ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

DISEÑO E IMPLEMENTACION DE UN PROTOTIPO DE UN SISTEMA DE VIDEO VIGILANCIA PARA EL MONITOREO DE SEGURIDAD, ALERTA DE INTRUSION Y ALMACENAMIENTO DE VIDEO, PARA LA HOSTERIA D'MARCO'S

PROYECTO PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN ELECTRÓNICA Y TELECOMUNICACIONES

LUIS PABLO MORALES SALAZAR

DIRECTOR: Dr. Luis Corrales

CODIRECTOR: Msc. Carlos Herrera

Quito, Junio 2017

DECLARACIÓN

Yo, Luis Pablo Morales Salazar declaro bajo juramento que el trabajo aquí descrito es de mi autoría; que no ha sido previamente presentada para ningún grado o calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedo mis derechos de propiedad intelectual correspondientes a este trabajo, a la Escuela Politécnica Nacional, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normatividad institucional vigente.

_____

Luis Pablo Morales Salazar

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por Luis Pablo Morales Salazar, bajo mi supervisión.

_____

Dr. Luis Corrales

DIRECTOR DEL PROYECTO

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por Luis Pablo Morales Salazar, bajo mi supervisión.

_____

Ing. Carlos Herrera. Msc

CO-DIRECTOR DEL PROYECTO

AGRADECIMIENTO

A Dios, por ser esa guía y fortaleza que se necesita día a día.

A mis padres, Mercy y Luis, por su amor, apoyo, confianza y compresión en mi vida.

A mis hermanos, Marco y Martin por el apoyo y cariño, por estar ahí juntos siempre, en las buenas y malas.

A mi querida novia, Mercedes, por el apoyo en la consecución de esta meta y estar ahí junto a mí.

A mi amigo Patricio Montenegro, por su gran apoyo y amistad.

A mis amigos, con los que hemos compartido tanto y quienes de una u otra manera me ayudaron con sus consejos a conseguir mi objetivo.

A la Escuela Politécnica Nacional, por haberme transmitido tantos conocimientos científicos y de vida.

A la hostería D'Marco'S, por haberme brindado el apoyo y las facilidades para la realización del presente proyecto.

DEDICATORIA

A mis padres, que con sus sacrificios siempre estuvieron ahí junto mí,

A la suprema maestra, la vida

A mi amigo Jack.

CONTENIDO

ÍNDICE DE IMÁGENES

RESUMEN

El presente proyecto tiene como finalidad el diseño de un sistema de videovigilancia basado en Linux con la utilización de cámaras inalámbricas para el complejo turístico D'Marco'S en la ciudad de Puyo y la implementación de un prototipo del diseño propuesto.

El complejo turístico no presenta sistema de seguridad alguno y además incluye el domicilio del propietario. Ante la afluencia de turistas en el complejo y considerando la vulnerabilidad que representa el tener las instalaciones en una zona rural hace que la idea de tener un sistema de vigilancia sea de vital importancia.

Debido a la extensión del complejo una opción es el uso de un sistema de cámaras inalámbricas que se conectan con el servidor principal formando así un sistema híbrido entre conexiones cableadas y conexiones inalámbricas.

El sistema instalado permite el monitoreo local y remoto de huéspedes, visitantes, zonas vulnerables y alerta de intrusos. Posteriormente los eventos relevantes se almacenan en el servidor de video y se realiza un respaldo automático en un repositorio virtual. Para mayor eficiencia en el uso de almacenamiento se configura el sistema para almacenar únicamente cuando exista movimiento.

Con las pruebas realizadas con el prototipo se demostró que es una solución viable para la detección y almacenamiento de eventos en tiempo real, además se demostró que el prototipo es escalable y fácil de operar.

PRESENTACIÓN

La delincuencia en nuestra sociedad siempre está presente y cualquier tipo de esfuerzo económico en la implementación de un sistema que brinde seguridad debe ser contemplado como una inversión, ya que a más de proteger los bienes de una persona o empresa, también brinda tranquilidad al responsable de dichos bienes.

Ante esta realidad el presente proyecto pretende ser una solución viable para la implementación de un sistema de videovigilancia del complejo recreacional D'Marco'S, donde se pueda monitorear y gestionar el sistema de manera centralizada. A continuación se detalla el trabajo realizado en las siguientes secciones:

En el capítulo 1 se describe la situación del complejo y las tecnologías disponibles para solucionar el problema presentado.

En el capítulo 2 se establece el diseño del sistema en función de las necesidades descritas en el capítulo 1 y tomando en cuenta la infraestructura con la que se cuenta. Con esta información se dimensionan los equipos y el software a utilizarse.

En el capítulo 3 se implementa un prototipo tomando en cuenta la información base en el diseño propuesto con la finalidad de probar a menor escala los cálculos realizados en el capítulo anterior.

En el capítulo 4 se analizan los datos obtenidos de las pruebas con el prototipo y se realizan los respectivos correctivos.

En el capítulo 5 se describen los valores referenciales en el caso de la implementación del diseño propuesto.

En el capítulo 6 se indican las conclusiones y recomendaciones derivadas tanto del diseño como de la implementación del prototipo y sus respectivas pruebas.

CAPÍTULO 1.
DESCRIPCIÓN E IDENTIFICACIÓN DE LAS NECESIDADES DE LA EMPRESA

El concepto de seguridad, ya sea para proteger una propiedad o una persona, ha ido evolucionando a lo largo de los años. En la actualidad, las tecnologías de las que se dispone nos permiten tener un contacto desde cualquier parte del mundo en cualquier momento e incluso de forma móvil, lo que hasta unos pocos años atrás eran solo ideas en laboratorios.

Esta evolución de la tecnología ha permitido la difusión y desarrollo de nuevas aplicaciones en distintos campos de intervención humana. Esto además conlleva al hecho de hacer a la tecnología asequible al usuario promedio, sin que requiera desembolsar ingentes cantidades económicas para poder implementar algún tipo de tecnología de punta.

Una de las razones por los cuales la tecnología va ocupando un espacio importante en la vida del ser humano es la solvencia ante errores o deficiencias de carácter humano. Por eso en el tema de seguridad, tiene muy buena presencia.

Los sistemas de videovigilancia han ido evolucionando de tal modo que actualmente se puede monitorear un bebé, una casa, una empresa e incluso una ciudad entera, como es el caso de los sistemas de vigilancia dentro de las grandes ciudades.

Desde cámaras analógicas monocromáticas con conexión cableada hasta cámaras digitales inalámbricas con visión nocturna y sensores de movimiento, desde tamaños nada prácticos y de altos costos hasta cámaras diminutas imperceptibles y algunas de bajo costo son parte de muchos sistemas de vigilancia actualmente.

A pesar de todas estas ventajas, ningún sistema de videovigilancia permite reducir el índice delictivo a cero y es que al igual que la sociedad y todos sus elementos, la delincuencia también se beneficia del desarrollo. En este sentido es importante el poder mejorar los sistemas de vigilancia en todos los niveles.

Si bien un sistema de videovigilancia no permite evitar el crimen, como se ha indicado, éste se ve mermado ante los mecanismos y procesos que el sistema posee, y es que una alerta temprana permite tomar acciones correctivas ante cualquier acción hostil para con lo que se desea proteger. Este es el objetivo global de este proyecto: Diseñar un sistema de videovigilancia para ayudar a proteger bienes y clientes de un complejo turístico.

1.1 DESCRIPCIÓN DE LA EMPRESA.

El complejo turístico Hotel Pirámide D'Marco'S, ubicado en la ciudad de Puyo, en la provincia de Pastaza, a 5 minutos de la ciudad, en el Km 2 ½ de la vía Puyo – Tena, abrió sus puertas al público en 1997 prestando desde ese año servicios de alojamiento, piscinas, y demás distracciones para el turista que visita la zona central de la amazonía ecuatoriana.

En los actuales momentos el complejo se encuentra en un proceso de readecuación de las instalaciones por lo cual mantiene sus puertas cerradas al turismo dentro del mismo se ha contemplado la instalación de un sistema de video vigilancia para mejorar la seguridad de sus clientes.

El complejo turístico D'Marco'S es una instalación de recreación ubicada en una zona rural, en un sector donde a más de domicilios también existen otros complejos turísticos más pequeños.

Actualmente el complejo carece de sistema de seguridad alguno, aproximadamente el 75 % de su perímetro no tiene más protección que de jardinería y perros del propietario.

Si bien un sistema de seguridad completo debe incluir seguridades físicas, como murallas y cercas además de un sistema de vigilancia automatizado, el presente proyecto tiene como finalidad proponer una solución a esta última parte.

1.1.1 DESCRIPCIÓN DE INSTALACIONES

A pesar de que la empresa lleva varios años en funcionamiento, debido a que fue creciendo progresivamente, no se disponía de los planos respectivos, por tanto se procedió a la realización de los mismos para empezar el diseño del sistema de videovigilancia.

El complejo turístico se encuentra es una zona geográfica irregular, tiene una extensión aproximada de 13000 m^2, está instalado sobre una pequeña elevación montañosa, razón por la cual se la puede dividir en tres secciones principales; la parte alta y las dos zonas laterales.

La parte principal del complejo empieza desde la puerta principal, que está junto a la zona de parqueadero y junto a la torre de hospedaje piramidal, la cual consta de 5 pisos de habitaciones. Luego de esta torre y del parqueadero se encuentra un espacio cubierto, junto a este está la zona administrativa, que consta de un bar y la gerencia, además de incluir una pequeña cocina. Luego de estas instalaciones se encuentra el domicilio del propietario y tras de este, un taller de reparación y afines.

La zona suroeste consta de un pequeño laberinto, una cancha multiuso, una salsoteca y un acceso vehicular secundario al complejo.

La zona noreste, consta de dos piscinas con vestidores, toboganes y 3 cabañas de hospedaje pequeñas.

En la Figura 1.1 se puede apreciar un esquema geográfico del complejo.

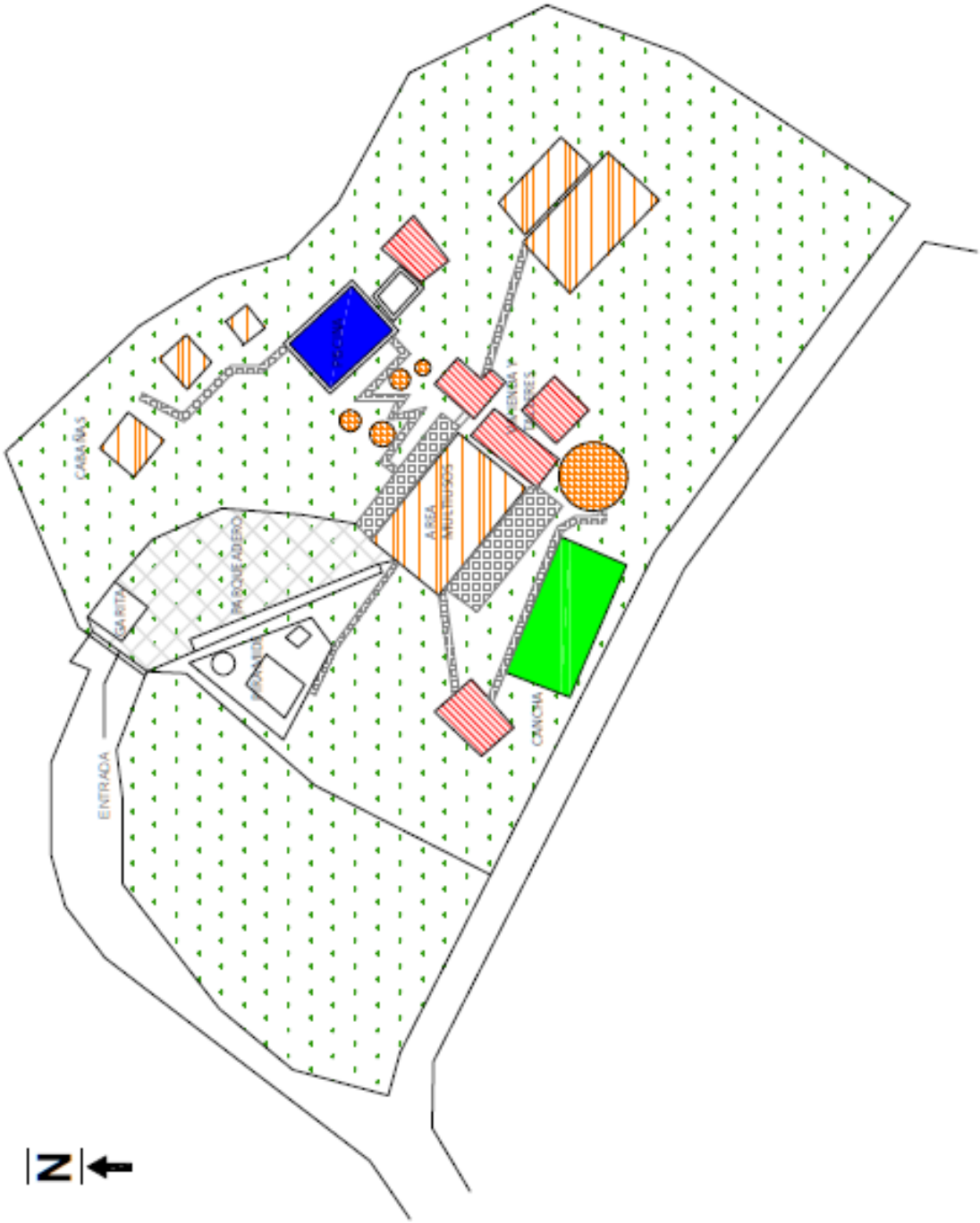

Figura 1.1 Diagrama geográfico del complejo D'Marco'S

.

1.1.1.1 Zona central del complejo

La zona central o alta del complejo tiene el acceso principal, donde, luego de atravesar la puerta y una caseta de acceso, se tiene el parqueadero, a la derecha del mismo se encuentra la torre piramidal de hospedaje, la cual posee 6 pisos de alojamiento y en su parte baja se encuentran juegos infantiles.

Continuando hacia el sur se tiene un espacio cubierto multiuso donde consta una cama elástica para entretenimiento, una pequeña tarima, mesas y sillas multiuso, en la parte norte de este espacio, se tiene la zona de gerencia, donde consta un pequeño espacio que hace de data center, donde está la conexión principal con el proveedor de internet CNT, una cocina y un pequeño bar.

Luego de esto se tiene una pequeña bodega y a 9 metros hacia el norte se tiene el domicilio del propietario, el cual tiene dos pisos, además de un pequeño espacio para parquear autos de su propiedad. Para acceder a este parqueadero, se debe ingresar desde la parte oeste del complejo, por el acceso secundario existente.

2 metros hacia el sur del domicilio se tiene un taller de reparaciones y soldaduras de dos pisos. En la Figura 1.2 se muestra la zona central descrita anteriormente.

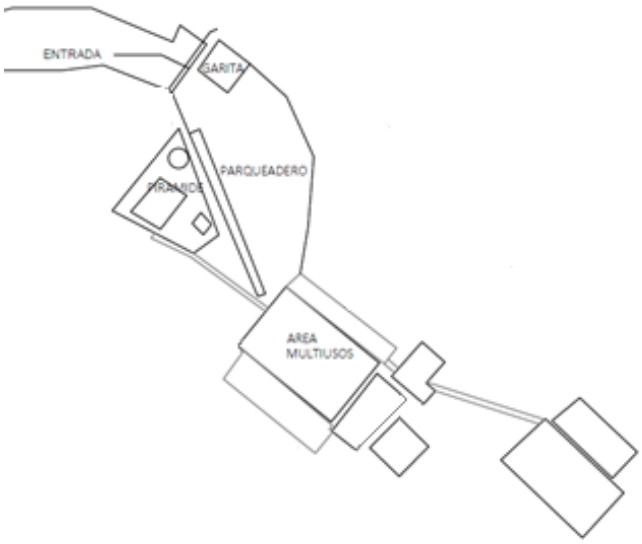

Figura 1.2 Zona Central

1.1.1.2 Zona suroeste.

La zona suroeste, esquematizada en la Figura 1.3, consta de una pequeña construcción que funciona como laberinto, una cancha multiuso y una salsoteca, además del acceso secundario para vehículos hacia el domicilio del propietario. Esta zona lateral oeste limita con una vía de acceso vehicular que conecta la avenida principal con un pequeño poblado que se encuentra a unos 6 kilómetros aproximadamente de distancia.

Figura 1.3 Zona suroeste

1.1.1.3 Zona noreste.

La zona noreste, mostrada en la Figura 1.4, consta de dos piscinas con sus respectivas áreas de vestidores, además de constar de toboganes, esta zona también cuenta con 4 cabañas para huéspedes. Esta zona limita con un rio, el cual da forma al perímetro del complejo turístico.

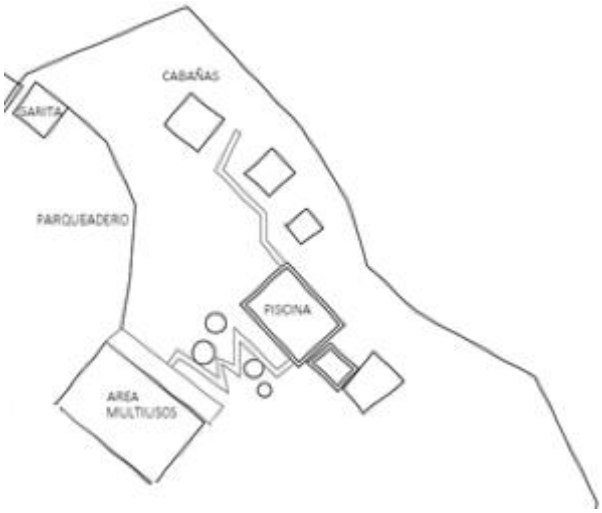

Figura 1.4 Zona noreste

1.1.2 SEGURIDAD FÍSICA EN LAS INSTALACIONES

El complejo turístico no posee sistema de alarma alguno, únicamente las puertas de acceso tienen posibilidad de limitar el acceso. Solamente en la parte frontal, donde está la puerta principal, se tiene cerramiento de protección, además de una caseta de guardianía que en la práctica no está siendo funcional.

El resto del perímetro del complejo, exceptuando la puerta de acceso secundaria, no dispone de infraestructura mínima física para impedir que un usuario no autorizado ingrese al complejo. Únicamente se tiene protección de jardinería en la mayor parte del perímetro e incluso la parte oeste del complejo tiene como límite un pequeño rio.

En la práctica, con estas características, el complejo es sumamente vulnerable, especialmente en la parte oeste, la cual tiene como frontera una vía vehicular que conecta la ciudad de Puyo con una pequeña parroquia rural.

El único mecanismo de alerta, si es que se lo puede calificar así, es la población canina propiedad del dueño del complejo, los cuales alertan a las tres personas que viven dentro del complejo en caso de un intruso.

1.1.3 INFRAESTRUCTURA DE DATOS

La infraestructura de datos del complejo es únicamente la instalada por el proveedor de internet doméstico, en este caso CNT[1].

El servicio de internet de CNT tiene las siguientes características: [1]

- Es un servicio de Internet asimétrico de compartición 2:1.
- Red de acceso por cobre ADSL.
- Equipo WIFI con 4 puertos de Ethernet.
- Ofrece disponibilidad de 98,3%.

[1] Corporación Nacional de Telecomunicaciones

1.2 CARACTERÍSTICAS DE LOS SISTEMAS CCTV [2]

Un sistema cerrado de cámaras, más conocido como CCTV en inglés, es un sistema que procesa imágenes en movimiento, las cuales se pueden almacenar y a las cuales se tiene restringido el acceso a un limitado número de usuarios. Puede estar compuesto de una variedad de cámaras, un equipo que centralice la información y dispositivos intermedios opcionales que sirven de enlace entre las cámaras y el dispositivo centralizado.

En un sistema de monitoreo moderno, todas las cámaras se pueden gestionar remotamente desde un sitio central donde se pueden modificar el zoom, su orientación y demás. Disponen de sistemas, que les permite optimizar los recursos, como activarse únicamente cuando se detecta movimiento delante de la cámara, por medio de sensores de movimiento. Además se puede acceder al sistema de forma remota para revisar el sistema o en caso de detección de algún evento.

1.2.1 CCTV ANALÓGICO

En un sistema de este tipo las cámaras que puedan existir se conectan de forma remota con un sistema centralizador denominado DVR (digital video recorder) por medio de un cable coaxial. Para poder hacer esto posible el DVR debía poseer una entrada física correspondiente a cada cámara que se haya dispuesto en el sistema.

La cámara por otro lado requiere poseer una conexión coaxial para la transmisión del video, otra conexión cableada para alimentación, y dependiendo del modelo de la misma, otro cable para manejo de las distintas funciones adicionales como paneo horizontal o vertical, zoom, etc.

Con este tipo de tecnología se podía lograr una frecuencia de 25 cuadros por segundo.

Uno de los principales inconvenientes de esta tecnología era la acumulación de cableado en los puntos de monitoreo, además de la capacidad limitada propia del sistema para agregar cámaras adicionales.

1.2.2 CCTV DIGITAL

Un sistema digital típico consta de cámaras IP, una red LAN, un dispositivo grabador de la red, conocido como NVR (Network Video Recorder), un router y un PC que permite visualizar la información.

En un CCTV digital se puede tener un control de lo que se desea grabar, es decir permite eliminar información que no es relevante y sólo almacenar escenas donde se detecte actividad. Se permite además realizar acercamientos, cambiar la velocidad o la resolución de la imagen. Permite un procesamiento posterior de la imagen.

Las cámaras IP dependiendo de sus capacidades pueden funcionar como estaciones transmisoras únicamente o como servidores de video. Para que funcione como servidor de video el dispositivo debe poseer un software propio, de tal modo que la propia cámara es capaz de gestionar el video sin necesidad de un nodo central. Al utilizar una dirección IP para comunicarse con la cámara es necesario que la computadora desde la cual se realiza la conexión cuente con el software necesario para el procesamiento de las imágenes.

En cambio, si funciona como un dispositivo transmisor, la información debe ser enviada a un dispositivo central para poder visualizar la información.

1.2.3 CCTV ANALÓGICO O DIGITAL

En el presente proyecto se decide trabajar con un sistema digital debido a la obsolescencia de los sistemas analógicos y a la naturaleza versátil de los sistemas digitales, los cuales permiten escalabilidad, mayor seguridad, mejor procesamiento de señal y compatibilidad con las nuevas tecnologías.

Los elementos que conforman un sistema de circuito cerrado de televisión típico son:

- Cámaras IP
- NVR Network video recorder
- Red LAN
- Router
- Access Point

1.3 CÁMARAS IP [3][4]

Se define como una cámara IP al dispositivo electrónico con el cual se puede capturar imágenes y sonidos para luego enviarlas a través de una red IP estándar hasta un dispositivo central capaz de gestionar esta información, el cual puede ser un NVR, un computador o un dispositivo móvil.

Al tener un servidor web interno, una dirección IP específica, y protocolos de streaming de video, la cámara permite a los usuarios, con las debidas credenciales de acceso, gestionar la información de forma remota y local.

A continuación en la Figura 1.5 con un diagrama estructural típico de una cámara IP, donde constan sus partes principales como son lente, procesador de video, sensor de imagen, CPU, compresor y terminales de conexión.

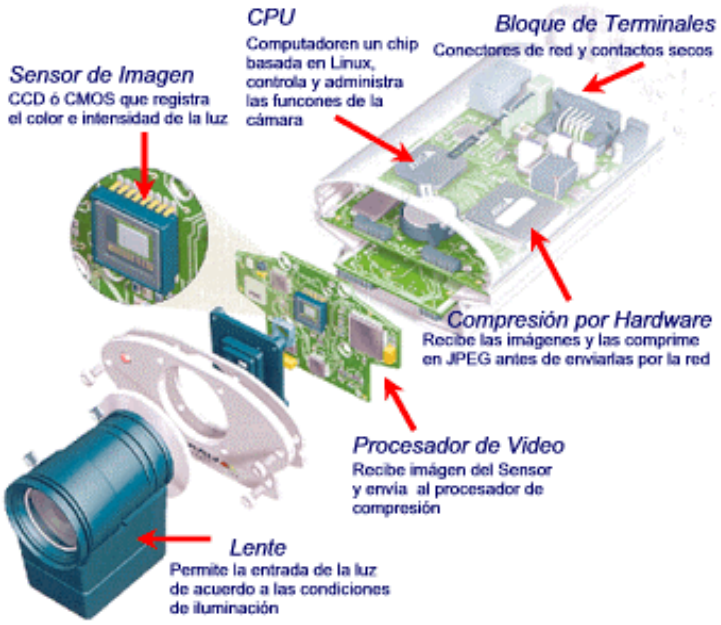

Figura 1.5 Componentes típicos de una cámara IP [4]

1.3.1 LENTE

Un lente se define como un elemento de cristal o de algún material transparente capaz de dispersar o de unir en un foco los rayos luminosos.

Se definen dos funciones primarias en un lente, la primera es captar la escena que se desea captar y observar en el monitor, lo que viene a ser por definición la función de la distancia focal, esta distancia focal puede ser fija o variable. La segunda función primaria es regular la cantidad de luz, la cual es una función del iris. Este iris puede ser regulado de forma manual o automática.

1.3.2 SENSOR DE IMAGEN

Es el encargado de recibir la luz filtrada por el lente y convertir estas señales en señales eléctricas.

1.3.3 PROCESADOR DE VIDEO

Es el encargado de convertir las señales eléctricas provenientes del sensor y convertirlas en señales digitales, para su posterior compresión.

1.3.4 COMPRESIÓN

[5]

Contempla la compresión de las imágenes digitales en formatos específicos para su transmisión por la red. La compresión es necesaria ya que las imágenes digitales que se obtienen requieren un alto ancho de banda para su transmisión.

Se pueden distinguir dos tipos de compresión, por video y por imagen, la primera apela a la similitud que se puede presentar entre distintas imágenes, y la segunda a la similitud que se puede presentar entre pixeles dentro de una misma imagen.

La relación de compresión es un factor clave en cada tipo de compresión existente, ya que ésta indica la relación entre el tamaño de la imagen original y la imagen comprimida. Se debe tener en cuenta que la compresión disminuye el consumo de ancho de banda pero también disminuye la calidad de la imagen, es por esto que se debe seleccionar en función de la aplicación a realizar.

Entre los principales métodos de compresión tenemos los siguientes.

1.3.4.1 Compresión MJPEG

Este formato tiene un uso generalizado en cámaras Web, IP y cámaras digitales. Este método se basa en la información de las imágenes anteriores y posteriores para comprimir la secuencia en una solo imagen JPEG.

1.3.4.2 Compresión MPEG

Apareciendo a finales de los años 80, este es un método aún utilizado actualmente, básicamente, éste estándar compara dos imágenes para transmisión y envía la primera como referencia agregando en la transmisión unos pocos elementos de la segunda de haber diferencia, todo esto haciendo que sea imperceptible para el ojo humano.

1.3.4.3 Compresión MPEG-4

Se aprobó en el año 2000 y está desarrollado para transmitir video en una baja cantidad de bits aunque si se requiere también se puede transmitir con una alta tasa de bits. Las imágenes que se transmiten son de menor tamaño al compararse con los archivos JPEG.

1.3.5 CPU

Es el componente encargado de la gestión de la información dentro del dispositivo, como el movimiento de la misma, la detección de movimiento, etc. Contiene un procesador que realiza el trabajo, así como una memoria flash y las comunicaciones por los distintos puertos disponibles.

1.3.6 DISTANCIA FOCAL

Esta distancia se conoce como la medida de la separación entre el sensor de imagen y el centro de la lente. Los rayos luminosos de un determinado objeto distante son concentrados de manera interna en la lente en un punto común del eje óptico. El punto en el que es posicionado el sensor de imagen dentro de la cámara IP es conocido como el punto focal. Por convención, las cámaras poseen dos puntos importantes, el punto principal primario y el secundario. Se conoce como distancia focal de la lente a la distancia entre el punto principal secundario y el sensor de la imagen o punto focal.

1.3.7 TECNOLOGÍA MEGAPÍXEL [6]

Dentro del ámbito de la fotografía es muy difundido el termino megapíxel, el cual está definido por 1 Mpx= 1 000 000 pixeles. En la Figura 1.6 se aprecia algunos valores de resolución.

Este término se asocia para expresar la resolución de las imágenes en las cámaras digitales. Si por ejemplo tenemos que una cámara tiene resolución de 3.1 megapixeles, este valor se obtiene de multiplicar 2048 x 1536 = 3 145 728.

Resolución	Megapíxel
1280x1024	1.3 MP
1600x1200	2 MP
2048x1536	3.1 MP
2592x1944	5 MP
6400x1200	8 MP

Figura 1.6 Varios valores de resolución

1.3.8 TECNOLOGÍA POE [3]

PoE (Power over Ethernet) es una tecnología que utiliza el cable de red también como línea de alimentación eléctrica. Este protocolo es muy difundido actualmente entre muchos dispositivos como teléfonos IP, cámaras IP, etc.

La gran acogida que tiene este protocolo se debe a la ventaja que presenta en cuanto a infraestructura, ya que permite que los dispositivos no requieran salidas eléctricas cercanas a los mismos, además de optimizar el cableado al disminuir la cantidad de cables.

Con esto, inherentemente se realiza un importante ahorro económico en el hardware del sistema y/o proyecto que se esté realizando.

1.3.9 NETWORK VIDEO RECORDER [7][8]

En un sistema donde uno de los objetivos es poder identificar con claridad los eventos que se registran con el lente, es importante la revisión en tiempo real y en tiempo diferido, por lo cual es importante considerar la implementación de un elemento que permita almacenar el video. En este papel es donde aparece el NVR o grabador de video en red, el cual, a más de grabar la información, presenta características de trabajo en red.

En el caso de utilizar cámaras analógicas es necesario un elemento extra para la conexión entre la cámara IP y el NVR. Este elemento extra es por lo general un servidor web de video o encoder.

EL NVR el mismo que se aprecia en la Figura 1.7 se dimensiona en función del número de cámaras existentes en la red. Esto facilita el funcionamiento en el caso de disponer de un menor número de cámaras disponibles.

