ESCUELA POLITÉCNICA NACIONAL

ESCUELA DE FORMACIÓN DE TECNÓLOGOS

DISEÑO E IMPLEMENTACIÓN DE UNA RED DE CÁMARAS DE SEGURIDAD WI-FI CON MONITOREO REMOTO Y ALERTA TEMPRANA PARA LA UNIDAD EDUCATIVA SALESIANA "DOMINGO SAVIO"

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

DIEGO ANDRÉS CEVALLOS GUERRA
diegocevallos702@hotmail.com

DIRECTOR: ING. FABIO GONZÁLEZ
fabio.gonzalez@epn.edu.ec

Quito, Diciembre 2015

DECLARACIÓN

Yo, DIEGO ANDRÉS CEVALLOS GUERRA, 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.

_____

Diego Andrés Cevallos Guerra.

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por DIEGO ANDRÉS CEVALLOS GUERRA, bajo mi supervisión.

_____

ING. FABIO GONZÁLEZ

DIRECTOR DEL PROYECTO

AGRADECIMIENTO

En primer lugar a Dios, por todos los favores inmerecidos que he recibido y por darme la sabiduría para poder cumplir mis sueños.

A mi madre Paulina Cevallos, por ser ejemplo de sacrificio y esfuerzo al educarme sin el apoyo de una figura paterna, por su apeo incondicional y sus consejos que siempre me ayudaron a salir de dificultades. A mi esposa Yadira Jácome, por su amor incondicional y por ser mi sostén emocional con sus incontables frases de ánimo.

A la Comunidad Salesiana Cayambe-Ibarra, en caso particular al Rev. Padre Marcelo Chávez Director de la Obra Salesiana en los años 2012-2014 por su apoyo incondicional, y a los rectores de turno de la Unidad Educativa Salesiana “Domingo Savio”, quienes siempre brindaron todas las facilidades para la culminación del proyecto.

Por último agradecer a mi Director de tesis, quien tuvo la paciencia y predisposición de brindarme su tiempo, y a sus invaluables conocimientos los cuales fueron muy importantes para el correcto desarrollo de este proyecto.

Diego Andrés Cevallos Guerra.

DEDICATORIA

El presente proyecto lo dedico a mi padre Vicente Cevallos que en paz descanse, por ser el faro que siempre guía mi camino, por ser ejemplo de trabajo y responsabilidad todos los días de su vida, por enseñarme a ser una persona correcta y de bien. Además dedico este proyecto a mi hijo Samuel, quien es el motor de mi vida.

Diego Andrés Cevallos Guerra.

CONTENIDO

ÍNDICE DE FIGURAS

CAPÍTULO I

CAPÍTULO II

CAPÍTULO III

ÍNDICE DE TABLAS

CAPÍTULO I

CAPÍTULO II

CAPÍTULO III

RESUMEN

El presente proyecto tiene como objeto el diseño e implementación de una red de cámaras de seguridad Wi-Fi, cuyo objetivo es crear una herramienta de prevención y control para el área administrativa de la Unidad Educativa Salesiana “Domingo Savio”.

En el edificio donde funciona la UESDS también se encuentran las oficinas de la Casa Campesina Cayambe, la cual es una institución financiera que trabaja con las comunidades rurales del cantón Cayambe, es por este motivo que el sistema de video vigilancia monitoreará las principales zonas de las dos obras Salesianas.

En el capítulo I se realiza una introducción a todos los aspectos importantes de las redes inalámbricas, sus aplicaciones, usos, ventajas, desventajas y estándares internacionales que requieren estas redes. Se analiza las topologías de red, selección de equipos, amenazas, seguridades de la red y mantenimiento de las mismas, todo esto sirve para la implementación de la red inalámbrica con cámaras de seguridad.

En el capítulo II se realiza un estudio espectral y pruebas de campo para determinar posibles interferencias y vulnerabilidades de la red, se determina los requerimientos para el diseño e implementación de la red de cámaras de seguridad inalámbricas. En base a los requerimientos planteados para la red de cámaras, se busca marcas existentes en el mercado para seleccionar los equipos que mejor se adapten a las necesidades de la Unidad Educativa Salesiana “Domingo Savio”, una vez adquiridas las cámaras se instalan en los lugares designados y se verifica su correcto funcionamiento.

En el capítulo III se detallan varias pruebas que permiten determinar la eficacia de la red, en base a los resultados de estas pruebas se determina la operatividad de la red y se realizan las calibraciones necesarias. Como apoyo para los beneficiarios se realizará un manual sencillo para el manejo y el mantenimiento de la red, en el caso de presentarse eventualidades y errores.

Para finalizar se realiza un estudio de costos, con el objetivo de tener una idea clara de la inversión requerida para un proyecto de estas características.

En el capítulo IV se presentan las conclusiones y las recomendaciones necesarias para que este proyecto sirva de guía en la implementación de sistemas similares.

PRESENTACIÓN

La seguridad como una necesidad en cualquier empresa, establecimiento comercial e incluso el hogar, es de mucha importancia, es por este motivo que los sistemas de video vigilancia proporcionan una herramienta útil y versátil para satisfacer esta problemática social.

En la actualidad los avances tecnológicos son inmensos, en especial los relacionados con cámaras digitales IP, es así que las cámaras digitales han remplazado a las analógicas, puesto que presentan más prestaciones, el proceso de instalación y configuración es sencillo, permiten la escalabilidad del sistema y solo necesita un computador el cual mediante un software será capaz de gestionar todas las acciones de monitoreo y control.

Este proyecto presenta una guía para instalar y configurar un sistema de video vigilancia, se muestran todos los aspectos teóricos y metodológicos necesarios para el correcto funcionamiento del sistema además de las acciones a tomar en el caso de presentarse eventualidades.

1 GENERALIDADES

1.1 La red de computadoras[1]

El comité IEEE 802 establece que "Una red es un sistema de comunicaciones que permite que un número de dispositivos independientes se comuniquen entre sí".

Esta definición abarca no solo a las computadoras, sino a todos los dispositivos involucrados en la comunicación de datos, además de que no establece un límite en el número de nodos que componen la red ni la distancia que los separa.

Los recursos que se pueden compartir en una red son: [9]

- Procesador y memoria RAM, al ejecutar aplicaciones de otras PC.
- Unidades de disco duro.
- Unidades de disco flexible.
- Unidades de CD-ROM/DVD-ROM.
- Impresoras.
- Fax.
- Módem.
- Conexión a Internet.
- Cámaras

1.1.1 Clasificación de las redes

Existen cuatro tipos básicos de redes según su cobertura: redes de área personal (PAN), redes de área local (LAN), redes de área metropolitana (MAN) y redes de área extensa (WAN).

1.1.1.1 Redes de área personal (PAN)

Redes inalámbricas dentro del área de trabajo (escritorio) de una persona. Sirve para conectar diversos dispositivos a la PC, entre celulares, celular con PC. Dos de los ejemplos más comunes hoy en día son el bluetooth y el infrarrojo.

1.1.1.2 Redes de área local (LAN)

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

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

1.1.1.3 Redes de área metropolitana (MAN)

Básicamente son una versión más grande de una red LAN y utiliza normalmente tecnología similar. Puede ser pública o privada. Una MAN puede soportar tanto voz como datos. Una MAN tiene uno o dos cables y no tiene elementos de intercambio de paquetes o conmutadores, lo cual simplifica bastante el diseño.

Teóricamente una MAN es de mayor velocidad que una LAN, pero ha habido una división o clasificación: privadas que son implementadas áreas de tipo campus debido a la facilidad de instalación de Fibra Óptica y publicas de baja velocidad (<2 Mbps), como Frame Relay, ISDN, T1-E1, etc.

1.1.1.4 Redes de área extensa (WAN)

Las redes del tipo WA N (Wide Area Network) tienen las computadoras situadas en lugares distantes, como diferentes ciudades, provincias, regiones países, continentes o, simplemente, edificios muy lejanos dentro de una misma zona. Esta peculiaridad las hace más vulnerable a las interferencias, lo cual disminuye su velocidad de transferencia a 30 Mbps.

1.1.2 Topologías de red [2]

El término “topología” se emplea para referirse a la disposición geométrica de las estaciones de una red y los cables que las conectan, y al trayecto seguido por las señales a través de la conexión física. La topología de la red es pues, la disposición de los diferentes componentes de una red y la forma que adopta el flujo de información.

Las topologías fueron ideadas para establecer un orden que evitase el caos que se produciría si las estaciones de una red fuesen colocadas de forma aleatoria.

La topología tiene por objetivo hallar cómo todos los usuarios pueden conectarse a todos los recursos de red de la manera más económica y eficaz; al mismo tiempo, capacita a la red para satisfacer las demandas de los usuarios con un tiempo de espera lo más reducido posible.

1.1.2.1 Tipos de Topologías

Existen varios tipos de topologías: en estrella, en bus, en anillo y topologías hibridas.

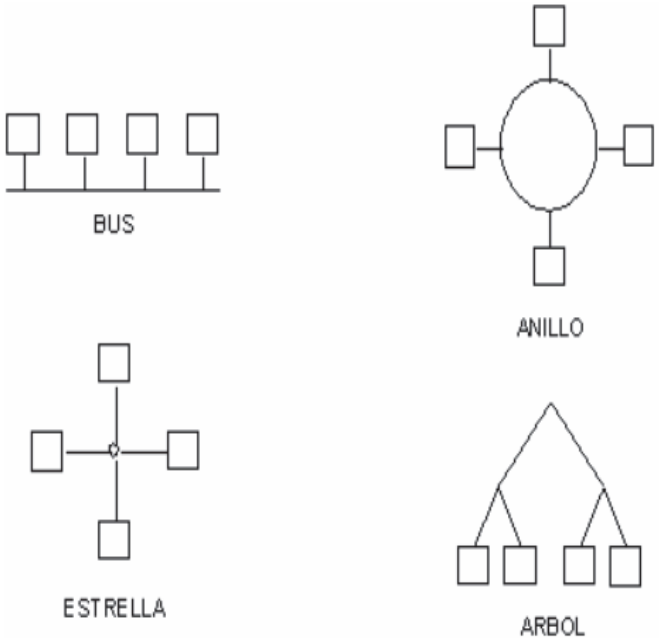


Figura 1.1.- Tipos de topologías [2]

1.1.2.1.1 Topología en bus

Tipo de topología usada antiguamente en la que los nodos que componen la red quedan unidos entre sí linealmente, uno a continuación del otro. Es necesario incluir en ambos extremos del bus unos dispositivos denominados terminadores, que evitan posibles rebotes de la señal.

Esta topología permite que todas las estaciones reciban la información que se transmite, una estación transmite y todas las restantes escuchan. Consiste en un cable con un terminador en cada extremo del que se cuelgan todos los elementos de una red. Todos los nodos de la red están unidos a este cable: el cual recibe el nombre de "Backbone Cable". Tanto Ethernet como Local Talk pueden utilizar esta topología.

1.1.2.1.2 Topología en anillo

Tipo de topología usada antiguamente donde las estaciones están unidas unas con otras formando un círculo por medio de un cable común.
El último nodo de la cadena se conecta al primero cerrando el anillo. Las señales circulan en un solo sentido alrededor del círculo, regenerándose en cada nodo. Con esta metodología, cada nodo examina la información que es enviada a través del anillo. Si la información no está dirigida al nodo que la examina, la pasa al siguiente en el anillo. La desventaja del anillo es que si se rompe una conexión, se cae la red completa.

El cableado es el más complejo de todos, debido, en parte, al mayor costo del cable, así como a la necesidad de emplear dispositivos MAU (Unidades de Acceso Multiestación) para implementar físicamente el anillo.

Cuando existen fallos o averías, es posible derivar partes de la red mediante los MAUs, aislando las partes defectuosas del resto de la red mientras se determina el problema.

Así, un fallo en una parte del cableado no detiene la red en su totalidad. Cuando se quieren añadir nuevas estaciones de trabajo se emplean también los MAUs, de modo que el proceso no posee una complicación excesiva

1.1.2.1.3 Topología en estrella

La topología en estrella es uno de los tipos más antiguos de topologías pero del más común en la actualidad. Se caracteriza porque en ella existe un nodo central al cual se conectan todos los equipos, de modo similar al radio de una rueda.

En esta topología, cada estación tiene una conexión directa a un acoplador (conmutador) central. Una manera de construir esta topología es con conmutadores telefónicos que usan la técnica de conmutación de circuitos, no son muy extensas de hasta 48 puntos.

Otra forma de esta topología es una estación que tiene dos conexiones directas al acoplador de la estrella (nodo central), una de entrada y otra de salida (la cual lógicamente opera como un bus). Cuando una transmisión llega al nodo central, este la retransmite por todas las líneas de salida.

1.1.2.1.4 Topología en árbol

Es una variante de la topología en bus. Esta topología comienza en un punto denominado cabezal o raíz (headend). Uno o más cables pueden salir de este punto y cada uno de ellos puede tener ramificaciones en cualquier otro punto. Una ramificación puede volver a ramificarse. En una topología en árbol no se deben formar ciclos. Son generalmente redes grandes pos su disposición y ramificación.

Una red como ésta representa una red completamente distribuida en la que computadoras alimentan de información a otras computadoras, que a su vez alimentan a otras. Las computadoras que se utilizan como dispositivos remotos pueden tener recursos de procesamientos independientes y recurren a los recursos en niveles superiores o inferiores conforme se requiera.

1.1.2.1.5 Topología en malla

En esta topología la esencia es buscar la interconexión de los nodos de tal manera que si uno falla los demás puedan redireccionar los datos rápida y fácilmente. Esta topología es la que más tolerancia tiene a los fallos porque es la que provee más caminos por donde puedan viajar los datos que van de un punto a otro.
La principal desventaja de las redes tipo malla es su costo, es por esto que se ha creado una alternativa que es la red de malla parcial en la cual los nodos más críticos se interconectan entre ellos y los demás nodos se interconectan a través de otra topología (estrella, anillo).

1.2 El modelo OSI [7]

El modelo de referencia OSI (Open System Interconnection, en español: Interconexión de Sistemas Abiertos), creado en 1984 por la ISO (International Organization for Standardization, en español: Organización Internacional para la Normalización), nació de la necesidad de poder comunicarse y trabajar de forma conjunta con las diferentes redes que existían tiempo atrás. Cada red podía usar una especificación diferente, lo que resultaba en incompatibilidades a la hora de comunicarse entre sí.
Estas incompatibilidades eran en su mayoría diferencias en el hardware y software que se utilizaba, y esto hacía imposible que la comunicación fuera exitosa. La ISO creó un idioma en común, de manera de asegurar la compatibilidad.

El modelo OSI consta de 7 capas numeradas, y cada una de ellas cumple una función de red específica. Con esta división en capas se logra que los usuarios puedan ver las funciones de red de cada capa y, así, comprendan cómo son transportados los datos.

Se podría decir que antes de modelos OSI se hablaban diferentes idiomas hasta que, con el modelo OSI, todos se unificaron en un idioma universal.

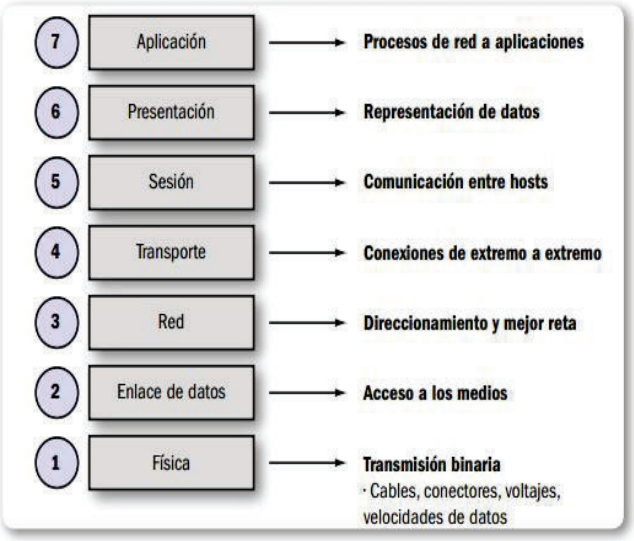


Figura 1.2.- División en capas del modelo OSI y sus funciones [7]

1.2.1 Funciones de cada capa

En el modelo OSI se identifica que cada una de las 7 capas debe realizar un conjunto de funciones para que los datos viajen en la red desde el emisor hasta el receptor, y que, de este modo, la información pueda ser transmitida sin problemas. Para ilustrar este proceso realizaremos una breve descripción de las capas, tomando como referencia el esquema que se presenta en la figura siguiente.

1.2.1.1 Capa de Aplicación:

Esta es la capa con la que más interactúa el usuario. No da servicios a las demás capas del modelo OSI, sino solo a aplicaciones fuera del modelo.
Cuando un usuario necesita realizar una actividad (leer o escribir e-mails, enviar archivos, usar una hoja de cálculo, un procesador de texto o similar), el sistema operativo va a interactuar con esta capa para llevarla a cabo.

1.2.1.2 Capa de Presentación:

En esta capa se busca tener un formato de datos en común, para garantizar que los datos enviados por la capa aplicación de un sistema puedan ser entendidos por la misma capa aplicación pero de otro sistema.

En caso de ser necesario, la información será traducida usando un formato en común. Algunos ejemplos en esta capa pueden ser los formatos MP3, JPG y GIF, entre otros.

1.2.1.3 Capa de Sesión:

En esta capa se establece, mantiene y terminan las comunicaciones entre los dispositivos de red que se están comunicando. Podemos pensar esta capa como una conversación.

1.2.1.4 Capa de Transporte:

Esta capa verifica si los datos vienen de más de una aplicación e integra cada uno de ellos en un solo flujo de datos dentro de la red física. A esto se llama control de flujo de datos. Por otra parte, se encarga de realizar la verificación de errores y también la recuperación de datos.

1.2.1.5 Capa de Red:

Es la capa que determina cómo serán enviados los datos al receptor. También efectúa la conexión y la selección de la ruta entre dispositivos que pueden estar en diferentes redes.

1.2.1.6 Capa de Enlace de Datos:

En esta capa a los datos provenientes de la capa red se les asigna el correspondiente protocolo físico (para hablar el mismo idioma), se establece el tipo de red y la secuencia de paquetes utilizada.

1.2.1.7 Capa Física:

Es la parte de hardware del modelo. Acá se definen las especificaciones o características físicas de la red, como niveles de voltaje, cableado, distancias de transmisión máximas y conectores físicos usados, entre otros atributos descriptos dentro de las especificaciones de la esta capa.

1.3 Arquitectura TCP/IP

Hay que tener en cuenta que existe otra arquitectura paralela al modelo OSI llamada TCP/IP. Se trata de una arquitectura que es mucho más conocida entre los usuarios de redes informáticas. Este es el estándar abierto de Internet, que hace posible la comunicación entre computadoras ubicadas en cualquier parte del mundo.

TCP/IP significa Protocolo de Control de Transmisión / Protocolo de Internet y, a diferencia del modelo OSI, posee cuatro capas: Aplicación, Transporte, Internet y Acceso a la red. Que son el resultado de entremezclar las capas del modelo OSI y dan como resultado las 4 capas que corresponden al modelo TCP/IP.

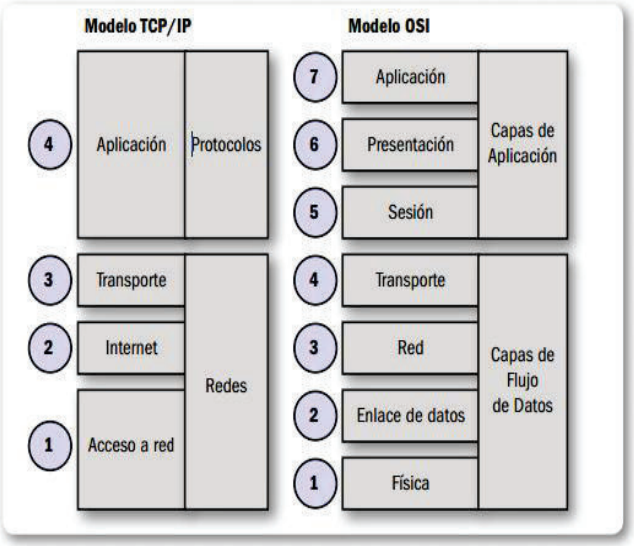


Figura 1.3.- Comparación entre las capas del modelo OSI y el TCP/IP [7]

1.3.1 Capa de Aplicación:

Aquí se combinan todos los aspectos relacionados con las aplicaciones. De esta forma, las capas de Sesión, Presentación y Aplicación del modelo OSI son equivalentes a la Capa de Aplicación en TCP/IP, que nos garantiza la correcta disposición de los datos para la siguiente capa.

1.3.2 Capa de Transporte:

Esta capa del modelo TCP/IP directamente se corresponde con la Capa de Transporte del modelo OSI.

1.3.3 Capa de Internet:

Corresponde a la Capa de Red del modelo OSI. El principal objetivo de esta capa es realizar el envío de datos desde cualquier red y que estos lleguen al destino, independientemente de la ruta o redes necesarias para llegar.

1.3.4 Capa de Red:

Es la combinando la Capa Física y la de Enlace de Datos del modelo OSI, obtenemos esta capa del modelo TCP/IP. Su objetivo es enrutar los datos entre dispositivos que se encuentren en la misma red informática.

1.4 Redes inalámbricas WLAN[7]

Una red de área local inalámbrica o WLAN (Wireless LAN) es la que utiliza ondas electromagnéticas (radio e infrarrojo) para enlazar (mediante un adaptador) los equipos conectados a la red, en lugar de los cables coaxiales o de fibra óptica que se utilizan en las LAN convencionales cableadas (Ethernet, Token Ring, ...).

Las redes locales inalámbricas más que una sustitución de las LANs convencionales son una extensión de las mismas, ya que permite el intercambio de información entre los distintos medios en una forma transparente al usuario.
En este sentido el objetivo fundamental de las redes WLAN es el de proporcionar las facilidades no disponibles en los sistemas cableados y formar una red total donde coexistan los dos tipos de sistemas. Enlazando los diferentes equipos o terminales móviles asociados a la red. Este hecho proporciona al usuario una gran movilidad sin perder conectividad.

