$

Se le resta 2 por la dirección de red y la dirección de broadcast – Ninguna de estas direcciones es válida es decir no puede ser usada para Host.

**b) VLSM:**

*(Variable Length Subnet Mask),* Máscara de Subred de Longitud Variable; a lo largo de la evolución informática resultó que el protocolo IpV4 fué teniendo un problema que se repitió varias veces y que al final ha desembocado en el actual IpV6, este problema no era otro que la falta de direcciones Ip. Las Clases A, B y C estrictamente y no disponemos de subnetting; es un desperdicio de Ip's para muchos casos y limitados a la hora de trabajar con ciertas infraestructuras de red.

- **El VLSM no entiende de clases de red** es decir podemos tener una Ip 192.132.34.67 con una máscara de subred 255 255 128.0 perfectamente y no se considerará ni una clase C ni una clase B se considerará mejor una ip 192.132.34.67/17. Uso más eficiente del espacio de direcciones.

- Soporta subredes no contiguas (subredes separadas por parte de otra subred).

- Reglas de asignación de direcciones

  - El espacio de direcciones en el que el campo subred es 0 ó -1 para una máscara de una cierta longitud, puede ser utilizado en una subred con una máscara de menor longitud.

  - Bajo una cierta máscara, las direcciones con campos de subred o host 0 o -1 no pueden ser utilizados

  - El espacio de direcciones asignado bajo una máscara no puede ser asignado bajo otra máscara (prefijo más largo).

**c) VLAN:**

(*Red de área local virtual* o *LAN virtual*) es una red de área local que agrupa un conjunto de equipos de manera lógica y no física; la comunicación entre los diferentes equipos en una red de área local está regida por la arquitectura física. Gracias a las redes virtuales (VLAN), es posible liberarse de las limitaciones de la arquitectura física (limitaciones geográficas, limitaciones de dirección, etc.), ya que se define una segmentación lógica basada en el agrupamiento de equipos.

- **Tipos de VLAN**

Se han definido diversos tipos de VLAN, según criterios de conmutación y el nivel en el que se lleve a cabo:

- La **VLAN de nivel 1** (también denominada *VLAN basada en puerto*) define una red virtual según los puertos de conexión del conmutador.

- La **VLAN de nivel 2** (también denominada *VLAN basada en la dirección MAC*) define una red virtual según las direcciones MAC de las estaciones. Este tipo de VLAN es más flexible que la VLAN basada en puerto, ya que la red es independiente de la ubicación de la estación.

- La **VLAN de nivel 3**: existen diferentes tipos de VLAN de nivel 3:
  - La **VLAN basada en la dirección de red** conecta subredes según la dirección IP de origen de los datagramas. Este tipo de solución brinda gran flexibilidad, en la medida en que la configuración de los conmutadores cambia automáticamente cuando se mueve una estación. En contrapartida, puede haber una ligera disminución del rendimiento, ya que la información contenida en los paquetes debe analizarse detenidamente.

  - La **VLAN basada en protocolo** permite crear una red virtual por tipo de protocolo (por ejemplo, TCP/IP, IPX, appletalk, etc.). Por lo tanto, se pueden agrupar todos los equipos que utilizan el mismo protocolo en la misma red.

- **Ventajas de la VLAN**

  La VLAN permite definir una nueva red por encima de la red física y, por lo tanto, ofrece las siguientes ventajas:

  - Mayor flexibilidad en la administración y en los cambios de la red, ya que la arquitectura puede cambiarse usando los parámetros de los conmutadores.
  - Aumento de la seguridad, ya que la información se encapsula en un nivel adicional y posiblemente se analiza.
  - Disminución en la transmisión de tráfico en la red.

### 6.6.2.1 Diseño Lógico para la red del SECAP – CEFIA

***Topología lógica:*** es la forma de circulación y la regulación de la información. Para el diseño lógico de la red del SECAP – CEFIA se utilizó la técnica VLSM *(Máscara de Subred de Longitud Variable)* en el direccionamiento de la IP's para las cámaras y las máquinas de la Institución.

Se estableció 3 VLAN's basadas en el direccionamiento de la RED; la primera y segunda VLAN lo conforma las máquinas del Establecimiento y la tercera VLAN las cámaras IP.

- Primera y Segunda VLAN en Área Administrativa con la Área de Electricidad y Electrónica son las que poseen máquinas.