Figura 1.7 Esquema de conexión de un NVR [8]

1.3.10 ENCODER O SERVIDOR WEB

El encoder o servidor web permite convertir la información de las cámaras analógicas en información digital, para que pueda ser procesada por el NVR.

Una de las ventajas más considerables de las cámaras analógicas sobre las digitales es el costo y el mantenimiento, es por esto que los servidores web tienen una amplia difusión en este campo.

Un esquema de conexión típico, como el que se aprecia en la Figura 1.8, es conectar una cámara analógica con un encoder a través de un cable coaxial, el cual al convertir las señales a información digital la envía a la red respectiva. Para la visualización de esta información se utiliza por lo general un computador, si el volumen de la información es de tamaño considerable se considera utilizar un NVR.

Figura 1.8 Esquema de conexión Encoder

1.3.11 ROUTER [10]

Un router, como el que se puede ver en la Figura 1.9, es un dispositivo que permite la interconexión de redes de computadoras. Como su nombre lo indica, su función principal es la de enrutar o dirigir a través de determinar cuál es la mejor ruta que debe tomar un paquete de datos.

Figura 1.9 Enrutador inalámbrico

1.4 SISTEMA ELÉCTRICO DE RESPALDO [11]

Debido a la naturaleza del sistema, es prioritario el poder disponer de una fuente de alimentación eléctrica continua que mantenga todos los equipos funcionando en caso de una interrupción del servicio eléctrico. Esta fuente se conoce como UPS. Este UPS debe estar conectado junto con el servidor y las cámaras en un circuito independiente del sistema eléctrico propio del complejo para más seguridad. Así en caso de una interrupción del servicio eléctrico, el sistema de vigilancia continuará funcionando por un tiempo adicional.

Un UPS es en síntesis un dispositivo conformado por varios dispositivos eléctricos y electrónicos que almacenan energía eléctrica y la liberan por un tiempo determinado en caso de una interrupción del suministro principal.

El UPS además puede servir como filtro frente a las distintas variaciones que se puedan presentar en el suministro eléctrico principal, de esta manera se asegura el correcto funcionamiento y preservación de los equipos que se utilizan.

Para que el UPS realice su trabajo, éste debe ser conectado entre la salida de energía eléctrica y el dispositivo a proteger.

1.4.1 TIPOS DE UPS

Dependiendo de su funcionamiento se los puede clasificar como UPS on-line y UPS off-line.

1.4.1.1 UPS off-line

Internamente, el voltaje alterno ingresa al UPS, este voltaje se monitoreado por un interruptor, el cual monitorea el nivel que tiene y, de presentarse algún cambio brusco o fuera de los márgenes permitidos, activa la batería para que entregue el voltaje correcto. Además de esto, mientras el voltaje de entrada esté en los niveles aceptables simultáneamente se pone en funcionamiento el proceso de carga de la batería interna mientras brinda electricidad al equipo final.

1.4.1.2 UPS on-line

Este sistema entrega energía a la red a proteger desde las baterías internas del mismo, por tanto no tiene interrupciones de energía a ningún nivel.

Estos dispositivos de soporte, deben ser instalados a poca distancia del servidor de monitoreo y el NVR, ya que no cuentan con la tecnología PoE.

En un sistema de vigilancia se hace imperativo el disponer de un sistema de UPS on-line.

Internamente el voltaje alterno ingresa al UPS, éste voltaje es monitoreado por un interruptor, el cual monitorea el nivel que tiene y de presentarse algún cambio brusco o fuera de los márgenes permitidos, activa la batería para que entregue el voltaje correcto. Esto se ha esquematizado en la Figura 1.10. Además de esto, mientras el voltaje de entrada este en los niveles aceptables simultáneamente se pone en funcionamiento el proceso de carga de la batería interna mientras brinda electricidad al equipo final.

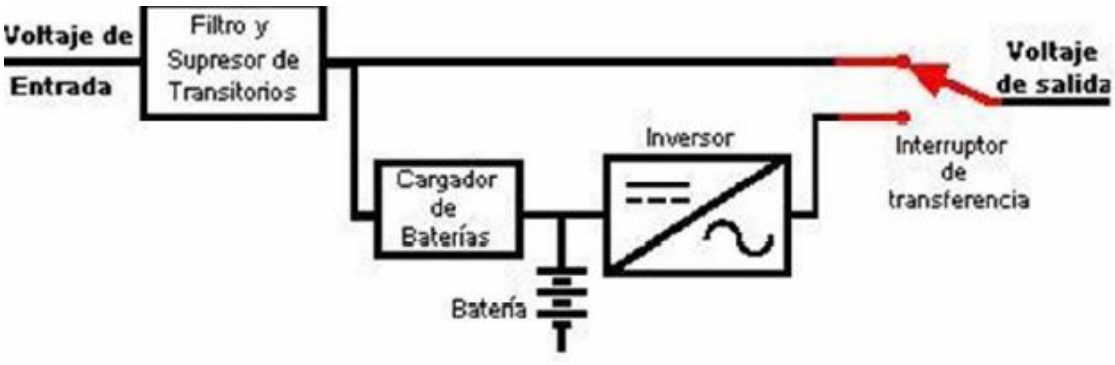

Figura 1.10 Esquema básico de un UPS [11]

1.5 SOFTWARE DE GESTIÓN DE VIDEO ZONEMINDER [12]

1.5.1 INTRODUCCIÓN

Zoneminder se puede definir como una colección de aplicaciones que permiten controlar un sistema de vigilancia a través de la gestión de video. Zoneminder se encarga de realizar la captura de video para su posterior, análisis, registro y seguimiento, por lo cual tiene muchas características que pueden ser configuradas por el usuario, como notificaciones de correo en caso de detectarse un evento, también se puede controlar las cámaras que se hayan conectado al sistema, etc.

Zoneminder es una alternativa muy difundida entre los distintos software de gestión de video al ser de licencia libre.

1.5.2 REQUERIMIENTOS

Para un correcto funcionamiento de zoneminder, se requiere cumplir los siguientes puntos, tanto para software como para hardware

Sistema operativo Linux

Base de datos MySQL

Librerias libjpeg, ffmpeg, PHP

Compilador PHP

Servidor Apache

Procesador mínimo Pentium III, AMD Atlon, Dual Core o AMD Turion x2

Una memoria mínima de 128 MB

Tarjeta de red Ethernet de 10 Mbps

Tarjeta gráfica de 32 MB

Espacio en disco 300 MB

El sistema operativo a utilizarse, así como la versión de zoneminder corresponde a recomendaciones realizadas por la comunidad activa de la página web de zoneminder. En el Anexo A se indica el proceso para la instalación del programa en el sistema operativo especificado.

1.6 CENTOS [13]

CentOS[2] es una distribución de Linux, derivada de Red Hat, de clase empresarial. Como la mayoría de las distribuciones Linux cuenta con la colaboración continua de muchos desarrolladores a nivel mundial.

CentOS incluye software de muchos otros proyectos basados en software libre, entre el software que conforman CentOS se puede encontrar:

- Apache Web Server
- Samba
- Sendmail
- CUPS
- vsFTPD
- MySQL
- BIND

Existen muchas versiones de CentOS, tanto como servidor o para escritorio.

Una de las grandes ventajas que ofrece esta distribución es que es muy estable para trabajar como servidor, razón por la cual, el presente proyecto tomará como base el trabajar en esta versión de Linux.

Otra de las prestaciones de CentOS es que puede trabajar en clusters, en grupos de servidores que pueden compartir una misma base de datos, una extensa variedad de aplicaciones, balanceo de carga, etc.

---

[2] Community Enterprise Operating System

1.7 REDES DE INFORMACIÓN [14]

1.7.1 GENERALIDADES

Se conoce como una red al conjunto de elementos o dispositivos de red que se interconectan mediante un medio de transmisión físico o inalámbrico con la finalidad de intercambiar información entre sí.

1.7.2 TIPOS DE REDES

No existe una clasificación oficial que abarque a todas las redes, sin embargo se aceptan generalmente, la tecnología de transmisión y el tamaño de las mismas.

En cuanto a la tecnología de transmisión se puede distinguir dos tipos, broadcast o punto a punto.

En la tecnología punto a punto, la forma de conexión es entre pares, es decir si la información tiene que ir de un punto origen a un punto destino, es posible que tenga que pasar a través de muchos puntos intermedios, con la posibilidad de encontrarse con varias rutas que han sido conformadas por múltiples conexiones punto a punto. En este caso, se debe realizar la tarea de encontrar el camino más óptimo.

En la tecnología broadcast, todos los dispositivos usan el mismo canal de comunicación, la información enviada por uno de los terminales es recibido por todos los demás, donde dependiendo de a quien está dirigida la información, el bloque de datos es ignorado o aceptado por el receptor, ya que la información pudo haber sido enviada a un destinatario en específico o para todos los miembros.

Un ejemplo de una red que utiliza el mismo medio de comunicación es una red inalámbrica.

Otra forma de clasificar las redes es por su tamaño, así puede ser redes de área personal (PAN), de área local (LAN), de área metropolitana (MAN), y de área amplia (WAN), donde cada una de ellas presenta mayor escala que la anterior. Una idea del área que pueden abarcar los diferentes tipos de redes se puede ver en la Figura 1.11.

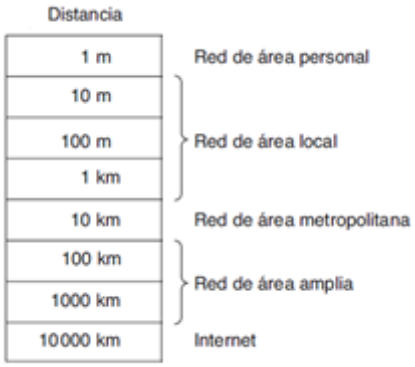

Figura 1.11 Clasificación de redes por tamaño [14]

1.7.2.1 Redes de área personal (PAN)

Este tipo de redes se caracteriza por tener conexiones del rango de una persona. Un ejemplo común es un computador y sus periféricos, los cuales pueden estar interconectados por medio de cables o de señales inalámbricas. Una tecnología muy difundida para este tipo de aplicaciones es Bluetooth.

1.7.2.2 Redes de área local (LAN)

Se pueden definir como redes de área local a redes determinadas por espacios reducidos como oficinas, edificios u hogares, pero mayores que una PAN.

Este tipo de redes es muy difundido en la actualidad, especialmente en ambientes empresariales y domésticos. La mayoría de ellos en un ambiente inalámbrico, donde los dispositivos se conectan con un dispositivo centralizador, conocido como punto de acceso o AP, el cual sirve de intermediario entre los dispositivos e internet. Cabe recalcar que también pueden darse comunicaciones directamente entre los dispositivos.

La mayoría de las redes LAN consisten en la interconexión de varios enlaces punto a punto, basados en el estándar 802.3. Este estándar permite que varios computadores en una red se interconecten a un dispositivo conocido como switch, con lo cual se puede realizar la interconexión entre switches, para expandir la red.

1.7.2.3 Redes de Área Metropolitana (MAN)

Se define como una red que abarca una extensión de una ciudad. La más común es la red que presta servicios de televisión por cable. Con la evolución de la tecnología, estas mismas redes empezaron a prestar el servicio de internet dentro de las ciudades.

Un ejemplo de esto se puede observar en la Figura1.12.

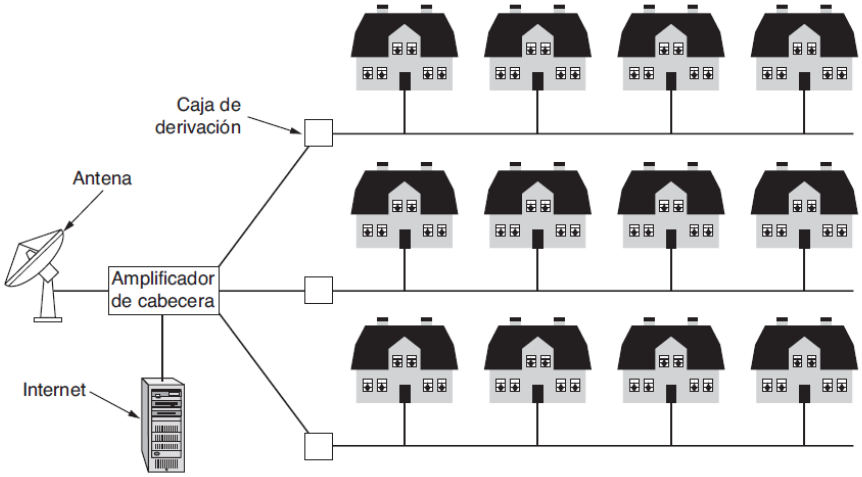

Figura 1.12 Ejemplos de red MAN para Tv por cable [14]

1.7.2.4 Redes de Área Extensa (WAN)

El término WAN (Wide Area Network o red de área extensa) se aplica realmente a la infraestructura que permite la conexión de redes o dispositivos ubicados en diferentes zonas geográficas sin límite de distancia. Un ejemplo de estas redes puede ser la interconexión de muchas sucursales de una empresa dentro de un país, de un continente o incluso a escala mundial. Una característica muy significativa en este tipo de redes es el uso de las infraestructuras proporcionadas por los operadores de telecomunicación cuyo ámbito de actuación esté dentro de las zonas que cubren este tipo de redes.

Otro ejemplo de este tipo de redes son los sistemas satelitales, donde se tiene un alcance global aunque con una latencia considerable dependiendo de los fines requeridos, es decir, si se requiere una comunicación en tiempo real, un sistema satelital no presta las condiciones necesarias para que esta aplicación se ejecute satisfactoriamente, no así para un intercambio de datos en tiempo diferido.

Se puede tener un ejemplo adicional de las redes WAN en los sistemas de telefonía celular, donde se puede tener comunicación en el orden de kilómetros entre una radio base y un dispositivo celular. Al comunicarse entre radio bases una comunicación extremo a extremo entre celulares es posible a escala mundial.

1.7.2.5 Redes de área local inalámbricas (WLAN)

Un tipo de redes que ha aparecido junto con la evolución de la tecnología es la red de área local inalámbrica. Básicamente se trata de una red LAN sin cables, es decir, una red donde cada terminal presenta una antena para poder comunicarse inalámbricamente a corta distancia.

Se utiliza ondas de radio como tecnología más difundida. Este tipo de redes ha tenido un gran impacto, esto en parte a la facilidad de instalación, bajos costos, movilidad y comodidad del usuario.

La principal clasificación en este tipo de redes es el tipo de conexión infraestructura y ad hoc. Como se muestra en la Figura 1.13

Una conexión en infraestructura (Figura 1.13 (a)) se refiere a una conexión en jerarquía, donde existe un punto centralizador que se comunica con los demás dispositivos, de tal manera que para que dos dispositivos finales se comuniquen entre si necesariamente la información debe pasar a través del dispositivo centralizador o también conocido como punto de acceso.

Cuando en una red no existe el dispositivo centralizador y la comunicación se realiza entre dispositivos finales directamente se dice que se está trabajando en una red ad hoc. Figura 1.13 (b)

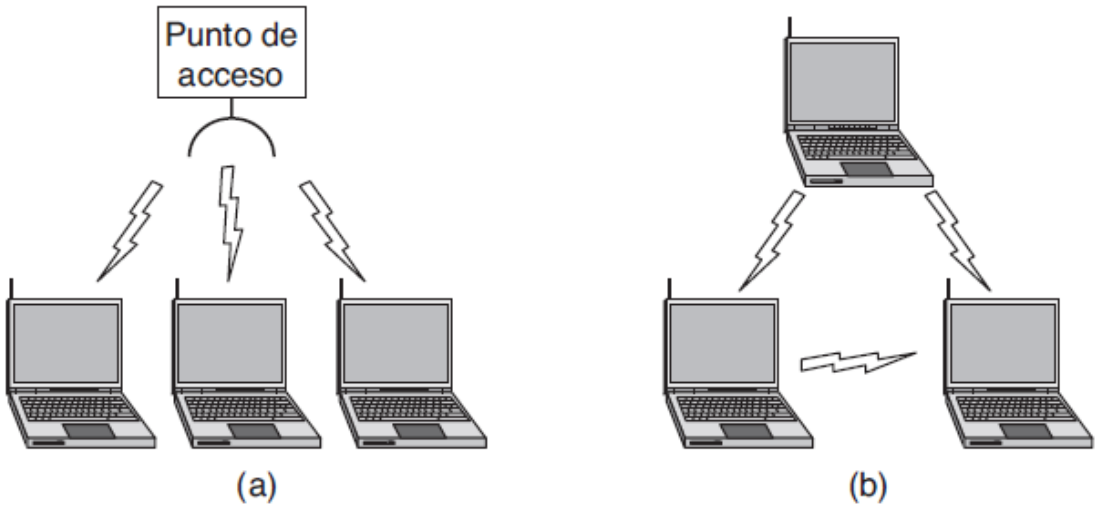

Figura 1.13 (a) Red de infraestructura (b) Red Ad hoc [14]

1.8 EL ESTÁNDAR IEEE 802.11 [14]

Para normar las comunicaciones en las redes inalámbricas entre fabricantes se desarrolló el estándar IEEE 802.11, conocido como WiFi. Este estándar trabaja en las bandas ISM (Industrial, Scientific y Medical).

Al trabajar en esta banda se limita la potencia de la señal. Por otro lado uno de los principales problemas con este tipo de transmisión es la alteración que sufre la señal ante los obstáculos, debido a objetos solidos presentes en el medio de transmisión. Esto produce ecos que pueden aumentar o disminuir la señal hasta su destino, conociéndose esto como desvanecimiento multitrayectoria.

Hasta la fecha se han desarrollado varias versiones de este estándar como 802.11b, 802.11a, 802.11g, etc. En cada versión en general se mejoraba la velocidad y se variaba la frecuencia con el objetivo de ofrecer al público un estándar más acorde a sus necesidades.

A continuación una breve descripción de cada uno de los estándares 802.11.

1.8.1 802.11A

Fue un estándar desarrollado para trabajar en la banda de los 5 GHz, con la utilización de OFDM, podía alcanzar hasta 54 Mbps en velocidad de transferencia de datos. Tiene una alta tasa de perdida de datos debido a que ante obstáculos presenta una atenuación considerable, también carece de calidad de servicio, con lo cual no era recomendable para aplicaciones de voz.

1.8.2 802.11B

Desarrollado para trabajar en la banda de los 2,4 GHz, lograba velocidades de 5,5 y 11 Mbps. Además de utilizar DHSS para la transmisión de datos, este estándar tiene QoS, pero presenta interferencia con otros dispositivos que trabajaban en la misma banda, como hornos microondas, teléfonos celulares, dispositivos bluetooth, etc.

1.8.3 802.11G

Tiene similitud con el estándar anterior pues trabajaba en la misma banda de 2,4 GHz y puede alcanzar velocidades de hasta 48 Mbps.

1.8.4 803.11N

Fue desarrollado para trabajar tanto en la banda de los 2,4 GHz y de los 5 GHz, pudiendo alcanzar una velocidad máxima de 300 Mbps, su principal innovación fue utilizar el sistema de varias antenas, conocido como MIMO, en inglés, múltiples entradas, múltiples salidas.

Una situación desfavorable adicional en las redes hasta aquí descritas es la movilidad, la cual, dependiendo de la distancia, hace que para que la comunicación se realice de forma eficiente se requieran celdas con su propio punto de acceso para poder otorgar cobertura al usuario.

Otro de los problemas de este tipo de redes y tal vez uno de los más importantes es el tema de la seguridad. Dado que las redes trabajan en difusión, muchos de los dispositivos finales reciben información que no era destinado para ellos.

Para disminuir esta falta de seguridad se han desarrollado en este estándar técnicas de cifrado, como WEP[3], WPA[4], WPA2[5].

1.9 SEGURIDAD Y ADMINISTRACION EN REDES. [16]

La tecnología inalámbrica, debido a su naturaleza, al transmitir información a través de un medio libre no alámbrico tiene menos prestaciones de seguridad que las redes alámbricas.

Junto con la evolución de la tecnología, también el crimen y los métodos de aprovecharse de información valiosa que se transmite en los distintos medios de transmisión han ido evolucionando a la par. Por tanto es necesario establecer un nivel de seguridad que permita asegurar la información.

Se pueden clasificar las amenazas en 4 temas: confidencialidad, autentificación, no repudio y control de integridad.

La confidencialidad se entiende como el aseguramiento de la información impidiendo que esté al alcance de usuarios no autorizados.

La autenticación se entiende como la verificación de un usuario autorizado, antes de revelar la información comprometedora.

El no repudio se refiere a verificar las firmas digitales de los usuarios.

El control de integridad está relacionado con el aseguramiento de la información desde el punto de origen hasta el destino.

---

[3] Wired Equivalent Privacy

[4] WI-FI Protected Access

[5] WI-FI Protected Access 2

Los Access points (APs) que se utilizan para la cobertura inalámbrica, en ambientes ideales, es decir con obstáculos casi nulos pueden llegar a tener una cobertura de varias decenas de metros. Estos APs sirven de nexo entre la red cableada y los dispositivos inalámbricos. Justamente es en esta parte, donde la seguridad es clave y donde los parámetros antes descritos deben ser tomados en cuenta.

1.9.1 AMENAZAS

En el estándar IEEE 802.11 la seguridad nació como una opción, mas no como una prioridad, es por esto que si bien la mayor parte de la responsabilidad de la seguridad recae en el usuario, actualmente existen mejoras importantes de seguridad en cada nuevo estándar.

Al igual que las redes cableadas, las redes inalámbricas comparten algunas de las amenazas de las redes cableadas, además de otras amenazas propias únicamente de las redes inalámbricas, entre las cuales se tiene:

1.9.2 ESPIONAJE

Consiste en que un usuario no autorizado utiliza un dispositivo específico para realizar una escucha o intercepción de los datos que se transmiten en el aire y los utiliza a su conveniencia. Este método se considera un ataque pasivo, ya que este usuario no autorizado no realiza ningún cambio en el información que intercepta, simplemente “escucha” el paquete de datos entre el origen y el destino, al no realizar acción alguna sobre la información, tanto el remitente como el receptor no detectan a este usuario no autorizado.

Actualmente la mayoría de la redes utilizan la tecnología de codificación de espectro ensanchado, el cual es resistente a “escuchas” de usuarios externos, además, si la información también es encriptada, se vuelve una doble protección.

A pesar de estas mejoras en seguridad en los sistemas actuales, las “escuchas” de parte de terceros no pueden ser ignoradas.

1.9.3 ACCESO NO AUTORIZADO.

Se conoce como acceso no autorizado al ingreso de un usuario no autorizado como si fuera un usuario autorizado. Este viene a ser un ataque activo ya que el usuario no autorizado no está esperando que se realicen transmisiones sino que vulnera las seguridades para ingresar a la red utilizando un dispositivo especial o alguno conectado a la parte cableada de la red.

La mejor manera de mermar este tipo de ataques es mejorando los sistemas de autenticación de los usuarios. En una red inalámbrica es difícil distinguir cuando un usuario no autorizado está intentando ingresar ya que estos intentos se los puede confundir con accesos fallidos de los usuarios autorizados.

Una variante de un acceso no autorizado es un atacante quien engaña a las estaciones con un AP falso. Cuando una estación se enciende por primera vez, automáticamente selecciona un AP que tenga una señal muy fuerte para conectarse, así, el atacante al configurar un AP como señuelo, puede recibir información de autenticación o incluso puede negar el servicio pero almacenar la información de autenticación.

1.9.4 INTERFERENCIA

Una de las amenazas más importantes para las comunicaciones inalámbricas es la degradación de la señal por interferencia, esto debido a que estas comunicaciones se realizan en bandas de frecuencia alrededor de los 2,4 GHz y son las mismas que las frecuencias en las que trabajan muchos de los electrodomésticos.

Si bien este tipo de interferencia es accidental, existe también la interferencia intencionada, la cual se presenta cuando un atacante utiliza un transmisor con una potencia considerable con la intención de solapar total o parcialmente una determinada señal.

1.9.5 AMENAZAS FÍSICAS.

Como cualquier red, las redes inalámbricas están expuestas a daños en su parte física, dependiendo del daño la red puede ser inhabilitada parcial o totalmente

Los elementos físicos son más susceptibles de recibir daños en exteriores, al estar expuestos a las condiciones ambientales. Además de afectaciones físicas propias a los equipos, las condiciones ambientales afectan a las comunicaciones en sí, provocando perdida de información.

Si bien una red inalámbrica posee menos infraestructura física que una red cableada, está igualmente expuesta a que un atacante provoque daños físicos a la red ya sea para inhabilitarla parcial o totalmente o ya sea para vulnerar su seguridad y robar los datos internos de la misma.

1.9.6 MEDIDAS DE SEGURIDAD

Para mermar las amenazas antes descritas se han desarrollado tecnologías como Spread-Spectrum (Espectro Ensanchado), la cual se creó para evitar el espionaje, la interferencia y el ruido. Básicamente esta tecnología hace que la señal se escuche como ruido para el atacante pero es descifrable para el usuario que conoce los parámetros de la transmisión.

Entre los tipos de seguridades se tiene:

1.9.6.1 Filtrado

Permite realizar una discriminación de los usuarios autorizados y no autorizados.

- Filtrado por SSID.- En inglés Service Set Identifier, es básicamente el nombre que se le asigna a la red como tal. Para que se permita la conexión entre el dispositivo final y el AP se pueden presentar dos escenarios, el primero en donde el AP envía el SSID a los dispositivos por medio de una transmisión en tipo broadcast y el segundo escenario en donde no se hace broadcast y donde solo los usuarios que conozcan el SSID se puedan conectar a la red.
- Filtrado MAC.- En inglés Media Access Control. Este filtrado establece que para que un determinado dispositivo pueda conectarse, el administrador de la red debe registrar la dirección MAC del dispositivo en la lista de direcciones MAC autorizadas previamente.

- Filtrado por protocolos.- Permite discriminar que protocolos están autorizados en el AP para los usuarios y cuáles no.

1.9.6.2 Seguridad por estándares

Este tipo de seguridad permite realizar la conexión entre el dispositivo y el AP a través de la autenticación del dispositivo. Así, el dispositivo envía un mensaje de solicitud al AP, este le contesta con otro mensaje para que el dispositivo lo reenvíe. Si el mensaje que envió el dispositivo coincide con el mensaje encriptado en el AP, se autentica al usuario, de lo contrario no se establece la conexión.

Entre los estándares de cifrado se tiene:

- WEP.- En inglés Wired Equivalent Privacy, que en español significa equivalente de privacidad inalámbrica, es uno de los primeros estándares de descifrado que se desarrolló, y por tanto es una tecnología algo básica, la cual puede descifrarse fácilmente.
- WAP.- En inglés Wireless Aplication Protocol, fue el estándar que se desarrolló como una mejora ante las fallas de seguridad de WEP.
- WAP2.- Fue la segunda versión de WAP, siendo una mejora de los dos estándares adicionales

En base a la información recopilada de los equipos a utilizarse y del estado y dimensiones del complejo, así como de las condiciones en las cuales se debe implementar el proyecto se deben definir los criterios básicos para el diseño del sistema de video vigilancia.

- Debido a la falta de infraestructura en el perímetro del complejo, además de no contar con el cableado necesario se opta por implementar cámaras de vigilancia inalámbricas.
- Para poder cubrir el complejo de manera satisfactoria se utilizarán cámaras inalámbricas internas y externas con capacidad de visión nocturna y diurna.

- Se seleccionará los dispositivos que trabajaran como puntos de acceso, los elementos de almacenamiento de la información, el sistema operativo, el software adecuado y demás elementos que conformaran el sistema de video vigilancia en base a la situación del complejo.
- Se determinará el ancho de banda necesario para un óptimo funcionamiento del sistema en cuestión.

1.10 EVALUACIÓN PRELIMINAR DE ZONAS DE RIESGO

Tomando en cuenta las condiciones e infraestructura del complejo, se pueden definir las zonas donde se contempla el uso de cámaras y el número de las mismas.

La siguiente Tabla muestra las zonas en cuestión, así como el número de cámaras a ser utilizado.

Tabla 1.1 Número de cámaras por zona

ZONA	NUMERO DE CAMARAS
ZONA CENTRAL	
Parqueadero	1
Torre de Hospedaje	1
Juegos infantiles	1
Espacio cubierto	1
Bar	2
Administración	1
Domicilio	2
Hospedaje	1

Taller	2
ZONA NORESTE	
Laberinto y cancha	1
Salsoteca	1
Acceso secundario	1
ZONA SUROESTE	
Piscinas	2
Vestidores	1
Cabañas	2

Al ser un establecimiento turístico y de un considerable movimiento de personas, se trata de cubrir no solo el área del perímetro sino las localidades internas del mismo.

Dependiendo de la ubicación, la cámara puede ser PTZ o puede ser únicamente PT, esto, tratando de combinar tanto funcionalidad y costo.

En la Figura 1.14 se puede apreciar una tentativa ubicación de las cámaras y del servidor en el complejo.