El atractivo fundamental de este tipo de redes es la facilidad de instalación y el ahorro que supone la supresión del medio de transmisión cableado.

Aun así sus prestaciones son menores en lo referente a la velocidad de transmisión que se sitúa entre los 2 y los 10 Mbps frente a los 10 y hasta los 100 Mbps ofrecidos por una red convencional.

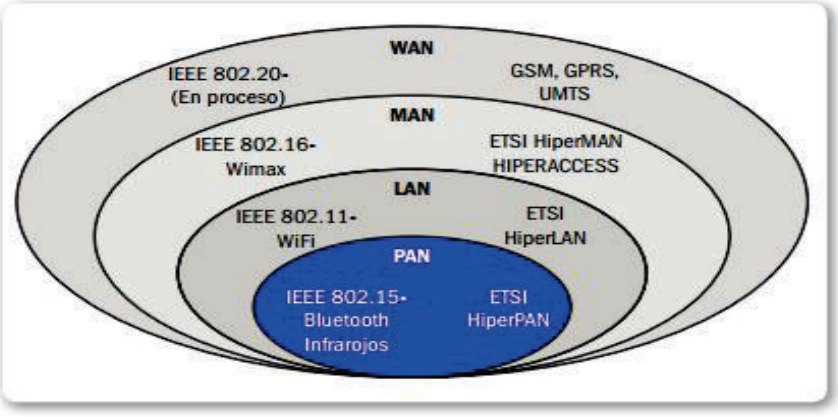


Figura 1.4.- Tecnologías inalámbricas son su estándar [7]

1.4.1 Historia de la redes inalámbricas WLAN

El origen de las LAN inalámbricas (WLAN) se remonta a la publicación en 1979 de los resultados de un experimento realizado por ingenieros de IBM en Suiza, consistente en utilizar enlaces infrarrojos para crear una red local en una fábrica. Estos resultados, pueden considerarse como el punto de partida en la línea evolutiva de esta tecnología.

Las investigaciones siguieron adelante tanto con infrarrojos como con microondas. En mayo de 1985 el FCC3 (Federal Communications Comission) asignó las bandas IMS4 (Industrial, Scientific and Medical) 902-928 MHz, 2,400-2,4835 GHz, 5,725-5,850 GHz a las redes inalámbricas basadas en spread spectrum.

La asignación de una banda de frecuencias propició una mayor actividad en el seno de la industria: ese respaldo hizo que las WLAN empezaran a dejar ya el laboratorio para iniciar el camino hacia el mercado.

Desde 1985 hasta 1990 se siguió trabajando ya más en la fase de desarrollo, hasta que en mayo de 1991 se publicaron varios trabajos referentes a WLAN operativas que superaban la velocidad de 1 Mbps, el mínimo establecido por el IEEE 802 para que la red sea considerada realmente una LAN.

Hasta ese momento las WLAN habían tenido una aceptación marginal en el mercado por dos razones fundamentales: falta de un estándar y los precios elevados de una solución inalámbrica. Sin embargo, se viene produciendo estos últimos años un crecimiento explosivo en este mercado (de hasta un 100% anual). Y esto es debido a distintas razones:

- El desarrollo del mercado de los equipos portátiles y de las comunicaciones móviles.

- La conclusión de la norma IEEE 802.11 para redes de área local inalámbricas que ha establecido un punto de referencia y ha mejorado en muchos aspectos de estas redes.

1.4.2 Funcionamiento de las redes inalámbricas WLAN[6]

En estas redes usamos las ondas electromagnéticas para enlazar, mediante un concentrador, los dispositivos de una red, reemplazando los cables de las redes LAN convencionales.

Dar conectividad y acceso a las redes cableadas son las funciones principales de este tipo de redes. Podemos pensar que son una especie de extensión de las redes cableadas pero que nos ofrecen la flexibilidad y la movilidad de las comunicaciones inalámbricas. Al utilizar frecuencias de uso libre, no necesitamos pedir autorización o permiso para usar estas redes. Lo que sí debemos tener en cuenta es la regularización del espectro de frecuencias que varía de país en país.

Una desventaja que se presenta, cuando usamos las frecuencias de uso libre (estas son las de 2.4 GHz y 5 GHz), es que las comunicaciones pueden sufrir interferencias y errores de transmisión. Al tener estos errores, los datos se reenvían una y otra vez. Entonces, si en una transmisión la mitad de los datos no llegan a destino a causa de estos errores, tendremos una reducción a las dos terceras partes de la velocidad eficaz real. Esto dará como resultado una variación en la velocidad máxima especificada en teoría comparándola con la que obtenemos en la realidad.

Teniendo largas distancias, la velocidad real en las redes Wi-Fi estará muy por debajo que la especificada en las normas, dado que factores como la potencia de transmisión, las distancias o el área de cobertura, el tipo de modulación empleada, el ambiente propenso a la interferencia, entre otros, afectan directamente a esta velocidad.

El término SSID (Service Set Identifier: identificador del conjunto de servicio) es el mecanismo que utilizan los usuarios para identificarse en la red al momento de conectarse. Este debe ser el mismo para todos los integrantes de una red inalámbrica específica. Todos los puntos de acceso y usuarios del mismo ESS (Extended Service Set: conjunto de servicio extendido) deben configurarse con el mismo identificador (ESSID). Este identificado es el nombre de la red inalámbrica a la que se desea conectar, todos los usuarios conectados a esta tendrán idéntica etiqueta.

1.4.3 Aplicación de las redes inalámbricas [7]

Las aplicaciones más típicas de las redes de área local que podemos encontrar actualmente son las siguientes:

- Implementación de redes de área local en edificios históricos, de difícil acceso y en general en entornos donde la solución cableada es inviable.

- Posibilidad de reconfiguración de la topología de la red sin añadir costes adicionales. Esta solución es muy típica en entornos cambiantes que necesitan una estructura de red flexible que se adapte a estos cambios.

- Redes locales para situaciones de emergencia o congestión de la red cableada.

- Estas redes permiten el acceso a la información mientras el usuario se encuentra en movimiento. Habitualmente esta solución es requerida en hospitales, fábricas, almacenes, etc.

- Generación de grupos de trabajo eventuales y reuniones ad-hoc. En estos casos no valdría la pena instalar una red cableada. Con la solución inalámbrica es viable implementar una red de área local aunque sea para un plazo corto de tiempo.
- En ambientes industriales con severas condiciones ambientales este tipo de redes sirve para interconectar diferentes dispositivos y máquinas.

- Interconexión de redes de área local que se encuentran en lugares físicos distintos. Por ejemplo, se puede utilizar una red de área local inalámbrica para interconectar dos o más redes de área local cableada situadas en dos edificios distintos.

1.4.4 Ventajas de las redes inalámbricas WLAN [6]

Se describirán algunas ventajas que se tendrá al usar una red inalámbrica comparándola con las redes cableadas clásicas. La primer ventaja que aparece y una de la más importante es la movilidad que adquiere el usuario de estas redes.

Una computadora o cualquier dispositivo (laptop, teléfono, impresora, entre otros) pueden acomodarse en cualquier punto dentro del área de cobertura de la red, sin tener que preocuparse si es posible o no hacer llegar un cable de red hasta este lugar. No es necesario estar atado a un cable para imprimir documentos, compartir música o navegar por Internet, entre otras muchas tareas que podemos realizar.

La portabilidades otro punto importante de las redes inalámbricas, ya que permite a los usuarios moverse junto con los dispositivos conectados a la red inalámbrica, tales como notebooks, notebooks o similares, sin perder el acceso a la red. Se facilita el trabajo permitiendo la movilidad por toda el área de cobertura.

La flexibilidades otra ventaja de las redes sin cables. Podemos situar nuestra notebook sobre la mesa del escritorio para luego desplazarla hacia el dormitorio, sin tener que realizar el más mínimo cambio de configuración de la red.

También el uso de las redes inalámbricas es indicado para lugares donde se necesitan accesos esporádicos o temporales (como lo son las conferencias, los entrenamientos empresariales, charlas, hoteles, lugares públicos, instituciones educativas, entre otros.)

Al tratar de extender una red cableada clásica se presentan ciertos problemas, ya que esto no es una tarea fácil ni barata. En cambio, cuando al expandir la red inalámbrica, luego de su instalación inicial, simplemente se adquiere una placa de red inalámbrica (si es que la computadora no cuenta con ella) para la conexión. Esto se llama escalabilidad, que se define como la facilidad de expandir la red luego de ser instalada. Al diferenciar con las redes cableadas, se necesita instalar un nuevo cable para esa nueva computadora, lo que implica pérdida de tiempo y dinero.

Y este último punto es otra ventaja, el ahorro de costos que genera este tipo de redes, ya que no existe el gasto en diseñar e instalar que tenemos en una red cableada.

1.4.5 Desventajas de las redes inalámbricas WLAN

Las redes inalámbricas también presentan ciertas desventajas, no todo es color de rosa cuando se utilizan estas redes. Los principales puntos en contra que tenemos.

Las redes cableadas, en la actualidad, trabajan con velocidades de 100 Mbps a 10.000 Mbps, que se reduce en redes sin cables y se traduce en una menor velocidad. Wi-Fi trabaja en velocidades de 11 a 108 Mbps, aunque existen soluciones y estándares propietarios (veremos más adelante qué significa esto) que llegan a mejores velocidades pero el precio es muy superior.

Una de las ventajas de las redes inalámbricas es la de no necesitar un medio físico para funcionar. Esto se convierte en desventaja cuando se tiene en cuenta la seguridad de nuestra red.

Considerar que cualquier persona con una notebook o un teléfono con Wi-Fi pueden intentar acceder a nuestra red tan solo estando en el área de cobertura.

Ya que esta área no está delimitada por paredes u otra barrera, la persona interesada en ingresar a nuestra red no necesita estar dentro de nuestra casa o edificio y menos estar conectada por medio de un cable.

El alcance de una red inalámbrica está determinado por la potencia de los equipos y la ganancia de las antenas, así si estos parámetros no son suficientes habrá puntos en nuestra casa u oficina donde no tengamos cobertura, suele haber obstáculos que interfieren.

Por último, pero no menos importante, se tienen las interferencias sufridas en la banda de frecuencias de 2.4 GHz como desventaja. Al no requerir licencia para operar en la banda de 2.4 GHz, muchos equipos del mercado la utilizan (teléfonos inalámbricos, microondas, entre otros) sumado a que todas las redes Wi-Fi funcionan en la misma banda de frecuencias, incluida la de nuestro vecino.

Cuanto mayores sean las interferencias producidas por otros equipos o que existan en el ambiente, menor será el rendimiento de nuestra red. No obstante, el hecho de tener probabilidades de sufrir interferencias no quiere decir que existirán las mismas ya que la mayoría de las redes inalámbricas funciona sin problemas.

1.4.6 Componentes de la red inalámbrica

Los diferentes dispositivos que son fundamentales para el correcto funcionamiento de una red inalámbrica son: placa de red inalámbrica, punto de acceso (AP, Access Pointen inglés), router inalámbrico y las antenas.

1.4.6.1 Placa de red inalámbrica

Recibe y envía información entre las computadoras de la red, es una parte imprescindible para conectarnos de forma inalámbrica. Existen placas de diferentes velocidades, entre 54 Mbps y 108 Mbps.

Todas tienen una antena (que puede ser externa o interna) en general de baja ganancia, que puede ser reemplazada por otra de mayor ganancia para mejorar la conexión (cuando el dispositivo lo permita). Al poseer una notebook o algún celular nuevo, la placa viene integrada.

1.4.6.2 Puntos de acceso

Se considera como el punto principal de emisión y recepción. Este punto concentra la señal de los nodos inalámbricos y centraliza el reparto de la información de toda la red local. También realiza el vínculo entre los nodos inalámbricos y la red cableada; por esto se lo suele llamar puente.

1.4.6.3 Router inalámbrico:

Este dispositivo permite la conexión a internet si se tiene una conexión ADSL a través de una línea telefónica. Pero esta no es la única función, ya que, además, permite distribuir Internet mediante cables y de forma inalámbrica mediante el punto de acceso que tiene integrado.

También realiza restricciones de acceso, por usuarios, servicios y horarios, entre otras opciones, y puede controlar el ancho de banda y las prioridades de acceso por cliente conectado o servicio

1.4.6.4 Antena:

Es un elemento muy importante en la red, porque se encarga de transformar la energía de corriente alterna, generada en los equipos inalámbricos de la red, en un campo electromagnético, o viceversa, para que la comunicación pueda realizarse entre los equipos. Si la transformación es eficaz, se obtendrá una mayor área de cobertura (o alcance) sin importar el equipo. La antena es un en un dispositivo que permite convertir la señal eléctrica en ondas electromagnéticas. Solamente de la antena depende más del 50% de la calidad de conexión para un dispositivo de la red; por eso necesitamos que este elemento sea bueno o superior.

Existen otros equipos y accesorios en una red inalámbrica que no son fundamentales para su funcionamiento y se transforman en soluciones puntuales o específicas para ciertos casos. Estos son: **cámaras de vigilancia inalámbricas**, amplificadores de señal, protectores de rayos, equipos PoE (de sus siglas en inglés, Power over Ethernet) que permiten recibir con un cable de red UTP no solo datos sino también energía y así alimentar, por ejemplo, un AP. Divisores de señal, cajas Estanca (o weather proof) y torres para montar equipos son tenidos en cuenta al armar una red inalámbrica de largo alcance, comúnmente llamados enlaces de larga distancia.

1.4.7 Modos de operación

Cuando pensamos en los modos de operación de las redes inalámbricas, y refiriéndonos a los estándares 802.11, podemos definir dos modos fundamentales: ad hoc e infraestructura.

1.4.7.1 Modo ad hoc

Este modo se presenta como el más sencillo para configurar. Los únicos elementos necesarios para conformar una red en modo ad hoc son los dispositivos móviles que poseen placas de red inalámbricas.
También se lo conoce con el nombre de punto a punto, ya que permite establecer comunicación directa entre los usuarios sin necesidad de involucrar un punto de acceso central que realice el vínculo.

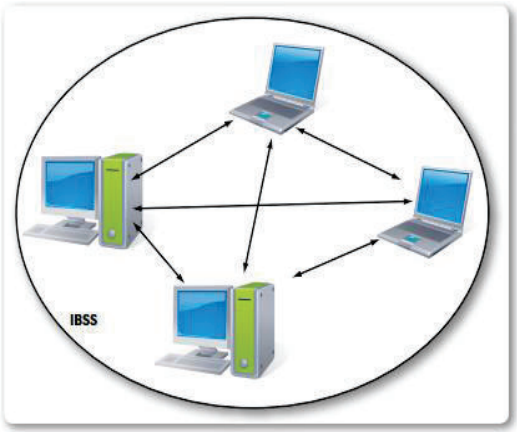


Figura 1.5.- El modo ad hoc o Conjunto de Servicios Básicos Independientes [6]

1.4.7.2 Modo Infraestructura

En las configuraciones en modo infraestructura se usa el concepto de celda, similar al implementado en la red de telefonía celular. Una celda es al área en la que una señal radioeléctrica es efectiva. Así, una red inalámbrica puede tener una celda de tamaño reducido y, por medio de varios puntos de emisión, es posible combinar las celdas y tener un área mayor.

Se logrará esto utilizando los famosos puntos de acceso, que funcionan como repetidores y, por eso, pueden duplicar el alcance de la red, ya que en este caso, la distancia máxima no es entre estaciones, sino entre una estación y un punto de acceso. Estos dispositivos capaces de extender una red son colocados en lugares estratégicos, en general, altos y, además, realizan la coordinación del funcionamiento entre usuarios. Con solo un punto de acceso podemos soportar un grupo acotado de usuarios, y el rango será de entre 30 metros y varios cientos de metros. Si se desea conectar varios puntos de acceso y usuarios, todos deben configurar el mismo SSID.

1.5 Wi-Fi [5]

Wi-Fi es una tecnología de redes de área local inalámbricas (WLAN) de paquetes no guiados basados en la transmisión de la señal por ondas electromagnéticas de radio en torno a los 2,4 GHz o los 5 GHz.

Aunque al principio el ancho de banda era sensiblemente menor con respecto a las redes guiadas que utilizan cableado, actualmente, con la **versión 802.11n** hasta 600 Mbps (pero, sobre todo, con la **802.11ac** a 1 Gbps) esta diferencia ya es inapreciable en instalaciones profesionales. Su implantación prolifera de forma significativa gracias a la disminución de los costos de los componentes, a los estándares en que se basan y a la producción de los mismos a gran escala.

Las WLAN no surgen para sustituir a las LAN, sino más bien para complementarlas, ya que permiten tanto a los usuarios como a los dispositivos mantenerse conectados y disfrutar de plena libertad de movimientos, siempre conviviendo en armonía ambas tecnologías y pudiendo compartir entre ambas todo tipo de información.

Sin embargo, no se han resuelto por completo los problemas de seguridad: los algoritmos de protección que van apareciendo se vuelven ineficaces cada vez que se aumenta el cómputo de cálculo de los equipos, tal como se verá a lo largo de esta unidad. Los primeros algoritmos de cifrado pudieron romperse con bastante facilidad, si bien de un tiempo a esta parte se han desarrollado otros mucho más fiables y robustos.

Por lo tanto, esta tecnología de red inalámbrica resulta imprescindible para cualquier empresa del siglo XXI. Sin ella, la Internet móvil que se agrega como herramientas de trabajo, los smartphones y tablets sería imposible.

DIFICULTADES	VENTAJAS
Ancho de banda inferior.	Disminución de costos.
Pueden sufrir interferencias entre distintos aparatos.	Fácil instalación (no requiere cableado).
Requiere un mayor mantenimiento.	Reducción del tiempo de implantación.
Menor seguridad.	Mayor flexibilidad para ampliar o modificar la red.
Cobertura a distancia de conexión limitada.	Permite total movilidad de los clientes (roaming).

Tabla 1.1.Ventajas y dificultades de la tecnología inalámbrica frente a la cableada [5]

Antes de proceder al diseño de una red Wi-Fi, habrá que realizar un estudio para establecer los espacios físicos que se requieren cubrir, el tipo de cobertura que se dará y la funcionalidad deseada, así como los canales y los identificadores de red que se utilizarán. Además, conviene tener en cuenta los obstáculos, los materiales existentes, la cantidad de usuarios a los que se debe dar servicio, etc.

De cara a su implantación, y a la hora de adquirir el hardware Wi-Fi, hay que considerar los factores siguientes:

- **Alta disponibilidad**: la conexión inalámbrica tiene que estar en servicio en todo momento, todos los días del año, siendo un servicio 24x7.
- **Arquitectura abierta:** todos sus elementos siguen los estándares existentes, de modo que los dispositivos suministrados por fabricantes distintos funcionan correctamente entre sí, siempre que estén certificados por la asociación Wi-Fi.
- **Escalabilidad:** permite disponer de diversos puntos de acceso (PA o AP, Access Point) en una misma red para proporcionar un mayor ancho de banda. A partir de una configuración mínima de un AP, la tecnología permite su ampliación para llegar a cubrir las nuevas necesidades o requerimientos de la empresa, pudiendo ampliar tanto el espacio físico a cubrir como el ancho de banda a suministrar en cada zona.
- **Manejabilidad:** todos los elementos implicados en las redes inalámbricas han de ser de fácil configuración y manejo, como por ejemplo, oprimiendo un simple botón en cada dispositivo a conectar e introduciendo un PIN (entre enroutador/PA y/o equipo o impresora Wi-Fi o cualquier otro), como lo permite la tecnología WPS (parecida al emparejamiento en Bluetooth).

1.6 Estándares de conexión [5]

La organización de las tecnologías WLAN con soporte Wi-Fi que ha llevado a la estandarización de los diferentes grupos de trabajo ha sido la IEEE, aunque no es la única que los respalda. De hecho, se ha desarrollado a partir de los dos rangos de frecuencias libres ISM: 2,4 GHz y 5 GHz.

1.6.1 Estándar IEEE[8]

Es un estándar que se define como un conjunto de normas y recomendaciones técnicas que regula la realización de ciertos procesos o la fabricación de componentes para garantizar la interoperabilidad.

Los estándares se utilizan por vendedores para darles garantías a sus clientes de la seguridad, la calidad y la consistencia de sus productos y a los clientes les permite no estar vinculados a un único vendedor.

Estándar abierto y cerrado: es similar a decir estándar que es público o propio de un fabricante o vendedor. Para graficarlo de alguna forma, al crear un documento de Excel será un estándar cerrado, mientras que un ejemplo de estándar abierto es escribir código para una página web en lenguaje HTML.

Cualquiera puede hacer uso de un estándar abierto, esto incrementa la compatibilidad entre el hardware, el software o los sistemas. Analizando desde el lado práctico, seguir el estándar abierto cuando se desarrolla un producto permitirá crear algo que pueda trabajar en conjunto con otros productos que sigan las mismas especificaciones de ese estándar.

En el campo de las telecomunicaciones, el **Instituto de Ingenieros Eléctricos y Electrónicos (IEEE por sus siglas en inglés)** es líder en la promoción de estándares internacionales.

Los estándares para redes LAN/MAN son unos de los productos más conocidos, en los que se incluyen el de redes cableadas (Ethernet IEEE 802.3) y el de redes inalámbricas (IEEE 802.11).

1.6.2 Familia IEEE 802

La IEEE es la principal generadora de estándares para redes, el estándar IEEE 802 fue definido como una familia de estándares referentes a redes LAN y MAN. La norma solo abarca las redes que transportan paquetes de información con tamaño variable (redes Ethernet) y no redes con paquetes fijos.