*Tabla 6.10 Diseño Lógico de la Primera y Segunda VLAN*

| RED | Dirección de Red | Broadcast | Gateway | Rango | Mascara |
|---|---|---|---|---|---|
| **Área Administrativa 65 Máquinas** | 192.168.0.0/25 | 192.168.0.127 | 192.168.0.1 | .2-.126 | 255.255.255.128 |
| **Área de Electricidad y Electrónica 25 Máquinas** | 192.168.0.128/27 | 192.168.0.159 | 192.168.0.129 | .129-.158 | 255.255.255.224 |
| | | | | | |

- Tercera VLAN Área Metal Mecánica, Mecánica Automotriz y Confecciones Industriales, Área Administrativa y la Área de Electricidad.

*Tabla 6.11 Diseño Lógico de la Tercera VLAN*

| RED | Dirección de Red | Broadcast | Gateway | Rango | Mascara |
|---|---|---|---|---|---|
| **Áreas Administrativa, Electricidad y Electrónica, Metal Mecánica, Mecánica Automotriz y Confecciones Industriales 20 Cámaras** | 192.168.0.160/27 | 192.168.0.191 | 192.168.0.161 | .162-.190 | 255.255.255.224 |

La figura 6.18 esquematiza las VLAN's para la red del SECAP – CEFIA.

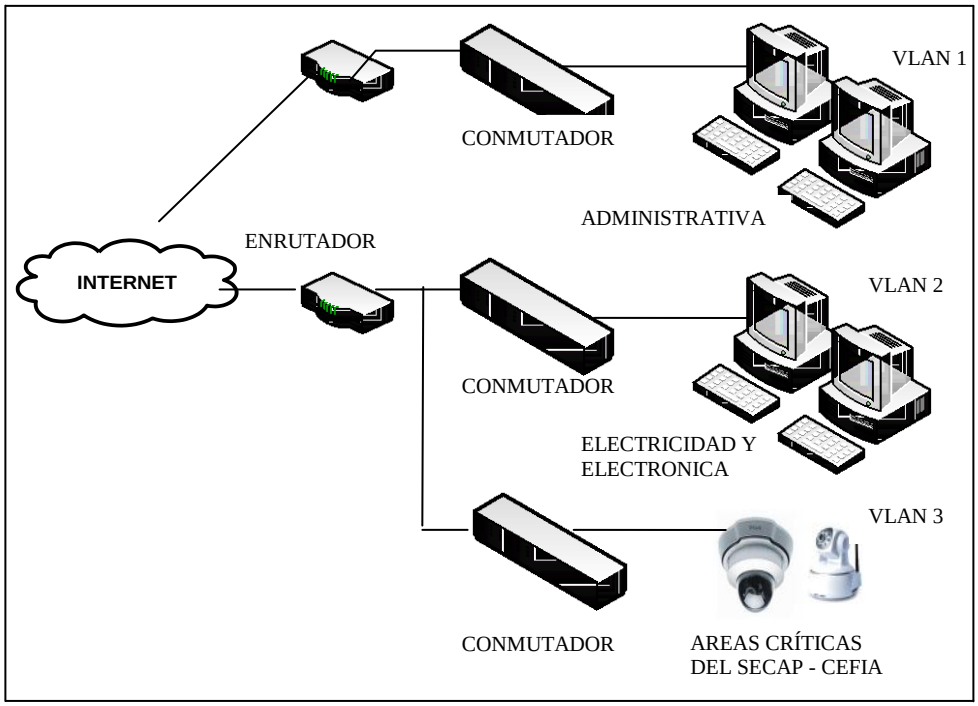



*Figura 6.18 Diseño de VLAN en el SECAP – CEFIA*

### 6.6.3 Análisis de requerimientos de almacenamiento y transferencia de datos del sistema de vigilancia Ip para el SECAP – CEFIA.

*Tabla 6.12 Requerimientos de almacenamiento y transferencia de datos.*

| **Cámara** | **Formato** | **Velocidad binaria aproximada** | **GB/día** |
|---|---|---|---|
| 11 Cámara Seguridad Ip DLINK DCS-6110 | MPEG - 4 | 3.2 Mbps | 18Gb/día |
| 9 Cámara Ip Inalámbrica | H.264 | 1.8 Mbps | 10Gb/día |

El SECAP – CEFIA para la implementación de este sistema de seguridad necesita un AB (ancho de banda) de 5 Mbps más 568.5 Kbps que consumen en la parte pedagógica, operativa y de administración.

### 6.6.4 Análisis Económico

Estadísticamente la presente investigación se desglosa en tablas que reflejan el aspecto económico que implica la posible instalación del Sistema de Seguridad Ip en el SECAP – CEFIA.

En la tabla 6.13 consta el analiza precios de los equipos necesarios para el sistema de vigilancia Ip.