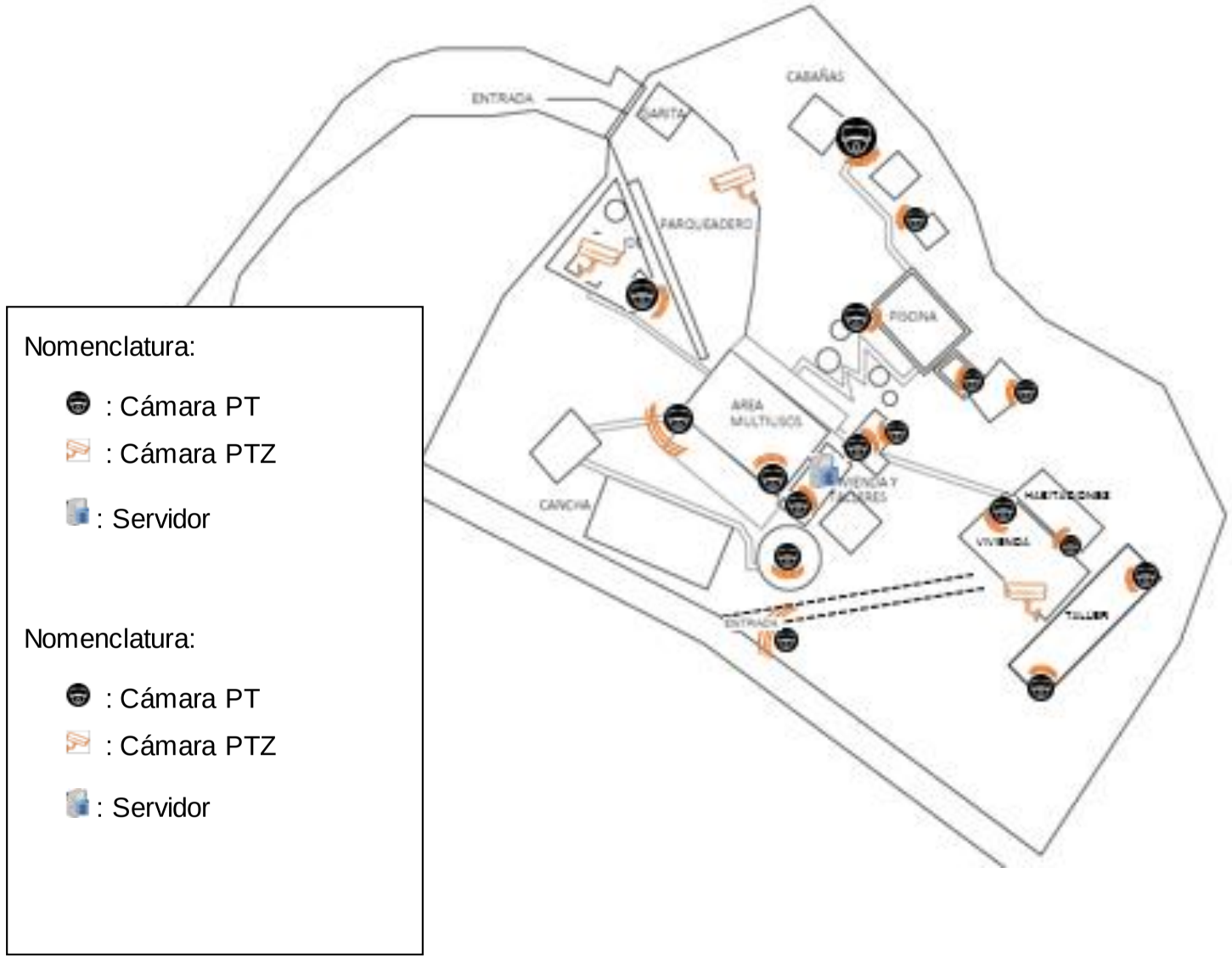

Figura 1.14 Esquema preliminar de la ubicación de los equipos

De lo expuesto en este capítulo se logra concluir que la solución que se va a adoptar un sistema de videovigilancia digital, el mismo que constará de un conjunto de cámaras inalámbricas distribuidas por el complejo. Las mismas serán gestionadas por un servidor, al cual se podrá acceder de forma remota. Debido a la extensión del complejo y a que no existe un sistema de cableado de comunicaciones instalado, es necesario la instalación de puntos de acceso inalámbricos, de esta forma se potenciará la cobertura inalámbrica necesaria para cursar el tráfico generado por las cámaras.

Se decide que el sistema operativo del servidor estará basada en la distribución CentOS que mejor convenga, y se montará sobre el mismo un servidor LAMP (Linux, Apache, MySQL y PHP) que dará soporte al software de gestión de cámaras Zoneminder.

Los eventos que se registren serán almacenados en una unidad DVR, que funcionará ligada al servidor.

En cuanto a la seguridad se considerarán las siguientes políticas:

La red inalámbrica del sistema deberá estar oculta, lo que implica que el SSID no se esté difundiendo.

Cada una de las cámaras tendrá una dirección IPv4 fija por facilidades de gestión, además se implementará la técnica de filtrado de MAC para mejorar la seguridad.

En cuanto al protocolo de encriptación, se usará WPA2-PSK para asegurar la autenticación de los equipos.

Por otro lado, los usuarios autorizados dispondrán de las credenciales necesarias para gestionar el sistema, contemplando dos tipos de usuarios administradores y observadores.

Todo el sistema anteriormente descrito será respaldado eléctricamente por medio de un UPS on-line.

En el capítulo siguiente se procederá a realizar el diseño del sistema de videovigilancia, comprobando en la práctica el modelo propuesto anteriormente.

CAPÍTULO 2.
DISEÑO E IMPLEMENTACION DEL SISTEMA DE VIDEOVIGILANCIA

2.1 INTRODUCCIÓN

En base a la información recopilada de los equipos que podrían utilizarse y del estado y dimensiones del complejo, así como de las condiciones en las cuales se debe implementar el proyecto se deben definir los criterios básicos para el diseño del sistema de video vigilancia.

- Debido a la falta de infraestructura en el perímetro del complejo, el cual únicamente cuenta con cerca viva, espacios abiertos, además de no contar con el cableado necesario, se decide en primera instancia optar por instalar cámaras de vigilancia inalámbricas.
- Para poder cubrir el complejo de manera satisfactoria se decide utilizar cámaras para interior y para exterior con capacidad de visión nocturna.
- Debido a las dimensiones del complejo se decide utilizar varios puntos de acceso para permitir la comunicación entre las cámaras y el servidor central.
- En cuanto a los dispositivos de almacenamiento de video, se decide utilizar un NVR, el cual va a estar conectado al servidor que gestiona las cámaras.

2.2 DISEÑO DE LA RED

2.2.1 ANALISIS DE SITE SURVEY. [3]

La evaluación de sitio, también conocida como site survey, es un proceso en el cual se estudian las redes inalámbricas existentes en una zona geográfica determinada donde se planea implementar una nueva red inalámbrica.

Este análisis permite obtener información de intensidad, frecuencia de trabajo, tipo de encriptación, etc., de redes existentes y en base a estos datos poder determinar la ubicación de los dispositivos activos de la red a implementarse.

El site survey implica la realización de un análisis pasivo y un análisis activo. Para esto, en este proyecto se utilizarán los programas inSSIDer 2.0 su logotipo se aprecia en la Figura 2.1 y Ekahau HeatMapper, cuyo logotipo se ve en la Figura 2.2, para el site survey pasivo y activo, respectivamente.

Figura 2.1 Logotipo de InSSIDer [17]

Figura 2.2 Logotipo de Ekahau HeatMapper [18]

2.2.1.1 Site survey pasivo.

Para la realización del site survey pasivo se utiliza el programa inSSIDer. Este site survey permite conocer las redes inalámbricas que están presentes en una determinada área geográfica. Con este programa se puede detectar el número de redes presentes, el canal utilizado, la intensidad, entre otros valores.

Con esta información se identifica cuáles son los canales más utilizados para evitarlos el momento de configurar la red inalámbrica del presente proyecto.

2.2.1.2 Site survey activo.

En la realización de este site survey se colocan puntos de acceso inalámbricos dentro del complejo para observar cobertura y nivel de señal respectivo. Estos puntos de acceso se deben mover en función de mejorar la cobertura y la señal procurando el desempeño óptimo de los equipos en función de sus especificaciones.

2.2.1.3 Análisis del Site Survey en el complejo turístico.

Este análisis permite detectar las distintas redes inalámbricas que existen en un determinado lugar.

A continuación, se muestran los resultados de la realización del site survey pasivo en distintas ubicaciones en el complejo turístico D'Marco'S.

Para entender mejor las siguientes pantallas es importante explicar los campos que aparecen en las mitades superior e inferior de las mismas, que muestran las siguientes características de los APs que se van detectado:

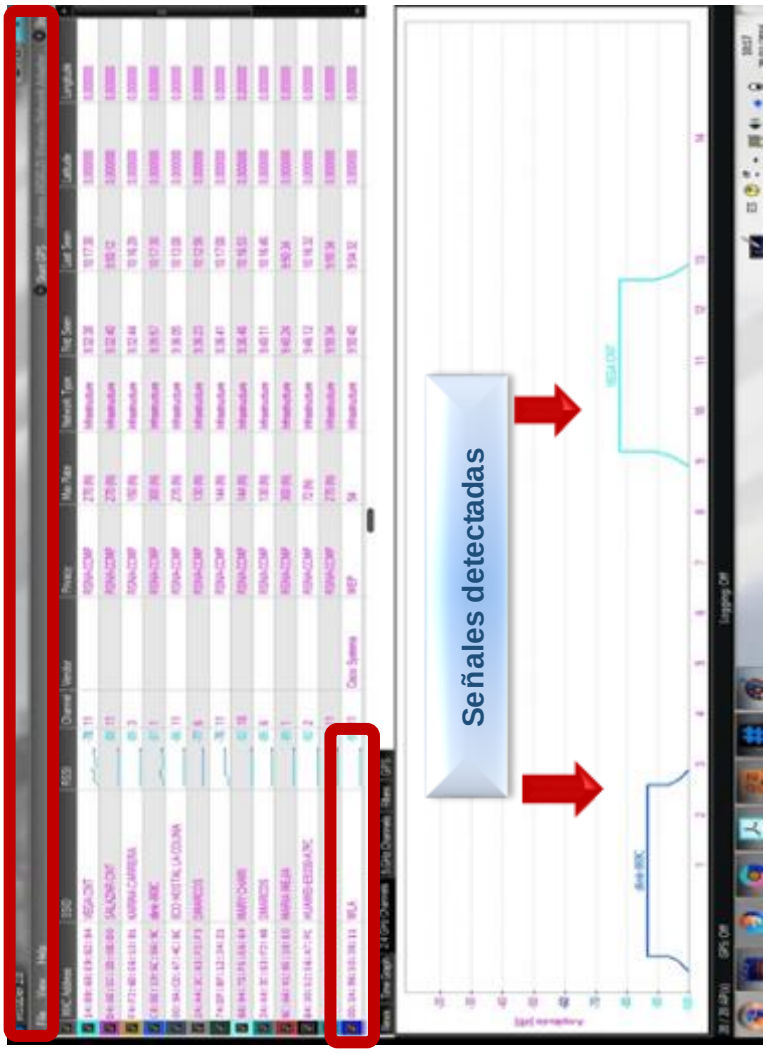

Figura 2.3 Ejemplo de pantalla obtenida con el programa Zoneminder

En la mitad superior de la Figura 2.3 se puede apreciar las características de las distintas redes que se van detectando mientras se camina por el complejo durante la ejecución del programa. Entre las características que se pueden reconocer están las siguientes: [19]

- MAC Address.- Muestra la dirección MAC.
- SSID.- En inglés “Service Set Identifier”, es el nombre asignado a la red WLAN provista con un Access Point detectado.
- RSSI.- En inglés “Received Signal Strength Indicator”, es un indicador que muestra el nivel de intensidad de la señal detectada.
- Channel.- Muestra el canal de operación.
- Vendor.- Muestra el nombre del fabricante respectivo.
- Privacy.- Muestra el tipo de cifrado utilizado por cada AP, los cuales pueden ser ninguno (NONE), WEP, WPA Personal (WPA-TKIP) y WPA2-CCMP (RSNA-CCMP).
- Max Rate.- Muestra el máximo valor teórico de transmisión de datos para esa red.
- Network Type.- Muestra que topología está siendo utilizada.
- First Seen.- Muestra la hora exacta en la que se detectó a esta red por primera vez.
- Last Seen.- Muestra la hora exacta en la que se detectó a esta red por última vez.
- Latitude.- Muestra la coordenada de latitud cuando la función de GPS se encuentra activada.
- Longitude.- Muestra la coordenada de longitud cuando la función de GPS se encuentra activada.

En la mitad inferior de las pantallas se puede apreciar las redes inalámbricas detectadas ese momento, donde se tiene un valor de intensidad basado en la escala izquierda vertical. En cuanto a la escala horizontal se debe entender que la señal forma una figura similar a un trapecio, donde el centro de la misma indica el canal que utiliza el AP. Además se pueden encontrar otras opciones de visualización entre las que se tiene: [19]

- News.- Indica si el programa tiene actualizaciones disponibles.
- Time Graph.- Muestra un gráfico compuesto de las distintas intensidades detectadas en una escala de tiempo real.
- 2.4 GHz Channels.- Indica la intensidad de las señales que operan en dicha banda.
- 5 GHz Channels.- Indica la intensidad de las señales que operan en dicha banda.
- Filters.- Permite definir búsquedas más específicas de las redes a detectar.
- GPS.- Esta función se activa únicamente con un dispositivo GPS conectado al puerto serial del equipo con el cual se realiza el site survey.

La Figura 2.4 muestra las redes inalámbricas detectadas en la zona del bar, donde se puede apreciar que las redes más fuertes detectadas son VEGA CNT, en la banda de los 2,4 GHZ, en el canal 11 y la dlink-869C en el canal 1.

Si bien en la parte superior aparecen señales adicionales, estas no se visualizan en la parte inferior debido a que la captura se la realiza a las 10:17 am y de acuerdo a la columna Last Seen, estas señales fueron detectadas minutos antes.

Se debe aclarar que no se apreciaron señales en la banda de los 5GHz en ningún sector.

Figura 2.4 Redes inalámbricas detectadas en la zona del bar

Figura 2.5 Redes inalámbricas detectadas en el domicilio.

La Figura 2.5 muestra las redes inalámbricas detectadas en la zona del domicilio donde se puede apreciar que las redes más fuertes detectadas en la banda de los 2,4 GHZ son VEGA CNT, una red no identificada, ambas en el canal 11, el dlink-869C en el canal 1 y la red Huawei-E5330-A7FC en el canal 2.

El mismo análisis se realiza en la figuras 2.6, 2.7, 2.8, 2.9, 2.10 y 2.11, donde en cada imagen se pueden apreciar las redes más importantes en la mitad inferior, la intensidad de las mismas, así como los canales que utilizan.

Figura 2.6 Redes inalámbricas detectadas en la base de la pirámide.

Figura 2.7 Redes inalámbricas detectadas en la zona del taller.

Figura 2.8 Redes inalámbricas detectadas en el espacio cubierto multiusos

Figura 2.9 Redes inalámbricas detectadas en la zona de la cancha.

Figura 2.10 Redes inalámbricas detectadas en la zona de la piscina.

Figura 2.11 Redes inalámbricas detectadas en la zona de vestidores.

De acuerdo a la información obtenida, se aprecia que los canales donde se tiene el mayor número de redes son los canales 1 y 11 y el canal menos congestionado es el canal 6, por lo cual se utilizará este canal para la realización del presente proyecto.

Una vez realizado el site survey pasivo, se procede con el site survey activo, donde se colocan Access Points en lugares estratégicos.

Para este proceso se utiliza el programa Ekahau HeatMapper. En el cual se puede cargar un mapa de las instalaciones para verificar la cobertura de los Access Points.

El usuario debe recorrer las instalaciones con el programa ejecutándose mientras se va creando un esquema de la cobertura en el complejo. Para realizar esta simulación de campo se utilizó el router Linksys WRT54GL en los lugares indicados en el esquema de la Figura 1.9.

Se ubicó un AP, en la esquina del espacio cubierto. Con este AP se obtuvo el siguiente resultado al realizar el site survey activo en la zona de parqueadero:

En la Figura 2.12 se puede apreciar el recorrido realizado por el usuario en la línea punteada. Una vez concluido el recorrido el programa entrega un gráfico indicando el nivel de señal, en base a distintos niveles de verde, siendo el verde más intenso en las zonas con mayor nivel de cobertura.

Teniendo en cuenta lo descrito anteriormente se puede interpretar en la siguiente imagen que colocando un AP en la esquina del espacio cubierto que da al parqueadero se tiene una cobertura completa de todo el parqueadero. La línea punteada indica el recorrido del usuario.

Figura 2.12 Site Survey del parqueadero con AP en esquina de espacio cubierto.

Con esta misma ubicación se analizó la señal en el espacio cubierto en la Figura 2.13:

Figura 2.13 Site survey en la zona del espacio cubierto.

La segunda posición del AP fue en la zona del bar. El site survey entregó el siguiente resultado y se puede observar en la Figura 2.14.

Figura 2.14 Site Survey con el AP en la zona de bar.

Una tercera posición, en la Figura 2.15 se realizó en la parte de atrás de la salsoteca:

Figura 2.15 Site Survey con el AP en la zona de la salsoteca

Una cuarta posición se ubicó en la zona de las piscinas, Figura 2.16, con el siguiente resultado:

Figura 2.16 Site survey en la zona de piscinas.

Una quinta posición se ubicó en el área de las cabañas, en la Figura 2.17:

Figura 2.17 Site survey en la zona de cabañas.

Una sexta posición fue en el área de la torre piramidal se muestra en la Figura 2.18.

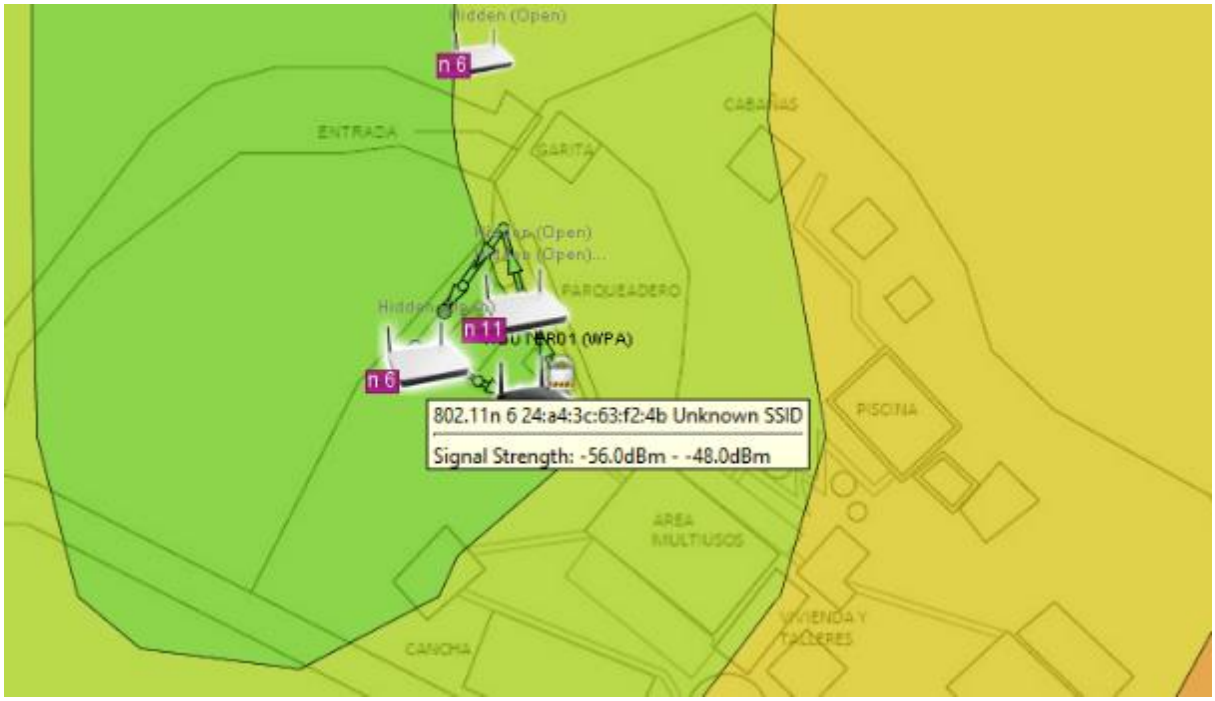

Figura 2.18 Site survey en la torre piramidal.

Otra ubicación se la realizó en la zona de los talleres en la Figura 2.19.

Figura 2.19 Site survey en talleres.

En base a las imágenes obtenidas con el site survey activo se concluye que las ubicaciones seleccionadas para los APs serán los definitivos ya que dan la cobertura suficiente. Esto permite ubicar las cámaras dentro de los sectores donde se aprecia mayor nivel de intensidad, es decir donde el color verde es más oscuro.

2.2.2 EVALUACIÓN DE ZONAS DE RIESGO

Tomando en cuenta las condiciones e infraestructura del complejo, se pueden definir las zonas donde se contempla el uso de cámaras, el tipo y el número de las mismas.

La Tabla 2.1 muestra las zonas en cuestión, así como el número de cámaras a ser utilizado.

Tabla 2.1 Número de cámaras por zona

ZONA	NÚMERO DE CAMARAS	TIPO DE CAMARA
ZONA CENTRAL		
Parqueadero	1	PTZ
Garita	1	PT
Torre de Hospedaje	2	PT
Espacio cubierto	1	PT
Bar	1	PT
Habitaciones	1	PT

Domicilio	1	PTZ
Taller	2	PT
ZONA SUROESTE		
Laberinto y cancha	1	PT
Salsoteca	1	PT
Acceso secundario	1	PT
ZONA NOROESTE		
Piscinas	1	PT
Cabañas	2	PT

Se concluye finalmente, en base a los análisis site survey y a las zonas de riesgo, que el número de cámaras a utilizar estará determinado por la Tabla 2.1 y la ubicación final de los equipos estará determinado por la Figura 2.20 mostrada a continuación.

Se consideran únicamente utilizar dos cámaras tipo PTZ, en parte debido a su alto costo y en parte debido a que sólo existen dos zonas críticas que necesitan acercamiento. El parqueadero, donde se tiene una vista de águila del ingreso y en el domicilio donde se puede apreciar el acceso de personas no autorizadas. En cuanto al resto de las instalaciones la cámara tipo PT que se va a utilizar cubre satisfactoriamente todos los puntos críticos.

Al ser un establecimiento turístico y de un considerable movimiento de personas, se trata de cubrir no solo el área del perímetro sino las localidades internas del mismo.

La red debe poseer 7 Access Points en los lugares donde se los ubicó para la realización del site survey activo.

El servidor será ubicado en la parte central, junto a la administración. Este servidor será implementado con sistema operativo Linux, permitirá a los usuarios administradores el control y monitoreo de la red, además se encargará del almacenamiento del video.

Si bien en el esquema se observan aparentes áreas sin cobertura, no es el caso, ya que estos espacios corresponden a zonas con pendientes considerables, áreas verdes vacías, zonas donde hay paredes o zonas donde la vegetación se convierte en una barrera natural. Se debe recordar que si bien el mapa del complejo expuesto en el presente proyecto muestra una infraestructura sobre una planicie, no es así. El complejo está instalado sobre una pequeña montaña de tal manera que la parte de las piscinas y la cancha no tienen línea de vista entre sí y la parte del espacio cubierto, administración y domicilio están en la parte alta.

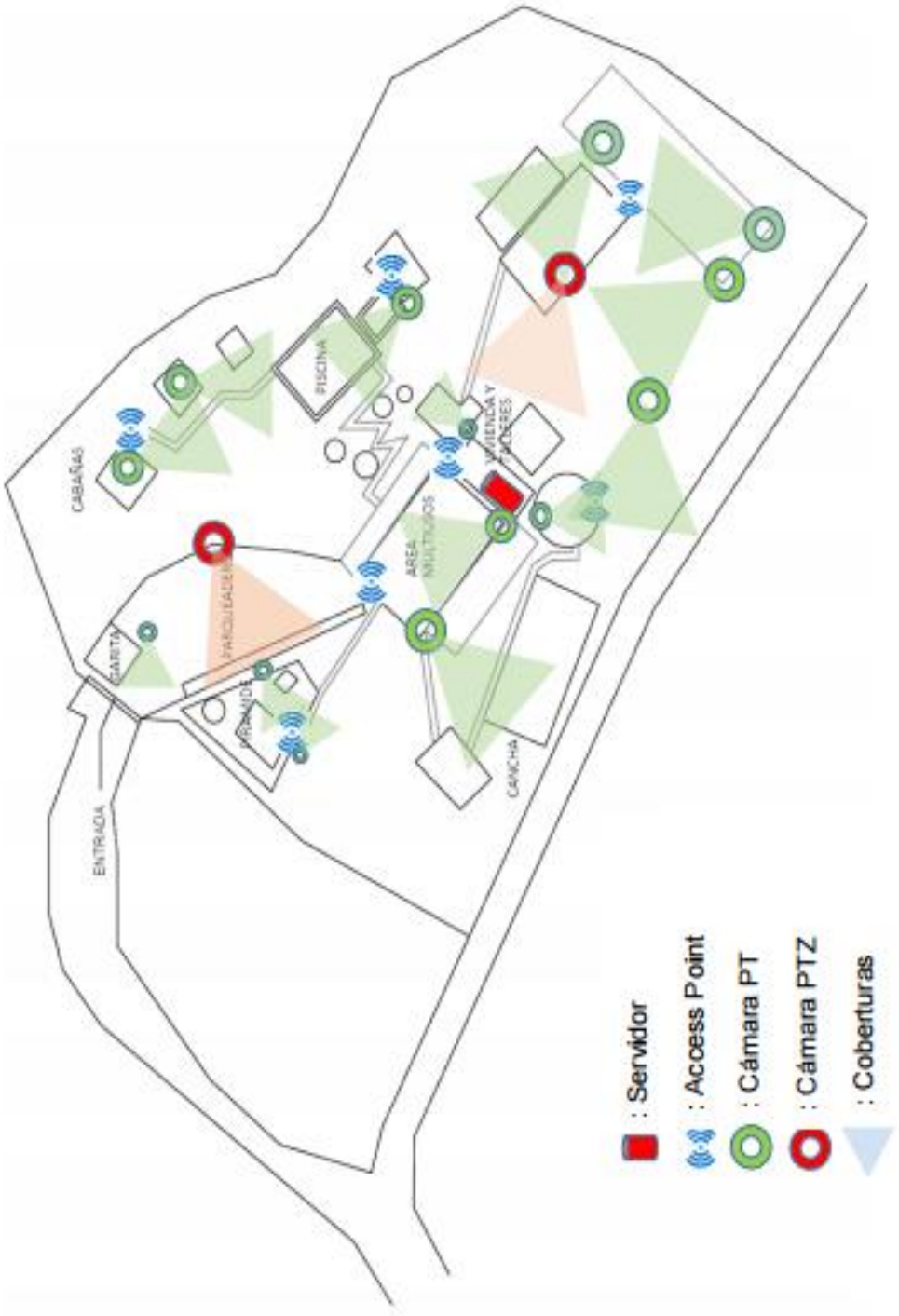

Figura 2.20 Esquema de ubicación de los equipos

2.3 REQUERIMIENTOS Y ELECCIÓN DE LAS CÁMARAS

El dispositivo principal de un sistema de video vigilancia es de hecho la cámara, según las necesidades expuestas en el primer capítulo las cámaras deberán cumplir los siguientes requerimientos de la Tabla 2.2.

Tabla 2.2 Especificaciones técnicas de las cámaras

ESPECIFICACIONES TÉCNICAS CÁMARAS	
Compresión de video	MJPEG
Resolución mínima (pixeles)	640 x 480
Capacidad de trabajar a la intemperie	0.5
Estándar Inalámbrico	IEE 802.11 b/g/n
Velocidad de imágenes	15fps o 30 fps
Zoom	Si

De las características consultadas en diferentes cámaras se ha encontrado que al menos tres modelos cumplen con los requerimientos y cuyo costo no es muy elevado.

2.3.1 FOSCAM FI8918W [19]

La Foscam FI8918W es una cámara IP para interiores que combina la alta calidad de video con la conectividad a redes alámbricas e inalámbricas, sus características técnicas se pueden visualizar en la Tabla 2.3.

Tabla 2.3 Características cámara Foscam FI8918W

CARACTERISTICAS CAMARA FOSCAM FI8918W		
Sensor de Imagen	Sensor de Imagen	Sensor de alta definición CMOS
	Resolución	640 x 480 pixeles
	Lentes	f: 3.6mmm
	Iluminación mínima	0.5 Lux
Lentes	Tipo	Vidrio
Video	Compresión de imagen	MJPEG
	Tasa de cuadros de imagen	15 fps, 30 fps
	Resolución	640 x 480 o 320 x 240
	Espero de imágenes	Vertical / Horizontal
	Frecuencia de luz	50 Hz, 60 Hz
	Parámetros de Video	Brillo, Contraste
Comunicación	Ethernet	Un puerto 10/100 Mbps RJ45
	Protocolos	HTTP, FTP, TCP/IP, UDP, SMTP, DHCP, PPPoE, DDNS
	Estándar inalámbrico	IEEE 802.11 b/g/n
	Tasa de Datos	802.11b: 11 Mbps(Max); 802.11g: 54 Mbps(Max); 802.11n: 150 Mbps (max)
	Seguridad Inalámbrica	Encripción WEP, WPA, WPA2

	Infrarrojo	11 Leds IR
Alimentación	Fuente de poder	5 Vdc/ 2 A
	Consumo	5.5 Watts (max)

2.3.2 DLINK DCS 2330L [20]

La cámara DCS 2330L es una cámara inalámbrica para exteriores que dispone de zoom por software, lo que lo que se conoce como ePTZ, a continuación se detallan las principales características en la Tabla 2.4.

Tabla 2.4 Características cámara Dlink DCS 2330L

CARACTERISTICAS CAMARA DLINK DCS 2330L		
Sensor de Imagen	Sensor de Imagen	CMOS progresivo
	Resolución	HD 1280 x 720 pixeles
	Lentes	f: 3.45 mm
	Iluminación mínima	0 Lux con LED IR encendido
Video	Compresión de imagen	MJPEG / H.264
	Tasa de cuadros de imagen	15 fps, 30 fps
	Resolución	1280x720, 800x448,640x360, 480x272, 320x176
Comunicación	Ethernet	Un puerto 10/100 Mbps, puerto Fast Ethernet
	Protocolos	IPv6, IPv4, TCP/IP, UDP, ICMP

		DHCP client, NTP client (D-Link) DNS client, DDNS client (D-Link) SMTP client, FTP client HTTP / HTTPS, PPPoE, RTP / RTSP/ RTCP, IP filtering QoS, CoS, Multicast, IGMP ONVIF compliant
	Estándar inalámbrico	802.11 n/g/b
	Tasa de Datos	1.5 Mbps
	Seguridad	Múltiple usuario con contraseñas
	Infrarrojo	5 m
Alimentación	Fuente de poder	5 Vdc/ 1.2 A
	Consumo	5 Watts (max)

2.3.3 LOFTEK SENTINEL [21]

La cámara Loftek Sentinel es una cámara inalámbrica tipo PTZ diseñada para trabajar en interiores como en exteriores, a continuación se detallan las principales características en la Tabla 2.5.