Las dos capas más bajas nivel del modelo OSI son la capa física y la de enlace de datos, estas son las capas que se relacionan directamente con las especificaciones detalladas en la IEEE 802. Dentro de la IEEE, existe un comité de estándares LAN/MAN que mantiene la familia IEEE 802, en el que se establecen grupos de trabajo para cada una de las 22 áreas que incluye.

1.6.2.1 IEEE 802.11

IEEE 802.11 también recibe el nombre de Wi-Fi y hace referencia a los sistemas DSSS operando a 1, 2, 5.5 y 11 Mbps, donde todos cumplen con la norma de forma retrospectiva (o sea ofrecen compatibilidad con productos anteriores). Tener esta **compatibilidad para atrás** es importante, ya que permite actualizar nuestra red sin necesidad de cambiar nada. Luego, en el estándar IEEE 802.11a abarca los dispositivos WLAN que operan en la banda de 5 GHz, por lo tanto no se permite la interoperabilidad con dispositivos funcionando a 2,4 GHz como los de 802.11b, dada su frecuencia. Una nueva enmienda llamada IEEE 802.11g ofrece compatibilidad para atrás para dispositivos 802.11b utilizando una tecnología de modulación llamada **multiplexión por división de frecuencia ortogonal** (OFDM por sus siglas en inglés) y además se obtiene la misma tasa de transferencia que 802.11a.

ESTÁNDAR WLAN	EEE 802.11B	EEE 802.11A	EEE 802.44G	EEE 802.11N
Organismo	IEEE	IEEE	IEEE	IEEE
Finalización	1999	2002	2003	2005
Denominación	Wi-Fi	Wi-Fi 5	Wi-Fi	
Banda de Frecuencia	2,4 GHz	5 GHz	2,4 GHz	2,4 GHz y 5,8 GHz
Velocidad Máxima	11Mbps	54 Mbps	54 Mbps	108 Mbps
Thoughput medio	5,5 Mbps	36 Mbps		
Interface aire	DSSS	OFDM	OFDM	OFDM

Tabla 1.2: Diferentes tecnologías normalizadas por la IEEE [8]

1.6.2.1.1 Mejoras del estándar IEEE 802.11

- **802.11b**

  En este estándar se mejoró, en comparación con el estándar original, la tasa de transmisión de datos, se la elevó hasta 11 Mbit/s (se lee mega bits por segundo), lo que significa una gran mejoría.

  Como dato extra, se puede decir que inicialmente se soportan hasta 32 usuarios por AP si utilizamos este estándar.

- **802.11a**

  Al igual que el estándar anterior, usa la misma tecnología de base que el estándar original, la principal diferencia está en que opera en la banda de 5 GHz usando OFDM, lo que permite una tasa de transmisión máxima de 54 Mbit/s. La mayor velocidad de transmisión es una de las ventajas, así como la ausencia de interferencias en esta frecuencia de trabajo. Como desventaja se tiene la incompatibilidad con 802.11b, ya que opera en diferente frecuencia.

- **802.11g**

  Funciona en la misma banda de 802.11b, lo que hace que exista compatibilidad con dispositivos trabajando bajo este estándar. La tasa máxima de transferencia de datos es de 54 Mbit/s, ya que se usa la modulación OFDM.

- **802.11s**

  Este es el estándar para redes malladas (Mesh), las cuales mezclan las topologías de redes ad-hoc e infraestructura. La norma 802.11s trata de regular la interoperabilidad entre diferentes fabricantes en cuanto a este protocolo malla, ya que cada uno tiene sus propios protocolos para la autoconfiguración de rutas entre AP. Esto extiende el estándar IEEE 802.11 con un protocolo y arquitectura totalmente nuevos.

- **802.11n**

  Se presenta como la cuarta generación en los sistemas sin cables Wi-Fi, compatible con estándares anteriores. Trabaja en las frecuencias de 2.4 GHz y 5 GHz y brinda una mejora importante respecto a estándares anteriores, que es el uso de varias antenas de transmisión y recepción.

Este concepto es llamado MIMO y aumenta la tasa de transferencia de datos y el alcance. Lo notables es que MIMO aprovecha lo que otros estándares consideran un obstáculo: la **multitrayectoria.**

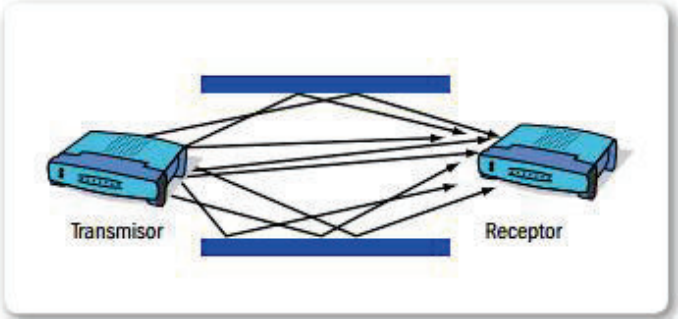


Figura 1.6.- Concepto MIMO [8]

ESTÁNDAR	FRECUENCIA	TÉCNICA DE MODULACIÓN	TASA DE TRANSMISIÓN	ÁREA DE COBERTURA
802.11ª	5 GHz.	OFDM	54 Mbit/s	50 metro aprox.
802.11b	2,4 GHz	DSSS, CCK	11 Mbit/s	100 metros aprox.
802.11g	2,4 GHz	OFDM, CSSK, DSSS	54 Mbit/s	100 metros aprox.
802.11n	2,4 GHz y 5 GHz	OFDM	540Mbit/s	250 metros aprox.

Tabla 1.3: Tasa de transmisión y área de cobertura por estándar. [8]

En la tabla1.4 se tiene un resumen de cada uno de los estándares IEEE 802.11 con sus principales mejoras o cambios dictados por la IEEE.

ESTÁNDAR	DESCRIPCIÓN
802.11	El original, tasas de 1 y 2 Mbit/s en 2,4 GHz. Estándar de RF e IR (1999)
802.11ª	54 Mbit/s, en 5GHz (1999, los productos salen en 2001)

ESTÁNDAR	DESCRIPCIÓN
802.11b	Mejoras en 802.11 para soportar 5,5 y 11 Mbit/s (1999)
802.11c	Procedimientos en operación Puente, incluido en 802.11d (2001)
802.11d	Extensión del roaming internacional (país a país) (2001)
802.11e	Mejoras en Calidad de Servicio (QoS)(2005)
802.11f	Protocolo Inter-Access Point (2003)
802.11g	54 Mbit/s, en 2,4 GHz. Compatible para atrás con 802.11b (2003)
802.11h	Manejo del espectro 802.11ª (5 GHz) para compatibilidad Europa
802.11i	Manejo en seguridad (2004)
802.11j	Extensión para Japón (2004)
802.11k	Mejoras en la medición de recursos de radio (2007)
802.11l	(Reservado y no disponible para el uso)
802.11m	Mantenimiento del estándar.
802.11n	Incremento en la tasa de transmisión usando MMO (2009)
802.11º	(Reservado y no disponible para el uso)
802.11p	WAVE (acceso inalámbrico para el automóvil) Intercambio de datos entre vehículos.
802.11q	(Reservado y no disponible para el uso)
802.11r	Fast Roaming Working. Permite que el cambio de AP sea rápido. Importante en VoIP

ESTÁNDAR	DESCRIPCIÓN
892.11s	ESS Protocolo para redes Malla o Mesh
802.11T	Wpp (Wireless Performance Prediction)
802.11u	Interoperabilidad con redes no 802 (redes celulares)
802.11v	Configuración remota de dispositivos cliente.
802.11w	Protección para redes a causa de sistemas externos.
892.11x	(Reservado y no disponible para el uso)
802.11y	Operación en banda 3650 a 3700 MHz en USA.

Tabla 1.4: Estándares de la IEEE para uso comercial, científico y militar. [8]

1.6.2.2 Capa Física 802.11 [7]

La Capa Física de cualquier red define la modulación y la señalización características de la transmisión de datos. IEEE 802.11 define tres posibles opciones para la elección de la capa física:

- Espectro expandido por secuencia directa o DSSS.
- Espectro expandido por salto de frecuencias o ambas en la banda de frecuencia 2.4 GHz ISM
- Luz infrarroja en banda base o sea sin modular.

En cualquier caso, la definición de tres capas físicas distintas se debe a las sugerencias realizadas por los distintos miembros del comité de normalización, que han manifestado la necesidad de dar a los usuarios la posibilidad de elegir en función de la relación entre costes y complejidad de implementación, por un lado, y prestaciones y fiabilidad, por otra.

No obstante, es previsible que, al cabo de un cierto tiempo, alguna de las opciones acabe obteniendo una clara preponderancia en el mercado. Entretanto, los usuarios se verán obligados a examinar de forma pormenorizada la capa física de cada producto hasta que sea el mercado el que actúe como árbitro final.

1.6.2.2.1 Radiofrecuencia

Aunque existen dos tipos de tecnologías que emplean las radiofrecuencias, la banda estrecha y la banda ancha, también conocida espectro ensanchado, ésta última es la que más se utiliza.

La tecnología de espectro ensanchado, utiliza todo el ancho de banda disponible, en lugar de utilizar una portadora para concentrar la energía a su alrededor. Tiene muchas características que le hacen sobresalir sobre otras tecnologías de radiofrecuencias (como la de banda estrecha, que utiliza microondas), ya que, por ejemplo, posee excelentes propiedades en cuanto a inmunidad a interferencias y a sus posibilidades de encriptación. Esta, como muchas otras tecnologías, proviene del sector militar.

Existen dos técnicas de espectro expandido:

- **Espectro Ensanchado por Secuencia Directa (DSSS)**

  En esta técnica se genera un patrón de bits redundante (señal de chip) para cada uno de los bits que componen la señal. Cuanto mayor sea esta señal, mayor será la resistencia de la señal a las interferencias.

  El estándar IEEE 802.11 recomienda un tamaño de 11 bits, pero el óptimo es de 100. En recepción es necesario realizar el proceso inverso para obtener la información original.

  La secuencia de bits utilizada para modular los bits se conoce como secuencia de Barker (también llamado código de dispersión o PseudoNoise). Es una secuencia rápida diseñada para que aparezca aproximadamente la misma cantidad de 1 que de 0.

Solo los receptores a los que el emisor haya enviado previamente la secuencia podrán recomponer la señal original. Además, al sustituir cada bit de datos a transmitir, por una secuencia de 11 bits equivalente, aunque parte de la señal de transmisión se vea afectada por interferencias, el receptor aún puede reconstruir fácilmente la información a partir de la señal recibida.

Esta secuencia proporciona 10,4dB de aumento del proceso, el cual reúne los requisitos mínimos para las reglas fijadas por la FCC.

Una vez aplicada la señal de chip, el estándar IEEE 802.11 ha definido dos tipos de modulación para la técnica de espectro ensanchado por secuencia directa (DSSS), la modulación DBPSK y la modulación DQPSK, que proporcionan una velocidad de transferencia de 1 y 2 Mbps respectivamente.

- **Espectro ensanchado por salto de frecuencia (FHSS)**

La tecnología de espectro ensanchado por salto en frecuencia (FHSS) consiste en transmitir una parte de la información en una determinada frecuencia durante un intervalo de tiempo llamado dwell time e inferior a 400 ms. Pasado este tiempo se cambia la frecuencia de emisión y se sigue transmitiendo a otra frecuencia. De esta manera cada tramo de información se va transmitiendo en una frecuencia distinta durante un intervalo muy corto de tiempo.

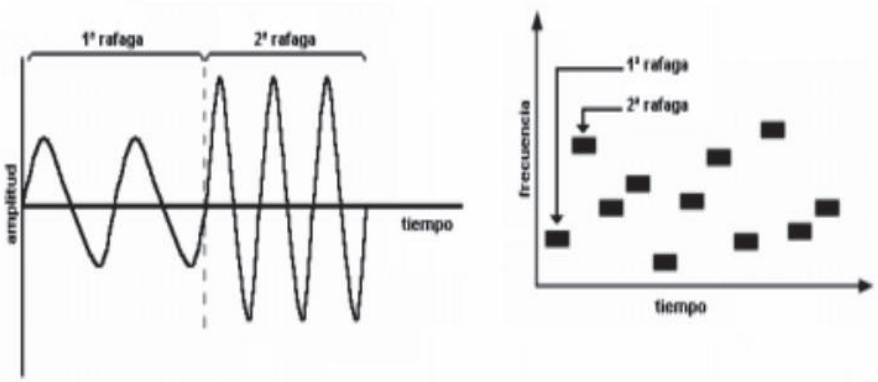


Figura 1.7.- Codificación con salto de frecuencia [7]

El orden en los saltos en frecuencia se determina según una secuencia pseudoaleatoria almacenada en unas tablas, y que tanto el emisor y el receptor deben conocer.

Si se mantiene la sincronización en los saltos de frecuencias se consigue que, aunque en el tiempo se cambie de canal físico, a nivel lógico se mantiene un solo canal por el que se realiza la comunicación.

El estándar IEEE 802.11 define la modulación aplicable en este caso. Se utiliza la modulación en frecuencia FSK (Frequency Shift Keying), con una velocidad de 1Mbps ampliable a 2Mbps. En la revisión del estándar, la 802.11b, esta velocidad también ha aumentado a 11Mbps.

1.6.2.3 La capa MAC

Diseñar un protocolo de acceso al medio, para las redes inalámbricas es mucho más complejo que hacerlo para redes cableadas. Ya que deben de tenerse en cuenta las dos topologías de una red inalámbrica:

- **Ad-hoc:** redes peer-to-peer. Varios equipos forman una red de intercambio de información sin necesidad de elementos auxiliares. Este tipo de redes se utilizan en grupos de trabajo, reuniones, conferencias...
- **Basadas en infraestructura:** La red inalámbrica se crea como una extensión a la red existente basada en cable. Los elementos inalámbricos se conectan a la red cableada por medio de un punto de acceso o un PC Bridge, siendo estos los que controlan el tráfico entre las estaciones inalámbricas y las transmisiones entre la red inalámbrica y la red cableada.

Además de los dos tipos de topología diferentes se tiene que tener en cuenta:

- Perturbaciones ambientales (interferencias)
- Variaciones en la potencia de la señal
- Conexiones y desconexiones repentinas en la red
- Roaming. Nodos móviles que van pasando de celda en celda.

A pesar de todo ello la norma IEEE 802.11 define una única capa MAC (divida en dos subcapas) para todas las redes físicas. Ayudando a la fabricación en serie de chips.

1.7 Seguridad Inalámbrica [8]

La utilización del aire como medio de transmisión de información mediante la propagación de ondas electromagnéticas deja al descubierto nuevos riesgos de seguridad. Si estas ondas de radio salen del recinto donde está instalada la red inalámbrica, nuestros datos quedarán expuestos ante cualquier persona que pase caminando. De esta forma estos posibles intrusos tendrían acceso a nuestra información privada con solo poseer una notebook, netbook o tal vez algún teléfono celular con conexión Wi-Fi (SmartPhone).

También es posible crear interferencias y una posible caída o denegación del servicio con solo introducir un dispositivo que emita ondas de radio en la misma frecuencia de trabajo de nuestra red (en general 2.4 GHz).

En caso de tener una red donde no se utilice el punto de acceso (como es el caso de las redes ad hoc), la posibilidad de comunicación entre clientes inalámbricos permitiría al intruso atacar directamente a un usuario de la red. Así se podrá tener problemas si el cliente ofrece servicios o comparte archivos en la red. Algo muy utilizado también es la posibilidad de duplicar las direcciones IP o MAC de clientes legítimos de la red.

No se puede definir la palabra seguridad sin tener en cuenta el ámbito en el que se está manejando. Esta palabra abarca un amplio rango de campos dentro y fuera del ámbito de la informática o computación.

Se puede hablar de seguridad cuando describimos las medidas de seguridad en una ruta o cuando decimos que un nuevo sistema operativo que vamos a utilizar en nuestras computadoras es seguro contra virus.

En realidad se desarrollaron varias disciplinas para abordar cada uno de los aspectos de la seguridad. De esta forma se trata la seguridad inalámbrica ubicándola en el contexto de la seguridad de la información. Entonces, cuando se habla de seguridad inalámbrica se hace referencia a la seguridad de la información en redes inalámbricas.

1.7.1 Seguridad de la información

Se dice que la seguridad de la información abarca todas aquellas medidas preventivas y reactivas del hombre, de las organizaciones y de los sistemas tecnológicos que permiten proteger la información. Se busca mantener tres aspectos básicos, que son la confidencialidad, la disponibilidad y la integridad de la información.
Es común confundir el concepto de seguridad de la información con el de seguridad informática. Este último solamente se encarga de la seguridad en el medio informático, por medio de estándares.

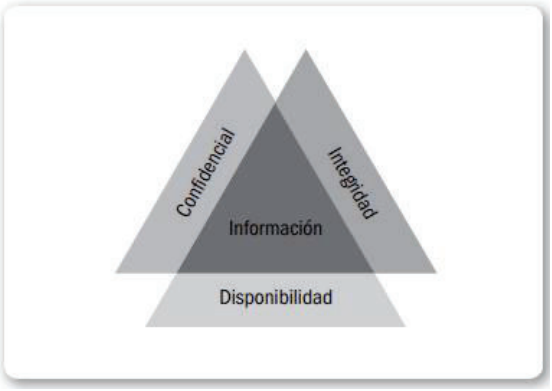


Figura 1.8: Aspectos básicos de la seguridad de la información [8]

El manejo de la seguridad de la información se basa en la tecnología. En el ámbito de una empresa, proteger la información es indispensable para obtener ventajas y poder sobre otras personas o empresas. A la información se la conoce como:

- **Crítica:** es indispensable para la operación de la empresa.
- **Valiosa:** es un activo de la empresa con alto valor.
- **Sensitiva:** debe ser conocida por las personas autorizadas.

Existen dos palabras importantes en la seguridad informática que son:

- **Riesgo:** es todo tipo de vulnerabilidades o amenazas que pueden ocurrir sin previo aviso y provocar pérdidas en la empresa.
- **Seguridad:** es una forma de protección contra los riesgos.

Los términos seguridad de la información, seguridad informática y garantía de la información son usados con frecuencia como sinónimos y aunque su significado no es el mismo, todos tienen una misma finalidad al proteger la confidencialidad, la integridad y la disponibilidad de la información.
Entre estos términos existen algunas diferencias sutiles que radican principalmente en el enfoque, las metodologías utilizadas y las zonas de aplicación. La seguridad de la información se refiere a la confidencialidad, integridad y disponibilidad de la información y datos, independientemente de la forma que los datos puedan tener (por ejemplo, medios impresos, electrónicos, audio u otras formas).

Se involucra también la implementación de estrategias que cubran los procesos en donde la información es el activo principal. Las estrategias deben establecer políticas, controles de seguridad, tecnologías y procedimientos para detectar amenazas que puedan explotar vulnerabilidades y que pongan en riesgo la información.

La seguridad es un proceso continuo de mejora por lo que las políticas y controles establecidos para la protección deberán revisarse y adecuarse ante los nuevos riesgos que aparezcan. De esta forma se deben reducir y en el mejor de los casos eliminar por completo.

De manera sintética se dice que la gestión de la seguridad de la información busca establecer y mantener programas, controles y políticas, que tengan como finalidad conservar la confidencialidad, integridad y disponibilidad de la información. Si alguna de estas características falla nuestro sistema correrá serios riesgos en su seguridad.

1.7.1.1 Confidencialidad

La confidencialidad es la propiedad de asegurar que la información no sea divulgada a personas, procesos o dispositivos no autorizados.

1.7.1.2 Autenticación

Es una medida de seguridad diseñada para establecer la validez de una transmisión, mensaje o remitente. También se puede considerar que es un medio para verificar la autorización de un individuo para recibir categorías específicas de información.

1.7.1.3 Integridad

Dado que es necesario proteger la información contra la modificación no permitida del dueño, se implementan características para conservar la integridad de la información. Así, se mantienen los datos libres de modificaciones no autorizadas.

1.7.1.4 Disponibilidad

La disponibilidad es la característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean procesos, personas o aplicaciones.

El acceso oportuno y confiable a datos y servicios de información para usuarios que tengan acceso autorizado. Tener sistemas que estén disponibles en todo momento y evitar interrupciones del servicio debido a cortes de energía, fallas de hardware y actualizaciones del sistema nos garantizan alta disponibilidad de la red. Garantizar la disponibilidad implica también la prevención de ataques a la red inalámbrica como el tan famoso ataque de denegación de servicio (DoS).

1.7.1.5 No repudio

El no repudio (non-repudiation) evita que el emisor o el receptor nieguen la transmisión de un mensaje. Con esta expresión se hace referencia a la capacidad de afirmar la autoría de un mensaje o información, evitando que el autor niegue la existencia de su recepción o creación. Por ejemplo, cuando se envía un mensaje, el receptor puede comprobar que efectivamente el supuesto emisor envió el mensaje.

De la misma forma, cuando se recibe un mensaje, el emisor puede verificar que el supuesto receptor recibió la información. Así, se puede probar la participación de las partes en una comunicación.

1.7.2 Seguridad de la información WLAN

El concepto de seguridad de sistemas de información lo definimos como la protección de los sistemas de información contra el acceso no autorizado o la modificación de la información.

El medio donde almacenan los datos, etapa de procesamiento o tránsito. Además, la protección contra la negación de servicio a los usuarios autorizados o la provisión de servicio a usuarios no autorizados. Por último se incluyen las medidas necesarias para detectar, documentar y contabilizar esas amenazas.

La seguridad inalámbrica es presentada desde el punto de vista de la seguridad de los sistemas de información. Teniendo en mente los cinco atributos de seguridad se podrá implementar y diseñar redes seguras.

1.7.2.1 Atributos de seguridad

El modelo de referencia OSI es una descripción abstracta para el diseño de protocolos de redes de computadoras. Este modelo divide las diferentes funciones de comunicación en siete capas que pueden funcionar de manera independiente una de otra.

Estas capas están apiladas e implican que cada capa usa únicamente la funcionalidad de la capa inferior y provee funcionalidad exclusiva a la capa inmediata superior.