*Tabla 6.13Analisis de precio de equipos.*

| **Equipos** | **Cantidad** | **Precio Unitario** | **Precio Total** |
|---|---|---|---|
| Cámara Seguridad Ip D - LINK DCS-6110 | 11 | 550,00 | 6050,00 |
| Switch D-LINK DES-1008P 8-Port 10/100M | 3 | 192,25 | 576,75 |
| 3 Com Access Point 3150 | 1 | 392,16 | 392,16 |
| Camara Ip Inalambrica | 9 | 180,00 | 1620,00 |
| Rollo Cable UTP Categoría 5e | 1 | 95,00 | 95,00 |
| Conectores Rj45 Cat5e (10 Unid) | 2 | 2,50 | 5,00 |
| **Total Equipos:** | | | **8738,91** |

La tabla 6.14 se encuentra un aproximado del pago por servicio de internet al momento de ensanchar el ancho de banda para el sistema de vigilancia mediante cámaras Ip.

*Tabla 6.14 Análisis económico por servicio de internet*

| **Servicio de Internet** | **Pago Mensual del Servicio de Internet** | **Pago anual del Servicio de Internet** |
|---|---|---|
| 3891.2Kbps | 372,40 | 4468,00 |
| 1843.2Kbps | 270,00 | 3240,00 |
| **Total** | **642,40** | **7708,00** |

La tabla 6.15 y 6.16 presenta el pago por el servicio de guardianía privado y lo que actualmente la Institución cancela por el servicio de Internet.

*Tabla 6.15 Cancelación por Servicio de Guardianía Privado*

| **# de Guardias** | **Pago mensual del Servicio de Guardianía** | **Pago anual del Servicio de Guardianía** |
|---|---|---|
| 2 | 2976,00 | 35712,00 |

*Tabla 6.16 Cancelación por Servicio de Internet*

| **Servicio de Internet** | **Pago Mensual del Servicio de Internet** | **Pago anual del Servicio de Internet** |
|---|---|---|
| 512Kbps | 49,00 | 588,00 |
| 512Kbps | 75,00 | 900,00 |
| **Total** | **124,00** | **1488,00** |

**Costo total de desembolsos para el Sistema de vigilancia Ip**

*Tabla 6.17 Cancelación por Sistema de Vigilancia Ip*

| **Descripción** | **Valores** |
|---|---|
| Equipos | 8738,91 |
| Servicio de Internet (anual) | 7708,00 |
| **Total** | **16446,91** |

**Costo total de gastos para el servicio de guardianía e internet**

*Tabla 6.18 Cancelación por Servicio de Guardianía e Internet*

| **Descripción** | **Valores** |
|---|---|
| Pago anual del Servicio de Guardianía | 35712,00 |
| Pago anual del Servicio de Internet | 1488,00 |
| **Total** | **37200,00** |

- Si el SECAP – CEFIA incrementara su seguridad con un guardia más a parte de los dos que existe actualmente en la Institución se tendría el siguiente egreso.

*Tabla 6.19 Cancelación por Servicio de Guardianía Incrementado*

| **# de Guardias a Incrementar** | **Pago mensual del Servicio de Guardianía** | **Pago anual del Servicio de Guardianía** |
|---|---|---|
| 1 | 1488,00 | 17856,00 |

- En las siguientes tablas se realiza la comparación de los gastos anuales que actualmente el SECAP – CEFIA realiza por servicio de guardianía e internet; en la *Tabla 6.21* muestra el desembolso anual que el Establecimiento tendría que hacer, en caso de optimizar su seguridad al incrementar el servicio de guardianía.

*Tabla 6.20 Cancelación Actual*

| **Descripción** | **Valores** |
|---|---|
| Pago anual del Servicio de Guardianía | 35712,00 |
| Pago anual del Servicio de Internet | 1488,00 |
| **Total** | **37200,00** |

*Tabla 6.21 Pago por Incremento del Servicio de Guardianía*

| **Descripción** | **Valores** |
|---|---|
| Incrementar el Servicio de Guardianía | 53568,00 |
| Pago anual del Servicio de Internet | 1488,00 |
| **Total** | **55056,00** |

### 6.6.5 Factibilidad

Técnicamente con el AB (ancho de banda) actual de la Institución no es posible incrementar el Sistema de Vigilancia Ip por consiguiente se debe incrementar el AB(ancho de banda) a un valor de 5Mbps lo que ocasiona un egreso $7708.00 según la tabla 6.14.

Para un mejor control y administración de la Red debería existir un profesional que se dedique al mantenimiento y administración de la Red.