Tabla 2.5 Características cámara Loftek Sentinel

CARACTERISTICAS CAMARA LOFTEK SENTINEL		
Sensor de Imagen	Sensor de Imagen	CMOS
	Resolución	640 X 480
	Lentes	3x Zoom Optico (4mm – 9mm)
	Iluminación mínima	0,5 Lux
Video	Compresión de imagen	MJPEG
	Tasa de cuadros de imagen	15 fps, 30 fps
	Resolución	640x480, 320x240
Comunicación	Ethernet	Puerto Ethernet 10Base-T/100Base-TX
	Protocolos	TCP/IP,DHCP,SMTP,HTTP,DDNS,UPNP,PPPoE,FTP,DNS
	Estándar inalámbrico	802.11 b/g/n
	Seguridad	WEP, WPA, WPA2
	Infrarrojo	5 m
Alimentación	Fuente de poder	10 Vdc/ 1.2 A
	Consumo	10 Watts (max)

2.3.4 ELECCIÓN DE LAS CÁMARAS

Al comparar los requerimientos y las características de las cámaras antes detalladas, se concluye que se utilizarán los equipos anteriormente descritos, distribuyendo los mismos en las ubicaciones antes detalladas. El costo que representan las cámaras para interiores respecto de las cámaras para exteriores promueve el uso de ambos tipos de cámaras dependiendo de la ubicación de las mismas.

2.4 DETERMINACION DEL ANCHO DE BANDA.

Una vez determinado el número de cámaras, routers y access points a utilizarse, se procede a determinar el ancho de banda que se requerirá para el funcionamiento de la red. Para ello se deben tener en cuenta parámetros como:

- Sobrecarga de encapsulamiento
- Cuadros por segundo
- Resolución
- Compresión
- Número de cámaras

2.4.1 SOBRECARGA POR ENCAPSULAMIENTO [14]

Se entiende por sobrecarga de encapsulamiento al conjunto de bits adicionales que surgen del encapsulamiento de las capas superiores.

En el presente proyecto, por tratarse de un sistema de comunicación inalámbrica, se considerará para el análisis la trama del estándar IEEE 802.11g. Se toma este estándar ya que presenta buen alcance tanto para zonas internas como externas además de una velocidad de transmisión de 54 Mbps.

Se puede apreciar la trama IEEE 802.11g en la figura 2.21.

Cabecera PLCP	Cabecera MAC	Cabecera LLC	Cabecera IP	Cabecera TCP	Datos de Información	CRC	Trailer
353 Bytes	38 Bytes	4 Bytes	20 Bytes	20 Bytes	2268 Bytes	12 Bytes	12 bits

Figura 2.21 Formato de trama IEEE 802.11g. [14]

De acuerdo a la anterior figura, se puede apreciar que únicamente la información corresponde a 2268 bytes o 18144 bits del bloque de color amarillo, tomando como base el modelo OSI, todos los demás bloques que conforman la trama corresponden a los campos de cabecera y bloques de control. Estos bloques adicionales suman un total de 3588 bits, que agregados al bloque de información forman un total de 21723 bits.

Tomando en cuenta estos valores se puede determinar el valor de la sobrecarga de encapsulamiento.

$$Sobrecarga\ de\ encapsulamiento = Total\ bits\ trama - bits\ de\ información$$

$$Sobrecarga\ de\ encapsulamiento = 21732\ bits - 18144\ bits$$

$$Sobrecarga\ de\ encapsulamiento = 3588\ bits\ \approx 448.5\ Bytes$$

Este valor se obtiene siempre y cuando se esté transportando 18144 bits de información.

Toda esta cantidad de bits influye significativamente en el ancho de banda a considerar para el cálculo del sistema de vigilancia.

2.4.2 RESOLUCIÓN Y COMPRESIÓN DE VIDEO. [3]

En función del tipo de compresión y de la resolución que pueden tener las imágenes, se puede hablar de “Tamaño de cuadro”.

En la Tabla 2.5 se puede tener algunos valores para tamaño de cuadro para la compresión MJPEG.

Tabla 2.5 Resolución y comprensión de video MJPEG

Resolución	Compresión de video						
	MJPEG-10	MJPEG-20	MJPEG-30	MJPEG-40	MJPEG-50	MJPEG-70	MJPEG-90
320x240 (QVGA)	12 KB	9 KB	8 KB	7 KB	6 KB	5 KB	4 KB
352X240 (CIF NTSC)	13 KB	10 KB	9 KB	8 KB	7 KB	6 KB	4 KB
352X288 (CIF PAL)	15 KB	12 KB	11 KB	9 KB	8 KB	7 KB	5 KB
480X360	26 KB	21 KB	18 KB	16 KB	14 KB	11 KB	9 KB
640X480 (VGA)	46 KB	38 KB	32 KB	28 KB	25 KB	20 KB	16 KB
704X240 (2CIF NTSC)	26 KB	21 KB	18 KB	16 KB	14 KB	11 KB	9 KB
704X288 (2CIF PAL)	31 KB	25 KB	21 KB	19 KB	17 KB	13 KB	10 KB
704X480 (4CIF NTSC)	51 KB	41 KB	36 KB	31 KB	28 KB	22 KB	17 KB
800x600	73 KB	59 KB	50 KB	44 KB	40 KB	31 KB	24 KB

Estos valores corresponden a una iluminación de 50 lúmenes, se debe tener en cuenta que el concepto de tamaño de cuadro se ve directamente afectado por la luminosidad de las instalaciones.

En la Tabla 2.6 se puede apreciar los valores de tamaño de cuadro para la compresión MPEG4.

Tabla 2.6 Resolución y compresión de video MPEG4

Resolución	Compresión de video					
	MPEG4-10	MPEG4-20	MPEG4-30	MPEG4-50	MPEG4-70	MPEG4-90
320X240 (QVGA)	3 KB	2 KB	2 KB	1 KB	1 KB	1 KB
352X240 (CIF NTSC)	3 KB	3 KB	2 KB	2 KB	1 KB	1 KB
352X288 (CIF PAL)	4 KB	3 KB	3 KB	2 KB	1 KB	1 KB
480X360	7 KB	5 KB	4 KB	3 KB	2 KB	2 KB
640X480 (VGA)	12 KB	9 KB	8 KB	6 KB	4 KB	3 KB
704X240 (2CIF NTSC)	7 KB	5 KB	4 KB	3 KB	2 KB	2 KB

Es posible hallar la cantidad de tramas 802.11g necesarias para enviar un cuadro completo a partir de los valores de sobrecarga de encapsulamiento, datos de información, resolución y compresión de video.

Para este fin se dispone la siguiente fórmula:

$$Número\ total\ de\ tramas = \frac{Tamaño\ de\ un\ cuadro\ [Kbytes]}{Tamaño\ de\ información\ [Bytes]} \qquad \text{EC. 2.1}$$

Tomando como ejemplo la compresión 640 x 480 pixeles y empleando la compresión MJPEG-10, se tiene que:

$$Número\ total\ de\ tramas = \frac{46\ [Kbytes]}{2268\ [Bytes]} * \frac{1024\ Bytes}{1\ Kbyte} \qquad \text{EC. 2.2}$$

$$Número\ total\ de\ tramas = 21\ tramas \qquad \text{EC. 2.3}$$

2.4.3 TAMAÑO DE UN CUADRO DE VIDEO. [22]

Para obtener el valor de un cuadro de video, además de conocer el valor del número total de tramas es importante conocer el valor total de la sobrecarga producida por el total de las tramas presentes en la transmisión.

Con la siguiente ecuación se puede determinar la sobrecarga total en función del número de tramas.

$$Sobrecarga\ total = Número\ de\ Tramas\ * Sobrecarga\ total\ por\ trama \quad \text{EC. 2.4}$$

$$Sobrecarga\ total = 21\ tramas\ * 448{,}5\ bytes \quad \text{EC. 2.5}$$

$$Sobrecarga\ total = 9418{,}5\ bytes\ * \frac{1\ Kbytes}{1024\ Bytes} \quad \text{EC. 2.6}$$

$$Sobrecarga\ total = 9{,}2\ Kbytes \quad \text{EC. 2.7}$$

Conociendo los valores de la sobrecarga total y del tamaño del cuadro es posible hallar el valor de tamaño de cuadro:

$$Tamaño\ de\ cuadro\ [Bytes] = 46\ Kbytes + 9{,}2\ Kbytes \quad \text{EC. 2.8}$$

$$Tamaño\ de\ cuadro\ [Bytes] = 55{,}2\ Kbytes * 8\ bits \quad \text{EC. 2.9}$$

$$Tamaño\ de\ cuadro\ [Bytes] = 441{,}6\ Kbits \quad \text{EC 2.10}$$

2.4.4 CUADROS POR SEGUNDO [22]

Se conoce como cuadros por segundo a la cantidad de imágenes que son transmitidas en un segundo. A mayor número de cuadros por segundo, la imagen presenta menos parpadeo y mayor cantidad de información.

El valor de cuadros por segundo es un valor determinado por la cámara a utilizarse, dependiendo del fabricante, este valor puede venir por defecto o puede ser seleccionado en la misma cámara.

La velocidad de transmisión de imágenes o cuadros por segundo, en un sistema de videovigilancia es importante ya que define el ancho de banda que van a ocupar las cámaras a utilizarse.

Para obtener el ancho de banda que va a ocupar una determinada cámara se debe utilizar la ecuación 2.11

$$Ancho\ de\ banda\ [Mbps] = Tamaño\ de\ cuadro\ [Kbits] * fps\ [Mbps] \qquad \text{EC. 2.11}$$

Para obtener el ancho de banda de todas la cámaras a utilizarse de debe multiplicar el valor obtenido del ancho de banda de cada cámara por el número de cámaras que se van a utilizar en el sistema.

$$Ancho\ de\ banda\ [Mbps] = Ancho\ de\ banda * número\ de\ cámaras \qquad \text{EC. 2.12}$$

2.4.5 CALCULO DEL ANCHO DE BANDA [22]

Para obtener el ancho de banda del sistema de videovigilancia generado por las cámaras es necesario conocer el valor de cuadros por segundo de cada cámara, la resolución y la compresión que se va a utilizar.

Tomando en cuenta el número de cámaras a utilizarse en el presente proyecto, 19, se determina el valor del ancho de banda. Se tendrá en cuenta el valor de resolución de 640x480 (QVGA). Con ese valor se tiene un tamaño de cuadro de 46 Kbytes, MJPEG -10 será el formato de compresión a utilizarse debido a su amplia difusión entre los fabricantes de cámaras. Se tomará además una velocidad de transmisión de imágenes de 30 cuadros por segundo.

Por medio de la expresión matemática 2.1 se procede a determinar el número total de tramas que se requerirán para transmitir un cuadro.

$$Número\ total\ de\ tramas = \frac{Tamaño\ de\ un\ cuadro\ [Kbytes]}{Tamaño\ de\ información\ [Bytes]}$$

$$Número\ total\ de\ tramas = \frac{46\ [Kbytes]}{2268\ [Bytes]} * \frac{1024\ [Bytes]}{1\ [Kbyte]} = 20{,}76$$

$$Número\ total\ de\ tramas = 21$$

Entonces se tiene que por cada cuadro transmitido en las condiciones establecidas, se van a necesitar 21 tramas, en base a esto se debe calcular la sobrecarga de encapsulamiento que conlleva este número de tramas.

$$Sobrecarga\ total = Número\ de\ Tramas\ * Sobrecarga\ total\ por\ trama$$

$$Sobrecarga\ total = 21\ [tramas]\ * 448{,}5\ [Bytes]$$

$$Sobrecarga\ total = 9418{,}5\ [Bytes] * \frac{1\ [Kbytes]}{1024\ [Bytes]}$$

$$Sobrecarga\ total = 9{,}2\ [Kbytes]$$

A partir de esto se debe determinar el valor real de un cuadro tomando en cuenta el valor de sobrecarga y el tamaño de cuadro en función del tipo de compresión.

$$Tamaño\ real\ cuadro = Tamaño\ de\ cuadro + Sobrecarga\ total$$

$$Tamaño\ real\ cuadro = 46\ [Kbytes] + 2{,}63\ [Kbytes]$$

$$Tamaño\ real\ cuadro = 48{,}63\ [Kbytes]$$

Con el tamaño real de uno de los cuadros se procede a determinar el ancho de banda que este utilizará al momento de ser transmitido

$$Ancho\ de\ Banda\ [Mbps] = Tamaño\ real\ cuadro\ [Kbytes] * fps$$
$$Ancho\ de\ Banda\ [Mbps] = 48.63\ [Kbytes] * 30\ fps * 8[bits]$$
$$Ancho\ de\ Banda\ [Mbps] = 11{,}67\ [Mbps]$$

Al multiplicar este valor por 16, que es el número total de cámaras se obtiene que el tráfico aproximado será de 187 Mbps.

Sin embargo, tomando en cuenta el crecimiento de la red inalámbrica y de las posibles cámaras que con el pasar del tiempo se agreguen la capacidad del canal inalámbrico, este valor debe ser multiplicado por un 20 % obteniéndose un valor final de 224 Mbps.

2.5 DIRECCIONAMIENTO IPv4 [14]

Para el presente proyecto es necesario utilizar un direccionamiento IPv4 estático, de esta forma se puede monitorear cada una de las cámaras y a los dispositivos intermedios con el fin de detectar si estos están activos o no.

Debido a que la red de área local sobre la cual se implementa el sistema de video vigilancia es una red privada se debe utilizar direcciones IP privadas las mismas que se especifican en la regulación RFC 1918, estos rangos de direcciones son:

CLASE A: 10.0.0.0 a 10.255.255.255

CLASE B: 172.16.0.0 a 172.16.255.255

CLASE C: 192.168.0.0 a 192.168.255.255

Siendo la elección del rango completamente arbitrario, se tomara para este proyecto la siguiente red 192.168.100.0 con mascara 255.255.255.0, la misma que será segmentada para ordenar de mejor manera los dispositivos.

Los dispositivos que actualmente son considerados en el diseño son: 16 cámaras, 1 servidor, 7 puntos de acceso inalámbrico; sin embargo, es necesario tener en cuenta que el sistema de video vigilancia tiende a crecer por lo cual se considera un 20% de crecimiento en el número de dispositivos; por lo tanto, el direccionamiento se hará tomando generosamente en cuenta un número de dispositivos total de 28 dispositivos.

A continuación, se muestra el procedimiento para el cálculo de las direcciones IPv4 en este proyecto. Inicialmente es necesario identificar la porción de red y de host para esto se ha de usar la siguiente expresión:

$$Número\ de\ host \leq 2^N - 2$$

En la ecuación anterior N representa el número de bits que corresponde al segmento de host. Reemplazando los valores se tiene:

$$28 \leq 2^N - 2$$

Despejando N de la expresión anterior se tiene que N es igual a 5. Por tanto, el número de bits para la porción de host es 5 lo que permite incluir dentro de este segmento de red hasta 30 dispositivos. La red segmentada será entonces: 192.168.1.0 con máscara 255.255.255.224. En la Tabla 2.7 se muestra las direcciones de red, de broadcast y las direcciones utilizables.

Tabla 2.7 Cálculo de la subred

DESCRIPCION	**IP**	**MÁSCARA**
Dirección de Red	192.168.200.0/27	255.255.255.224
Primera dirección utilizable	192.168.200.1/27	255.255.255.224
Última dirección utilizable	192.168.200.30/27	255.255.255.224
Dirección de Broadcast	192.168.200.31/27	255.255.255.224

2.5.1 DIRECCIONAMIENTO DE DISPOSITIVOS DE LA RED

Como dispositivos finales se entiende a las cámaras y al servidor. Las direcciones IP que se van a utilizar para los mismos, constan en la Tabla 2.8:

Tabla 2.8 Direccionamiento de dispositivos

DISPOSITIVO	**IP**	**MASCARA**	**GATEWAY**
Router-AP	192.168.100.1	255.255.255.224	-
Servidor	192.168.100.2	255.255.255.224	192.168.100.1
Cámara 01	192.168.100.3	255.255.255.224	192.168.100.1
Cámara 02	192.168.100.4	255.255.255.224	192.168.100.1
Cámara 03	192.168.100.5	255.255.255.224	192.168.100.1
Cámara 04	192.168.100.6	255.255.255.224	192.168.100.1
Cámara 05	192.168.100.7	255.255.255.224	192.168.100.1
Cámara 06	192.168.100.8	255.255.255.224	192.168.100.1
Cámara 07	192.168.100.9	255.255.255.224	192.168.100.1
Cámara 08	192.168.100.10	255.255.255.224	192.168.100.1
Cámara 09	192.168.100.11	255.255.255.224	192.168.100.1
Cámara 10	192.168.100.12	255.255.255.224	192.168.100.1
Cámara 11	192.168.100.13	255.255.255.224	192.168.100.1
Cámara 12	192.168.100.14	255.255.255.224	192.168.100.1
Cámara 13	192.168.100.15	255.255.255.224	192.168.100.1

Cámara 14	192.168.100.16	255.255.255.224	192.168.100.1
Cámara 15	192.168.100.17	255.255.255.224	192.168.100.1

2.6 DIMENSIONAMIENTO Y SELECCIÓN DEL SERVIDOR

Elegir el equipo que se va a utilizar como servidor del sistema de video vigilancia se torna vital, para esto se ha de tener en cuenta los requerimientos de hardware (procesador, tarjeta de red, almacenamiento, etc.) y de software (sistema operativo).

2.6.1 REQUERIMIENTOS DE HARDWARE Y SOFTWARE [23]

Zoneminder requiere un sistema operativo estable por lo cual se ha decidido utilizar Linux en su distribución CentOS 6, Los requerimientos mínimos para instalar este sistema operativo son:

- Memoria Ram: 64 MB
- Espacio en Disco: 1024 GB
- Procesador: Intel Pentium I/II/III/IV, Intel Celeron o AMD Duron, etc.
- Tarjeta de Red: Ethernet 100/1000 Mbps

2.6.2 REQUERIMIENTOS DE ALMACENAMIENTO

La información que genera el sistema de video vigilancia debe ser almacenada en discos duros, estos pueden estar dentro del servidor o en discos externos. En este apartado se calculará el tamaño del disco duro que guardará la información.

Con la capacidad de canal antes calculada, y el tiempo que este operará continuamente se estimará aproximadamente cuanta información se almacenará utilizando la siguiente expresión:

$$Almacenamiento = \frac{AB[Mbps] * tiempo}{8\ bits}$$

El tiempo que se utilizará en este caso es un día, pasado este tiempo la información será comprimida y destinada a otros dispositivos de almacenamiento que no vienen al caso dentro de este proyecto.

Aplicando la expresión a este caso en particular se tiene:

$$Almacenamiento = \frac{224[Mbps] * 86400\ \left[\frac{s}{dia}\right]}{8bits}$$

$$Almacemaniento = 2.42\ Terabytes$$

El valor obtenido es demasiado elevado, el costo técnico y económico entonces volvería a este proyecto irrealizable, sin embargo, Zoneminder puede ser configurado para que grabe únicamente cuando se detecte movimiento, en un horario determinado, con lo cual el valor real a utilizarse será más bajo.

Otra política a implementarse para lograr disminuir la cantidad de información es definir cada cámara con un valor de FPS en función de la ubicación de la misma.

Considerando esto se puede definir que las únicas cámaras con un FPS de 30 serán las dos cámaras PTZ, la cámara ubicada en el parqueadero y en el área del domicilio. Todas las demás tendrán un valor de 1 FPS, el cual entrega un parpadeo casi imperceptible al ojo humano y es suficiente para tener un monitoreo satisfactorio de las instalaciones.

Además se configurará una barrera virtual, o zonas, donde el sistema envíe una notificación de correo electrónico cuando se detecte movimiento y al mismo tiempo empiece a grabar el evento mientras dure.

Con estas aseveraciones se procede a realizar el nuevo cálculo en cuanto a almacenamiento.

Se procede a calcular el valor del ancho de banda para las cámaras que trabajarán a 1 FPS:

$$Ancho\ de\ Banda\ [Mbps] = Tamaño\ real\ cuadro\ [Kbytes] * fps$$

$$Ancho\ de\ Banda\ [Mbps] = 48.63\ [Kbytes] * 1\ fps * 8[bits]$$

$$Ancho\ de\ Banda\ [Mbps] = \ 0{,}4\ [Mbps]$$

Se tenía el valor de las cámaras que trabajarán a 30 fps:

$$Ancho\ de\ Banda\ [Mbps] = Tamaño\ real\ cuadro\ [Kbytes] * fps$$

$$Ancho\ de\ Banda\ [Mbps] = 48.63\ [Kbytes] * 30\ fps * 8[bits]$$

$$Ancho\ de\ Banda\ [Mbps] = \ 11{,}67\ [Mbps]$$

Para el número total de cámaras se tendría:

$$Ancho\ de\ Banda\ [Mbps] = Ancho\ de\ banda * \ número\ de\ cámaras$$

$$Ancho\ de\ Banda\ [Mbps] = 0{,}4 * \ 14 + 11{,}67 * 2$$

$$Ancho\ de\ Banda\ [Mbps] = 5{,}6 + 58{,}35$$

$$Ancho\ de\ Banda\ [Mbps] = 23{,}34\ Mbps$$

Se utiliza el criterio de un 20% de crecimiento de la red y se tiene 28 Mbps de ancho de banda; entonces el nuevo valor de almacenamiento requerido para una semana es:

$$Almacenamiento\ = \frac{AB[Mbps] * tiempo}{8\ bits}$$

$$Almacenamiento\ = \frac{28[Mbps] * 86400\ \left[\frac{s}{dia}\right] * 7dias}{8\ bits}$$

$$Almacenamiento\ = \frac{28[Mbps] * 8640 0\ \left[\frac{s}{dia}\right] * 7dias}{8\ bits}$$

$$Almacenamiento\ = 2{,}11\ Tb$$

Como este valor está calculado con el mayor valor para una trama, así como con estimaciones de crecimiento. Un arreglo de discos duros de 4 Tb sería más que suficiente para la información a utilizarse.

2.6.3 ELECCIÓN DEL SERVIDOR

Establecidos los requerimientos para el servidor de video es necesario seleccionar un equipo que los cumpla e incluso los aventaje para el buen funcionamiento del sistema. El equipo que se utilizaría como servidor debe cumplir con los requisitos mínimos exigidos por zoneminder, Linux y los cálculos obtenidos

- PROCESADOR: Intel Pentium 4 o superior
- MEMORIA RAM: mínimo 1 GB
- DISCO DURO: 4 TB, puede ser almacenamiento externo.
- TARJETA DE RED:10/100/1000 Ethernet

Si bien se puede personalizar las capacidades de los servidores dependiendo de las necesidades, se detalla en la Tabla 2.9 las características del servidor DELL POWEREDGE T130 II, el cual cumple con los requerimientos mínimos antes indicados, además de que la marca DELL ofrece garantía de un año en todos sus equipos y además presenta valores inferiores con respecto a sus competidores como HP.

Tabla 2.9 Características Servidor Dell [24]

Servidor Dell PowerEdge T130 II	
Procesador	Familia de productos de procesadores E3-1200 v6 Intel® Xeon® Intel Pentium® Intel Core i3® Intel Celeron®
Sistema Operativo	Sin sistema operativo
Memoria	Arquitectura: hasta 2400 MT/s DDR4 DIMM Tipo de memoria: UDIMM Sockets del módulo de memoria: 4 RAM máximo: hasta 64 GB
Almacenamiento	Discos duros de 3,5" Enterprise SATA (7200) Discos duros de 3,5" nearline SAS y 7200 RPM Unidades de entrada SATA de 3,5” y 7200
Compartimientos de unidades	4 discos duros de 3,5" con cables
Ranuras	4 ranuras:

	1x8 PCIe de 3.0 (de 16 conectores) 1x4 PCIe de 3.0 (de 8 conectores) 1x4 PCIe de 3.0 (de 8 conectores) 1x1 PCIe de 3.0 (de 1 conector)
Controladoras RAID	S130,H330,H730, H830
Controladora de red	Broadcom® BCM5720
Comunicaciones	2 LOM de 1 GbE
Alimentación	PSU de 290W con cable
Chasis	Minitorre
Acceso al dispositivo	8 USB en total: USB posterior: dos USB 3.0 más cuatro USB 2.0 USB frontal: un USB 2.0 más un USB 3.0

2.7 ENRUTADOR INALÁMBRICO

Para el presente proyecto se utilizará un enrutador inalámbrico Linksys WRT54GL, sus características principales se detallan en la Tabla 2.10.

Tabla 2.10 Características enrutador Linksys WRT54GL [25]

CARACTERISTICAS ENRUTADOR LINKSYS WRT54GL	
MODELO	WRT54GL
ESTANDAR	IEE802.3, IEE802.3u, IEEE802.11g, IEEE802.11b
CANALES	11 canales
PUERTOS	Internet: 1 puerto 10/100 RJ45; LAN: 4 puertos 10/100 conmutados RJ45
POTENCIA DE SALIDA RF	18dBm
SEGURIDAD	SPI, Firewall
SEGURIDAD INALAMBRICA	WPA2, WEP, MAC Filtering

2.8 SERVICIO DE INTERNET

Es conveniente que se pueda acceder al sistema de video vigilancia de manera remota, para ello es necesario contar con el servicio de internet. El ISP deberá cumplir dos requerimientos: velocidad adecuada del enlace de subida y bajada y que se provea una IP fija.

En el presente proyecto la velocidad de subida debe permitir que el video se pueda transmitir de manera continua al dispositivo remoto que el administrador del sistema esté utilizando. El proveedor de internet debe tener planes que se acomodan a las necesidades de la hostería.

La IP fija pública, una vez que esta esté asignada, se utilizará NAT (Network Address Traslation) para que la red interna intercambie paquetes con la red pública.

En la Tabla 2.11 se resumen los requerimientos del acceso de internet:

Tabla 2.11 Requerimientos del acceso a Internet

REQUERIMIENTOS DE ACCESO A INTERNET	
Tipo de conexión	IP fija
Velocidad Up/Down	75 Mbps simétrica
Compartición de servicio	2 a 1
Seguridad	Firewall

En base a estas necesidades se comparan dos ofertas de proveedores nacionales, los cuales se indican en la Tabla 2.12.

Tabla 2.12 Ofertas de servicios de internet empresarial

Características servicios de Internet [31] [32]		
Especificaciones	Netlife	CNT Pymes
Tipo de conexión	IP Fija	IP Fija
Velocidad Up/Down	1024/512 Mbps	1024/512 Mbps
Compartición de servicio	2 a 1	2:1
Seguridad	Firewall	Firewall
Costo mensual dólares	65,50/mensual	50,40/mensual
Costo instalación dólares	112,00	89,60

En base a esta información se decide por el servicio de CNT, el cual es más económico y cuenta ya con una instalación previa de internet doméstico. Además en la provincia de Pastaza Netlife no cuenta con cobertura de fibra óptica.

2.9 SISTEMA DE ALIMENTACIÓN ININTERRUMPIDA (UPS) [11]

Un UPS es un dispositivo que permite un suministro continuo de energía eléctrica en caso de alguna falla en la red pública, además cumple funciones secundarias como la corrección de la frecuencia y forma de onda, incluso permite el monitoreo de la línea eléctrica.

Dentro del presente proyecto un UPS debe cumplir con lo siguiente:

- Protección contra transitorios
- Alta eficiencia de la batería
- Tipo de funcionamiento online.
- Cubrir los requerimientos de potencia de los equipos de CCTV

Con respecto a este último requerimiento es necesario realizar los cálculos respectivos con el fin de elegir un UPS que los cumpla con sobra, se seguirá el siguiente procedimiento:

Listar las potencias de todos los elementos del sistema

- Convertir dichas potencias en VA
- Sumar las potencias de los dispositivos
- Añadir un factor de seguridad

En la Tabla 2.12 se puede apreciar el cálculo para el dimensionamiento del UPS

Tabla 2.13 Dimensionamiento del UPS

DIMENSIONAMIENTO DEL UPS			
CANTIDAD	EQUIPO	VATIOS (Watts)	VA
4	Cámara Foscam FI8919W	5,5.00	22.00
10	Cámara DCS 2330L	5.00	50.00
2	Cámara PTZ Sentinel	10.00	28.00

1	Enrutador Inalámbrico Linksys WRT54GL	6.00	8.40
7	Access Point Lynksys	3.00	21.00
1	Servidor Dell	290.00	406.00
SUBTOTAL			535.4
FACTOR DE SEGURIDAD 25%			133.85
TOTAL			669.25

Con este valor obtenido, se decide por el siguiente equipo UPS. El forza FDC - 1000T con las siguientes características que se indican en la Tabla 2.13.

Tabla 2.13 Características UPS Forza FDC 100T [26]

Capacidad	1000 VA / 800 W
Topología	Doble conversión
Tensión Nominal entrada	100-127 VCA
Margen de tensión (transferencia por pérdida de tensión en la línea	55 VCA +- 5% con una carga del 50% 85 VCA +- 5% con una carga del 100%
Frecuencia entrada	40 Hz – 70 Hz
Factor de potencia	0.99 con una carga del 100%
Tipo de toma de CA	NEMA 5-15 P
Tensión nominal salida	100-127 VCA

Tiempo de transferencia de línea a batería	0 ms
Tipo y cantidad de baterías	12 V / 9Ah
Tiempo de autonomía	14 min a plena capacidad
Tiempo de recarga	4 horas con una capacidad del 90%
Indicadores visuales	Pantalla LCD con iluminación de fondo azul
Peso	9,8 Kg
Garantía	2 años para la UPS, 1 año para la batería.

2.10 CONFIGURACION DE LOS EQUIPOS [23]

A continuación se describe mediante capturas de pantalla los parámetros configurados en los equipos a utilizarse.