Si se considera la confidencialidad del tráfico de los datos entre dos puntos de acceso, se logrará resultados similares (proteger la información enviada) actuando en tres capas diferentes del modelo OSI:

- La capa de aplicación
- La capa IP
- La capa de enlace (cifrado o encriptado de datos)

Al examinar los mecanismos de seguridad en las capas 1 y 2. Otros mecanismos de seguridad de nivel 3 y superiores son parte de la seguridad implementada en las capas de red o aplicación.

Por lo tanto el cifrado en el nivel de enlace es básicamente el proceso de asegurar los datos cuando son transmitidos entre dos nodos de una red instalada sobre el mismo enlace físico (también podemos considerar el caso de dos enlaces diferentes mediante un repetidor, por ejemplo, un satélite).

Con este cifrado a nivel de enlace, cualquier otro protocolo o aplicación de datos que se ejecute sobre el mismo enlace físico queda protegido de intercepciones.

El proceso requiere una clave secreta compartida entre las partes y un algoritmo previamente acordado. En caso de que el transmisor y el receptor no compartan el medio de transporte, la información debe ser descifrada y cifrada nuevamente en cada uno de los nodos en su camino al receptor. El cifrado en este nivel de enlace se usa en caso de que no se aplique un protocolo de mayor nivel.
En el estándar IEEE 802.11, el algoritmo de cifrado más conocido es el llamado Privacidad Equivalente a Cableado o WEP (Wired Equivalent Privacy). Desde hace mucho tiempo está probado que WEP es inseguro, hoy en día existen otras alternativas como el protocolo WPA.

1.7.2.2 Confidencialidad en WLAN

La confidencialidad en redes inalámbricas es asegurar que la información transmitida entre los puntos de acceso y los clientes no sea revelada a personas no autorizadas.

El objetivo es garantizar que la comunicación entre un grupo de puntos de acceso o bien entre un punto de acceso y un cliente esté protegida contra intercepciones.

WEP (Wired Equivalent Privacy) y **WPA** (WiFi Protected Access) son los estándares usados por la mayoría de los dispositivos inalámbricos. Analizando estos dos estándares, WPA es muy superior en todos los aspectos y se debe usar siempre que sea posible.

1.7.2.2.1 Cifrado WEP

El cifrado WEP fue parte del estándar IEEE 802.11del año 1999. Su propósito era darles a las redes inalámbricas un nivel de seguridad comparable al de las redes cableadas tradicionales. La necesidad de un protocolo como WEP fue obvia, ya que las redes inalámbricas utilizan ondas de radio y son más susceptibles a ser interceptadas.

La vida de WEP fue demasiado corta: un diseño malo y poco transparente desencadenó ataques muy efectivos a su implantación. Algunos meses después de que WEP fuera publicado, se consideró este protocolo como obsoleto.

1.7.2.2.2 Cifrado WPA

WPA (Acceso Protegido WiFi) es un sistema para proteger las redes inalámbricas, creado para corregir las deficiencias del sistema previo WEP.

Luego de WEP, en el año 2003, se propone WPA como una medida intermedia para ocupar el lugar de aquel, y más tarde se certifica como parte del estándar IEEE 802.11i. Esto se realiza con el nombre de WPA2en el año 2004.

WPA y WPA2 son protocolos diseñados para trabajar con y sin servidor de manejo de claves. WPA fue diseñado para utilizar un servidor de claves o autentificación (normalmente, un servidor RADIUS), que distribuye claves diferentes a cada usuario. Sin embargo, también se puede utilizar en un modo menos seguro de clave previamente compartida o PSK (Pre-Shared Key). Esto se destina para usuarios hogareños o de pequeña oficina. El modo PSK se conoce como WPA o WPA2-Personal.Cuando se emplea un servidor de claves, a WPA2 se lo conoce como WPA2-Corporativo(o WPA2-Enterprise). La información es cifrada utilizando el algoritmo RC4 (esto es debido a que WPA no elimina el proceso de cifrado WEP, solo lo fortalece), con una clave de 128 bits. Una de las mejoras sobre WEP es la implementación del Protocolo de Integridad de Clave Temporal o TKIP (Temporal Key Integrit Protocol). Este protocolo cambia claves dinámicamente a medida que el sistema es utilizado por el usuario.

Adicionalmente a la autenticación y cifrado, WPA también mejora la integridad de la información cifrada. La comprobación de redundancia cíclica o CRC (Cyclic Redundancy Check) utilizada en WEP es insegura, dado que se puede alterar la información CRC del mensaje sin conocer la clave WEP.
En cambio, WPA implementa un código de integridad del mensaje MIC (Message Integrity Code) también conocido como Michael. Sumado a esto, WPA incluye protección contra ataques de repetición (Replay Attacks).

Al incrementar el tamaño de las claves, el número de claves en uso y al agregar un sistema de verificación de mensajes, WPA hace que el ingreso no autorizado a redes inalámbricas sea mucho más difícil.

- **WPA-RADIUS**

RADIUS (acrónimo en inglés de Remote Access Dial-In User Server) es un protocolo de autenticación, autorización y administración (AAA) para aplicaciones de acceso a la red o Movilidad IP.

Un ejemplo común de uso de este tipo de servicio es cuando se realizan conexiones a un ISP con un módem DSL, cable módem, Ethernet o Wi-Fi. En este caso se envía información (que generalmente es un nombre de usuario y contraseña) que luego llegará hasta un servidor de RADIUS sobre el protocolo RADIUS. Ahí se comprueba que la información es correcta. Si es aceptado, el servidor autoriza el acceso al sistema del ISP y le asigna los recursos de red como una dirección IP, y otros parámetros para que podamos navegar sin problemas. Con este tipo de servicio estamos permitiendo que las organizaciones centralicen su autentificación, autorización y administración.

- **WPA-PSK (Pre Shared Key)**

Destinado para entornos en los que no hay disponible un servidor de autentificación y en los cuales no es necesario llegar al mismo nivel de seguridad que los usados en las comunicaciones corporativas. Este modo de uso está destinado para hogares, oficinas pequeñas o en lugares donde la seguridad no es un tema demasiado importante.

El principio de funcionamiento de este sistema se basa en una clave compartida por todos los dispositivos involucrados en la comunicación (por ejemplo, clientes inalámbricos y AP) llamada Pre-shared key, password o master key. La gestión de esta clave es manual en todos los equipos, no hay un mecanismo estándar para modificar esta clave secreta compartida.

1.7.2.2.3 Modos de funcionamiento WPA2

El protocolo WPA2 está basado en el estándar 802.11i. WPA. Por ser una versión previa, que se podría considerar de migración, no incluye todas las características del IEEE 802.11i. Así, se puede decir que WPA2 es la versión certificada del estándar 802.11i. La Alianza Wi-Fi llama a la versión de clave precompartida WPA-Personaly WPA2-Personal, y a la versión con autenticación RADIUS (también la podemos encontrar como autenticación 802.1x/EAP), como WPA-Enterprisey WPA2-Enterprise.

Los fabricantes manufacturan productos basados en el protocolo WPA2 que utiliza el algoritmo de cifrado AES. Con este algoritmo es posible cumplir con los requerimientos de seguridad impuestos por algunos gobiernos.

1.7.2.3 Autentificación en redes inalámbricas

En las redes inalámbricas la autenticación es la medida diseñada para establecer la validez de una transmisión entre puntos de acceso de la red y/o clientes inalámbricos. Dicho de otra forma, la autenticación inalámbrica significa tener el derecho a enviar hacia y mediante el punto de acceso.

Para facilitar la comprensión del concepto de autenticación en redes inalámbricas, a continuación se explica qué es lo que sucede en el inicio de la sesión de comunicación entre un AP y un cliente inalámbrico. El inicio de una comunicación empieza por un proceso llamado asociación.

Existen dos mecanismos de asociación que fueron agregados al estándar IEEE 802.11b al momento de diseñarlo:

1.7.2.3.1 Autentificación abierta

Significa no tener seguridad, entonces cualquier cliente inalámbrico puede hablarle al punto de acceso sin necesidad de identificarse durante el proceso.

De esta forma, cualquier cliente, independientemente de su clave WEP, puede verificarse en el punto de acceso y luego intentar conectarse (esto es, por ejemplo, ingresando la contraseña cuando se solicita identificarse a la red).

1.7.2.3.2 Autentificación de llave compartida

Se comparte una contraseña entre el punto de acceso y el cliente de la red inalámbrica. Un mecanismo de **confirmación/denegación** le permite al punto de acceso verificar que el cliente conoce la llave compartida y entonces le concede el acceso.

La autenticación con llave compartida implementada en el protocolo WEP también es obsoleta. Existen varios ataques de tipo texto plano versus texto cifrado con los cuales se puede vulnerar la autenticación basada en WEP. Esto es porque la llave de cifrado y autentificación son el mismo secreto compartido, entonces una vez que una resulta comprometida, la otra también.

1.7.2.3.3 Red cerrada o CNAC

Es una variación de la autentificación abierta, desarrollada por Lucent Technologiesen el año 2000. Las redes cerradas se diferencian del estándar 802.11b en que el punto de acceso no difunde periódicamente las llamadas **Tramas Baliza** (Beacom Frames). De esta forma se evita la publicación de la SSID.

Esto implica que los clientes de la red inalámbrica necesitarán saber de manera previa qué SSID deben asociar con un punto de acceso. Esto fue considerado por muchos fabricantes de equipo como una mejora de seguridad.

Mientras detener la difusión del SSID previene a los clientes de enterarse del SSID por medio de una trama baliza, nada asegura que otro cliente con un programa de intercepción (Wi-Fi Inspector, por ejemplo) detecte la asociación que provenga de otro punto de la red cuando esto oportunamente ocurra.

1.7.2.3.4 Filtrar direcciones MAC

Conocido como Filtrado por MAC o Lista de control de acceso ACL (Access Control List), es un método mediante el cual solo se permite unirse a la red a aquellas direcciones físicas (MAC) que estén dadas de alta en una lista de direcciones permitidas. Este filtrado permite hacer una lista de equipos que tienen acceso al AP, o bien denegar ciertas direcciones MAC.

Se ha convertido en una práctica común usar la dirección MAC de la interfaz inalámbrica como un mecanismo de seguridad.

Existen dos realidades: una para el usuario común con pocos conocimientos, que piensa que las direcciones MAC son únicas y no pueden ser modificadas por cualquiera; debemos saber que la otra realidad más fuerte es que las direcciones MAC en casi cualquier red inalámbrica pueden ser fácilmente modificadas o clonadas por usuarios que posean un nivel de conocimientos algo avanzado, de modo de obtener una MAC de una entrada válida en el punto de acceso.

1.7.2.3.5 Portal Cautivo

Es un software o hardware en una red que tiene como objetivo vigilar el tráfico HTTP (protocolo usado en Internet). Además, obliga a los usuarios de la red a pasar por una página web especial si es que quieren navegar por Internet.

En una red donde la autenticación se realiza mediante este sistema, a los clientes se les permite asociarse a un punto de acceso (sin autenticación inalámbrica) y obtener una dirección IP con DHCP (no hace falta autenticación para obtener esta dirección). Cuando el cliente tiene la IP, todas las solicitudes HTTP se capturan y se envían al portal cautivo. Así, el cliente es forzado a identificarse en una página web. Los portales cautivos son responsables de verificar la validez de la contraseña y luego modificar el acceso del cliente.

1.7.2.4 Integridad de datos en WLAN

Si un protocolo inalámbrico puede asegurar que la información transmitida no ha sido alterada por personas no autorizadas, entonces el protocolo cumple con la integridad de datos.

En los primeros años, WEP intentaba cumplir con esta premisa. Desafortunadamente, el mecanismo de integridad implementado llamado CRC (Código de redundancia cíclica) resultó inseguro. Utilizar un mecanismo inseguro permite que el tráfico de información sea alterado sin que se note nada.

Luego, los protocolos WPA y WPA2 resolvieron el problema de la integridad de datos que poseía WEP agregando un mensaje de código de autenticación más seguro. Además de un contador de segmentos, que previene los ataques por repetición (replay attack o también llamados ataques de reinyección).

En estos **ataques de repetición**, el atacante registra la conversación entre un cliente y el AP para así obtener un acceso no autorizado. La información capturada por el atacante es luego reenviada con el objetivo de falsificar la identidad del usuario que posee acceso a la red.

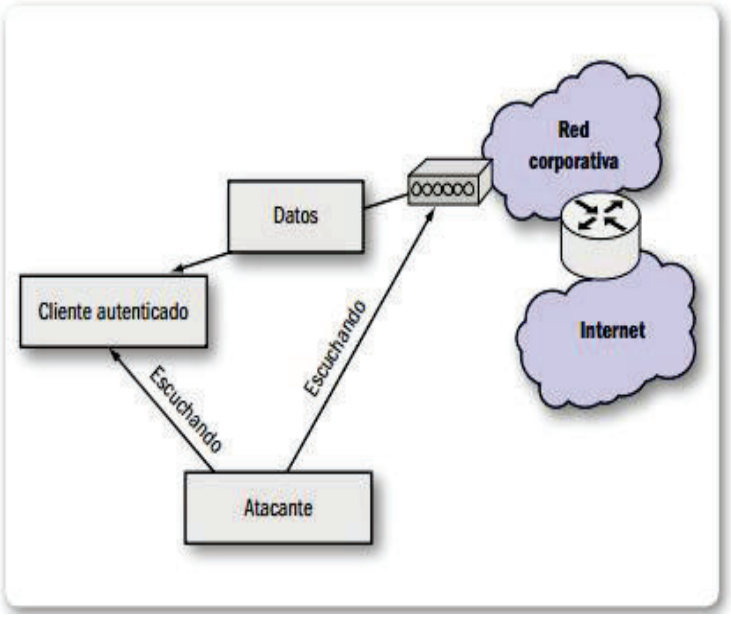


Figura 1.9: Ataque de repetición [8]

La integridad de datos mediante WEP es obsoleta. Hay que recordar que implementar WPA o WPA2 permite lograr integridad de datos en una red inalámbrica.

MODO/CIFRADO		**WPA**	**WPA2**
Modo corporativo	**Autentificación**	IEE802.1X/EAP	IEE802.1X/EAP
	Cifrado	TKIP/MIC	AES/CCMP
Modo Personal	**Autentificación**	PSK	PSK
	Cifrado	TKIP/MIC	AES/CCMP

Tabla 1.5: Autentificación y cifrado WPA y WPA2 [8]

1.7.2.5 Disponibilidad en WLAN

Tener una red donde se asegure un acceso confiable a servicios de datos e información para usuarios que están autorizados es poseer disponibilidad en la red. Se debe considerar que las redes inalámbricas trabajan en canales predefinidos, que cualquiera puede usar para enviar información. No es simple detener a alguien que busca interferir con su señal de radio nuestra red. Lo único que se hace es monitorear cuidadosamente la red para identificar fuentes potenciales de interferencia (por ejemplo, una red de un vecino que opera en el mismo canal que nosotros).

La negación de servicio mediante interferencia de radio es algo común en redes inalámbricas. Por ejemplo, considerar si un vecino, además de tener su red configurada en el mismo canal que la nuestra, decide usar el mismo SSID.

Para evitar esta clase de ataques, intencionales o no, se realizará un rastreo diario de frecuencias de radio. Para evitar interferencias con otras redes, no se debe usar demasiada potencia en el punto de acceso.

Otras razones por las cuales nuestra red se puede desempeñar de manera deficiente o no estar disponible son los clientes con virus, programas de intercambio de archivos (P2P), SPAM, etc.

Todo esto puede inundar nuestra red con tráfico y dejar menos ancho de banda disponible para los usuarios. La disponibilidad en redes inalámbricas necesita de buenas prácticas de monitoreo.

1.7.2.6 No repudio en redes inalámbricas

Los protocolos inalámbricos existentes carecen de un mecanismo para asegurar que el emisor de la información tenga una prueba de envío de esta y que el receptor obtenga una prueba de la identidad del emisor. Los estándares 802.11 no se hacen responsables de la rendición de cuentas en el tráfico de datos. Esta rendición de cuentas debe ser implementada por protocolos de capas superiores en el modelo OSI.

2 IMPLEMENTACIÓN DE LA RED DE CÁMARAS DE SEGURIDAD WI-FI

2.1 Introducción

En este capítulo se detallará el estudio, diseño e instalación de la red de cámaras de seguridad inalámbricas para la Unidad Educativa Salesiana "Domingo Savio", se empezará mostrando la situación geográfica de la institución, los lugares donde se instalarán las cámaras de seguridad, el proceso de instalación, configuración y la forma de almacenamiento de los datos obtenidos del circuito de cámaras.

2.2 Antecedentes

La Unidad Educativa Salesiana "Domingo Savio", es una institución de renombre en el norte de la provincia de Pichincha, está dedicada a fomentar el desarrollo académico y de valores en la juventud Cayambeña y Pedro Moncayense, posee una infraestructura de primer nivel, laboratorios y equipos de alta tecnología que ayudan a fortalecer la propuesta educativa para sus destinatarios. Por este motivo, y por la cantidad de personas que acuden diariamente a sus instalaciones, es conveniente colocar un tipo de sistema de videovigilacia para salvaguardar sus bienes humanos y materiales de posibles delitos.

La Unidad Educativa Salesiana "Domingo Savio" pertenece a un ente superior como es la Comunidad Salesiana Cayambe-Ibarra, una de sus obras es la Casa Campesina Cayambe que brinda financiamiento en las zonas rurales del cantón Cayambe, por lo que maneja diariamente cantidades importantes de dinero. Por este motivo el sistema de videovigilacia propuesto en el presente proyecto de tesis, no solo se centrará en la Unidad Educativa Salesiana "Domingo Savio" sino también en la Casa Campesina Cayambe, puesto que las instalaciones de las dos instituciones funcionan en el mismo edificio.

2.3 Ubicación geográfica de la institución

La Unidad Educativa Salesiana "Domingo Savio" se encuentra ubicada en la ciudad de Cayambe, en la provincia de Pichincha y como se puede observar en la figura 2.1 la Casa Campesina Cayambe se encuentra dentro de la institución educativa.

Figura 2.1. Ubicación de la Unidad Educativa Salesiana "Domingo Savio"

2.4 Requerimientos para la ubicación de las cámaras

Como se puede observar en la figura 2.1 la Unidad Educativa Salesiana "Domingo Savio" cuenta con una infraestructura amplia, es por este motivo que se solicita la colaboración de las autoridades institucionales para generar requerimientos mínimos en la implementación del sistema los mismos que se detallan a continuación:

- La ubicación de las cámaras se la realizará en la zona administrativa y de laboratorios de la institución.
- Las cámaras deberán estar ubicadas en puntos estratégicos que permitan generar una herramienta de supervisión y control.
- Las cámaras deberán tener acceso web (desde una computadora, celular, tablet, etc.)
- Las cámaras deben tener sensor de movimiento.
- Las cámaras deben ser WiFi y soportar el estándar IEEE 802.11
- Las cámaras deben poseer led infrarrojos que permitan las grabaciones sin luz.
- Las cámaras deben tener capacidad de escalabilidad.

- Mediante el software de gestión se podrá tener acceso a las grabaciones almacenadas.
- Se garantizará la confiabilidad y seguridad en el sistema.

Considerando los requerimientos ya establecidos, las autoridades manifiestan que no es necesaria la ubicación de las cámaras en la zona de laboratorios como se había determinado inicialmente, solicitan que las cámaras se ubiquen en la Casa Campesina, institución que brinda servicios de financiamiento a las comunidades rurales del Cantón Cayambe, puesto que es un punto de mayor interés para las necesidades institucionales.

Luego de acatar esta solicitud y con el visto bueno de las autoridades se han designado las siguientes zonas para ubicar las cámaras:

- ZONA 1: Entrada Principal de la Institución
- ZONA 2: Oficinas de la Casa Campesina Cayambe
- ZONA 3: Oficinas Administrativas de la Unidad Educativa Salesiana "Domingo Savio"

A continuación se detalla de mejor manera cada una de las zonas:

2.4.1 Zona 1. Entrada Principal de la Institución

Permite cubrir la puerta de entrada a la institución, entrada al parqueadero, entrada a las oficinas de la Unidad Educativa Salesiana "Domingo Savio" y de la Casa Campesina Cayambe.

2.4.2 Zona 2. Oficinas de la Casa Campesina Cayambe

Permite cubrir el hall de la Casa Campesina, cajeros, pasillos y oficinas.

2.4.3 Zona 3. Oficinas Administrativas de la Unidad Educativa "Domingo Savio"

Permite cubrir el hall de secretaría, inspección general, departamento médico, archivo y colecturía.

2.4.4 Selección de los puntos idóneos para ubicar las cámaras

Como se ha mencionado en la sección anterior las zonas seleccionadas son las de más concurrencia a la Unidad Educativa Salesiana "Domingo Savio" y la Casa Campesina Cayambe, lo cual permite cumplir uno de los requerimientos planteados en la sección 4.1.

Para que las cámaras se conviertan en una herramienta de supervisión y control deben ubicarse de forma adecuada en cada una de las tres zonas antes designadas, en las figuras 2.2, 2.3 y 2.4 se muestra como se realizó esta selección.