*Tabla 6.22 Cancelación del Administrador de Red*

| **Administrador de la Red** | **Pago mensual del Administrador de la Red** | **Pago anual del Administrador de la Red** |
|---|---|---|
| 1 | 800,00 | 9600,00 |
| 1 Área de Mantenimiento | 200,00 | 2400,00 |

En cuanto se refiere a la Factibilidad Económica se debe realizar un análisis de Ingresos y Egresos anuales así como también de parámetros económicos tales como:

VAN --- Valor Actual Neto

TIR --- Tasa de retorno interna

PR --- Tiempo de recuperación de la Inversión

Que indiquen si el sistema es rentable.

A continuación se realiza el dicho análisis Económico:

***Egresos 1:***

*Tabla 6.23 Egresos Anuales*

| **Descripción** | **Valores** |
|---|---|
| Equipos | 8738,91 |
| Servicio de Internet (anual) | 7708,00 |
| Administrador de Red | 9600,00 |
| Mantenimiento de la Red | 2400,00 |
| **Total** | **28446,91** |

***Egreso 2:***

*Tabla 6.24 Egreso al Incrementar el Servicio de Guardianía*

| **Descripción** | **Valores** |
|---|---|
| Incrementar el Servicio de Guardianía | 53568,00 |

Si el SECAP – CEFIA optimiza la Seguridad de sus instalaciones, por medio de Cámaras Ip tendría el siguiente ahorro anual haciendo comparación con la otra opción que es de incrementar el Servicio de Guardianía.

*Tabla 6.25 Ahorro anual*

| **Descripción** | **Valores** |
|---|---|
| Ahorro anual con el Sistema de Vigilancia Ip | 25121,09 |

*Tabla 6.26 Análisis de la Recuperación de la inversión*

| ***RESUMEN DE FLUJOS NETOS DE EFECTIVO*** | | | | | | |
|---|---|---|---|---|---|---|
| ***ENTRADAS DE EFECTIVO*** | ***AÑO 0*** | ***AÑO 1*** | ***AÑO 2*** | ***AÑO 3*** | ***AÑO 4*** | ***AÑO 5*** |
| Ingreso equipos no financiados | 8738,91 | | | | | |
| Instalación de equipos | 0,00 | | | | | |
| Ingreso por servicio medido | | 25121,09 | 25121,09 | 25121,09 | 25121,09 | 25121,09 |
| Ingreso cancelación antes de vida útil | | | | | | 2184,73 |
| ***TOTAL*** | ***8738,91*** | ***25121,09*** | ***25121,09*** | ***25121,09*** | ***25121,09*** | ***27305,82*** |
| ***SALIDAS DE EFECTIVO*** | | | | | | |
| Costos NRC | 9600,00 | | | | | |
| Costos operativos NC | | 19708,00 | 19708,00 | 19708,00 | 19708,00 | 19708,00 |
| Costos equipos | 8738,91 | | | | | |
| ***TOTAL*** | ***18338,91*** | ***19708,00*** | ***19708,00*** | ***19708,00*** | ***19708,00*** | ***19708,00*** |
| Flujos netos de efectivo FNE | -9600,00 | 5413,09 | 5413,09 | 5413,09 | 5413,09 | 7597,82 |
| FNE acumulados | -9600,00 | -4186,91 | 1226,18 | 6639,27 | 12052,36 | 19650,18 |
| Recuperación | | 1,77 | | | | |
| Flujos netos de efectivo FNE a valor presente | -9600,00 | 4707,03 | 4093,07 | 3559,19 | 3094,95 | 3777,46 |
| FNE acumulados a valor presente | -9600,00 | -4892,97 | -799,89 | 2759,30 | 5854,25 | 9631,71 |
| Recuperación con flujos descontados | | 2,04 | | | | |

*Tabla 6.27 Inversiones y Costos*

| **Descripción** | **Inversiones NRC** | **Costo RC** |
|---|---|---|
| | USD | Anuales |
| Administrador de la Red | 9600,00 | 9600,00 |
| Mantenimiento de la Red | | 2400,00 |
| Pago Internet | | 7708,00 |
| **TOTAL COSTOS** | 9600,00 | 19708,00 |

La evaluación se toma en cuenta el valor del dinero a través del tiempo o valor presente neto (VPN), la Tasa interna de retorno (TIR), y el período de recuperación de la inversión.

*Tabla 6.28 Parámetros de Evaluación Económica*

| | |
|---|---|
| Valor Presente Neto (VPN) | 9631,71 |
| Tasa Interna de Retorno (TIR) | 30,95% |
| Período de Recuperación (PR) | 1,77 |
| Período de Recuperación Descontado (PRD) | 2,04 |

Analizando la tabla 6.28 se puede observar que la Tasa Interna de Retorno (30,95%) es mayor que el (15%); y el tiempo de recuperación de la inversión es de 1,77 aproximadamente 2 años en la recuperación del Sistema de vigilancia Ip.