2.10.1 CONFIGURACIÓN DE LAS CÁMARAS IP

Utilizando un cable de red, y una computadora se asigna manualmente direcciones IP a las cámaras según la distribución que se hizo anteriormente. En las siguientes figuras se puede ver los pasos que se siguieron para la configuración de las cámaras. En la Figura 2.22 se puede apreciar la asignación de las direcciones IP.

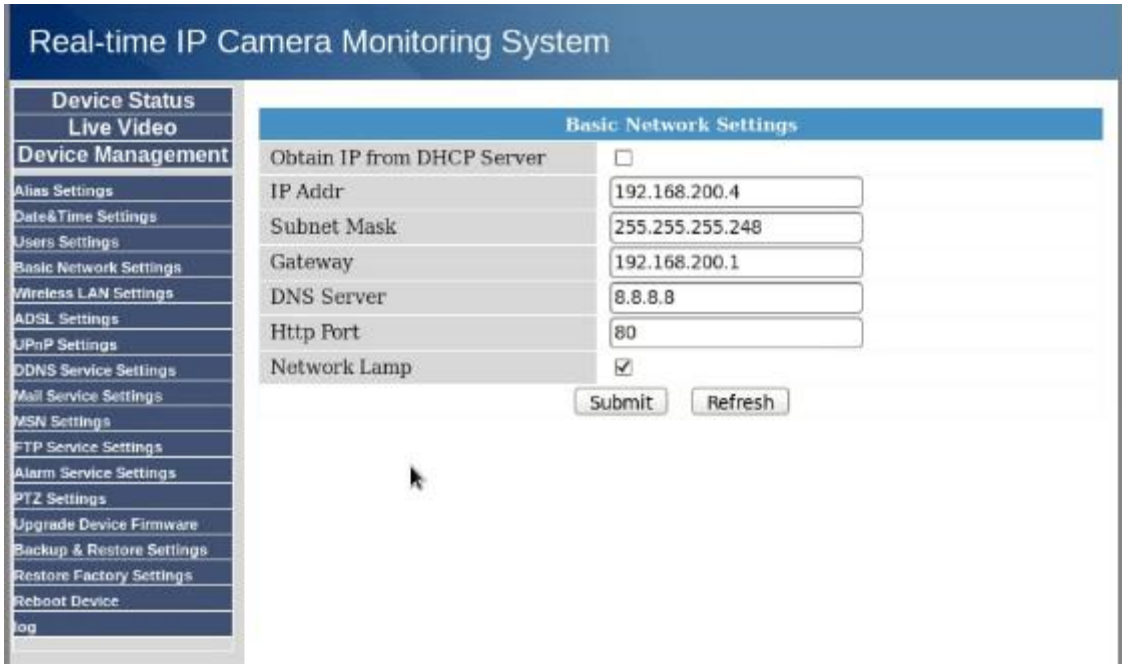

Figura 2.22 Configuración de dirección IP fija

En la Figura 2.23 se configura que la conexión debe ser con un AP determinado y la clave de conexión respectiva.

Seguidamente se configura el usuario y contraseña de acceso a la cámara en la Figura 2.24.

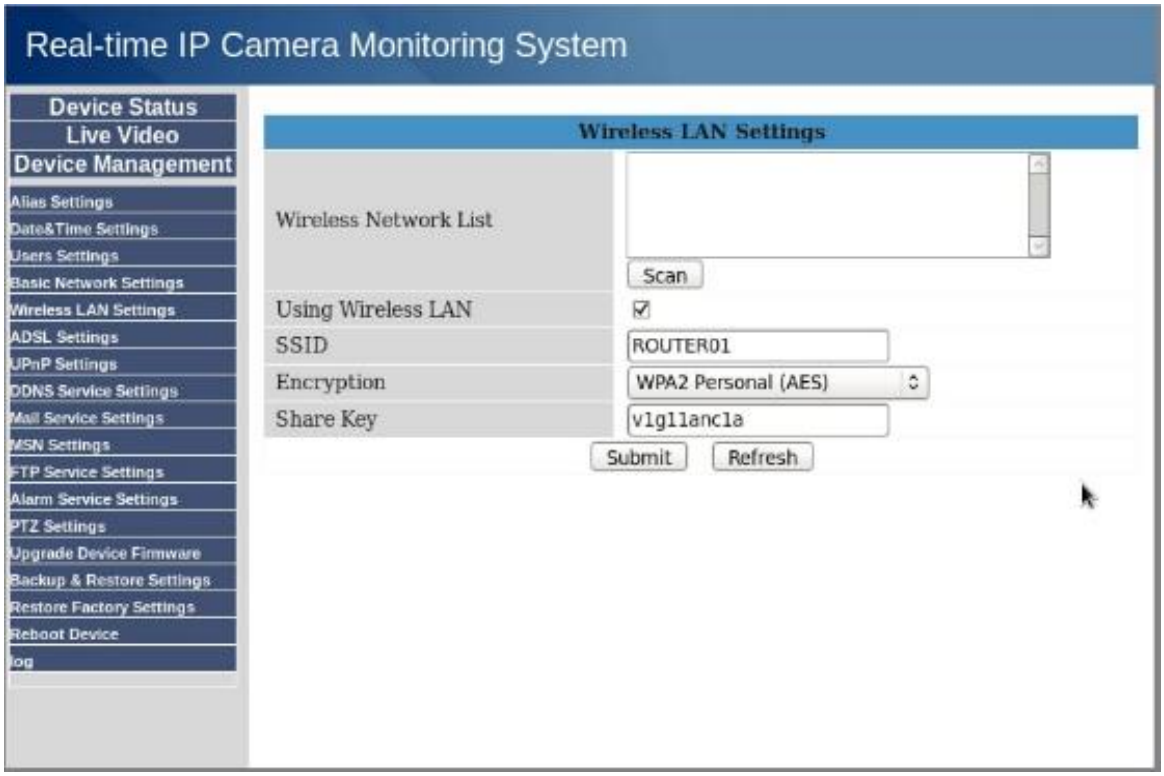

Figura 2.23 Configuración de la red inalámbrica en la cámara

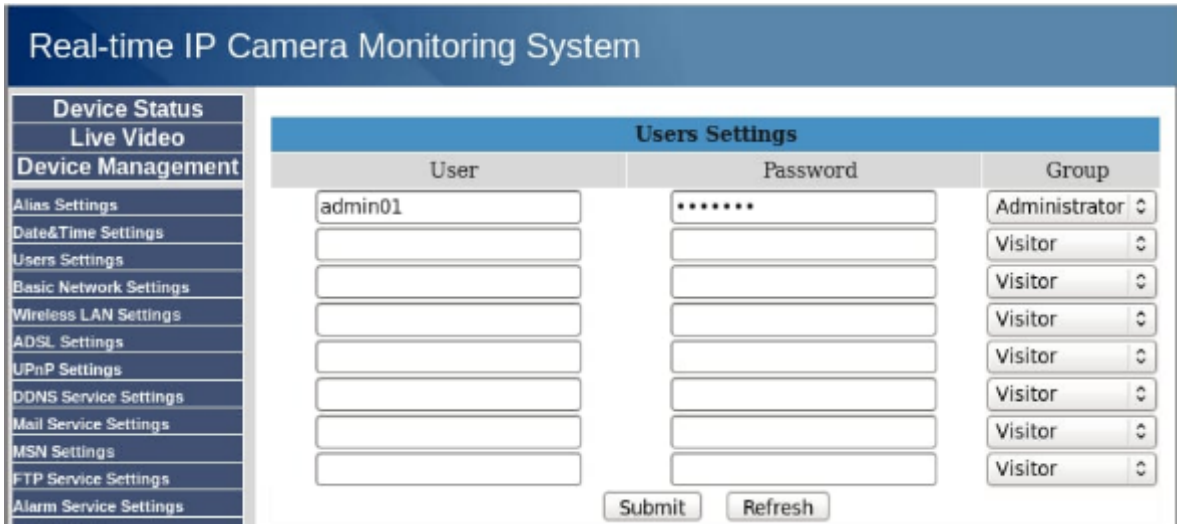

Figura 2.24 Configuración de usuario y contraseña

2.10.2 CONFIGURACIÓN DEL ENRUTADOR INALÁMBRICO [23]

La configuración del enrutador inalámbrico comprende dos partes, a saber: el lado de la red interna donde van conectadas las cámaras y el servidor, y el lado de la conexión a internet.

2.10.2.1 Configuración de la red interna

La dirección IP que se le asigna al enrutador inalámbrico es: 192.168.100.1, con máscara: 255.255.255.224, esta dirección será utilizada como puerta de salida para el resto de los dispositivos. Adicionalmente se configura la red interna inalámbrica para que las cámaras se conecten a la misma

En primer término, se puede observar la configuración del direccionamiento interno en la Figura 2.25:

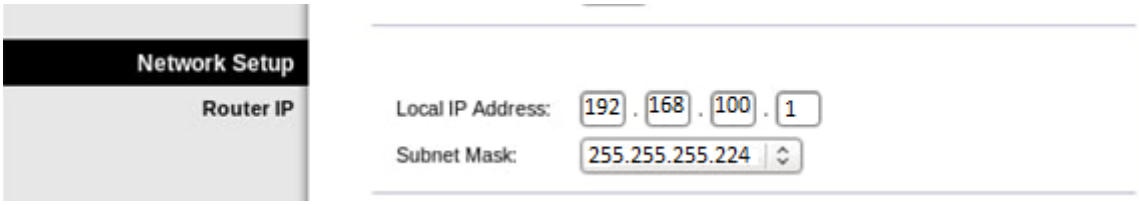

Figura 2.25 Configuración de dirección interna en el enrutador

Se establece el canal de operación y el nombre del SSID en la Figura 2.26.

Figura 2.26 Configuración de la red inalámbrica

El tipo de seguridad que se va a utilizar inicialmente es WPA2 Personal, la misma que contempla una contraseña que tanto la cámara como el enrutador conocen, esto se muestra en la Figura 2.27.

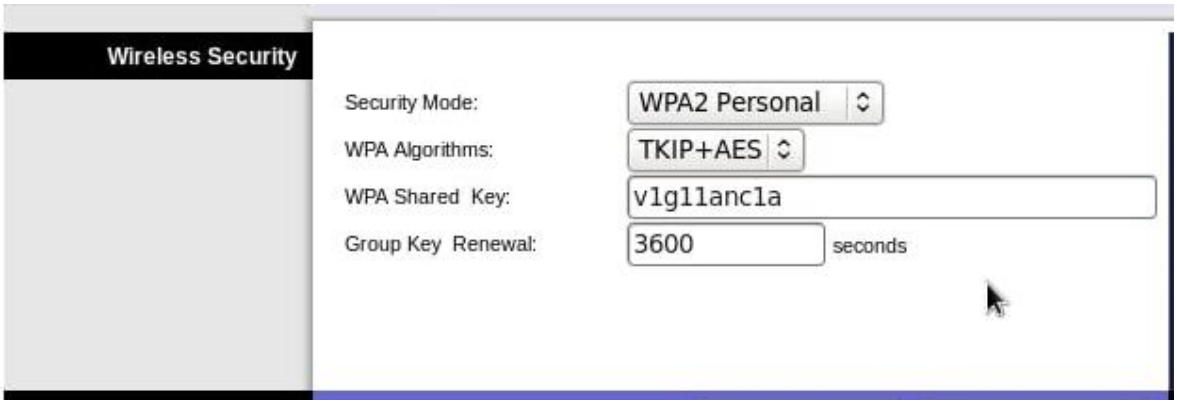

Figura 2.27 Configuración de seguridad para red inalámbrica

2.10.2.2 Configuración de la red externa

Para lograr este propósito es necesario conocer que direccionamiento está brindando el proveedor de internet. Este direccionamiento normalmente es por medio de DHCP así que se procede a conectar un dispositivo a uno de los puntos del modem del proveedor y se obtiene la dirección IP, mascara y puerta de enlace. Con estos datos entonces se da una dirección a la interfaz del enrutador inalámbrico que está designada como salida hacia el internet. Figura 2.28.

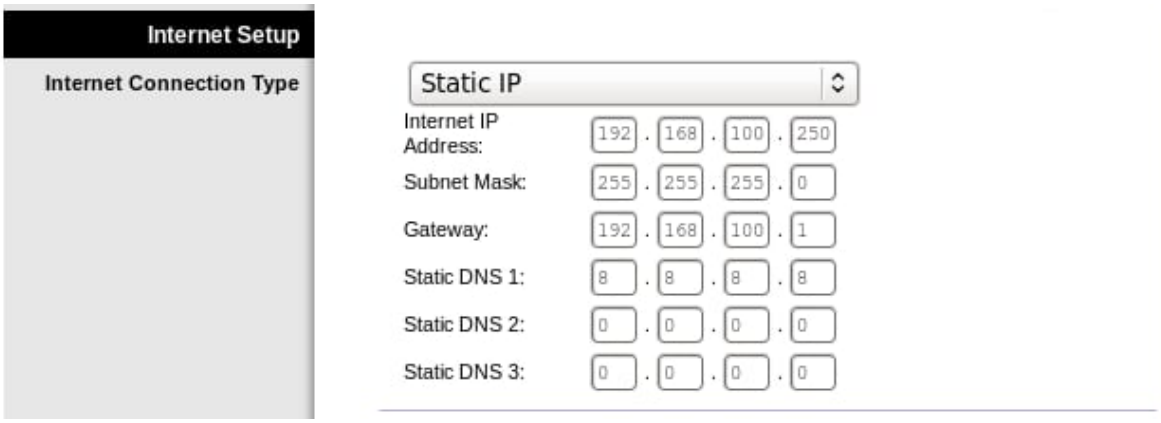

Figura 2.28 Configuración dirección IP externa

Seguidamente se configura el enrutador inalámbrico en la Figura 2.29 para que pueda salir al Internet. Para lograr este propósito se configura una ruta por defecto.

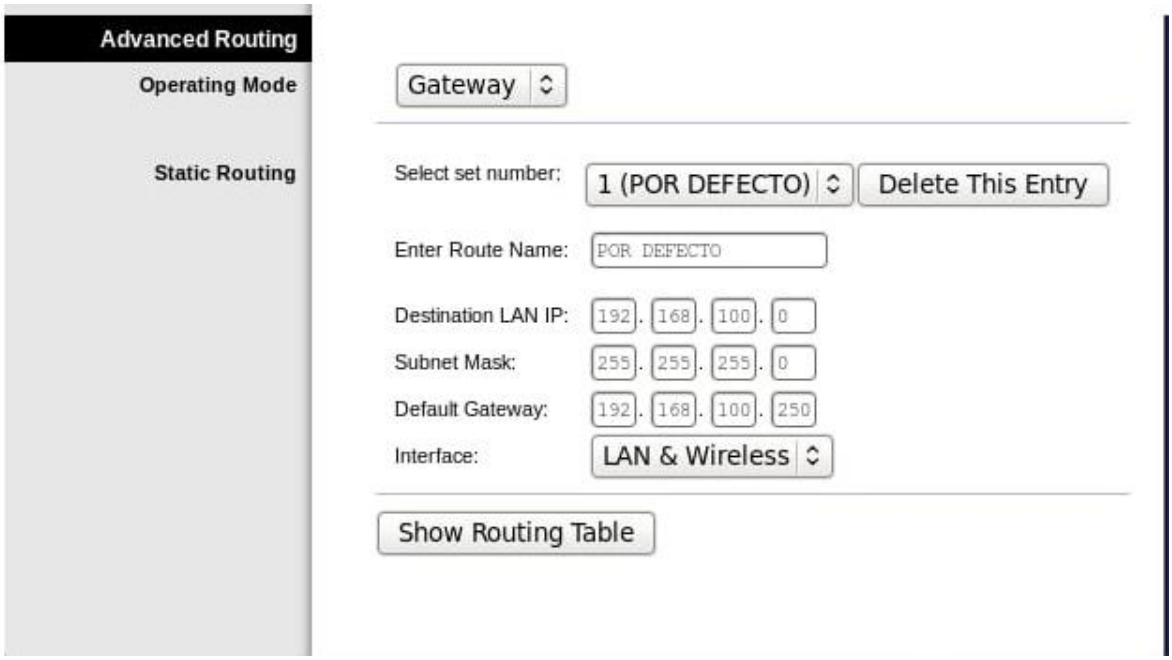

Figura 2.29 Configuración de ruta por defecto

2.10.3 CONFIGURACIÓN DE LAS CÁMARAS EN ZONEMINDER [23]

ZoneMinder dentro de su programación incluye algunos modos de obtención de imágenes a saber: Monitor, Modect, Record, Mocord, etc. De éstas, la que interesa es la función Modect que permite la visualización continua de las imágenes y graba únicamente cuando se presenta un evento. En las imágenes siguientes se muestra la configuración de la cámara Foscam FI8918W. La configuración para las demás cámaras es similar.

Después de dar clic sobre Añadir nuevo monitor en la plataforma de ZoneMinder la primera vista es la de la pantalla General, Figura 2.30 donde se configura la función de la cámara y el origen de la misma

La configuración comprende: Nombre del monitor, para asignar un nombre al monitor. Tipo de origen: remoto, en este caso, con esto se da a entender que es una cámara IP

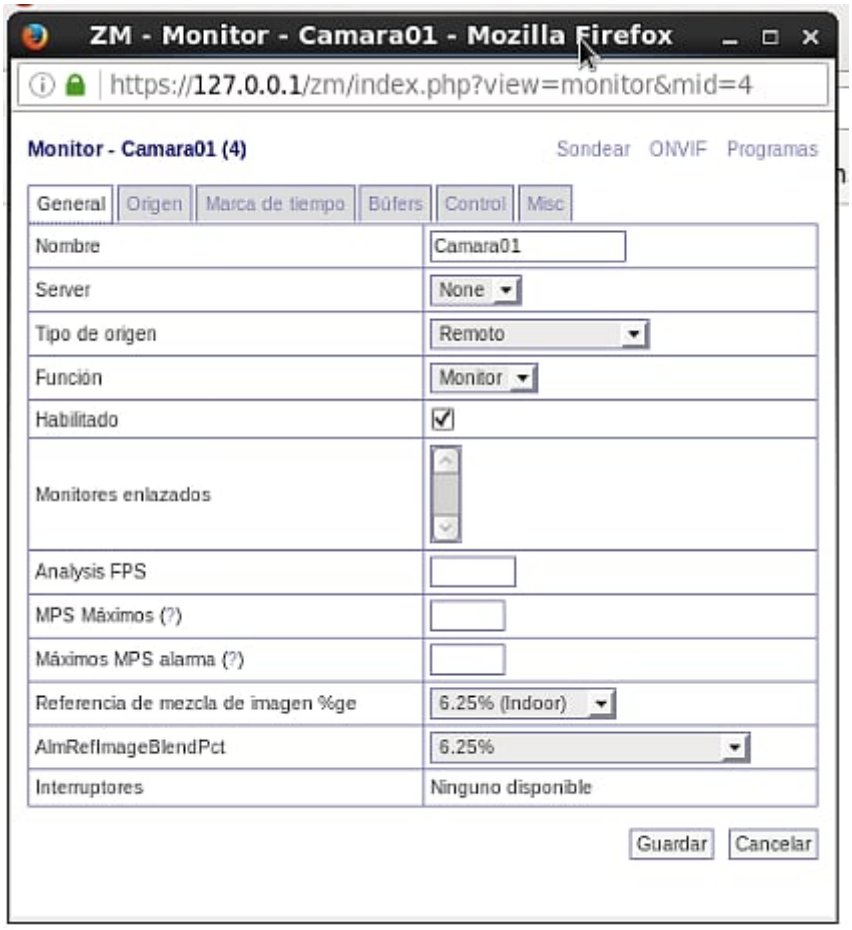

Figura 2.30 Pestaña General de ZoneMinder

La siguiente pestaña que compete analizar es la pestaña Origen. En esta pestaña se ha de configurar el protocolo que la cámara utiliza para comunicarse con el ZoneMinder, la dirección y puertos a los cuales debe apuntar ZoneMinder para extraer el flujo de imágenes. Otros parámetros importantes son la resolución, colores, etc.

Finalmente, la pestaña de Control, Figura 2.31, permite configurar los parámetros de comando a distancia de la cámara. Se especifica: tipo de control, el usuario y contraseña de las cámaras antes configuradas y la dirección IP de la cámara. Importante es recalcar que no todas las cámaras pueden interactuar con ZoneMinder.

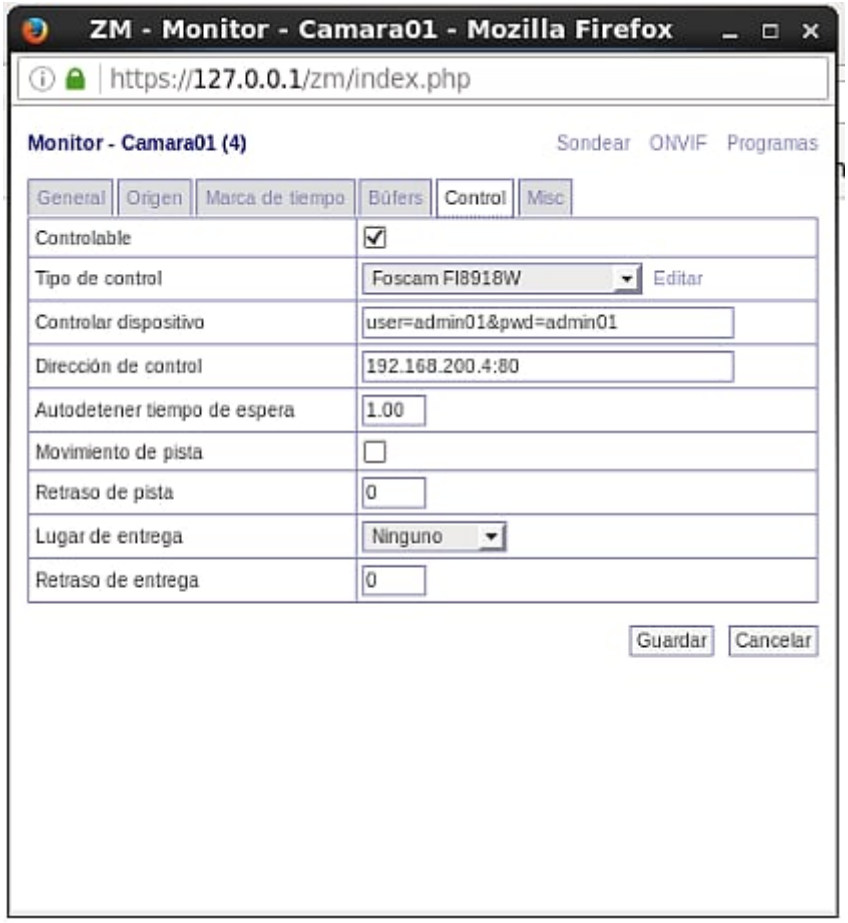

Figura 2.31 Pestaña Control de ZoneMinder

2.11 SEGURIDAD [23]

2.11.1 NIVELES DE ACCESO DE USUARIO

Zoneminder permite la configuración de usuarios con diferentes niveles de acceso, donde un usuario puede tener todos los privilegios de administrador y gestionar la red, otros usuarios pueden ser solamente observadores y puede haber usuarios con permisos limitados establecidos por el administrador.

Para la configuración de usuarios se lo debe realizar en la pestaña usuarios, en las opciones de Zoneminder. Figura 2.31

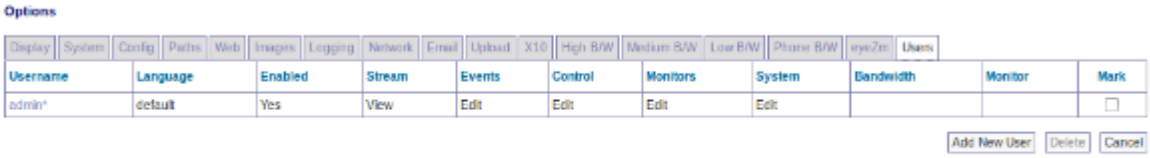

Figura 2.31 Pestaña usuarios

Para la creación de usuarios adicionales se debe ingresar en la opción agregar un nuevo usuario, Figura 2.32, con el botón respectivo. A continuación se muestra la ventana de creación de un determinado usuario.

Figura 2.32 Pestaña nuevo usuario

En la ventana anterior se puede configurar los diferentes permisos que puede tener un usuario determinado. Entre los campos a configurar se tienen los siguientes.

- Usuario.- Nombre del usuario.
- Nueva contraseña.- Contraseña del usuario.
- Confirmar contraseña.- Confirmación de la contraseña anterior del usuario.
- Lenguaje.- Determina el idioma de la interfaz para el usuario.
- Habilitado.- Habilitar o deshabilitar el usuario para su funcionamiento.

- Stream.- Determina la visualización o no de video.
- Eventos.- Determina el acceso a los eventos almacenados.
- Control.- Determina el acceso a gestionar el movimiento de las cámaras.
- Monitores.- Determina si el usuario puede o no agregar más monitores.
- Sistema.- Determina el acceso a las configuraciones avanzadas de Zoneminder.
- Máximo ancho de banda.- Determina el ancho de banda para el acceso remoto.
- Monitores restringidos.- Permite negar la visualización de determinados monitores.

Para el presente proyecto se crearán dos usuarios, un administrador y un visualizador, con el fin de que el usuario visualizador sólo pueda monitorear el sistema sin que modifique o ponga en riesgo el funcionamiento del sistema. El usuario administrador se deberá a asignar a una persona con los conocimientos necesarios para la gestión del sistema.

2.11.2 ALERTA DE INTRUSIÓN. [23]

Es necesario dentro del marco de este trabajo que el software de administración de cámaras Zoneminder envíe alertas a los administradores en caso de alguna intrusión en las instalaciones del edificio. Para lograr este propósito se cuenta con tres tipos de alertas: correo electrónico, por SMS, y por almacenamiento en el disco duro.

En este proyecto se ha considerado que la primera y tercera opciones son las más adecuadas puesto que la mayoría de usuarios en este momento tiene acceso a un plan de datos celular y puede visualizar los correos electrónicos en su teléfono inteligente.

Para lograr eso se debe configurar el servicio de correo electrónico en Zoneminder como se explica a continuación.

2.11.3 CONFIGURACIÓN DEL SERVIDOR DE CORREO [23]

Zoneminder permite enviar notificaciones por correo electrónico y por servicio SMS. En el presente proyecto se trabajará con la primera opción, instalando postfix en el servidor de gestión de las cámaras para el envío de las notificaciones. Sin embargo actualmente muchos de los servicios de correo que existen bloquean este tipo de correos por considerarlos spam.

Para evitar el bloqueo de las notificaciones se utiliza el servicio SMTP de google, lo cual hace que las alertas provenientes de Zoneminder utilicen como intermediario el servicio de google y lleguen al correo del usuario final.

Con esto se tiene como resultado que, en la bandeja de entrada del usuario, por ejemplo Hotmail, se reciba una alerta de Zoneminder desde Gmail.

En la Figura 2.33 ilustra el funcionamiento del servicio de SMTP de google para el envío de las notificaciones.

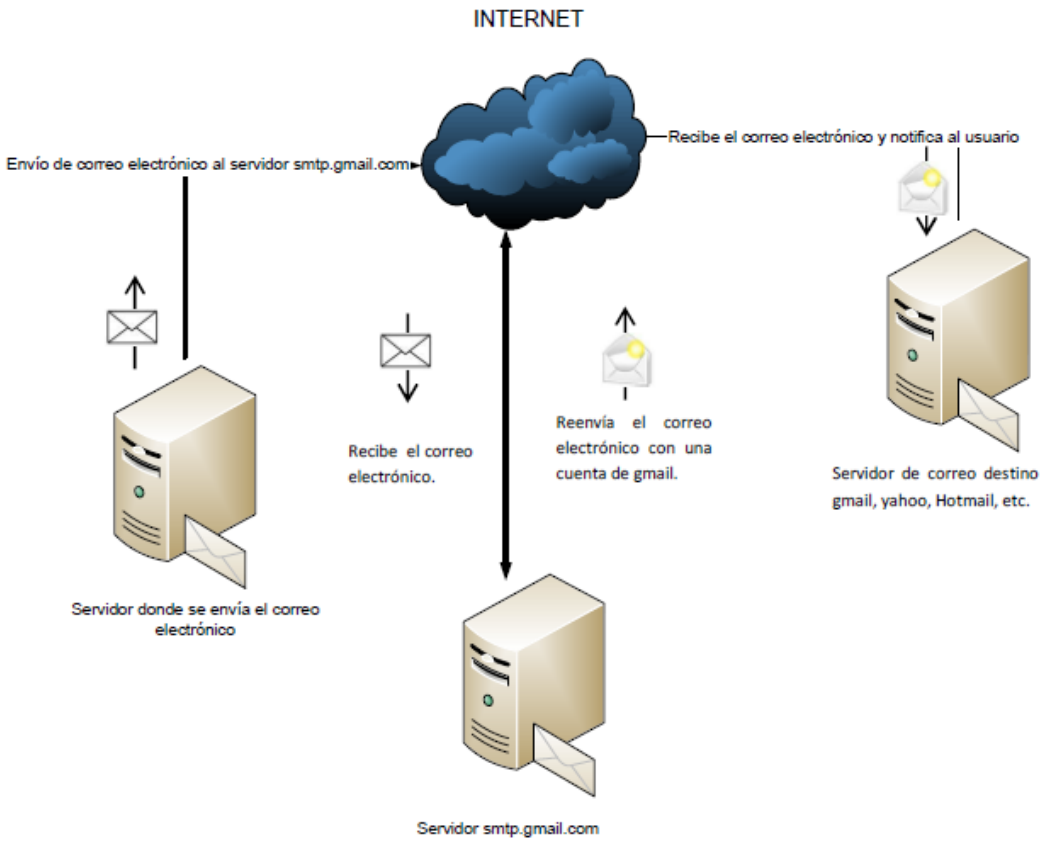

Figura 2.33 Esquema de correo utilizando SMTP de google

Se puede observar que el servidor de correo envía el correo electrónico hasta un servidor SMTP de Gmail, desde este sitio se reenvía el correo con una cuenta de Gmail hasta el servidor de correo destino, de esta manera se evita que el correo sea detectado como spam.