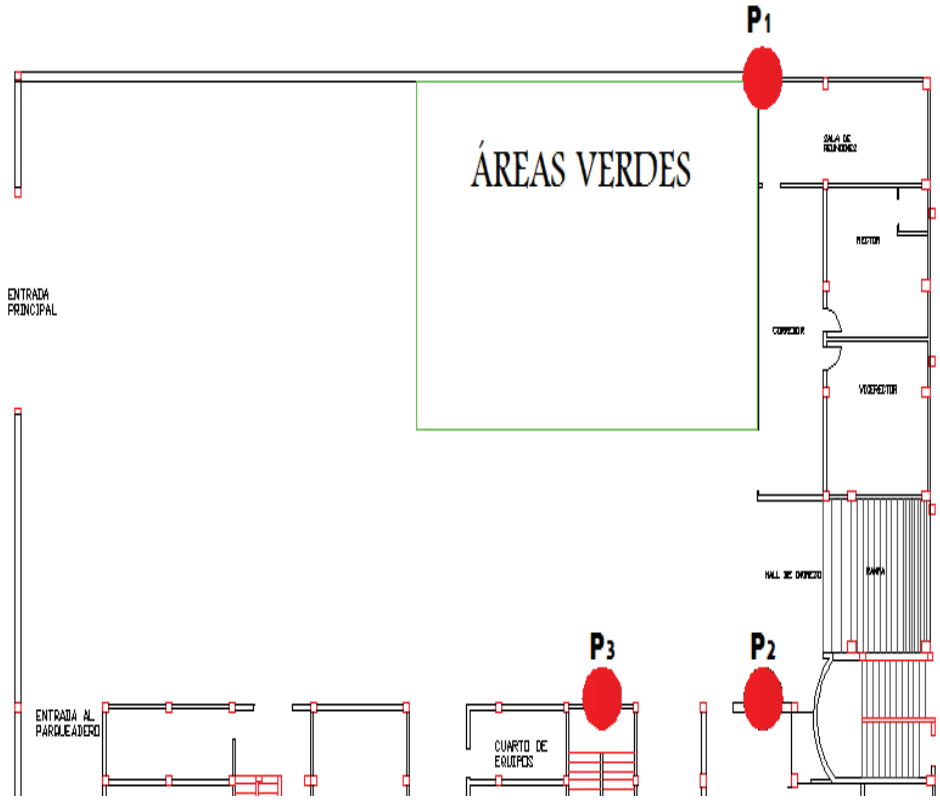


Figura 2.2. Posibles puntos para ubicar la cámara en la zona 1

Considerando que el objetivo de ubicar una cámara en la entrada principal de la institución es visualizar quien ingresa a la Unidad Educativa Salesiana "Domingo Savio", a la Casa Campesina Cayambe y controlar el uso de los vehículos de la Comunidad Salesiana, los posibles puntos deben estar en dirección hacia el portón principal, es por esto que se ha considerado tres posibles puntos como se observa en la figura 2.2.

Se descarta el punto P1 puesto que las áreas verdes obstaculizan la visualización, el punto P2 también se descarta puesto que el alcance de visualización puede generar inconvenientes.

El punto P3 es el seleccionado, ya que permite cubrir todas las zonas de interés con una buena visualización (entrada institucional, entrada parqueaderos, entrada a la Casa Campesina Cayambe y a las zonas administrativas de la UESDS).

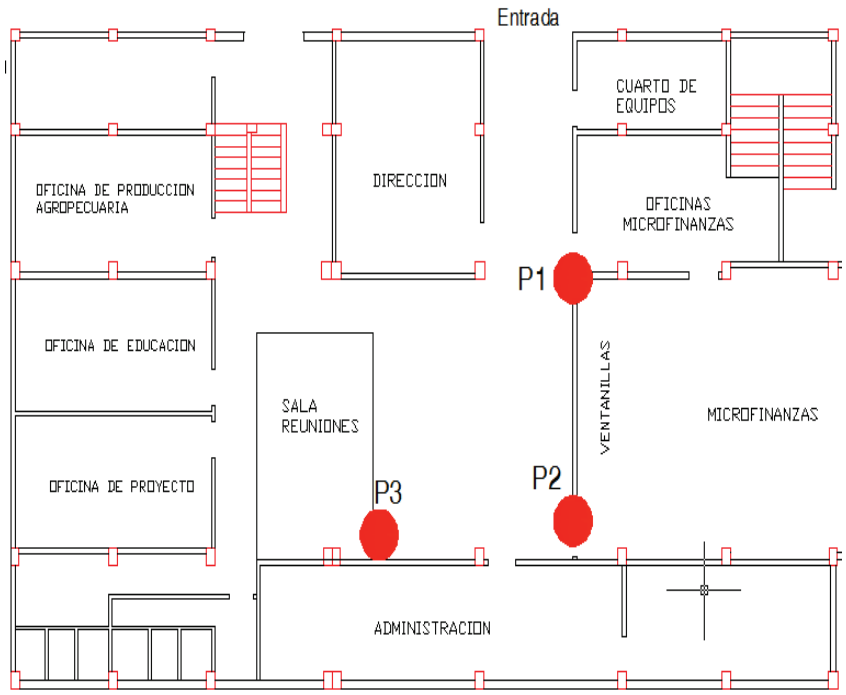


Figura 2.3. Posibles puntos para ubicar la cámara en la zona 2

El objetivo de ubicar la cámara en el hall de la Casa Campesina Cayambe es generar una herramienta de prevención para todos los beneficiarios de esta obra, es así que los lugares donde se ubicarán las cámaras deben cubrir la entrada principal y las ventanillas de los cajeros, considerando esto, se han designado tres puntos los cuales se visualizan en la figura 2.3.

El punto P1 se descarta puesto que solo cubre la entrada a la Casa Campesina, el punto P3 no se considera puesto que no cubre de forma adecuada la entrada.

El punto P2 es el punto idóneo para la ubicación de la cámara, puesto que cubre la entrada de la Casa Campesina y las ventanillas de los cajeros.

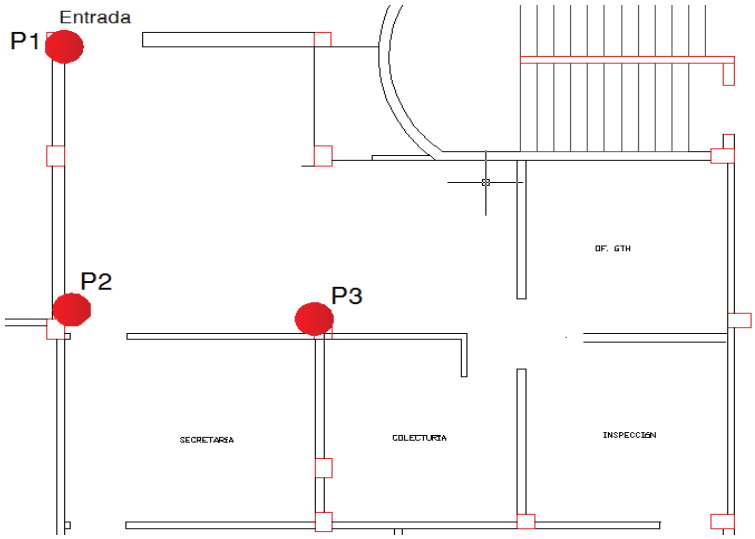


Figura 2.4. Posibles puntos para ubicar la cámara en la zona 3

El objetivo de ubicar la cámara en la zona 3 es monitorear la entrada al área administrativa de la Unidad Educativa Salesiana "Domingo Savio", lo idóneo es cubrir la entrada a este sector, es por esto que se han designado tres posibles puntos donde se ubicará la cámara los cuales se visualizan en la figura 2.4.

El punto P1 se descarta puesto que no cubre de forma directa la entrada, el punto P2 a pesar de ser un punto idóneo se los descarta por no generar un visualización directa a la entrada, además que por ese sector hay una puerta de acceso docente la cual permanece cerrada pero también debe ser cubierta de forma directa.

Con lo que el punto P3 es el punto donde se ubicará la cámara, el mismo permite visualizar de forma directa la entrada principal y la puerta de acceso docente, además se puede visualizar de frente a los usuarios de este sector de la UESDS.

A pesar de que la zona de laboratorios no será cubierta se deja sentado el análisis para la ubicación de la cámara en este sector, en el caso de posibles expansiones de la red de cámaras de seguridad. En la figura 2.5 se puede evidenciar el análisis de los puntos para la ubicación de la cámara.

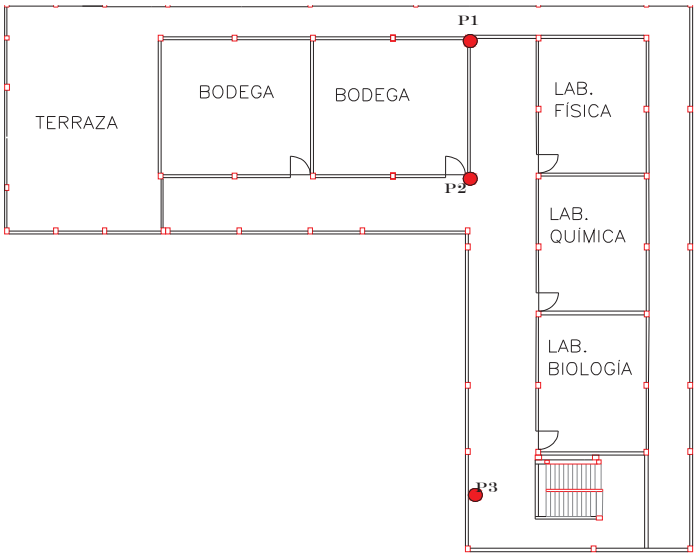


Figura 2.5. Posibles puntos para ubicar la cámara en la zona de laboratorios.

El objetivo de ubicar una cámara en la zona de laboratorios es crear una herramienta de prevención y control, por el alto valor económico que presentan los materiales y equipos que se encuentran en los laboratorios de física, química y biología, es por esto que se han propuesto tres posibles puntos para la ubicación de la cámara los mismos que se visualizan en la figura 2.5.

Cabe recalcar que los laboratorios se encuentran en la terraza del edificio principal de la institución y cuenta con accesos restringidos, los mismos que son administrados por los responsables de los laboratorios, así que el transitar por este sector es mínimo.

En consideración a los puntos de ubicación de la cámara, el punto P1 se descarta puesto que no se alcanza una buena visibilidad, el punto P3 cumbre nada más que la entrada sin evidenciar de forma directa las entradas a cada laboratorio, por lo que el punto P2 es el idóneo para la ubicación de la cámara.

2.5 Ubicación de las cámaras

En el siguiente plano se presentan las zonas y ubicaciones designadas para las cámaras, con el objetivo de conseguir una cobertura óptima de acuerdo a las necesidades de control antes detalladas.

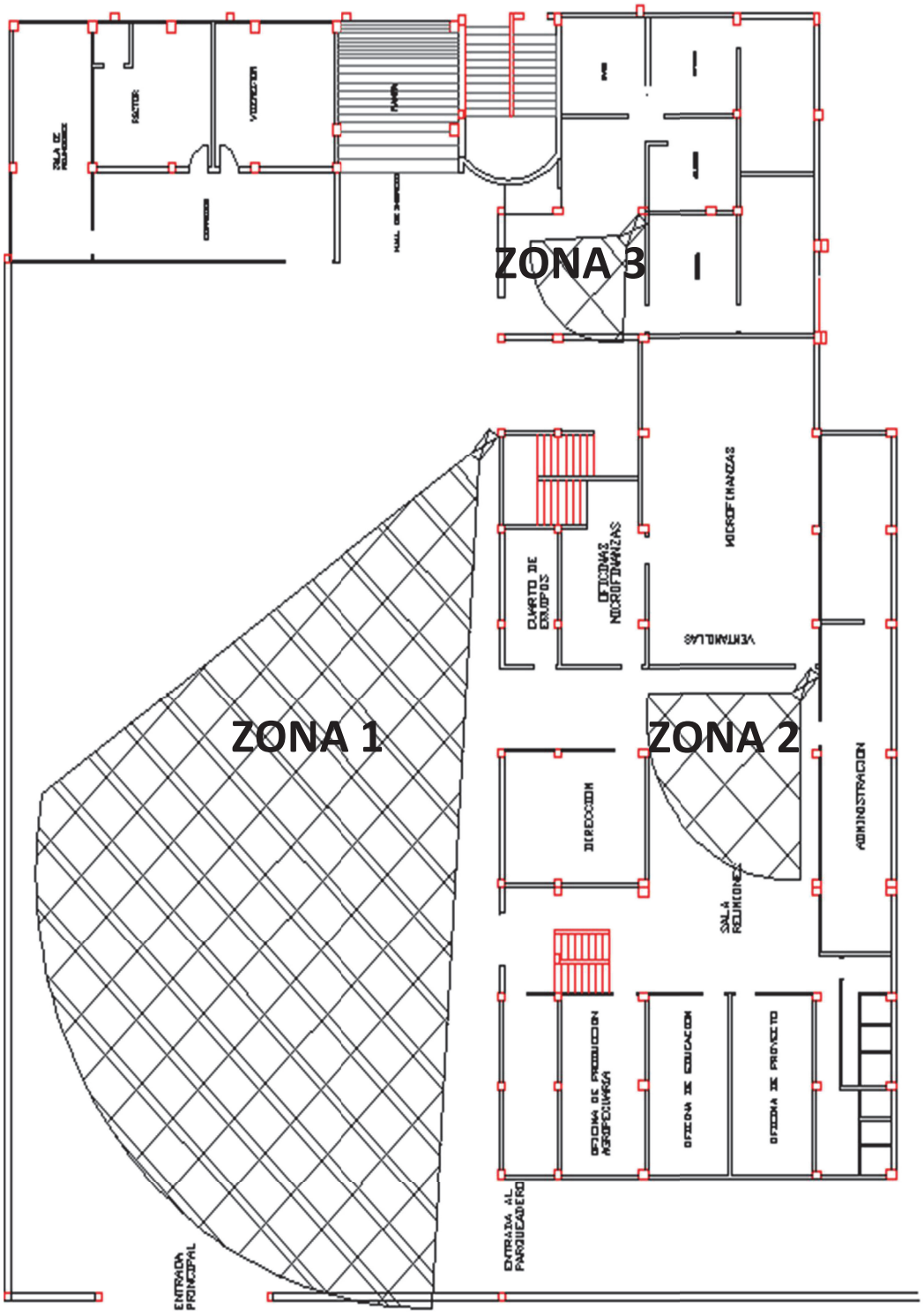


Figura 2.6. Plano donde se ubicarán las cámaras

2.6 Especificaciones de las cámaras por zona

Cada zona ya establecida, tiene diferentes necesidades a ser cubiertas en cuanto a la visualización de las cámaras, en la tabla 2.1 se da a conocer de forma general los requerimientos mínimos por cada zona, lo que permitirá tener una idea general de las características que debe tener cada cámara.

ZONA	REQUERIMIENTOS DE CÁMARA
ZONA 1	Exterior, visualización día/noche, largo alcance, ángulo de aproximadamente 90º , Wi-Fi, calidad de video medio-alto
ZONA 2	Interior, visualización día/noche, corto alcance, Wi-Fi, ángulo de aproximadamente 90º, calidad de video medio.
ZONA 3	Interior, visualización día/noche, corto alcance, Wi-Fi, ángulo de aproximadamente 90º, calidad de video medio.

Tabla 2.1 Requerimientos de cámaras por zona

2.7 Selección de equipos

Antes de realizar la compra de estos equipos se ha investigado distintas cámaras en internet y la variedad es inmensa, además la adquisición de las cámaras se debe realizar mediante el análisis de distintas proformas y en locales que emitan factura, puesto que la institución debe justificar estos gastos en su contabilidad.

En un sistema de video vigilancia las cámaras son la parte medular y la oferta que da el mercado es abrumadora desde las más básicas hasta ultra sofisticadas, al final la decisión para la selección de una cámara se fundamenta en que cumpla con los requisitos mínimos preestablecidos y la capacidad adquisitiva de quienes necesitan el servicio, esto último puede marcar una gran diferencia en cuanto a prestaciones extras para el sistema.

Considerando lo expuesto anteriormente se han solicitado proformas de los siguientes almacenes:

- CyG Computer, Quito
- AD Consultands, Quito
- Pro System, Cayambe
- Easy Compu, Cayambe
- Grupo Maxi, Quito

Las cámaras presentadas por cada uno de los distribuidores cumplen en su mayoría con los requerimientos establecidos, por lo que la adquisición depende de las autoridades en la tabla 2.2 se plantea un resumen de las posibles cámaras a seleccionar:

POSIBLE CÁMARA	DISTRIBUIDOR	CUMPLE CON LAS CARACTERÍSTICAS	OBSERVACIÓN
Cámara **Polarid**	C&G Computer	Si	
Cámara Exterior **EasyN**	C&G Computer	Si	
CAMARA DLINK DCS-932A	Easy Compu	Si	La proforma no está bien elaborada.
CAMARA DLINK DCS-7010L	Easy Compu	Si	
ZKTeco ZKTP531	ID Consultants	Si	
Dericam H216W	ID Consultants	Si	
D-Link DCS-942L MM720DLN73	Pro-System	Si	
D-Link UNIDAD IMB-V13MPW	Pro- System	No	La cámara no es Wi-Fi
HIKVISION DS2CD2132I	Maxi Group	No	La cámara no es Wi-Fi
HIKVISION DS2CD2120FIW	Maxi Group	Si	

Tabla 2.2 Posibles marcas de cámaras a seleccionar[1]

[1] Revisar el anexo D (proformas presentadas por distribuidores)

En base a lo expuesto en las tablas 2.1 y 2.2, se puede evidenciar que la mayoría de cámaras que se han buscado y cotizado cumplen y por mucho con los requerimientos planteados para la implementación de las cámaras, por lo tanto la selección depende exclusivamente del presupuesto institucional disponible para la implementación de sistema, es por este motivo y con el visto bueno de las autoridades que se ha seleccionado a la empresa Id Consultants.

Las cámaras adquiridas son tres, dos interiores de iguales características y una exterior, las mismas se detallan a continuación:

2.7.1 ZKTeco ZKPT531[10]

Figura 2.7. Cámara Wi-Fi ZKTeco modelo ZKPT531[10]

La ZKPT531 es una cámara IP con movimiento remoto y compatible con NVR ONVIF, por lo que puede funcionar con diversos NVR del mercado. Compuesta por un sensor de imagen 1/4" CMOS color y con una extraordinaria resolución de 720P (1280x720). Formato de compresión de vídeo H.264 y tasa de transferencia de 25 FPS.

Óptica fija de 3.6 mm con un campo de visión diagonal de 90º. 8 Leds infrarrojos que se activan automáticamente, proporcionando así una imagen nítida a 0 Lux (oscuridad total) a una distancia máxima de 10 m. Dispone de filtro IR CUT automático que permite obtener durante el día una imagen con colores nítidos y reales.

Conexión a red por puerto Ethernet o Wifi. Audio bidireccional, con micrófono y altavoz incorporados. Dispone de 1 entrada y 1 salida de alarma. Movimiento Horizontal de 355º y Vertical de 120º, que permite mover la cámara remotamente.

Ranura para tarjeta MicroSD de hasta 32 GB, que permite guardar vídeos y capturas cuando la cámara detecte movimiento o reciba una alarma. Podrá acceder remotamente a la cámara a través de navegador, software para gestión de múltiples cámaras (disponible para Windows) y smartphone.[2]

2.7.2 Dericam H216W[3]

Figura 2.8. Dericam H216W[3]

La Dericam H216W es una cámara CMOS con las siguientes características:

- Compatibilidad ONVIF.
- Vigilancia de audio bidireccional.
- IR-LED de iluminación para visión nocturna (hasta 30 metros).
- Permite la visualización y la grabación de imágenes desde cualquier lugar y en cualquier momento.
- Soporta el navegador IE y la mayoría de los navegadores estándar.
- Conexión de red Wi-Fi compatible con los estándares IEEE 802.11b/g/n.
- Soporta encriptación WEP y WPA.
- Detección de movimiento con notificación por correo electrónico o envío de imágenes a través de FTP.
- Lente de 3.6 mm (Ángulo de 65 grados).
- Resistente al agua y polvo por lo que idónea para la instalación en exteriores[3]

[2] Revisar Anexo B
[3] Revisar Anexo C

2.8 Análisis de la red existente

La Unidad Educativa Salesiana "Domingo Savio" cuenta con una red interna ya existente. La cual se encarga de proveer servicios de internet, comunicación y manejo de datos (facturación, servicio web, sistemas de calificaciones) a todas las obras de la Comunidad Salesiana Cayambe.

La red brinda servicio de datos a las obras:

- UESDS (Pastoral, Edificio Nuevo)
- Casa Campesina Cayambe
- Universidad Politécnica Salesiana Sede Cayambe
- Fundación Tainate Huasi
- Maternidad Mitad del Mundo

Aproximadamente son unos 300 computadores a los que se brinda servicio de datos considerando que existen 4 laboratorios de informática, 2 salas de profesores, oficinas administrativas en cada una de las obras, 80 aulas y demás lugares donde es indispensable este servicio.

La Unidad Educativa Salesiana "Domingo Savio" ha contratado el servicio de TELCONET el cual ofrece servicio de internet mediante fibra óptica con ancho de banda de 10Mbps. Este proveedor brinda 14 direcciones IP públicas que van desde la **186.101.97.129** hasta la **186.101.97.142.**

La red se administra mediante cuatro servidores los cuales se detallan en la tabla 2.3.

SERVIDOR	SERVICIO
LINUX UBUNTU	Web (página web institucional) Plataforma MOODLE (Aulas virtuales)
WINDOWS SERVER 2003	Base Datos Alumnos Facturación de la Fundación Tainate Huasi
WINDOWS SERVER 2012	Facturación todas las obras (Maternidad,

	UESDS, Casa Campesina) Sistema de notas de alumnos
PFSENSE	Proxy

Tabla 2.3. Servidores de red de la UESDS

Los servidores antes detallados están ubicados en el cuarto frío del Data Center de comando marca APC, en el cual se encarga del almacenamiento, procesamiento y distribución de los datos de toda la red. La red se distribuye desde el cuarto frío (Cableado vertical) hacia ocho Racks, los mismos que se detallan en la tabla 2.4.

RACK	**MEDIO TX (Cableado Vertical)**	**Distribución Cableado Horizontal**
Casa Campesina	Cable UTP Cat. 7	Oficinas Casa Campesina y UESDS
Coordinación Básico	Cable UTP Cat. 7	Aulas y Puntos de red Docentes
Coordinación Bachillerato	Cable UTP Cat. 7	Aulas y Puntos de red Docentes
Laboratorio Informática	Cable UTP Cat. 7	Laboratorio 1 y 2
Pastoral	Antena	Oficinas de pastoral
Edificio Nuevo UESDS	Fibra Óptica	Aulas y Puntos de red Docentes
Universidad	Fibra Óptica	Aulas y Oficinas Universidad Salesiana, Laboratorios 3 y 4
Maternidad Mitad del Mundo	Fibra Óptica	Oficinas

Tabla 2.4. Detalle de distribución de la red

Para un correcto funcionamiento y manejo de la red, los administradores de la red han creado diferentes VLAN las mismas que se detallan en la tabla 2.5.

VLAN	DIRECCIÓN IP
WAN	186.101.97.134
PROFESORES	172.17.197.252
LABORATORIOS 1	172.17.196.252
CASA CAMPESINA	172.17.199.252
PASTORAL	172.17.201.252
V192	192.168.1.252
COMUNIDAD	172.17.202.252
LAB. UPS	172.17.203.252
MATERNIDAD	172.17.204.252
LABORATORIOS 2	172.17.205.252
MNG	172.17.192.252

Tabla2.5. VLAN que gestionan la red de la UESDS

En consideración al análisis expuesto, la red institucional debe ser segura ante vulnerabilidades o ataques, para garantizar esto, la red de cámaras de seguridad no debe pertenecer red institucional, por lo contrario se debe asignar una dirección IP pública independiente a la nueva red.

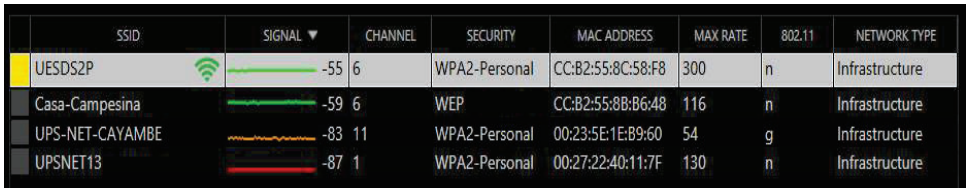
2.8.1 Escaneo de la señal Wi-Fi existente

El escaneo o también llamado Site Survey Pasivo, es un procedimiento que se lo realiza para analizar el lugar en el que se implementará la red inalámbrica. El estudio permite escanear todas las redes que están brindando cobertura en un determinado lugar, así como sus principales características: SSID, dirección MAC, canal, RSSI, tipo de red, seguridad, velocidad e intensidad de la señal. Los datos obtenidos de este estudio permiten configurar de una mejor manera la red a implementarse, con el objetivo de evitar en lo posibles interferencias y lograr un mejor rendimiento de la futura red.

Para realizar este estudio se utilizará el software **Inssider 3**, el cual es un software libre y fácil de usar que analiza y compara las redes inalámbricas existentes de una forma fácil, además brinda una herramienta gráfica que compara las intensidades de las distintas señales que existen en el lugar.

A continuación se presenta el informe generado por el Inssider 3 en cada una de las zonas designadas para la ubicación de las cámaras.

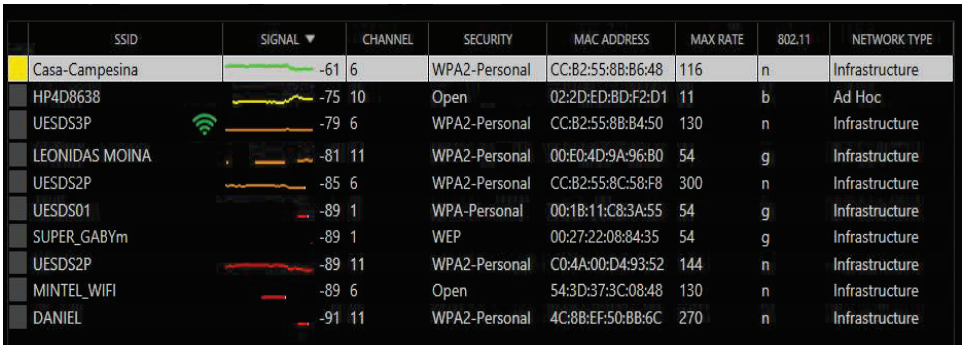
ZONA 1:



SSID	SIGNAL ▼	CHANNEL	SECURITY	MAC ADDRESS	MAX RATE	802.11	NETWORK TYPE
UESDS2P	-55	6	WPA2-Personal	CC:B2:55:8C:58:F8	300	n	Infrastructure
Casa-Campesina	-59	6	WEP	CC:B2:55:8B:B6:48	116	n	Infrastructure
UPS-NET-CAYAMBE	-83	11	WPA2-Personal	00:23:5E:1E:B9:60	54	g	Infrastructure
UPSNET13	-87	1	WPA2-Personal	00:27:22:40:11:7F	130	n	Infrastructure

Figura 2.9. Informe del Site Survey Pasivo para la ZONA 1

ZONA 2:



SSID	SIGNAL ▼	CHANNEL	SECURITY	MAC ADDRESS	MAX RATE	802.11	NETWORK TYPE
Casa-Campesina	-61	6	WPA2-Personal	CC:B2:55:8B:B6:48	116	n	Infrastructure
HP4D8638	-75	10	Open	02:2D:ED:BD:F2:D1	11	b	Ad Hoc
UESDS3P	-79	6	WPA2-Personal	CC:B2:55:8B:B4:50	130	n	Infrastructure
LEONIDAS MOINA	-81	11	WPA2-Personal	00:E0:4D:9A:96:B0	54	g	Infrastructure
UESDS2P	-85	6	WPA2-Personal	CC:B2:55:8C:58:F8	300	n	Infrastructure
UESDS01	-89	1	WPA-Personal	00:1B:11:C8:3A:55	54	g	Infrastructure
SUPER_GABYm	-89	1	WEP	00:27:22:08:84:35	54	g	Infrastructure
UESDS2P	-89	11	WPA2-Personal	C0:4A:00:D4:93:52	144	n	Infrastructure
MINTEL_WIFI	-89	6	Open	54:3D:37:3C:08:48	130	n	Infrastructure
DANIEL	-91	11	WPA2-Personal	4C:8B:EF:50:BB:6C	270	n	Infrastructure

Figura 2.10. Informe del Site Survey Pasivo para la ZONA 2

ZONA 3:

SSID	SIGNAL ▼	CHANNEL	SECURITY	MAC ADDRESS	MAX RATE	802.11	NETWORK TYPE
Casa-Campesina	-47	6	WPA2-Personal	CC:B2:55:8B:B6:48	116	n	Infrastructure
UESDS2P	-69	11	WPA2-Personal	C0:4A:00:D4:93:52	144	n	Infrastructure
UESDS2P	-77	6	WPA2-Personal	CC:B2:55:8C:58:F8	300	n	Infrastructure
UESDS3P	-78	6	WPA2-Personal	CC:B2:55:8B:B4:50	300	n	Infrastructure
HP4D8638	-87	10	Open	02:2D:ED:BD:F2:D1	11	b	Ad Hoc
MINTEL_WIFI	-91	6	Open	54:3D:37:3C:08:48	130	n	Infrastructure
LEONIDAS MOINA	-93	11	WPA2-Personal	00:E0:4D:9A:96:B0	54	g	Infrastructure

Figura 2.11. Informe del Site Survey Pasivo para la ZONA 3

Como se puede observar claramente en las figuras 2.9, 2.10 y 2.11 en las tres zonas las señales predominantes son las denominadas con los SSID: ***Casa-Campesina y UESDS2P,*** además se puede evidenciar que los canales en los que se están manejando todas las redes son ***1, 6, 10 y 11*** los mismos que se tomarán muy en cuenta para evitar interferencias co-canal y solapamiento de las señales.

Para mayor detalle en la tabla 2.6 se muestran las gráficas obtenidas por el programa Inssider 3, en las cuales se comparan las intensidades de las señales predominantes y sus canales de operación en la banda de 2,4GHz.

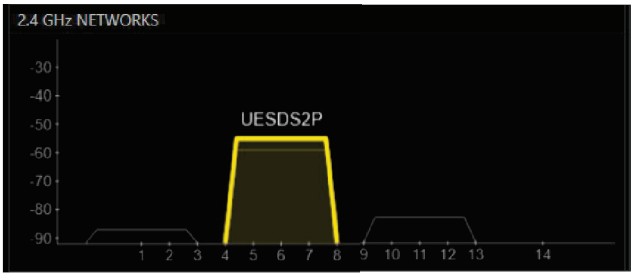
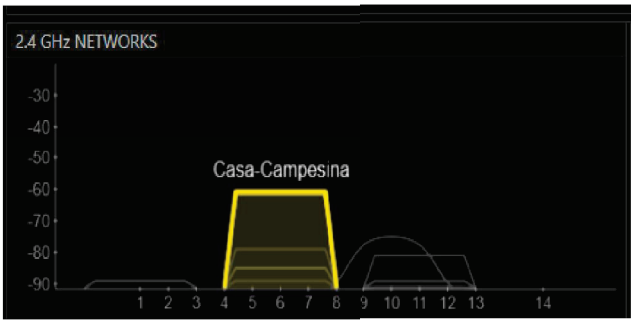
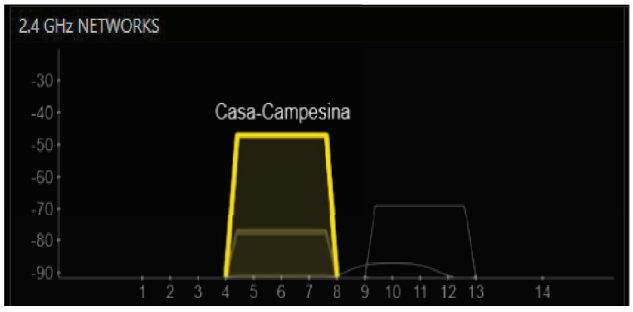
ZONA	GRÁFICA	EXPLICACIÓN
1		La gráfica muestra las señales desde los -90dB, la señal de mayor intensidad es la resaltada en la gráfica cuya SSID es *UESDS2P* la misma que tiene una señal de alrededor de -50dB, además opera entre los canales 4 y 8 de la banda de 2,4GHz del estandar 802.11
2		La gráfica muestra las señales desde los -90dB, la señal de mayor intensidad es la resaltada en la gráfica cuya SSID es *Casa-Campesina* la misma que tiene una señal de alrededor de -60dB, además opera entre los canales 4 y 8 de la banda de 2,4GHz del estandar 802.11
3		La gráfica muestra las señales desde los -90dB, la señal de mayor intensidad es la resaltada en la gráfica cuya SSID es *Casa-Campesina* la misma que tiene una señal de alrededor de -40dB, además opera entre los canales 4 y 8 de la banda de 2,4GHz del estandar 802.11

Tabla 2.6. Comparación gráfica de las señales predominantes en la banda de 2,4GHz.

2.9 Instalación y configuración del router

Previo a la instalación y configuración de un router se debe conocer cuál será la funcionalidad del mismo. En la red de cámaras de seguridad a implementar, dichas funcionalidades se detallan a continuación:

1. Permitir un enlace de comunicación (cableada e inalámbrica) entre los componentes de la red.

2. Garantizar acceso de forma remota a la red.

3. Dividir y optimizar el correcto uso de la red.

4. Ser una barrera de seguridad ante posibles vulnerabilidades a la red.

El router es un elemento clave y neurálgico en la funcionalidad del sistema a implementar, por lo tanto se debe adquirir un router que cumpla con características mínimas, las cuales se consideran a continuación:

- Wireless 802.11/b/n/g; puesto que la red de cámaras será inalámbrica

- Velocidades de transmisión de hasta 300Mbps; puesto que con estas velocidades se garantiza una mayor cobertura inalámbrica hacia las cámaras

- Puertos Ethernet; puesto que la etapa inicial de configuración debe realizarse con conexión física mediante cable UTP.

En el mercado la cantidad de routers es abrumadora y la mayoría superan por mucho las características antes mencionadas, es por esto que se ha designado un router de mediano costo el Linksys E900.

2.9.1 Router Linksys E900

Es un router de serie E marca Linksys ideal para instalaciones cableadas o Wireless de redes LAN domésticas o de oficinas a mediana escala. Alcanza un rendimiento máximo según lo establecido en las especificaciones de la norma IEE 802.11.

Posee dos antenas interiores con una potencia de trasmisión de alrededor de 13dBm alcanzando velocidades de hasta 300Mbps. [4] Lo que es ideal para el sistema que se va a implementar.

2.9.2 Ubicación del router

Como se ha analizado previamente la red de cámaras de seguridad a implementar estará ubicada en la planta baja del edificio de la Unidad Educativa Salesiana "Domingo Savio" (ver figura 2.6).

Motivo por el cual se debe conocer la cobertura aproximada en metros que brindará el router seleccionado y así determinar la ubicación del mismo, para ello consideramos la fórmula para el cálculo de la distancia en un enlace de telecomunicaciones con antenas.

$$20 * \log (D) = P_{TX} - P_{req} + G_{TX} + G_{RX} - 32.45 - 20 * \log (f)$$ **[13]**

De donde:

- **Frecuencia (f):** este parámetro es la banda de frecuencia utilizada por las antenas y dispositivos. Está en MHz y por defecto se escribe 2400.

- **Impedancia sistema (Z):** este dato no necesitamos variarlo para las instalaciones wifi típicas. Así que el valor que viene por defecto es de 50 ohmios.

[4] Revisar anexo A

- **Potencia entregada a la antena transmisora (Ptx):** Es la potencia de emisión del dispositivo que emite la red wifi, normalmente el router wifi. Se encuentra en dBm. Para saber cuántos dBm tiene un equipo se debe buscar en el data sheet o en las especificaciones del equipo.[5]

- **Sensibilidad en receptor (Srx):** Es la cantidad mínima de señal que necesita recibir un dispositivo para realizar una conexión a una velocidad dada.
  Si se pone una sensibilidad muy alta significa que la antena necesita recibir poca cantidad de señal, por tanto el alcance será muy grande pero muy lento, es decir, cuanto menor sea el valor ubicado mayor será la velocidad y menor la distancia. Lo mejor es utilizar un valor de sensibilidad para una velocidad aceptable, lo cual dará un alcance más corto pero real.

- **Margen ganancia para permitir error datos digital aceptable (M):** No es necesario modificarlo este valor es generalmente de 1dB.

- **Ganancia antena transmisora (Gtx):** Serán los dBi de la antena que emite la señal. Se debe buscar en las especificaciones del router wifi para encontrar el valor adecuado.[5]

- **Ganancia antena receptora (Grx):** Serán los dBi de la antena que recibe la señal. Se debe buscar en las especificaciones wifi de la antena receptora para encontrar el valor adecuado.

- **Potencia requerida en una antena receptora (Preq):** Es la potencia mínima que requiere la antena receptora para poder establecer el enlace de comunicaciones.

- **Longitudes de cable y atenuación:** Para la ganancia de la antena transmisora y receptora se puede determinar la pérdida por cable de antena. Podemos elegir la longitud y la pérdida por metro de cable (se ha seleccionado el valor por defecto para el cable tipo HDF200 o LMR200).

[5] Revisar anexo A.

PARÁMETRO	VALOR	OBSERVACIÓN
f	2400MHz	Banda de frecuencia da las señales Wi-Fi
Z	50Ω	Dato típico de las señales Wi-Fi
P_{TX}	13dBm	Valor promedio según las especificaciones del router Linksys E900
S_{RX}	-60dBm	Valor promedio y aceptable.
M	1dB	Valor típico
G_{TX}	4dBi	Valor máximo para dos antenas según especificaciones del router Linksys E900
G_{RX}	2dBi	Valor estándar de las antenas Wi-Fi
P_{req}	-89dBm	Dato Calculado
Distancia Aproximada	0,075212 Km	Distancia aproximada en kilómetros

Tabla 2.7. Cálculo del alcance de una antena Wi-Fi[6]

Considerando la tabla 2.7 el router debe ubicarse de tal manera que brinde cobertura Wi-Fi a las tres cámaras que se van a implementar por lo tanto y considerando el plano de la figura 2.6 se ubicará en router en el cuarto de equipos ubicado en la Casa Campesina Cayambe como se evidencia en la figura 2.12.

[6] Estos valores son teóricos para antenas con línea de visión directa. Los valores en la realidad cambian debido a otros factores.

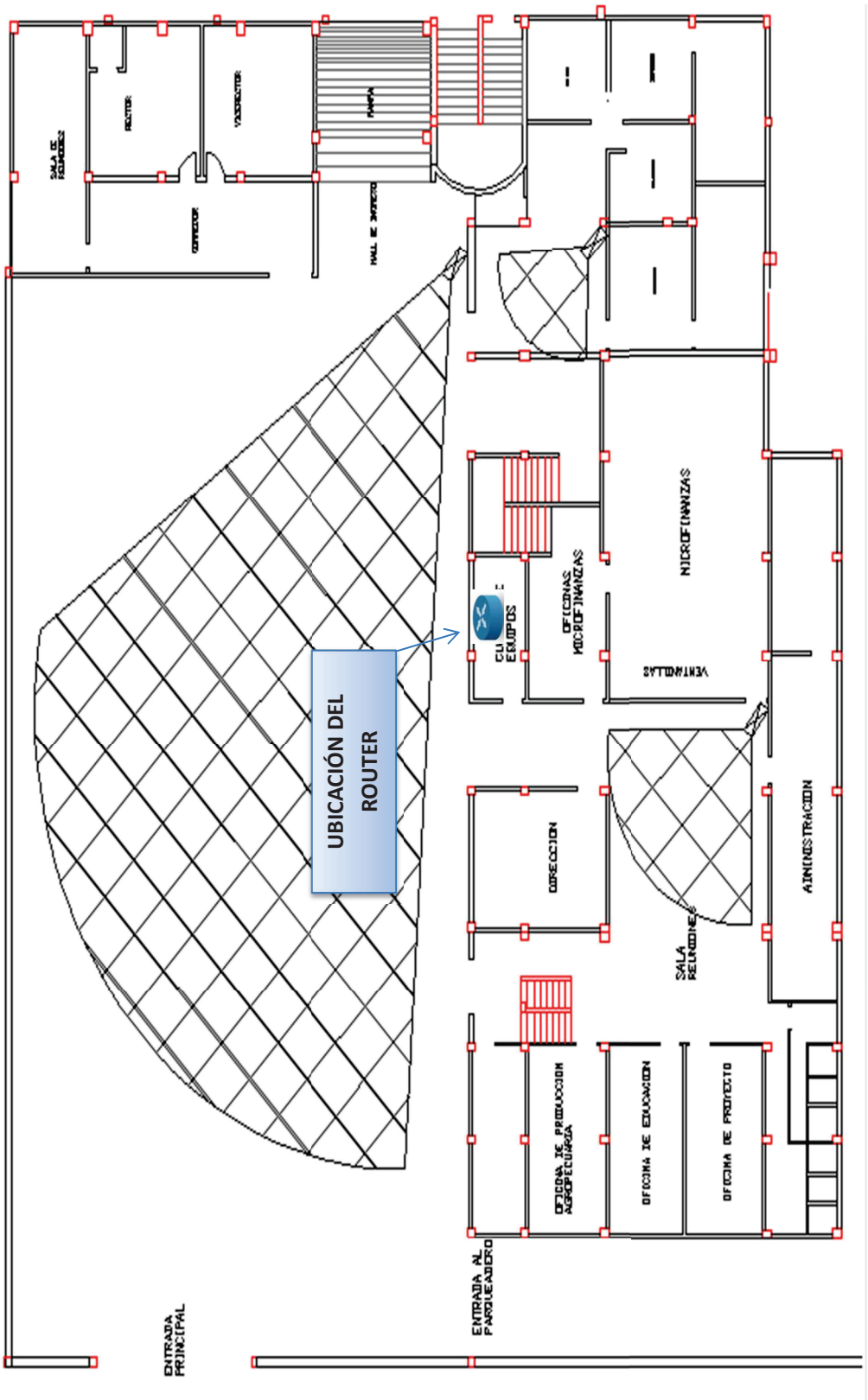


Figura 2.12. Ubicación del router

2.9.3 Esquema de la red

Uno de los usos del router es dividir y organizar la red, para este sistema es muy importante esta cuestión puesto que cada cámara necesita de una dirección IP a la misma que se accederá de forma remota.

La red a implementar será independiente a la red institucional puesto que se debe garantizar las seguridades de la misma, de ese modo la red de cámaras de seguridad no generará problemas a la red ya existente.

Como se analizó en la sección 2.8 el proveedor de internet entrega varias direcciones IP a la institución, todas ellas públicas, el administrador de la red institucional ha facilitado la dirección pública **186.101.97.134** para la implementación de la red de cámaras de seguridad.

Para el direccionamiento interno se considera una dirección IP de tipo C, la misma es ideal para redes de pequeño o mediano tamaño acoplándose de forma ideal a nuestro sistema, por lo tanto se escoge una dirección IP ordinaria, es la **192.168.1.0,** en base a esta dirección se realizará todo el direccionamiento para cada componente de la red, en la tabla 2.8 se puede evidenciar las direcciones IP asignadas a cada componente.

COMPONENTE	DIRECCIÓN IP
ROUTER	192.168.1.155
CÁMARA ZONA 1	192.168.1.12
CÁMARA ZONA 2	192.168.1.10
CÁMARA ZONA 3	192.168.1.11
PC DE CONTROL	192.168.1.15

Tabla 2.8. Direcciones IP asignadas a cada elemento de la red

Para tener una idea clara de cómo estarán conectados cada uno de los elementos que componen la red en la figura 2.14 se muestra un esquema de la red a implementar.