La configuración del servidor de correo se realiza utilizando Postfix como agente de transporte de correo.

Para la instalación del servidor Postfix se siguen los pasos en el anexo D.

Una vez instalado el servidor, se deben realizar configuraciones adicionales en la ventana de opciones de Zoneminder, en la pestaña Email, Figura 2.34. A continuación se muestra la pestaña en cuestión.

En la pestaña Email no sólo se configuran las notificaciones que se envían por correo sino también las configuraciones para el envío de notificaciones vía SMS. Como se mencionó anteriormente, en el presente proyecto se utilizará únicamente el envío de notificaciones vía correo electrónico, por tanto las opciones para el envío de las notificaciones vía SMS se dejarán en blanco.

Figura 2.34 Configuración de correo

Entre las opciones que se presentan en la pantalla anterior se puede editar el cuerpo de mensaje saliente, el asunto y cuando se deben generar estas alertas. Para ello se tienen los siguientes campos:

- OPT_EMAIL.- Activa la opción de enviar correos cuando se configuran determinados filtros como detección de movimientos o configuración de zonas de vigilancia, también llamadas perímetros virtuales.
- EMAIL-ADDRESS.- Establece la dirección de correo a donde se debe enviar la notificación de alarma.
- EMAIL-SUBJECT.- Establece el asunto del correo que se enviará.
- EMAIL_BODY.- Determina lo que se desea que esté en el cuerpo del correo electrónico a enviarse.
- Los campos que contienen la palabra MESSAGE son análogos a los descritas anteriormente y permiten la configuración de las notificaciones por SMS, que se omitirán para este proyecto.
- NEW_MAIL_MODULES.- Determina si se utilizará un método alternativo diferente al que viene por defecto en Zoneminder, lo cual no se va a emplear en el presente proyecto.
- EMAIL_HOST.- La dirección del host que enviará las notificaciones, en este caso es localhost por defecto.
- FROM_EMAIL.- Establece la dirección del servidor del SMTP que se va a utilizar.
- URL.- La dirección IP fija otorgada por el proveedor de internet.

En el campo EMAIL_BODY se deben configurar valores que se obtienen de Zoneminder, los cuales entregan detalles del evento detectado. A continuación se muestra la Tabla 2.12 con los diferentes valores a ser utilizados con sus respectivos significados:

Tabla 2.12 Métodos abreviados en Zoneminder

Valor	Descripción
%EI%	Id del evento
%EN%	Nombre del evento
%EC%	Causa del evento
%ED%	Descripción del evento
%ET%	Hora del evento
%EL%	Duración del evento
%EF%	Número de cuadros en el evento
%EFA%	Número de cuadros de alarma en el evento
%EST%	Puntaje total del evento
%ESA%	Puntaje promedio del evento
%ESM%	Puntaje máximo del evento
%EP%	Ruta del evento
%EPS%	Ruta del stream del evento
%EPI%	Ruta de las imágenes del evento
%EPI1%	Ruta de la primera imagen de alarma
%EPIM%	Ruta de la primera imagen de alarma con puntaje más alto
%EI1%	Adjunto de la primera imagen de alarma
%EIM%	Adjunto de la primera imagen de alarma con el puntaje más alto.
%EV%	Adjunto de evento en video
%MN%	Nombre del monitor
%MET%	Número total de eventos en el monitor
%MEH%	Número de eventos en el monitor en la ultima hora
%MED%	Número de eventos en el monitor en el último día

%MEW%	Número de eventos en el monitor en la última semana
%MEM%	Número de eventos en el monitor en el último mes
%MEA%	Número de eventos archivados del monitor
%MP%	Ruta a la pantalla del monitor
%MPS%	Ruta al streaming del monitor
%MPI%	Ruta a la imagen reciente en el monitor
%FN%	Nombre del filtro que se active
%FP%	Ruta al filtro que se active
%ZP%	Ruta a la consola de Zoneminder

2.11.4 FILTROS [23]

Los filtros en Zoneminder permiten ejecutar tareas automáticamente, como borrar información cuando el disco está lleno, enviar notificaciones por correo o SMS cuando se cumplan las condiciones configuradas en el filtro, etc.

Para optimizar el sistema de vigilancia se configurarán 3 filtros:

Uno para enviar las notificaciones de correo electrónico cuando se cumplan con la condición de que se haya detectado un cambio de al menos el 25 % de los pixeles en la zona respectiva. Las zonas se detallarán más adelante.

Un segundo filtro para la eliminación de la información del disco duro cuando la capacidad de éste haya llegado al 80 % del tamaño total.

Un tercer filtro para eliminar los eventos que tengan menos de 3 segundos de longitud.

La configuración de los filtros se lo realiza en la consola principal de Zoneminder, ingresando en la opción respectiva, como se muestra en la Figura 2.33:

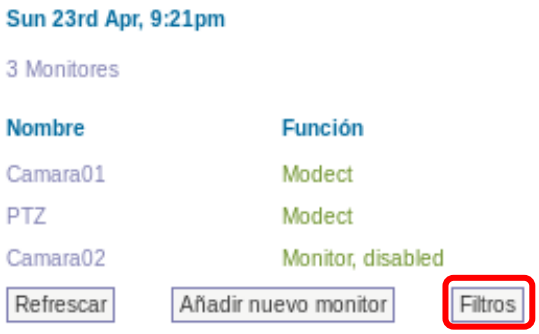

Figura 2.33 Menú filtros

En la Figura 2.34, se tienen los siguientes campos, los cuales permiten configurar los filtros necesarios.

Figura 2.34 Pantalla de configuración de filtros

Campo A: Permite seleccionar los distintos filtros configurados. Existe un único filtro preconfigurado, el cual es “purgar cuando está lleno”, que consiste en borrar eventos detectados que no se hayan almacenado cuando se ha llegado a un nivel determinado.

Campo B: Permite seleccionar la condición que debe cumplir el filtro.

Campo C: Un filtro puede tener más de una condición, con los botones más y menos se puede agregar o eliminar condiciones del filtro.

Campo D: Determina las acciones a realizar por el filtro cuando se cumplen las condiciones antes configuradas.

Campo E: Opciones a realizar cuando el filtro está completamente configurado.

A continuación, Figura 2.35, se muestra la configuración del filtro que viene por defecto, para eliminar los eventos que hayan sido almacenados y en conjunto lleguen a completar, para este ejemplo, el 80% de la capacidad total.

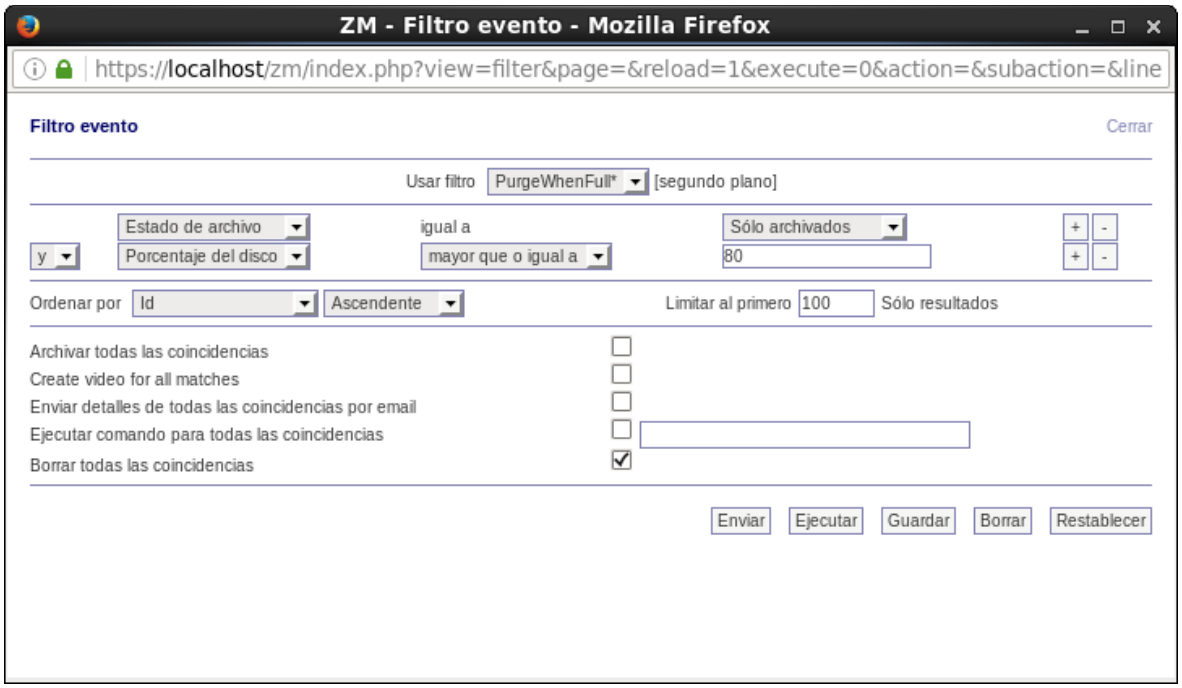

Figura 2.35 Filtro para eliminar los eventos almacenados cuando el espacio en disco ha llegado al 80% de capacidad.

En la figura 2.36 se muestra la configuración del filtro donde la alarma se dispara cuando el número de marcos o cuadros de alarma sea mayor a 20. Cuando esta condición se cumple se crea un video y se envía la alerta.

Figura 2.36 Configuración de filtro para enviar correos ante la detección de un evento.

De manera similar se puede configurar los filtros que se requieran para el funcionamiento del sistema de vigilancia.

2.11.5 ZONAS DE VIGILANCIA [23]

Zoneminder permite la configuración de zonas de vigilancia o perímetros virtuales, donde se puede especificar áreas más sensibles que otras para el caso de intrusiones.

Una zona de vigilancia puede ser toda el área de visualización de la cámara o se puede seccionar esta misma área de visualización en varias zonas más pequeñas con el fin de optimizar el funcionamiento de las alertas a detectarse.

Esto es útil por ejemplo para evitar que se generen falsas alarmas con las variaciones de luz o cuando una cámara tiene en su rango de visión dos entradas, haciendo que las dos entradas sean zonas sensibles a intrusiones.

En la Figura 2.37 se puede apreciar un ejemplo de la configuración de una zona de vigilancia, por ejemplo se tiene una vista de una calle, donde la zona activa, es decir, lo que se desea que se detecte es lo que ocurre en la calle, no en los arboles cercanos ya que el viento produce movimiento en éstos y generan falsas alarmas.

Figura 2.37 Ejemplo de zona de vigilancia activa.

En la imagen anterior se puede observar una zona activa, la cual se marca en color rojo. Como se dijo anteriormente, Zoneminder permite configurar más de una zona en cada área de visualización de cada cámara, además de que el programa ofrece la flexibilidad de que la zona pueda tener cualquier forma poligonal.

Además de zonas activas, se pueden configurar zonas a omitirse, las cuales son zonas donde no se deben generar alarmas cuando se detecte movimiento. Esto es útil en el caso donde se tenga por ejemplo un reloj de péndulo, luces que se encienden en el cielo raso o fluctuaciones de luz provenientes de cuartos contiguos por filtración de luz solar a través de alguna ventana. Es decir donde se tenga movimiento inevitable pero que no es relevante.

En el presente proyecto se determinarán zonas activas en las cámaras que tengan por área de visualización las zonas de ingreso al complejo turístico y la cámara del domicilio del propietario.

Estas zonas activas se combinarán con los filtros descritos anteriormente de tal manera que las cámaras que controlan el perímetro y el domicilio generen video y alarmas por correo en horas específicas, por ejemplo en la noche.

Durante el día todas las cámaras del complejo únicamente generarán video de los eventos, más no alarmas de correo.

En casos especiales si el administrador de la red lo requiere puede generar nuevas zonas y filtros para generar alarmas por correo diferente a lo descrito anteriormente. Por ejemplo si el complejo se debe cerrar en su totalidad por un día o dos, debido a un viaje y no exista una persona a cargo.

2.11.6 FIREWALL [14]

También conocidos como cortafuegos, los firewall son mecanismos que se implementan ya sea por software, por hardware, o una combinación de los dos, que gestionan el acceso a determinadas redes, bloqueando o permitiendo el ingreso de acuerdo a su configuración.

La configuración del firewall en el sistema de video vigilancia se debe configurar tanto en el servidor como en el equipo de red que permite el acceso a internet.

Por defecto todo el tráfico que trata de ingresar a la red de video vigilancia desde internet es bloqueado; para permitir el acceso a la interfaz del servidor y consecuentemente a las cámaras se va a utilizar la técnica del reenvío de puertos. La técnica de reenvío de puertos permite especificar cómo se va dirigir el tráfico hasta un equipo específico y al servicio específico que opera en el mencionado equipo, para esto es necesario indicar al servidor de seguridad o al enrutador la dirección IP y el puerto específico que se pretende utilizar para la conexión.

Para la administración del sistema de vigilancia se debe autorizar la conexión únicamente por determinados puertos en Zoneminder. La funcionalidad y descripción de los puertos disponibles se detallan en la Tabla 2.13.

Tabla 2.13 Descripción de puertos

PUERTO	PROTOCOLO	FUNCION
80	TCP	Permite la conexión al servidor web
22	TCP	Permite la administración remota del servidor
443	TCP	Permite conexiones seguras en el servidor
587	TCP	Permite conexiones con servidores externos SMTP
53	TCP	Permite resoluciones de dominio en servidores DNS.
123	TCP	Permite conexiones con servidores NTP

8081	TCP	Permite conexiones al router inalámbrico
8082	TCP	Permite conexiones al router inalámbrico
8083	TCP	Permite conexiones al router inalámbrico
8084	TCP	Permite conexiones al router inalámbrico

2.11.6.1 Apertura de puertos en el servidor

En el servidor se abrirán los puertos 80 y 443 los mismos que permiten el paso de los servicios de HTTP y HTTPS. Esta configuración se la realiza en el ambiente gráfico como se aprecia en la Figura 2.38.

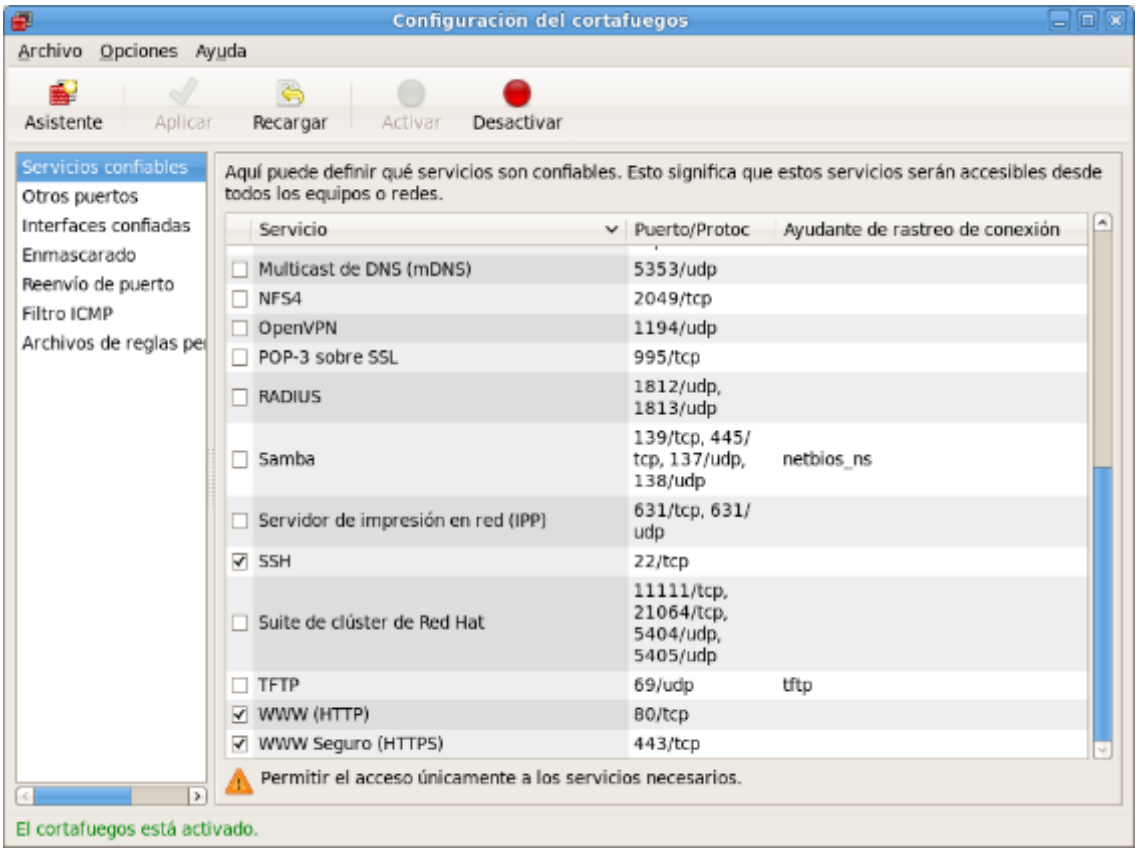

Figura 2.38 Apertura de puertos en modo gráfico

Además, esta configuración se verifica en el archivo de configuración del firewall en la Figura 2.39: /etc/sysconfig/iptables.

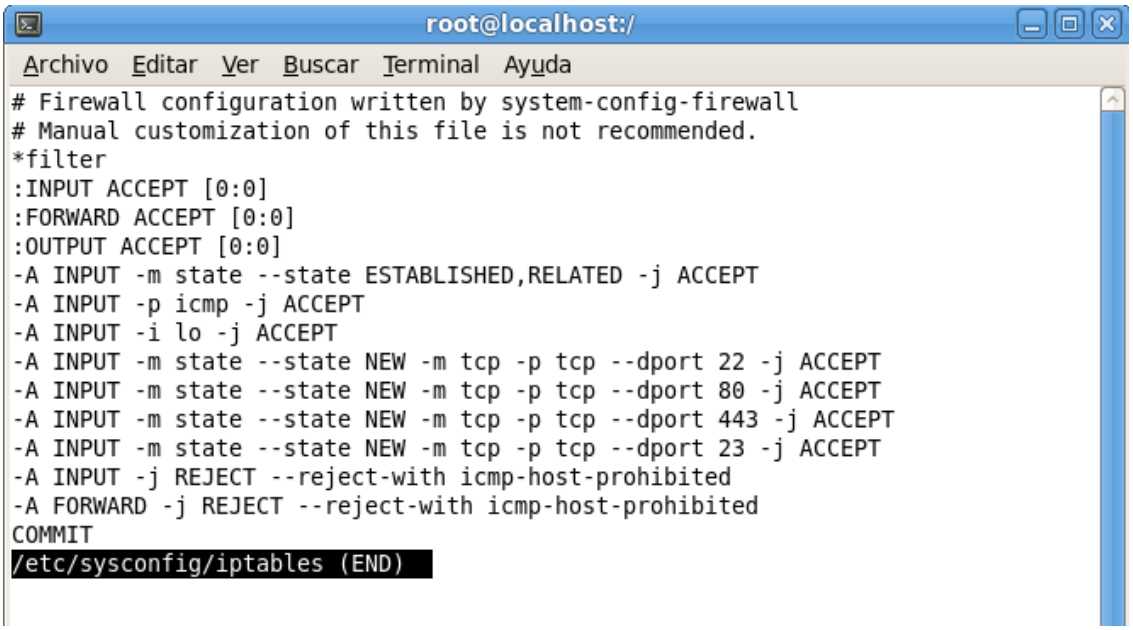

Figura 2.39 Apertura de puertos en modo consola

2.11.6.2 Configuración del reenvío de puertos en el enrutador [25]

Para el modelo que se presentará se utiliza un enrutador: Cisco Linksys WRT54GL en el mismo se configura el reenvío de puertos, lo cual es sencillo gracias a su interfaz web. En la Figura 2.40 se muestra la configuración de reenvío de puertos, de nuevo los puertos que se abren son el 80 y 443.

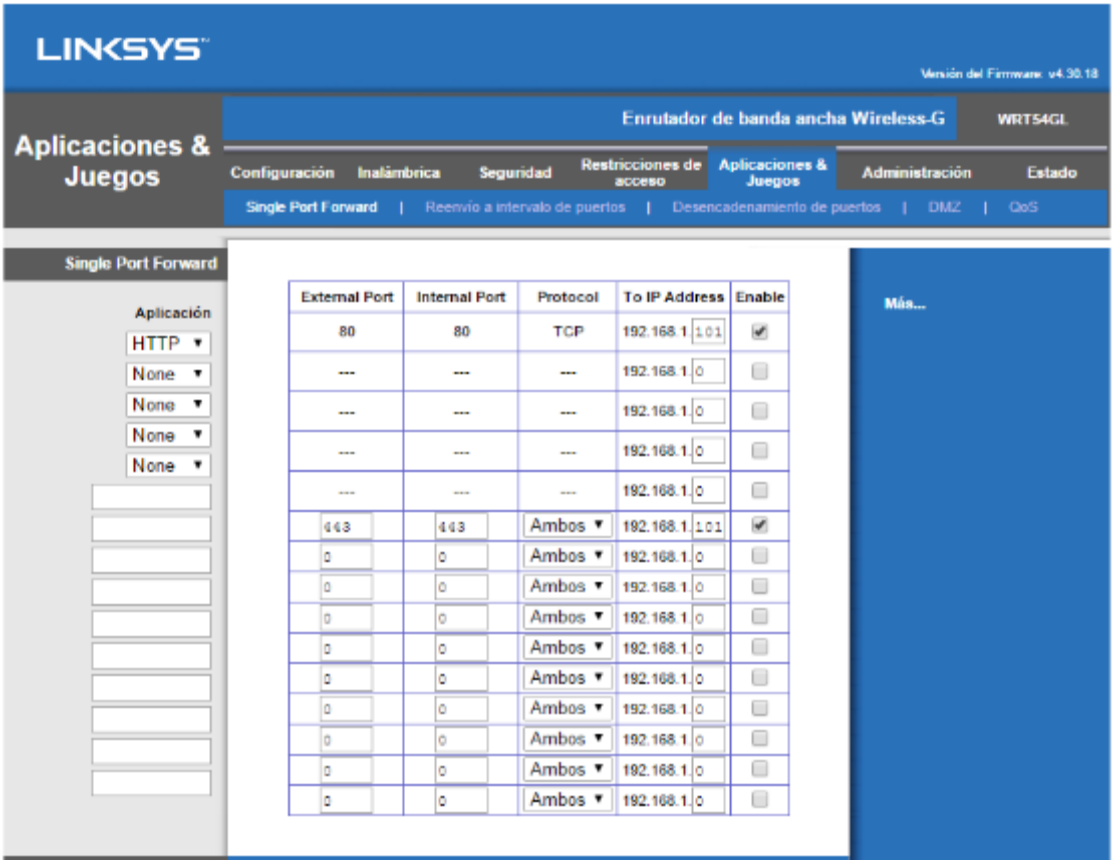

Figura 2.40 Reenvío de puertos en el router

Por otro lado es necesario desactivar la opción de protección por parte del ISP, esto se muestra en la Figura 2.41.

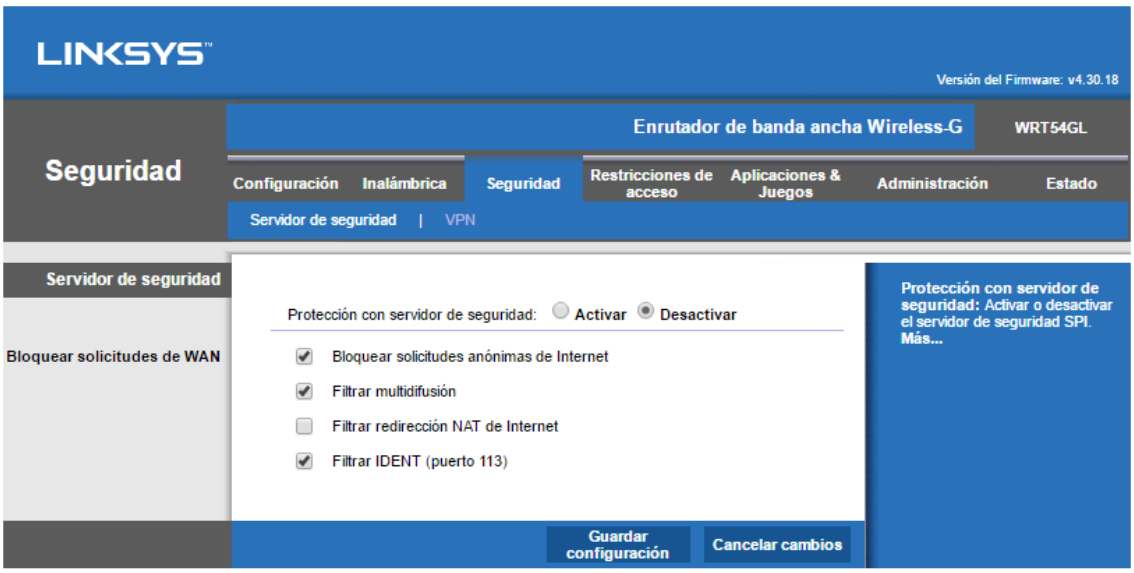

Figura 2.41 Configuración del firewall del ISP

Con las configuraciones mostradas ya es posible entrar a la interfaz de Zoneminder desde redes externas a través de internet.

2.12 MONTAJE DEL PROTOTIPO

Puesto que, tal como se definió en los objetivos de este trabajo, la red propuesta no será implementada, por razones económicas, en la Figura 2.42, se muestra un bosquejo de la red a implementarse como prototipo en el laboratorio de la EPN, donde constan elementos representativos de la red real, como el Access Point, el router principal para la conexión a internet y las cámaras IP.

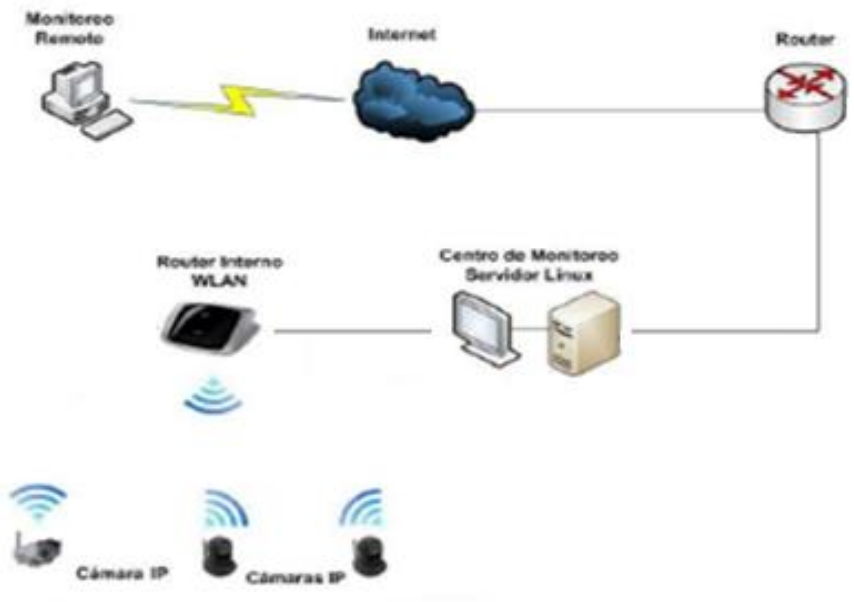

Figura 2.42 Topología del prototipo a implementarse

En el siguiente capítulo se procederá a realizar las pruebas pertinentes del prototipo propuesto con los debidos resultados y correctivos de ser el caso.

CAPÍTULO 3.
PRUEBAS Y RESULTADOS

3.1 INTRODUCCIÓN

El complejo turístico D'Marco'S no tiene sistema de vigilancia actualmente, y no dispone de los recursos económicos para implementar el sistema de vigilancia diseñado en el capítulo anterior, por tanto para comprobar los cálculos y el funcionamiento del mismo se procederá a implementar un prototipo con el equipo disponible, cumpliendo los requerimientos mínimos del diseño propuesto.

Las pruebas de funcionamiento se realizan en un periodo de tiempo determinado, para probar el funcionamiento de la transmisión de video, detección de movimiento y almacenamiento del evento, generación de alarmas, notificación por medio de correo electrónico de los eventos y determinación del ancho de banda utilizado por el sistema.

Se analizarán los datos recopilados durante las pruebas para detectar y solventar los posibles problemas que se presenten en el sistema.

3.2 IMPLEMENTACIÓN DEL PROTOTIPO

A continuación, Figura 3.1, se esquematiza el prototipo propuesto para la realización de las pruebas respectivas con el cual se pretende demostrar la validez del sistema diseñado.

El prototipo consta de un servidor, un router, un Access Point, dos cámaras inalámbricas y una alámbrica.

El propósito de la cámara alámbrica es reducir costos en el prototipo, demostrando, con análisis de tráfico, que reemplazar una cámara inalámbrica con una alámbrica no afecta el diseño del sistema propuesto de manera relevante.

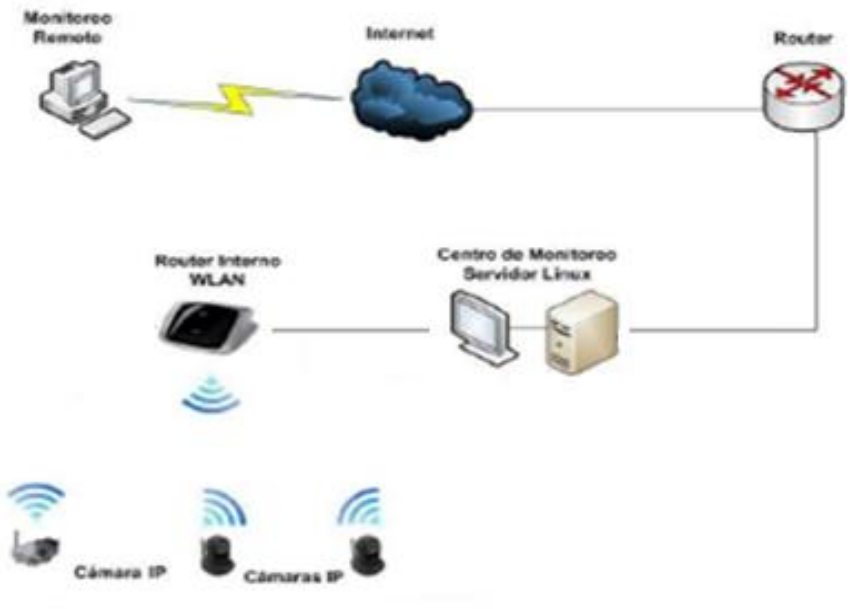

Figura 3.1 Topología del prototipo a implementarse

A continuación, se detallan los equipos a utilizarse.

3.2.1 ROUTER [25]

Para el presente prototipo se utilizará un enrutador inalámbrico Linksys WRT54GL, sus características principales se detallan en la Tabla 3.1.

Figura 3.2 Router Linksys WRT54GL [25]

Tabla 3.1 Características enrutador Linksys WRT54GL

CARACTERISTICAS ENRUTADOR LINKSYS WRT54GL	
MODELO	WRT54GL
ESTANDAR	IEE802.3, IEE802.3u, IEEE802.11g, IEEE802.11b
CANALES	11 canales
PUERTOS	Internet: 1 puerto 10/100 RJ45; LAN: 4 puertos 10/100 conmutados RJ45
POTENCIA DE SALIDA RF	18dBm
SEGURIDAD	SPI, Firewall
SEGURIDAD INALAMBRICA	WPA2, WEP, MAC Filtering

3.2.2 SERVIDOR NEC VERSA M4300 [27]

Como servidor se implementará un equipo antiguo disponible, que cumple con los requerimientos mínimos para ejecutar Zoneminder satisfactoriamente. Esto con el fin de disminuir costos y demostrar además que un equipo antiguo puede ser reutilizado para un sistema de vigilancia sin problemas. Aunque por obvios motivos se recomienda utilizar un equipo más avanzado para la implementación propia del sistema en el complejo.

Figura 3.3 Computador NEC versa 4300 [27]

Las características del servidor se detallan en la Tabla 3.2:

Tabla 3.2 Características Computador NEC

CARACTERISTICAS COMPUTADOR NEC	
MODELO	VERSA M4300
PROCESADOR	Intel Celeron
VELOCIDAD DE PROCESAMIENTO	2 GHz
DISCO DURO	120 GB
MEMORIA RAM	3 GB

3.2.3 CÁMARA INALÁMBRICA IP FOSCAM FI8918W [20]

Una cámara que cumple con los requerimientos necesarios para el diseño es la cámara IP inalámbrica FOSCAM FI8918W, Figura 3.4, sus características se la muestra a continuación en la Tabla 3.3

Figura 3.4 Cámara IP Foscam FI8918W [19]

Para la implementación del prototipo se utilizarán dos cámaras de este tipo.

Tabla 3.3 Características cámara Foscam FI8918W

CARACTERISTICAS CAMARA FOSCAM FI8918W		
Sensor de Imagen	Sensor de Imagen	Sensor de alta definición CMOS
	Lentes	f: 3.6mmm
	Iluminación mínima	0.5 Lux
Lentes	Tipo	Vidrio
Video	Compresión de imagen	MJPEG
	Tasa de cuadros de imagen	15 fps, 30 fps
	Resolución	640 x 480 o 320 x 240
	Espero de imágenes	Vertical / Horizontal
	Frecuencia de luz	50 Hz, 60 Hz

	Parámetros de Video	Brillo, Contraste
Comunicación	Ethernet	Un puerto 10/100 Mbps RJ45
	Protocolos	HTTP, FTP, TCP/IP, UDP, SMTP, DHCP, PPPoE, DDNS
	Estándar inalámbrico	IEEE 802.11 b/g/n
	Tasa de Datos	802.11b: 11 Mbps(Max); 802.11g: 54 Mbps(Max); 802.11n: 150 Mbps (max)
	Seguridad Inalámbrica	Encripción WEP, WPA, WPA2
	Infrarrojo	11 Leds IR
Alimentación	Fuente de poder	5 Vdc/ 2 A
	Consumo	5.5 Watts (max)

3.2.4 CÁMARA AXIS 2130R PTZ [28]

Además de la cámara IP inalámbrica anterior se utiliza para el prototipo una cámara tipo PTZ, si bien esta cámara no será inalámbrica en el prototipo, en la siguiente imagen se puede observar comparativamente la carga de información que genera esta cámara y la carga de información que genera la cámara inalámbrica.

Para obtener este análisis comparativo de tráfico, Figura 3.5 se utilizó el programa Wireshark, el cual captura los paquetes de información para poder analizarlos.

Para poder realizar una comparación objetiva, ambas cámaras se colocaron orientadas a una misma área para que transmitan la misma información.

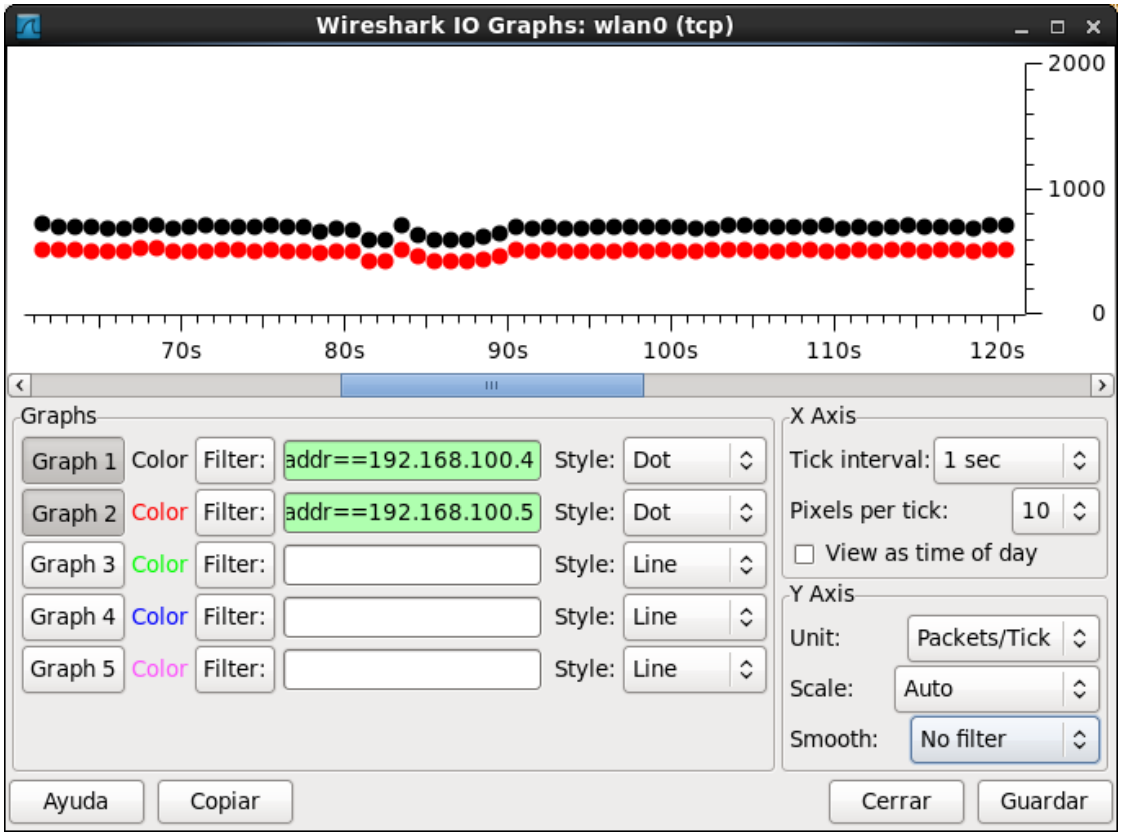

Figura 3.5 Paquetes detectados por Wireshark

En la figura se puede apreciar en color negro el tráfico de paquetes generados por la cámara Foscam inalámbrica, la cual tiene asignada la dirección IP 192.168.100.4.

En color rojo se representa los paquetes de información generados por la cámara Axis 213 PTZ, la cual tiene asignada la dirección IP 192.168.100.5.

De esta comparación se desprende que el tráfico generado por la cámara cableada es menor que el tráfico generado por la cámara inalámbrica, esto demuestra que el utilizar una cámara cableada en el prototipo no atenta contra los cálculos realizados en el diseño original con cámaras inalámbricas.

Se utilizará únicamente una de estas cámaras para completar en total tres cámaras para el prototipo a implementarse.

La cámara IP Axis 2130R PTZ, es un dispositivo que combina las habilidades de una cámara IP y un dispositivo PTZ (Pan, Tilt, Zoom). Al conectarse a una red de área local proporciona una imagen clara para vigilancia que puede ser apreciada en cualquier navegador de internet.

Figura 3.5 Cámara Axis 213 PTZ [28]

Sus características principales se pueden ver en la Tabla 3.4:

Tabla 3.4 Características cámara Axis 2130R PTZ

CARACTERISTICAS CAMARA AXIS 2130R PTZ		
Sensor de Imagen	Sensor de Imagen	Sensor foto sensible CCD
	Lentes	f: 3.6mmm
	Iluminación mínima	6 Lux
Lentes	Tipo	Vidrio
Video	Compresión de imagen	MJPEG
	Tasa de cuadros de imagen	15 fps, 30 fps
	Resolución	640 x 480 o 320 x 240

	Espero de imágenes	Vertical / Horizontal
	Frecuencia de luz	50 Hz, 60 Hz
	Parámetros de Video	Brillo, Contraste
Comunicación	Ethernet	Un puerto 10/100 Mbps RJ45
	Protocolos	HTTP, FTP, TCP/IP, SMTP, NTP, ARP, CHAP, MAP, DCHCP, BOOTP
	Estándar inalámbrico	-
	Tasa de Datos	1.5 Mbps
	Seguridad	Múltiple usuario con contraseñas
	Infrarrojo	-
Alimentación	Fuente de poder	13 Vdc/ 2 A
	Consumo	25 Watts (max)

3.2.5 REPETIDOR TP-LINK [30]

Como dispositivo intermedio entre el router y las cámaras se dispone de un Access Point, Figura 3.6, el cual presenta las siguientes características en la Tabla 3.5:

Figura 3.6 Access Point

Tabla 3.5 Características Access Point

CARACTERISTICAS ACCESS POINT TP - LINK	
MODELO	TL - WA830RE
MODOS INALAMBRICOS	Range extender, AP mode
ESTANDARES SOPORTADOS	802.11b/g/n
FRECUENCIA DE TRABAJO	2.4~2.4835GHz
ANTENAS	2 Antenas Fijas Omnidireccionales de 5dBi
TASA DE SEÑAL	11n: Hasta 300Mbps (dinámico) 11g: Hasta 54Mbps (dinámico) 11b: Hasta 11Mbps (dinámico)
SEGURIDAD INALÁMBRICA	WEP 64/128/152-bit WPA-PSK / WPA2-PSK

3.2.6 DIRECCIONAMIENTO DE DISPOSITIVOS DEL PROTOTIPO.

Como dispositivos finales se entiende a las cámaras y al servidor. Las direcciones IP que se van a utilizar para los mismos, constan en la Tabla 3.6:

Tabla 3.6 Direccionamiento de dispositivos

DISPOSITIVO	IP	MASCARA	GATEWAY
Router	192.168.100.1	255.255.255.224	-
Servidor	192.168.100.2	255.255.255.224	192.168.100.1
Access Point	192.168.100.3	255.255.255.224	192.168.100.1
Cámara 01	192.168.100.4	255.255.255.224	192.168.100.1
Cámara 02 PTZ	192.168.100.5	255.255.255.224	192.168.100.1
Cámara 03	192.168.100.6	255.255.255.224	192.168.100.1

El esquema lógico es el mostrado en la Figura 3.7:

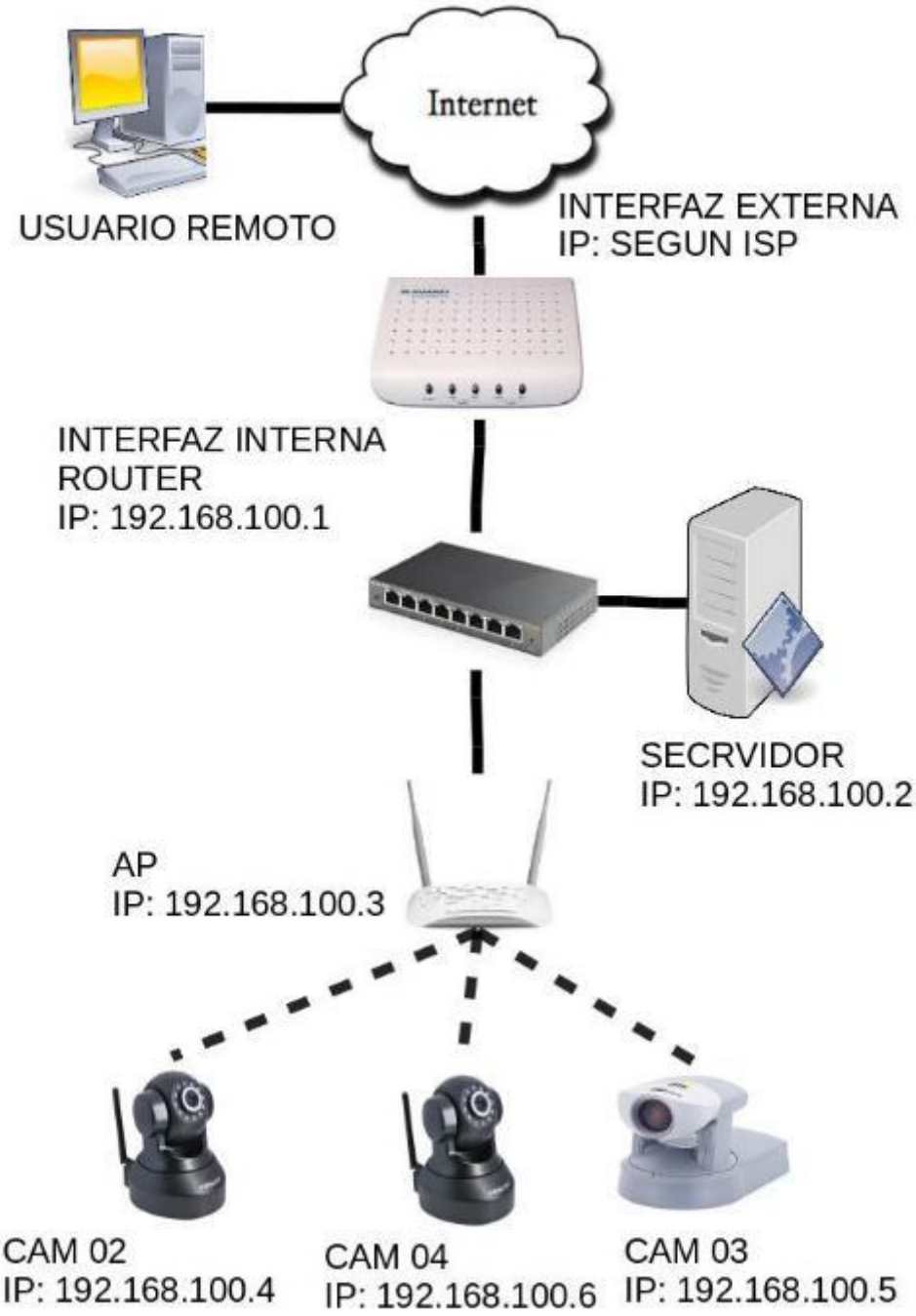

Figura 3.7 Topología del prototipo a implementarse

3.2.7 USUARIOS [23]

El sistema está diseñado para acceso local o remoto a través de la dirección asignada por el proveedor de internet.

En ambos casos el acceso está protegido por usuarios con un nombre de usuario y contraseña respectivo. Para este efecto demostrativo se han creado dos usuarios, uno administrador, con todos los permisos para monitorear, editar y cambiar las configuraciones del sistema y otro usuario con permiso únicamente para visualizar las cámaras.

La creación de los usuarios se muestra en la Figura 3.8:

Figura 3.8 Pestaña usuarios

En la figura se puede apreciar la existencia de un usuario manager y otro usuario guardián. El usuario manager tiene todos los permisos en el sistema y el usuario guardián únicamente puede visualizar las cámaras. Cada uno de ellos está protegido por una contraseña.

3.3 PRUEBAS

3.3.1 ACCESO DE USUARIOS

Para ingresar al sistema de forma local en el servidor se debe abrir un navegador y escribir la dirección https://localhost/zm. Para acceder de forma remota se debe abrir un navegador y digitar la dirección WAN del router asignada por el proveedor de internet.

En ambos casos, se desplegará la siguiente pantalla, Figura 3.9.

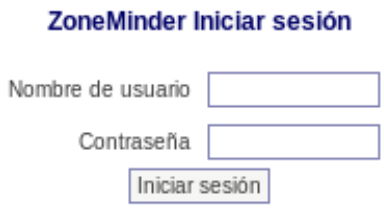

Figura 3.9 Pantalla de acceso.

En donde el usuario debe identificarse como uno de los dos usuarios antes descritos.

Para el siguiente ejemplo se ha procedido a ingresar como usuario administrador, donde se tiene la siguiente vista, Figura 3.10 de la consola principal de Zoneminder.

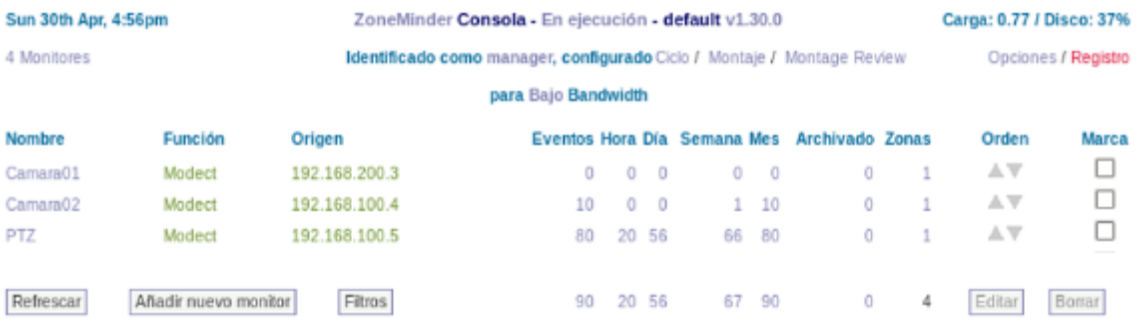

Figura 3.10 Consola de Zoneminder en ejecución

En la imagen anterior se puede apreciar desde el lado izquierdo, las cámaras conectadas, la función en la que están operando, la dirección IP respectiva, los eventos detectados por cada una de ellas y las zonas activas.

Para observar las cámaras una a una se puede dar click sobre el nombre respectivo. Para observar las cámaras simultáneamente se debe dar click sobre la opción Montaje en la parte superior, donde se puede apreciar una imagen similar a esta, Figura 3.11.

Figura 3.11 Montaje de cámaras en Zoneminder

3.3.2 MOVIMIENTO DE CÁMARAS

Desde la pantalla de visualización general o desde la vista individual se puede mover las cámaras en caso de que se requiera visualizar otra sección diferente de la que se visualiza ese momento.

Para eso se toma como ejemplo la cámara Foscam 01, Figura 3.12.

Figura 3.12 Cámara 01

Para poder controlar la cámara se debe dar click sobre la opción.control, Figura 3.13, que se encuentra en la parte superior de la ventana anterior. Con estos controles se puede realizar movimientos horizontales, verticales y en diagonal.

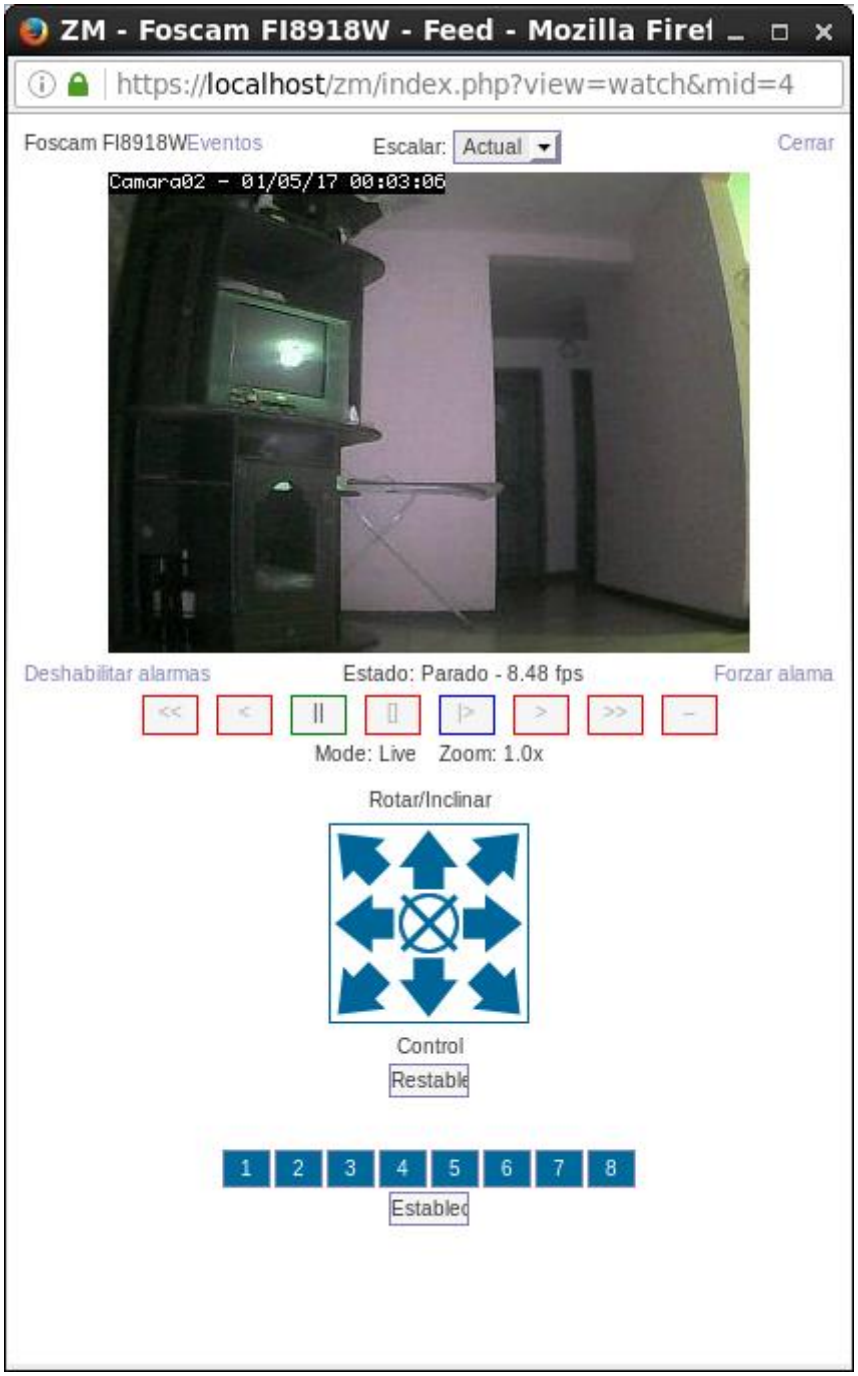

Figura 3.13 Cámara 03

3.3.3 CONFIGURACIÓN DE ZONAS [23]

En cada una de las cámaras se pueden configurar zonas, es decir partes específicas dentro del cuadro de imagen, que son más importantes que el resto de la imagen, también puede resultar que todo el cuadro es una zona. Depende de lo que se necesita.

Para este prototipo las dos cámaras IP Foscam tiene zonas predeterminadas, es decir todo el cuadro observable es una zona, Figura 3.15 en cambio en la cámara PTZ, como está orientada a una calle, se ha establecido una zona que cubre únicamente la calle, como se observa en la Figura 3.14, esto debido a que junto a la calle se encuentran varios árboles y el movimiento que se genera por causa del viento puede generar falsas alarmas.

Figura 3.14 Cámara PTZ orientada hacia la calle

Figura 3.15 Zona por defecto en Cámara Foscam01

Se puede configurar más de una zona en un solo cuadro, cada una con una sensibilidad diferente, como se muestra en la Figura 3.16, en este ejemplo se han configurado dos zonas, una activa en el lado izquierdo y otra inactiva en el lado derecho. Esta configuración permite que se disparen alarmas únicamente cuando haya movimiento en la zona activa y omite alarmas cuando se da el movimiento en la zona inactiva.

Figura 3.16 Persona en la zona inactiva

Con la persona realizando movimientos en la zona inactiva no se dispara ninguna alarma ni notificación.

Figura 3.17 Persona en la zona activa

Cuando el movimiento se realiza en la zona activa, Figura 3.17, se dispara la alarma.

3.3.4 DETECCIÓN DE MOVIMIENTO Y NOTIFICACIÓN DE ALARMAS [23]

En base a las pruebas realizadas y a la documentación guía de Zoneminder el valor promedio para sensibilidad es 25% de cambio en el número total de pixeles en un cuadro.

Todas las cámaras están configuradas para trabajar en modo Modect, es decir para grabar únicamente cuando se detecte un cambio de un cuadro a otro en un 25 %.

En este prototipo se ha configurado que las zonas deben tener un 25 % de diferencia entre un cuadro y otro para generar una alarma, esto evita que una pequeña hoja al viento o cualquier pequeño detalle no disparen una alarma. En las pruebas realizadas se determinó que con un valor de 25% se puede detectar cualquier evento relevante.

Además se ha configurado un filtro, el cual indica que las alarmas únicamente se dispararán en un horario determinado, entre las 18:00 hasta las 6:00 y únicamente al usuario administrador.

Todas estas configuraciones en conjunto permiten que el sistema almacene movimientos relevantes en el disco duro del servidor todo el día desde las 6:00 hasta las 18:00, y entre estas horas además de grabar genera una alerta por correo hasta el usuario asignado.

Un ejemplo de notificación de correo la podemos observar en la Figura 3.16, donde se puede apreciar la bandeja de entrada del usuario administrador.

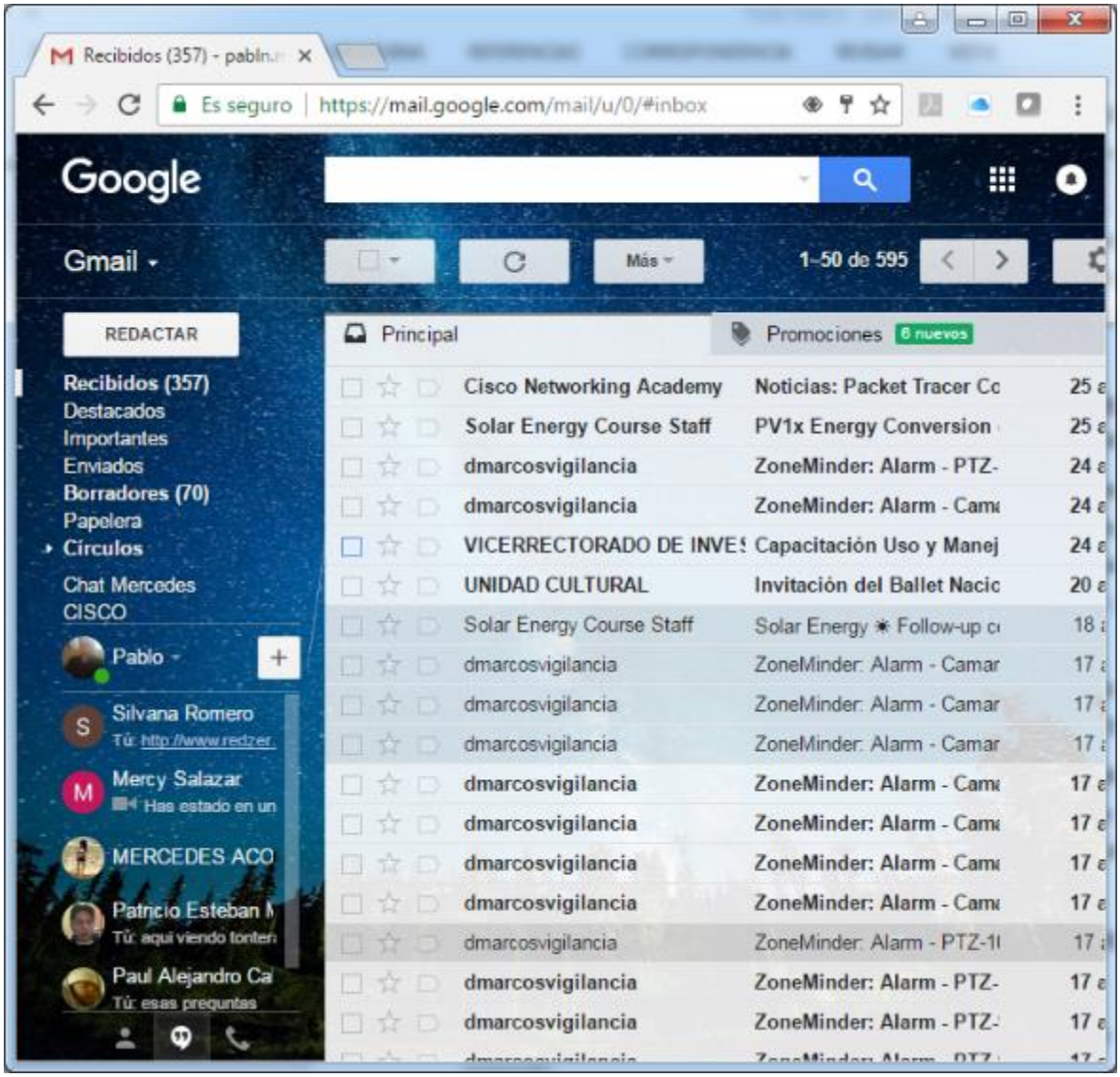

Figura 3.16 Bandeja de entrada de usuario.