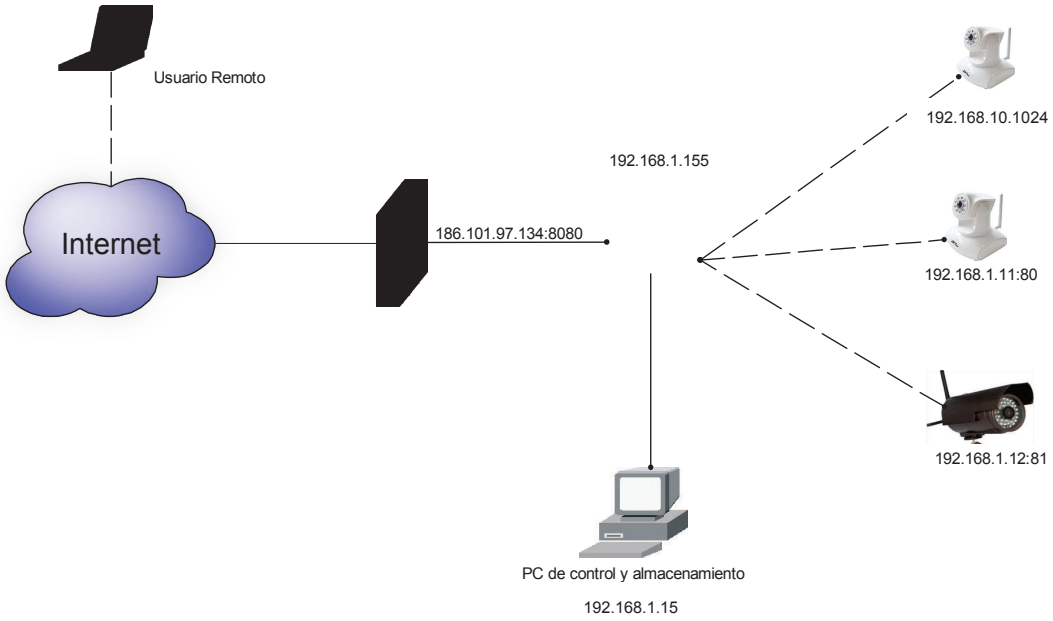


Figura 2.13. Esquema de la red

Luego de tener una noción clara de la forma de conexión de la red se procede a configurar el router, este proceso es sencillo y predictivo, el detalle se muestra en las figuras 2.14, 2.15 y 2.16.

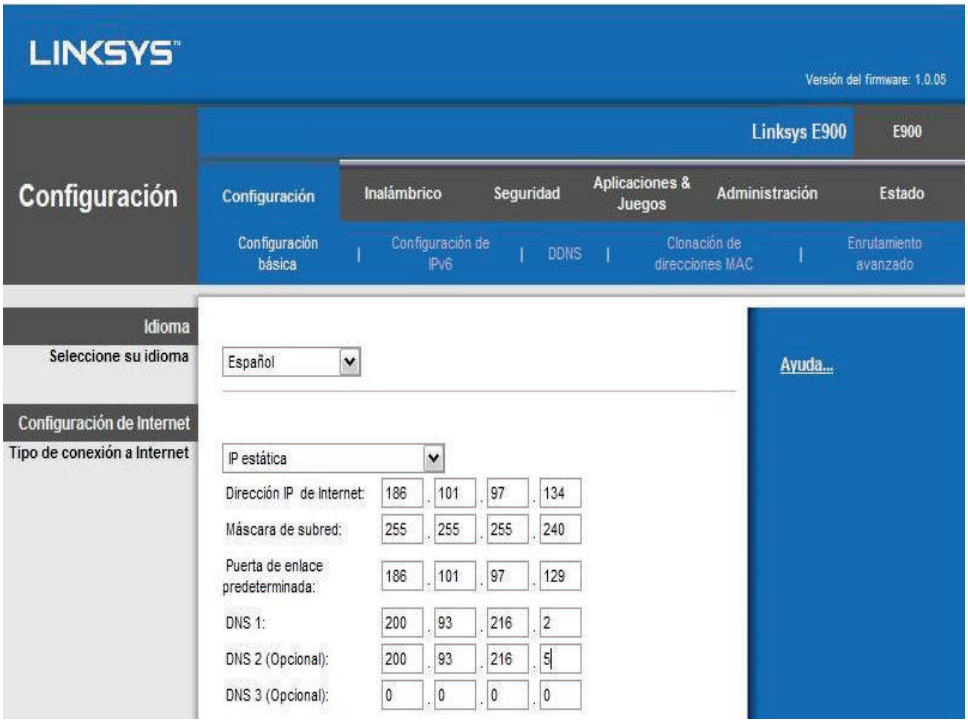


Figura 2.14. Configuración de internet del router (datos proporcionados por proveedor)

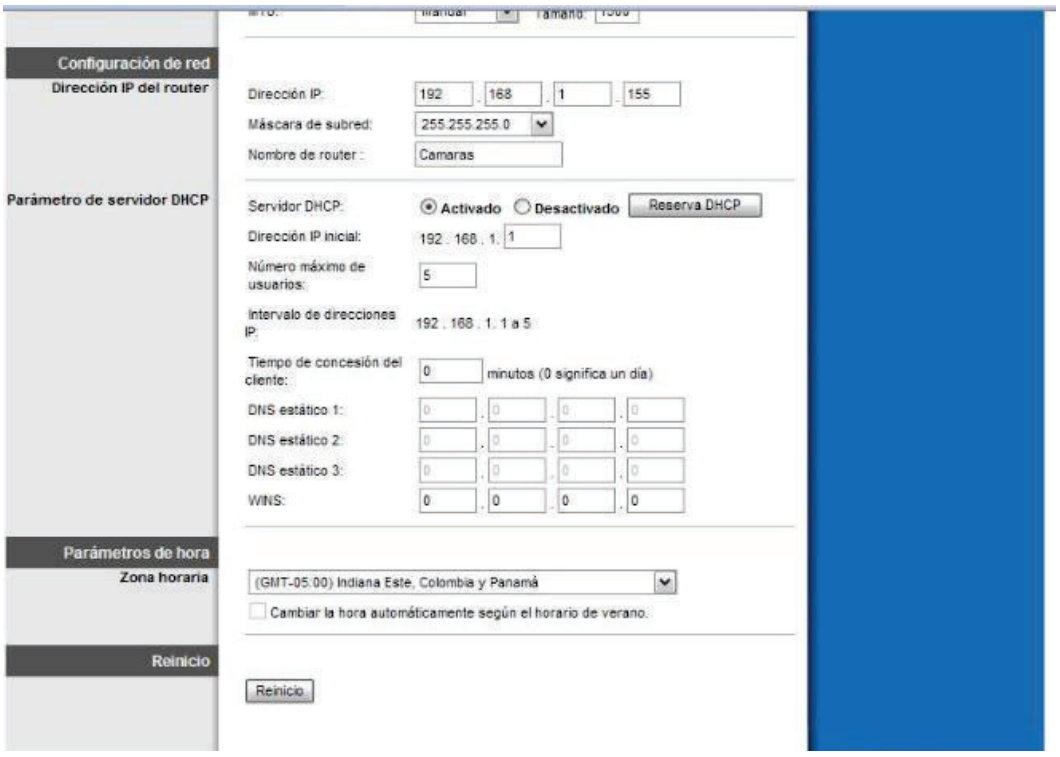


Figura 2.15. Asignación de la dirección IP privada del router

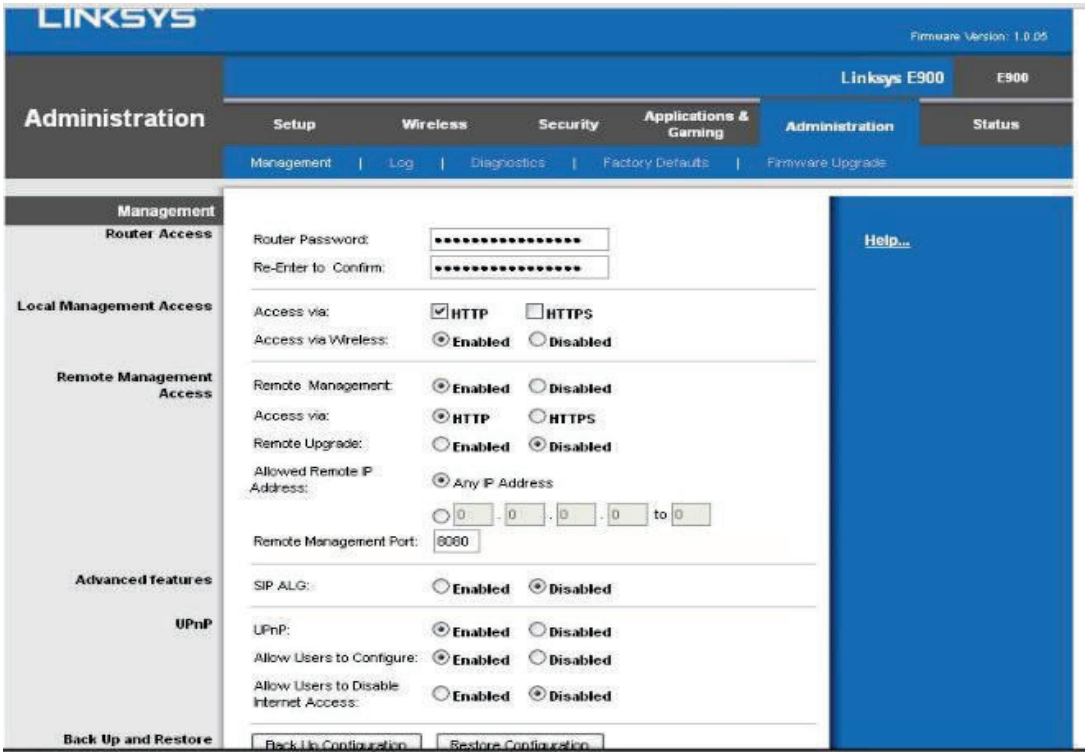


Figura 2.16. Habilitación del acceso remoto y encriptación del router

2.9.4 Site Survey Activo

Una vez instalado y configurado el router procedemos realizar el Site Survey Activo en el cual se visualiza el alcance de la señal implementada y tomar algún correctivo de ser necesario.

A continuación se presenta el informe generado por el Inssider 3 en cada una de las zonas designadas para la ubicación de las cámaras.

ZONA 1:

SSID	SIGNAL	CHANNEL	SECURITY	MAC ADDRESS	MAX RATE	802.11	NETWORK TYPE
Camaras	-62	1	WPA2-Personal	C8:B3:73:50:B6:AF	144	n	Infrastructure
Casa-Campesina	-69	9+5	WPA2-Personal	E8:94:F6:93:DE:2A	300	n	Infrastructure
HP4D8638	-69	10	Open	02:25:E5:5C:2D:58	11	b	Ad Hoc
CCC	-83	11	WPA2-Personal	CC:B2:55:8B:B6:48	116	n	Infrastructure
CONSISTEM	-85	4+8	WPA2-Personal	90:F6:52:C5:F3:48	300	n	Infrastructure
UESDS-Pastoral	-89	5	WPA2-Personal	DC:9F:DB:04:83:34	130	n	Infrastructure
UESDS01	-89	1	WPA-Personal	00:1B:11:C8:3A:55	54	g	Infrastructure
UESDS2P	-89	6+2	WPA2-Personal	C0:4A:00:D4:93:52	300	n	Infrastructure
NancyPerugachi	-91	6	WPA-Personal	00:21:63:DE:47:AF	54	g	Infrastructure
UESDS3P	-91	11+7	WEP	CC:B2:55:8B:B4:50	300	n	Infrastructure
CYBERUGA	-91	11+7	WPA2-Personal	60:E7:01:4F:DA:60	270	n	Infrastructure
Diego Cat System	-91	11+7	WPA2-Personal	E8:DE:27:9A:63:FC	150	n	Infrastructure
SUPER_GABYm	-93	1	WEP	00:27:22:08:84:35	54	g	Infrastructure

Figura 2.17. Informe del Site Survey Activo para la ZONA 1

ZONA 2:

SSID	SIGNAL	CHANNEL	SECURITY	MAC ADDRESS	MAX RATE	802.11	NETWORK TYPE
CCC	-58	11	WPA2-Personal	CC:B2:55:8B:B6:48	116	n	Infrastructure
Camaras	-65	1	WPA2-Personal	C8:B3:73:50:B6:AF	144	n	Infrastructure
Casa-Campesina	-71	9+5	WPA2-Personal	E8:94:F6:93:DE:2A	300	n	Infrastructure
HP4D8638	-75	10	Open	02:25:E5:5C:2D:58	11	b	Ad Hoc
CONSISTEM	-81	4+8	WPA2-Personal	90:F6:52:C5:F3:48	300	n	Infrastructure
UPS-NET-CAYAMBE	-83	11	WPA2-Personal	00:23:5E:1E:B9:60	54	g	Infrastructure
SUPER_GABYm	-83	1	WEP	00:27:22:08:84:35	54	g	Infrastructure
UESDS2P	-85	6+2	WPA2-Personal	C0:4A:00:D4:93:52	300	n	Infrastructure
UESDS3P	-87	11+7	WEP	CC:B2:55:8B:B4:50	300	n	Infrastructure
UPSNET13	-87	1	WPA2-Personal	00:27:22:40:11:7F	130	n	Infrastructure
UESDS-Pastoral	-87	5	WPA2-Personal	DC:9F:DB:04:83:34	130	n	Infrastructure
CYBERUGA	-89	11+7	WPA2-Personal	60:E7:01:4F:DA:60	270	n	Infrastructure
MINTEL_WIFI	-89	11	Open	54:3D:37:3C:08:48	130	n	Infrastructure

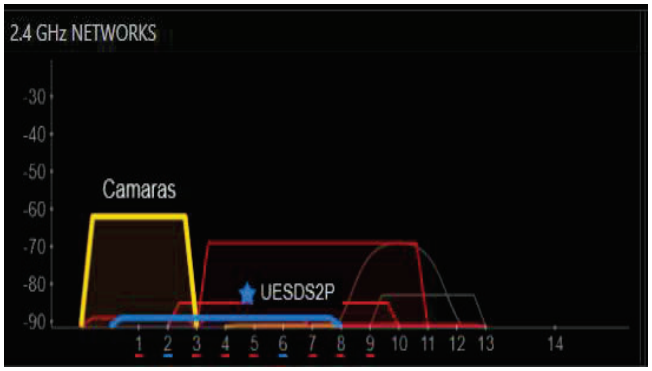
Figura 2.18. Informe del Site Survey Activo para la ZONA 2

ZONA 3:

SSID	SIGNAL ▼	CHANNEL	SECURITY	MAC ADDRESS	MAX RATE	802.11	NETWORK TYPE
HP4D8638	-63	10	Open	02:25:E5:5C:2D:58	11	b	Ad Hoc
Camaras	-65	1	WPA2-Personal	C8:B3:73:50:B6:AF	144	n	Infrastructure
Casa-Campesina	-73	9+5	WPA2-Personal	E8:94:F6:93:DE:2A	300	n	Infrastructure
CONSISTEM	-83	4+8	WPA2-Personal	90:F6:52:C5:F3:48	300	n	Infrastructure
UESDS2P	-84	6+2	WPA2-Personal	C0:4A:00:D4:93:52	300	n	Infrastructure
UESDS3P	-85	11+7	WPA2-Personal	CC:B2:55:8B:B4:50	300	n	Infrastructure
MINTEL_WIFI	-87	11	Open	54:3D:37:3C:08:48	130	n	Infrastructure
CCC	-87	11	WPA2-Personal	CC:B2:55:8B:B6:48	116	n	Infrastructure
Manuel_Parion	-89	6	WPA2-Personal	88:A5:BD:05:60:90	72	n	Infrastructure
UESDS01	-93	1	WPA-Personal	00:1B:11:C8:3A:55	54	g	Infrastructure
Diego Cat System	-97	11+7	WPA2-Personal	E8:DE:27:9A:63:FC	150	n	Infrastructure

Figura 2.19. Informe del Site Survey Activo para la ZONA 3

En las figuras 2.17, 2.18 y 2.19 se puede evidenciar que la señal ***CÁMARAS*** es predominante sobre el resto, esto se puede evidenciar en las gráficas obtenidas por el programa Inssedie 3 que se muestran en la tabla 2.9 y además porque uno de los datos proporcionado por el programa es el valor de la señal en dBm.

ZONA	GRÁFICA	EXPLICACIÓN
1		La gráfica muestra las señales predominanes desde los -90dBm, la señal predomiantes es la resaltada en la gráfica cuya SSID es *Camaras* la misma que tiene una señal de alrededor de -60dBm, además opera entre los canales 1 y 3 de la banda de 2,4GHz del estandar 802.11

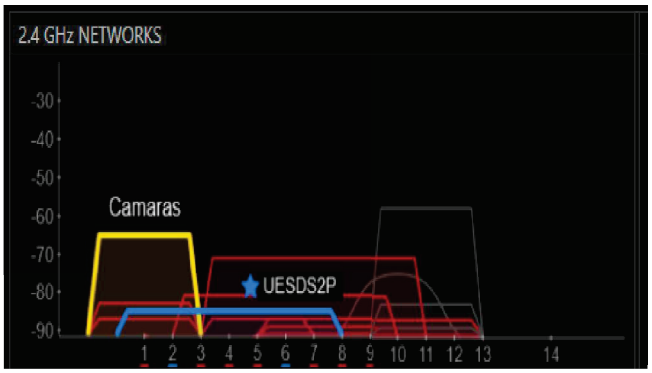
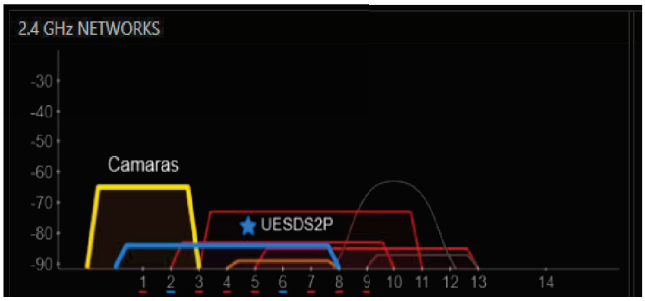
2		La gráfica muestra las señales predominanes desde los -90dBm, la señal predomiantes es la resaltada en la gráfica cuya SSID es *Camaras* la misma que tiene una señal de alrededor de -60dBm, además opera entre los canales 1 y 3 de la banda de 2,4GHz del estandar 802.11, como se puede evidenciar exixte otra señal con los mismos valores de la señal cámaras pero no existiría problema puesto que esta trabajando en los canales 9 al 13 de la banda de 2,4GHz del estandar 802.11
3		La gráfica muestra las señales predominanes desde los -90dBm, la señal predomiantes es la resaltada en la gráfica cuya SSID es *Camaras* la misma que tiene una señal de alrededor de -60dBm, además opera entre los canales 1 y 3 de la banda de 2,4GHz del estandar 802.11, como se puede evidenciar exixte otra señal con los mismos valores de la señal cámaras pero no existiría problema puesto que esta trabajando en los canales 9 al 13 de la banda de 2,4GHz del estandar 802.11

Tabla 2.9. Gráficas de las señales existentes en las zonas a instalar las cámaras

Como se puede ver en los cuadros comparativos anteriores hay varios solapamientos con la señal **CÁMARAS,** pero esta señal es predominante al resto además se encuentra operando en canales distintos.

Como conclusión del Site Survey se determinó que la señal instalada brindará un soporte fiable para el tráfico de datos de la red de cámaras de seguridad.

2.10 Instalación del computador de almacenamiento y control

Para el almacenamiento de las grabaciones captadas por las cámaras se instalará un computador con las siguientes características:

- Procesador Intel Pentium IV
- Memoria RAM 500MB
- Disco Duro 150GB

Este computador debe tener un software de control y gestión de las grabaciones emitidas desde las cámaras, el software seleccionado es el propio de cada cámara puesto que para la implementación del proyecto no está contemplada la instalación de un cuarto de control permanente, es decir solo se debe garantizar el almacenamiento de las grabaciones; los programas son:

- **ZKiVision:** cámaras ZKTeco (Zonas 2 y 3)
- **Master:** Cámara Dericam (Zona 1**)**

Los dos programas brindan gran facilidad en cuanto al control de cada cámara, además se evitan los problemas de compatibilidad que se tienen con un software multimarca, otro beneficio es evitar gastos de adquisición de licencias.

Como se puede evidenciar el computador no es de última tecnología, la capacidad del disco duro es un limitante para cualquier computador, es por este motivo que las grabaciones obtenidas de las cámaras se almacenarán en el computador por un lapso determinado de tiempo, luego de este periodo se transferirán los archivos de video hacia un disco externo y así liberar el disco duro, de esta manera se evitará que la máquina se sobrecargue de información y tenga problemas en cuanto a su velocidad.

El cálculo del tiempo de grabación se presenta a continuación.

2.10.1 Cálculo del tiempo aproximado de almacenamiento de las grabaciones

Mediante este cálculo se tendrá una clara idea de la cantidad de días que se deben almacenar las grabaciones para que el sistema no presente inconvenientes, para ellos se considera:

- Número de cámaras.
- Horas diarias que grabará cada cámara.
- Capacidad de almacenamiento.

Para el cálculo se debe conocer el ancho de banda por cada cámara, el mismo que no tiene mayores variaciones para cámaras con las características que hemos adquirido, indistintamente a su marca, lo que sí es relevante en el ancho de banda es el tipo de compresión utilizada, pero para el cálculo usaremos valores generalizados.

En consideración a las especificaciones técnicas de la marca AXIS que mencionan "La limitación de ancho de banda máxima configurable para evitar la saturación de la red a 30 (25) frames / s normalmente requiere alrededor de 1,5 Mbit / s." (AXIS, 2002)[11]

$$Bw\ cámara = 1{,}5\frac{Mbits}{s} \cdot \left(\frac{1byte}{8\ bits}\right) = 187{,}5Kbps$$

Por lo tanto el ancho de banda que utilizaremos es de 187,5 Kbps por cámara.

En promedio las cámaras grabarán alrededor de 16 horas diarias el detalle se muestra en la tabla2.10.