En el cuerpo del correo, Figura 3.17, se puede observar:

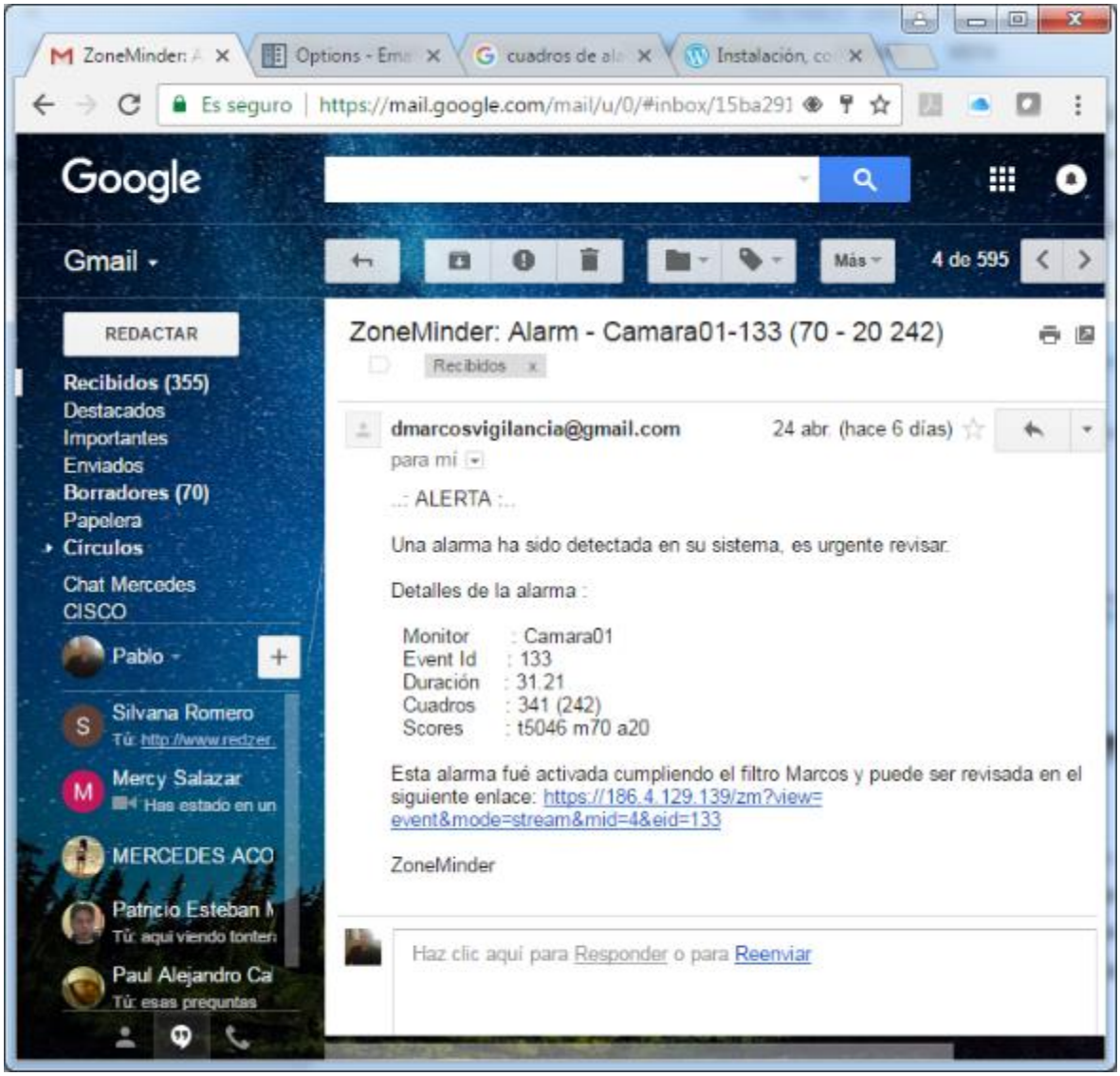

Figura 3.17 Correo enviado desde Zoneminder

En el correo recibido se puede identificar de donde proviene la alarma, la cual aparece en el asunto del mismo. En este caso se indica que la alarma proviene de la Cámara01, en el cuerpo del correo se identifican el número de evento, la longitud del mismo y el número de cuadros de alarma detectados, en este caso es 341.

Se detalla además que la alarma se activó al cumplirse el filtro determinado y que se puede revisar el evento en la dirección web indicada, la cual direcciona al usuario a la pantalla de acceso de Zoneminder para que pueda revisar la grabación del evento.

3.3.5 REVISIÓN DE EVENTOS

Una vez que el usuario accede a través de este link al sistema, puede revisar el evento dando click sobre la columna eventos de la cámara respectiva. Figura 3.18.

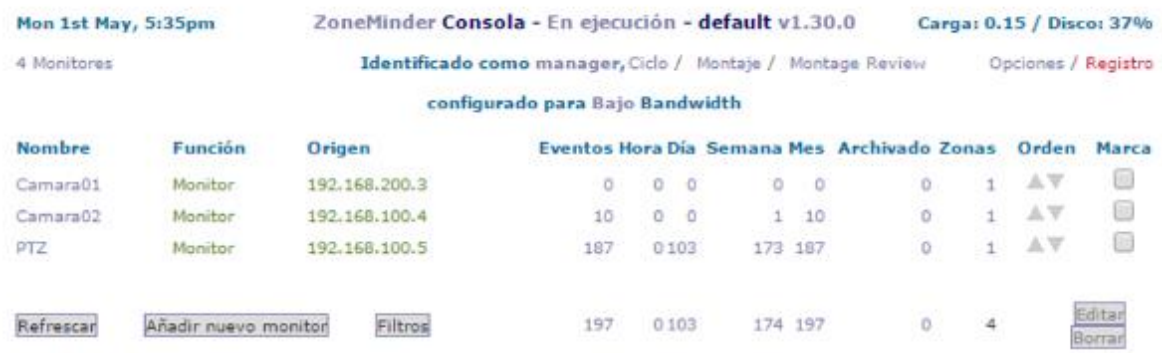

Figura 3.18 Consola de Zoneminder.

Al dar click sobre el número de eventos respectivo se muestra el listado de todos los eventos grabados por la cámara. Figura 3.19

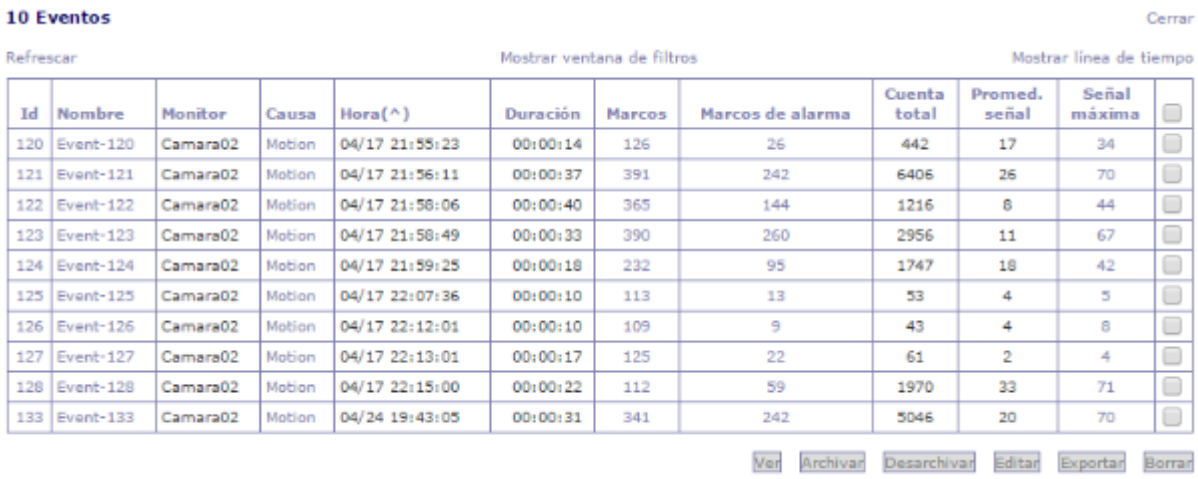

Figura 3.19 Listado de eventos detectados por la cámara 02

Para visualizar el evento que se indica en el correo de notificación, se lo puede identificar con el número ID, éste número está en la columna izquierda de la Figura 3.19.

Al dar click sobre el ID respectivo aparecerá una nueva ventana donde empezará a reproducirse automáticamente el evento almacenado. Figura 3.20.

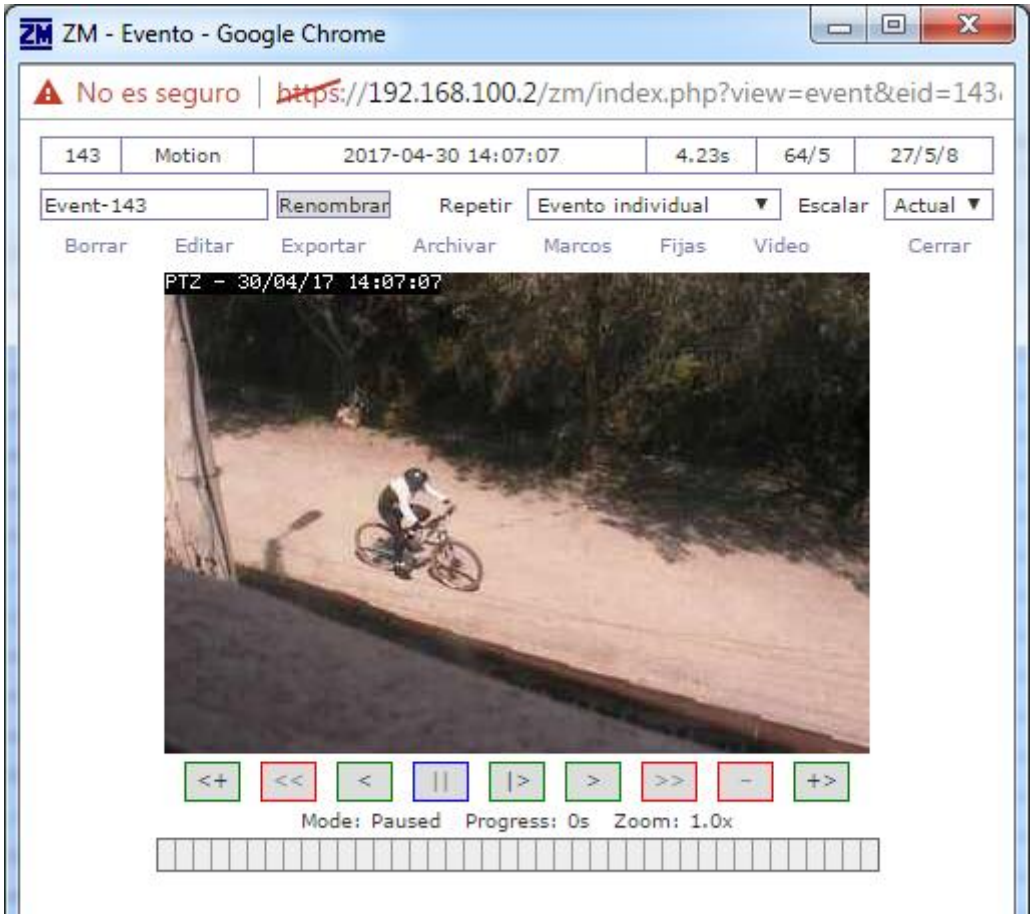

Figura 3.20 Movimiento detectado por la cámara.

3.4 EVALUACIÓN DE FUNCIONAMIENTO

Las pruebas de funcionamiento fueron satisfactorias, sin embargo se encontraron ciertos detalles, como por ejemplo, hubo que cambiar el número cuadros que debían almacenarse ya que cuando se detectaba un evento, la grabación se realizaba ya empezado el evento y no se grababa hasta que el evento termine. Por tanto se procedió a cambiar en la pestaña buffer de cada una de las cámaras y aumentar el valor de 25 a 50 en los campos cuenta de imagen pre evento y post evento, como se muestra en la Figura 3.21.

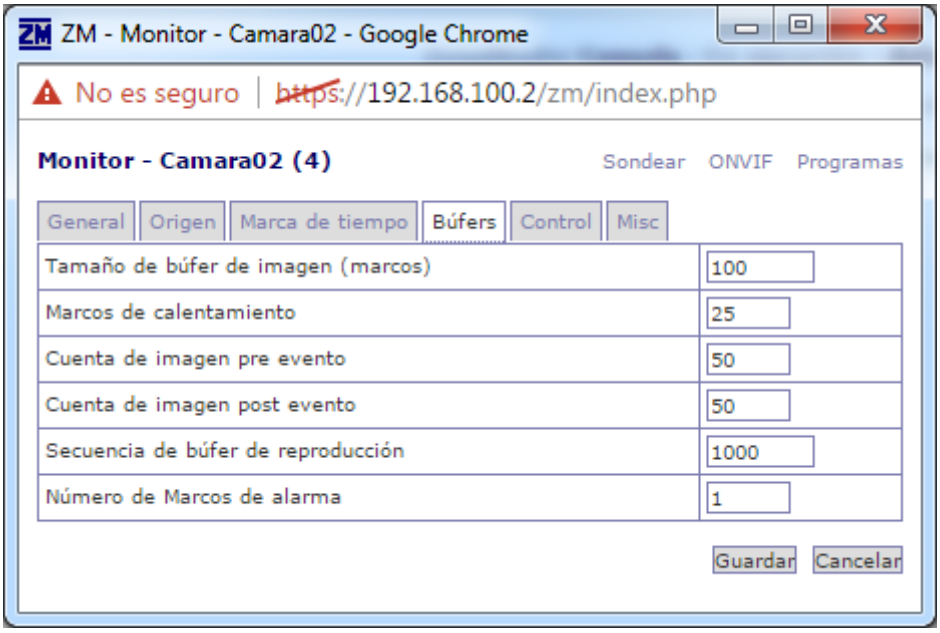

Figura 3.21 Búfer de control de la cámara

Otro de los detalles a tener en cuenta es la configuración de las zonas en las cámaras; ya que si se realizan movimientos con el menú de control de movimiento, las zonas quedan desconfiguradas. Por tanto dependiendo de la situación se puede volver la cámara a su posición original o se puede configurar una nueva zona de detección.

Una vez realizados los correctivos necesarios, se procede a describir los costos del proyecto diseñado.

CAPÍTULO 4.
DESCRIPCION DE COSTOS

4.1 INTRODUCCIÓN

En el presente capitulo se procederá a realizar un presupuesto referencial para la implementación del sistema propuesto. Se consideran todos los materiales necesarios y equipos a utilizarse para obtener un valor referencial final. Todos los elementos involucrados serán adquiridos en el local especializado mayorista para minimizar costos.

Todos los valores indicados se expresan en dólares de Estados Unidos.

4.2 ELEMENTOS DEL SISTEMA

El sistema propuesto requiere elementos tanto de hardware como de software, en la Tabla 4.1 se describe los elementos necesarios.

Tabla 4.1 Elementos del sistema de vigilancia

ELEMENTOS DEL SISTEMA	
DESCRIPCIÓN	CANTIDAD
Servidor	1
Software para gestión de vigilancia	1
Router	1
Access Point	7
Cámara IP inalámbrica tipo PTZ	2
Cámara IP inalámbrica	14
Dirección IP pública	1

Servicio de internet	1
UPS	1
Material eléctrico y de red	varios

4.3 COSTOS DE LOS ELEMENTOS ACTIVOS.

Los valores referenciales de los equipos activos se describen en la Tabla 4.2

Tabla 4.2 Costos elementos activos

Descripción	Cantidad	Costo Unitario	Costo total
Servidor DELL PowerEdge T130	1	2062,00	2062,00
Router WRT54GL	1	145,00	145,00
Access Point Linksys	7	49,00	343,00
Cámara inalámbrica PTZ LOFTEK Sentinel	2	300,00	600,00
Cámara IP inalámbrica FI 8918W DCS-2330L	14	200,00	2800,00
Servicio de Internet e IP fija	1	50,40	50,40
UPS	1	700,00	400,00

CDP UPS Online Torre 1000va 800w			
COSTO ELEMENTOS ACTIVOS			6400,40

4.4 COSTOS DE LOS ELEMENTOS DE RED

Para el caso de los elementos de red los costos son los indicados en la Tabla 4.3

Tabla 4.3 Costos elementos de red

Descripción	Cantidad	Costo Unitario	Costo total
Cable UTP Cat 6	700 m.	0,50	350,00
Conectores RJ-45	20	0,10	2,00
Capuchones	20	0,10	2,00
Canaletas plásticas 32x12	30	4,00	120,00
COSTO ELEMENTOS DE RED			474,00

4.5 COSTOS ELEMENTOS ELÉCTRICOS

En cuanto a los elementos eléctricos se tiene los siguientes valores.

Tabla 4.4 Costos elementos eléctricos

Descripción	Cantidad	Costo Unitario	Costo total
Cable eléctrico N°10	100 m.	63,00	63,00
Tomacorrientes	4	0,20	0,80

Enchufes	4	0,20	0,80
COSTO ELEMENTOS ELÉCTRICOS			64,60

4.6 COSTO TOTAL DEL PROYECTO

Para el costo final del sistema, se contemplan los valores antes descritos, así como los valores por mano de obra y diseño del mismo.

En la siguiente Tabla se puede apreciar el detalle del valor total del proyecto.

Tabla 4.5 Costo total del proyecto

Descripción	Valor
Costo elementos activos	6400,40
Costo elementos de red	474,00
Costo elementos eléctricos	64,60
Mano de obra	1500
Diseño del proyecto	1000,00
VALOR TOTAL	9439,00

En el valor total se contemplan valores estimados bajos para la fase de diseño e implementación, los cuales se establecieron asumiendo que se va a implementar el mismo. En caso de que no se fuera a implementar este sistema, el valor de la fase de diseño antes mencionado sería más alto.

Tomando como referencia el costo de un sistema de seguridad, de prestaciones parecidas a las del proyecto propuesto, el valor calculado es bastante competitivo y económico. Por otro lado, considerando el tamaño de la empresa para la que se realizó este trabajo no es un valor alto además el tema de la seguridad debe ser considerado desde la perspectiva de estar protegiendo los activos de la empresa y sus potenciales clientes.

Otro aspecto relevante para la empresa es que la instalación de este sistema sumaria valor agregado al complejo ya que existen otros complejos pequeños en el sector que tampoco disponen de sistema de vigilancia con cámaras. Por tanto sería un servicio adicional que se brinda a los visitantes, lo que le daría una ventaja subjetiva a la empresa.

CAPÍTULO 5.
CONCLUSIONES Y RECOMENDACIONES

De los resultados obtenidos de las pruebas del prototipo se pueden extraer las siguientes conclusiones.

5.1 CONCLUSIONES

Al comparar un sistema inalámbrico con un sistema cableado son evidentes algunas diferencias, que dependiendo de las situaciones que se presenten, pueden ser ventajas o desventajas. Entre las principales ventajas de los sistemas inalámbricos respecto de los sistemas cableados se pueden mencionar la movilidad, facilidad de instalación, escalabilidad, facilidad de comunicación en lugares o situaciones donde una conexión cableada sería muy complicada, supresión de cables, etc. Sin embargo se pueden presentar desventajas tales como interferencias, pérdida de señal, seguridad, etc. Considerando las fortalezas de cada tecnología se opta por un sistema híbrido para este proyecto, ya que si bien una gran parte del complejo tiene espacios abiertos, existen zonas que tienen estructuras que pueden generar una gran pérdida en la transmisión de la señal.

La utilización de un software de gestión de código abierto, como Zoneminder, para el sistema de vigilancia, permite ahorrar costos en cuanto a licenciamiento, sin embargo es necesario un conocimiento intermedio avanzado en Linux para poder instalar sus prerrequisitos y el programa en sí. Además de estar familiarizado con la búsqueda de soluciones mediante la información disponible en foros y demás portales de Linux. Dado que lo que se busca es lograr un sistema con un valor asequible, se opta por Zoneminder.

En un entorno como el del complejo turístico D'Marco'S, se observó en las pruebas, que no es muy relevante el problema de la interferencia causada por fuentes inalámbricas cercanas ya que al estar ubicado en una zona rural, las fuentes generadoras de señales peligrosas para la comunicación de las cámaras más relevantes son los equipos de internet inalámbrico doméstico de los hogares circuncidantes, los cuales están en promedio a más de 50 metros del perímetro. Por lo mismo se puede concluir que la decisión de usar cámaras IP inalámbricas es correcta.

Debido a la infraestructura existente en el complejo fué necesario realizar una instalación mixta, es decir, que exista una conexión cableada entre el router principal y los AP existentes y una comunicación inalámbrica entre los AP y las cámaras a utilizarse, con esto se evitaron interferencias por paredes u obstáculos que creaban zonas ciegas.

La utilización de zonas en las cámaras permite aumentar la eficiencia en el uso del programa, al permitir seleccionar áreas específicas en el cuadro que está visualizando la misma. Estas zonas pueden ser activas o exclusivas, en donde una zona activa es un área específica del cuadro donde se pone mayor énfasis en detectar un posible cambio en la imagen. Por otro lado, una zona excluyente es un área específica donde se espera que exista movimiento, y por tanto se la ignora a propósito para evitar falsas alarmas, por ejemplo un árbol de navidad, una luz intermitente de una alarma, o una luz automática en el cielo raso. Tomando en cuenta lo anteriormente expuesto, se implementarán zonas en las cámaras analizando la ubicación y necesidad de cada una de ellas.

La configuración de alarmas es una herramienta muy importante ya que permite que la persona encargada del sistema de vigilancia esté al tanto de los eventos más relevantes que suceden en el complejo sin requerir que esté constantemente viendo las cámaras en busca de alguna novedad. Incluso Zoneminder permite la grabación de los eventos una vez que la alarma ha sido disparada. Por tanto se implementará la función de alertas por correo electrónico y no con SMS ya que para esto último se requiere un módulo adicional GSM, lo cual no está contemplado en el presente proyecto.

El prototipo implementado demuestra con las pruebas realizadas, que los cálculos estimados, así como las configuraciones en cada uno de los equipos permiten comprobar que los cálculos estimados en el diseño se pueden aplicar a la escala indicada sin problema.

5.2 RECOMENDACIONES

De la experiencia adquirida durante la realización de este trabajo se pueden extraer las recomendaciones siguientes.

Zoneminder es un programa de gestión de sistemas de vigilancia de código abierto, compatible con cámaras inalámbricas o cableadas, con disponibilidad para trabajar con múltiples cámaras a la vez. El número de las mismas depende, entre otras cosas, de la calidad de imagen deseada y de los FPS, facilidad de operación, capacidad para grabar y enviar notificaciones ante eventos, detección de movimientos. Además cuenta con una amplia comunidad virtual e información de su portal oficial. De lo indicado se puede recomendar su uso para proyectos parecidos al aquí realizado.

La persona que esté a cargo del sistema de vigilancia debe ser una persona que tenga un dominio intermedio o avanzado de Linux ya que de lo contrario dicha persona puede encontrar graves dificultades para solventar cualquier falla durante la operación o el mantenimiento del sistema. De no disponer de una persona con ese perfil se recomienda disponer de un consultor permanente en el caso de fallas en el sistema.

Para la selección de las cámaras es importante basarse en la documentación oficial de Zoneminder. Existen en el mercado una muy amplia variedad de marcas y modelos de cámaras, sobre todo de origen chino, de las cuales se tiene poca o nula información en cuanto a su funcionamiento con Zoneminder.

Los factores más relevantes al momento de realizar el diseño del sistema son las necesidades específicas del complejo, la factibilidad técnica y económica en caso de una implementación y la tecnología disponible para ello, parámetros que se recomiendan sean siempre tomados en cuenta.

Uno de los aspectos más críticos en el diseño es la parte de almacenamiento ya que al tratarse de video y al tener muchas cámaras es necesaria la utilización de una gran capacidad en disco, esto se puede solucionar obteniendo un arreglo de discos de mucha capacidad, grabando únicamente lo más destacado en eventos o externalizando la información, es decir almacenando en la nube. En base a esto lo más eficiente es un almacenamiento hibrido, el cual permite almacenar los eventos más importantes y al mismo tiempo crear un respaldo de éste en almacenamiento en la nube, de tal manera que se libere memoria física en el disco duro del servidor al eliminar la información recurrentemente.

Si bien en la documentación oficial de Zoneminder se indica como configurar las cámaras de acuerdo a la marca y al modelo muchas de las guías están desactualizadas y es necesario analizar cada una de las configuraciones indicadas durante la implementación de las mismas para realizar modificaciones de ser el caso. En algunas ocasiones es necesario realizar un hibrido de las configuraciones entre modelos similares de las mismas marcas.

Para optimizar recursos de almacenamientos es importante configurar la grabación de eventos únicamente cuando éstos se presenten y no configurar la grabación permanentemente, ya que al tratarse de 16 cámaras la cantidad de video almacenado requeriría un almacenamiento del orden de las centenas de TB al mes. Además de eso, también es importante que la persona a cargo revise periódicamente los eventos detectados para borrarlos posteriormente y mantener siempre un espacio de almacenamiento prudente.

Para mejorar el funcionamiento del sistema, es posible, dependiendo de las características del dispositivo, configurar valores de FPS diferentes para cada cámara en función del área a cubrir, es decir puede que existan áreas donde se requiere mayor detalle en la imagen que en otras. Esto ayuda además en la cantidad de almacenamiento ocupado al final en el servidor.

Entre los métodos de seguridad implementados en el presente proyecto para minimizar la intercepción de datos se encuentran utilización de encriptación WPA 2 personal, filtrado por dirección MAC en las cámaras, dirección IP fija, contraseña de acceso para cada cámara, contraseña de acceso para Zoneminder para un usuario administrador y para un usuario visualizador, además se cuenta con filtrado de puertos en el router.

En la configuración de las zonas en las cámaras, se debe tener en cuenta que si la cámara se mueve la zona configurada perderá eficacia pues estará enfocando un área diferente, por tanto se debe considerar esto antes de ubicar las cámaras, de tal manera que no sea necesario el movimiento de las mismas durante la ejecución del sistema. Y si es que se produce algún cambio hay que recordar volver la cámara a la posición original o configurar una nueva zona, lo que sea mejor dependiendo de la situación.

De presentarse una ampliación en el número de cámaras del sistema, se recomienda que tenga el valor de FPS necesarios para la ubicación que va a tener la misma. Además de que trabaje en el estándar 802.11n y de que sea compatible con Zoneminder. Es muy importante el tener en cuenta el valor total de cámaras que puede soportar el diseño presentado, el cual únicamente contempla un crecimiento del 20 %. Un crecimiento superior a éste provocará inestabilidad en el funcionamiento del sistema.

BIBLIOGRAFIA

[1] https://www.cnt.gob.ec/internet/plan/internet-banda-ancha-hogar/, Octubre 2016

[2] http://www.accesor.com/esp/art2_query.php?fam=5, Diciembre 2016

[3] PUBLICACIONES VÉRTICE. Videovigilancia: CCTV usando videos IP. Editorial Vértice. España 2011.

[4] http://videovigilanciaperu.blogspot.com/2009/11/, Octubre 2016

[5] http://www.voxdata.com.ar/voxcompresionvideo.html, Diciembre 2016

[6] http://www.rnds.com.ar/articulos/059/Cap_06.pdf, Enero 2017

[7] KRUEGLE HERMAN. CCTV Surveillance: Video Practices and Technology. Segunda Edición. Elservier. 2007

[8] https://www.axis.com/ec/es/learning/web-articles/technical-guide-to-network-video/video-management-systems, Enero 2017

[9] https://www.axis.com/ve/es/learning/web-articles/technical-guide-to-network-video/overview, Enero 2017

[10] https://es.wikipedia.org/wiki/Router, Enero 2017

[11] http://electroprotecciones.com.ec/wp-content/uploads/2010/10/ups2.jpg, Enero 2017

[12] http://zoneminder.readthedocs.io/en/latest/userguide/introduction.html, Febrero 2017

[13] https://www.centos.org/, Febrero 2017

[14] TANENBAUM ANDREW, WHETERALL DAVID. Redes de computadores. Cuarta Edición. Pearson. México. 2012.

[15] http://www.x-net.es/tecnologia/wireless.pdf, Febrero. 2017

[16] RANDALL NICHOLS, PANOS LEKKAS. Wireless Security, Models, Threats, and Solutions. McGraw-Hill. USA. 2002.

[17] http://www.metageek.com/products/inssider/, Febrero. 2017

[18] https://www.ekahau.com/products/heatmapper/overview/, Febrero. 2017

[19] http://www.foscam.com/product/9.html, Febrero. 2017

[20] http://www.dlinkla.com/dcs-2330l, Febrero. 2017

[21] https://bestbuycamerajnsale.com/surveillance/-loftek-sentinel-d2-outdoor-indoor-waterproof-wireless-pan-tilt, Diciembre. 2016

[22] “Diseño e implementación de un circuito cerrado de televisión con cámaras IP inalámbricas y monitoreo remoto, notificación de eventualidades mediante el uso de un servidor para la grabación de video bajo linux usando zoneminder para el laboratorio de informática del edificio Eléctrica-Química”; Quito; Julio 2011; Capítulo 2.

[23] http://zoneminder.readthedocs.io/en/latest/, Febrero. 2017

[24] http://www.dell.com/sv/empresas/p/poweredge-t130/pd 2017

[25] http://www.linksys.com/es/p/P-WRT54GL/, Febrero. 2017

[26] http://www.forzaups.com/ec/fdc-3000rul, Febrero. 2017

[27] https://support.necam.com/legacy/notebooks/, Febrero. 2017

[28] https://www.axis.com/files/usermanual/2130_um_en.pdf Febrero. 2017

[29] https://www.wireshark.org/ Febrero. 2017

[30] http://www.tp-link.es/products/details/TL-WA830RE.html#overview Febrero 2017

[31] https://www.cnt.gob.ec/internet/plan-corporativo/internet-pymes/

[32] http://www.netlife.ec/planes/pymes/internet-de-alta-velocidad/nuestros-planes/