GRABACIÓN	DETALLE	TIEMPO (horas)
Permanente	Se realizará en los horarios de mayor afluencia de personas.	8
Al detectar movimiento	Horarios de poca afluencia de personas, en la noche y madrugada	8
	TOTAL	**16**

Tabla2.10. Horas que grabará en promedio cada cámara

Por lo tanto:

$$Cantidad\ de\ información\ por\ cámara = Bw \cdot tiempo$$

$$Cantidad\ de\ información\ por\ cámara = 187{,}5Kbps\left(\frac{3600\ s}{1\ h}\right) = 675\frac{Mbytes}{hora}$$

$$Cantidad\ de\ información\ por\ cámara = 675\frac{Mbytes}{hora} \cdot 16\frac{horas}{día}$$

$$Cantidad\ de\ información\ por\ cámara = 10{,}8\ \frac{Gbytes}{día}$$

$$Cantidad\ de\ información\ total = 10{,}8\ \frac{Gbytes}{día} \cdot (3\ cámaras)$$

$$Cantidad\ de\ información\ total = 32{,}4\frac{Gbytes}{día}$$

Considerando que la capacidad de almacenamiento disponible es de 150GB, tenemos:

$$Días\ de\ almacenamiento = \frac{Capacidad\ almacenamiento\ disco}{Almacenamiento\ diario\ total}$$

$$Días\ de\ almacenamiento = \frac{150GB}{36{,}45Gbpdía}$$

$$Días\ de\ almacenamiento = 4{,}6\ días$$

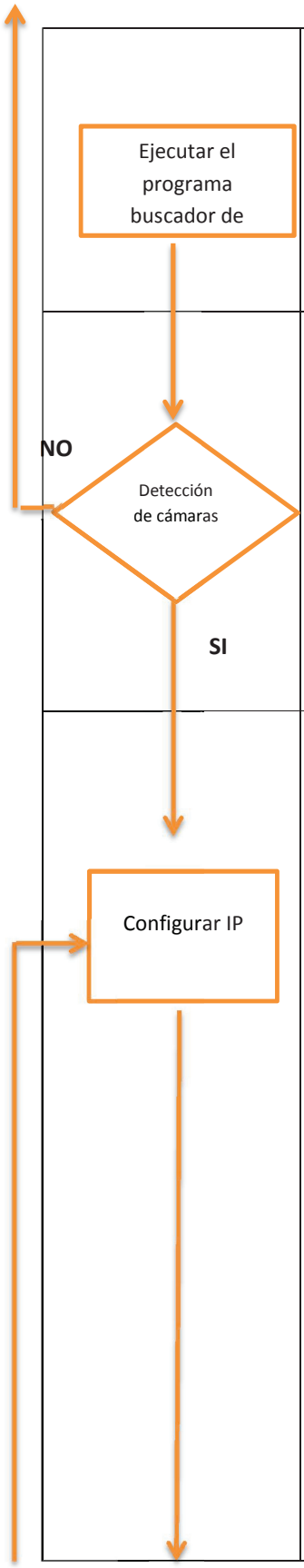
Considerando el cálculo se llega a la conclusión que las grabaciones se deben almacenar por un tiempo aproximado de alrededor de 5 días, de esta manera no se saturará el disco de almacenamiento.

2.11 Configuración de las cámaras

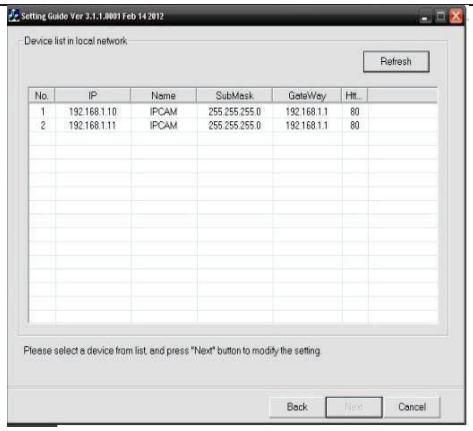
2.11.1 Configuración Inicial

Para la configuración de las cámaras se debe tomar en cuenta el siguiente diagrama de flujo, puesto que los pasos son los mismos indistintamente de la marca de la cámara:

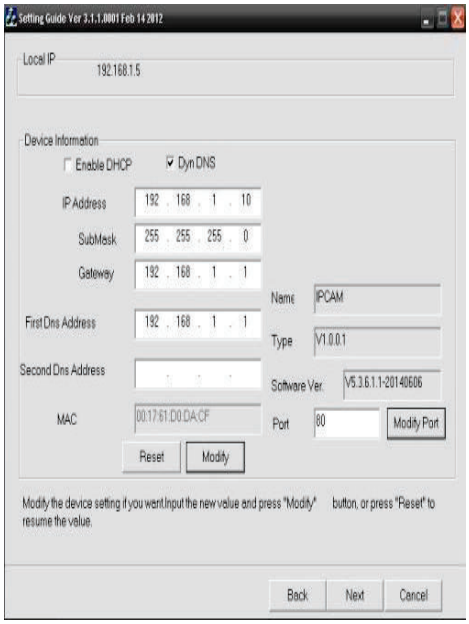
DIAGRAMA DE FLUJO	IMAGEN	OBSERVACIÓN
Conectar pc y cámara al router	Sin imagen	Es posible realizar la configuración directa, es decir configurar la cámara conectándola únicamente al computador pero se recomienda conectar las cámaras y la PC al router.
Colocar el CD de instalación de la cámara	Sin imagen	Con el CD tenemos acceso a programas de instalación del software de cada cámara.



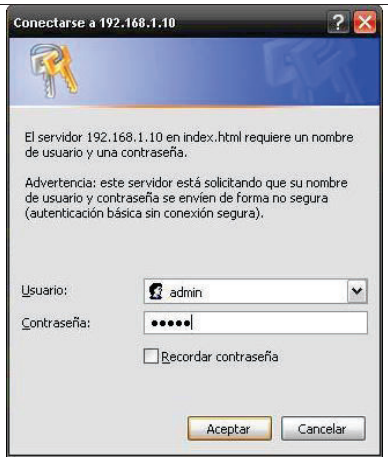
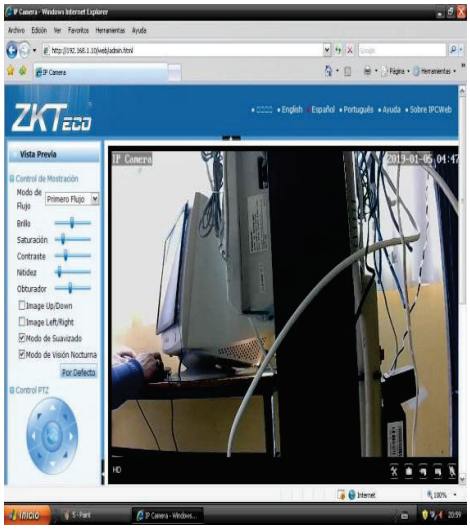
Buscar en las carpetas del CD de instalación el archivo ejecutable que permite la configuración de cada cámara, en los manuales se detalla cual es el archivo.



Ventana donde se evidencian las cámaras detectadas con su respectivo direccionamiento IP y puerto por defecto.



Ventana de configuración de la dirección IP de la cámara se debe considerar las direcciones expuestas en la tabla 2.5. Como se ve en la imagen de la izquierda el Gateway es distinto al asignado al router por lo que generará inconvenientes, es por esto que se lo debe modificar a la dirección interna del router es decir **192.168.1.155,** caso contrario será imposible acceder a las cámaras de forma remota.

NO Actualizar SI	Sin Imagen	Al guardar los cambios y actualizar el buscador de cámaras debe detectar la cámara con todas las modificaciones hechas.
http:// IP de la cámara/		En cualquier navegador web ingresar la dirección IP asignada a la cámara.
Ingresar usuario y contraseña		Generalmente el usuario es **admin** y la contraseña es la misma, pero suele cambiar según la marca, es recomendable leer el manual de instalación para evitar inconvenientes.
Acceso al video y configuraciones de control y gestión		Una vez que se accede a la cámara hay tres opciones: • Video • Vigilancia Móvil • Instalación de software La primera permite ver el video y configurar la cámara mediante su software de control (calidad de video, almacenamiento, detección de

		movimiento, Wireless, etc.) La segunda permite accesar al video de media calidad desde cualquier móvil o PC. La tercera se debe usar al acceder por primera vez, puesto que la PC necesita de un software para poder mostrar la vista previa de cada cámara. En la imagen se ha seleccionado la opción **VIDEO,** previo a la instalación de los controladores de la cámara.

Tabla 2.11. Configuración inicial de las cámaras.

2.11.1.1 Configuración Wireless de las cámaras

Una vez configuradas las cámaras se debe realizar la configuración Wireless para que se genere la conexión inalámbrica entre las cámaras y el router.

Para configurar la conexión inalámbrica, se debe ingresar a la cámara y elegir la configuración inalámbrica, la misma que no presenta mayores inconvenientes puesto que tiene una interfaz intuitiva, lo único que se debe conocer es la clave de acceso al router.

En la figura 2.20 se visualiza la ventana que permite generar la conexión.

Figura 2.20. Configuración inalámbrica de la cámara.

Se debe buscar la red que emite el router cuyo nombre es **Cámaras,** luego se debe ingresar la clave de acceso al router, se realiza la prueba de conexión y para finalizar se confirman los datos.

2.11.1.2 Configuración de acceso remoto a la cámara

Luego de la configuración inicial y de establecer la conexión inalámbrica con las cámaras se procede a configurar el acceso remoto para poder visualizarlas desde cualquier lugar, utilizando Internet.

De las varias maneras que existen para realizar esta configuración, se tomó la decisión de utilizar una herramienta del router denominada **reenvío de puerto único,** esta configuración se puede evidenciar en la figura 2.22**.**

Esta herramienta permite acceder de forma remota al router por medio de un puerto único que se asigna de forma libre y el router se encarga de redireccionar hacia la dirección IP de la cámara y su respectivo puerto el mismo que no se ha modificado y que en la mayoría de casos es 80 u 81, el puerto de cada cámara se lo evidencia en la configuración inicial luego de correr el programa buscador, puesto que este al detectar la cámara muestra la dirección IP con su puerto.

Los puertos asignados se los debe considerar dentro del rango de puertos registrados que van del 1 024 al 49 151, de este rango se puede seleccionar cualquiera es por esto que se han seleccionado los puertos descritos en la tabla 2.12.

CÁMARA	PUERTO EXTERNO	PUERTO INTERNO (Cámara)
CÁMARA ZONA 2	10001	80
CÁMARA ZONA 3	10002	80
CÁMARA ZONA1	10003	81

Tabla 2.12. Especificaciones de los puertos externos por cada cámara

La ventana de configuración en la interfaz del router se puede evidenciar en la figura 2.21.

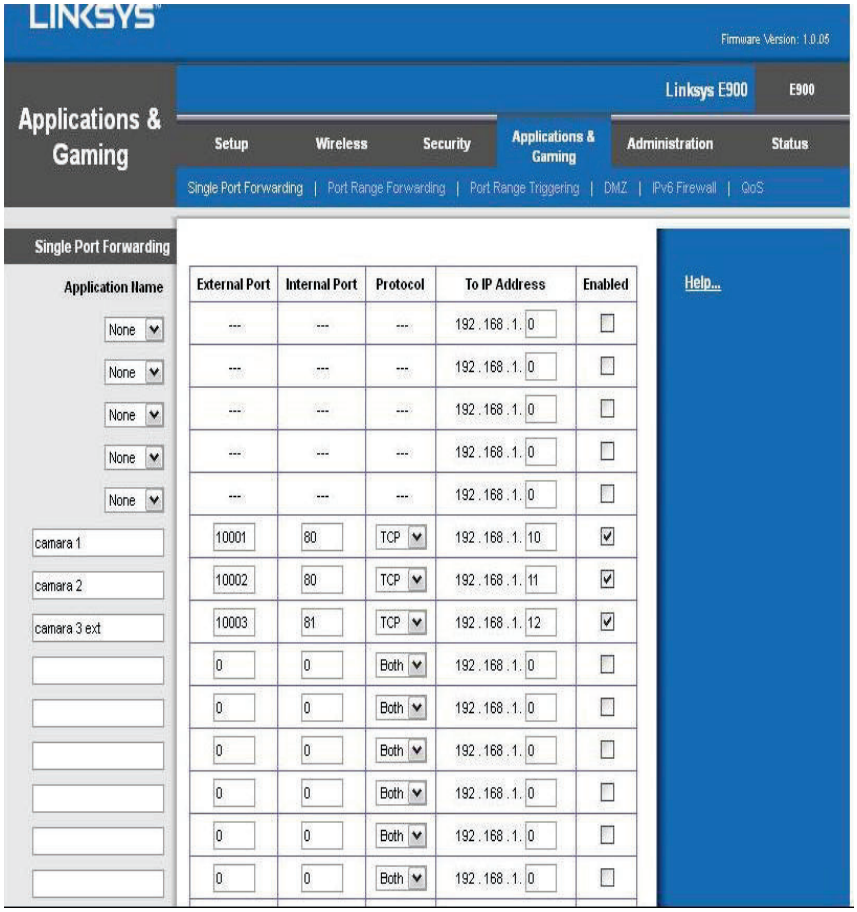


Figura 2.21. Reenvío de puerto, evita modificar el puerto de la cámara

2.11.2 Descripción de las herramientas de configuración de las cámaras

2.11.2.1 Cámara ZKTeco

Luego de acceder a la cámara por Internet se tienen las siguientes herramientas:

- Vista Previa
- Dispositivo
- Alarma
- Configuración de la Red
- Configuración Avanzada
- Sistema

- **Vista Previa**

En esta opción se puede visualizar la cámara y configurar los parámetros para mostrar las imágenes es decir el brillo, contraste, saturación, nitidez, etc.; además poseé el control PTZ el cual permite mover la cámara.

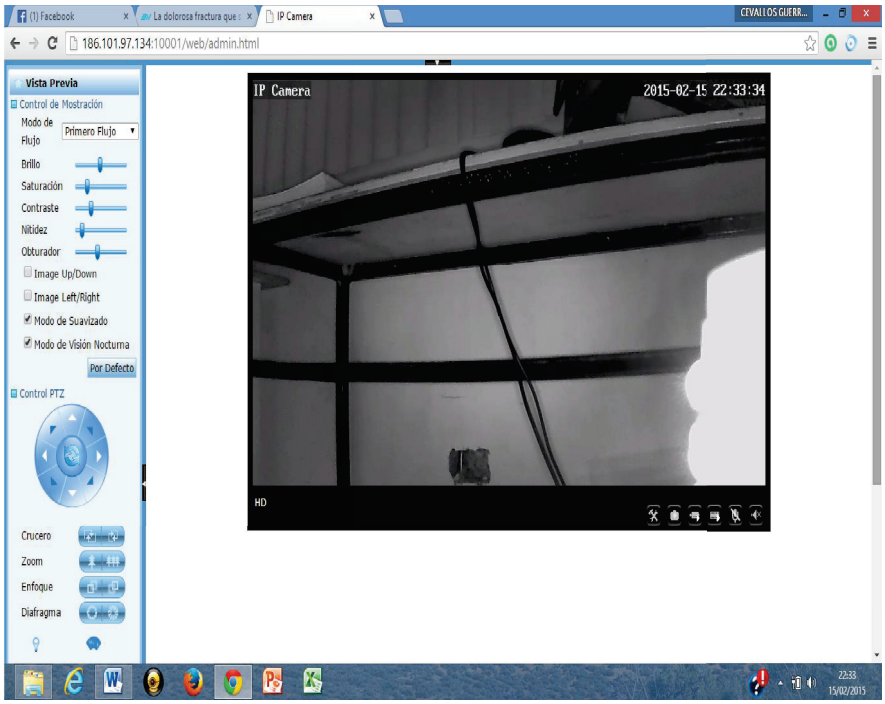


Figura 2.22. Vista previa

- **Dispositivo**

  - **Configuración de video**

Esta opción permite configurar tres calidades de video denominado primer, segundo y tercer flujo, cada uno de estos flujos tiene diferentes calidades de video.

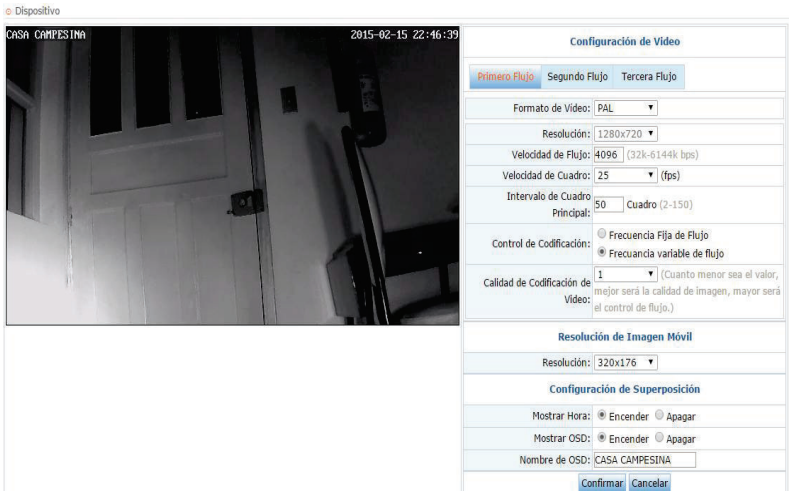


Figura 2.23. Configuración de video

  - **Configuración Audio**

Con esta opción se puede configurar el formato y la calidad de audio, además del volumen de entrada y salida. Los valores seleccionados son lo estándar, pero hay que considerar que las grabaciones serán únicamente de video sin audio por lo que no tiene mayor relevancia.

Figura 2.24. Configuración audio

- **Configuración PTZ**

Esta opción permite configurar el control de movimiento de la cámara.

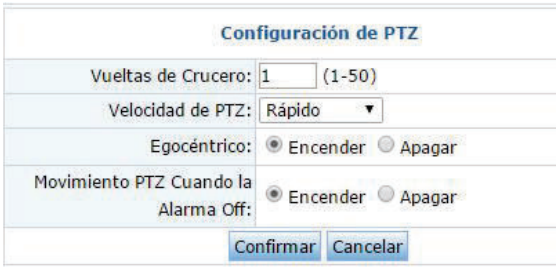


Figura 2.25. Configuración PTZ

- **Alarma**

Esta opción permite configurar la alarma, las zonas que detectarán el movimiento, las configuraciones de correo electrónico y del servidor FTP.

- **Configuración de la red**
  - **Configuración de red**

En esta opción permite configurar la dirección IP de la cámara, además de los puertos HTTP y RTSP.

Figura 2.26. Configuración de red

- **Configuración inalámbrica**

Esta opción permite configurar la conexión inalámbrica de la cámara.

- **Configuración Avanzada**

Esta opción permite configurar el almacenamiento temporizado, además de configurar el correo electrónico al cual se enviarán las alertas, también podemos configurar el servidor FTP.

- **Sistema**
  - **Configuración de usuarios**

    En esta opción se puede configurar los usuarios que pueden acceder a las cámaras, cada uno con sus atributos que se detallan en la tabla 2.13.

Usuario	Atribuciones
Admin	Todas las configuraciones
User	Operar PTZ, video de PC y captura de imágenes
Guest	Solo vista previa de video

Tabla 2.13. Usuarios de cámara y sus atribuciones

Además se puede cambiar las contraseñas de cada usuario, las que se entregarán a las autoridades institucionales para que ellos hagan uso de las mismas como consideren conveniente.

El resto de opciones permiten configurar la hora, muestra una información general del dispositivo y un registro de todas las acciones realizadas en la cámara y los usuarios que accedieron a la misma.

2.11.2.2 Cámara Dericam

Las configuraciones de esta cámara son similares a la de la ZKTeco, y sus herramientas son:

- Live Video

  Permite visualización de video en vivo de lo que está captando la cámara.
- Live Video (VLC)

  Muestra un video en vivo de formato VLC.

- IPad

  Muestra video de baja calidad ideal para teléfonos o tablets.

- Net Connection

  Permite accesar y modificar la configuración de la dirección IP de la cámara.

- Alarm Setting

  Permite la configuración la alarma de detección de movimiento que posee la cámara, además de programar los horarios en los que se activará la alarma.

- Front-end Record

  Esta opción sirve para programar los horarios de grabación de acuerdo a las necesidades existentes.

- Control Panel

  Permite realizar configuraciones específicas de la cámara con por ejemplo, fecha y hora, dirección de almacenamiento de las grabaciones, creación y control y creación de usuarios, habilitar accesos o permisos en la cámara etc.

- Diagnose Tool

  Permite realizar actualizaciones al software y controlar los usarios que han accedido a la cámara.

- Logout

  Salir de las opciones de configuración de la cámara.

Figura 2.27. Pantalla de inicio de la Dericam

2.11.3 Instalación de las cámaras

Para la instalación de las cámaras en primer lugar se debe guiar en los planos, para esto se debe verificar si en los lugares a instalar las cámaras se cuenta con alimentación eléctrica de 110v para poder encender las mismas.

Luego de un análisis de campo, se ha podido evidenciar que es necesario realizar obra civil para tener alimentación eléctrica para cada cámara, es por esto, que se han realizado los trabajos necesarios para satisfacer esta necesidad primordial para las cámaras.

Una ventaja de instalar el sistema ha sido los recursos que brinda la institución, la Comunidad Salesiana cuenta con una instalación eléctrica de primer nivel, uno de estos elementos es el generador, el cual funciona al momento de producirse una interrupción de la corriente eléctrica, es por esto que las tomas para las cámaras se deben conectar a los circuitos que tienen respaldo de cortes de energía por medio del generador de corriente. El proceso de instalación es el siguiente:

1. Buscar puntos de alimentación eléctrica con respaldo de cortes eléctricos cerca de los puntos designados para la ubicación de las cámaras. Esta búsqueda se realizó con ayuda del Ing. Holger Baca quien fue el encargado de la implementación de la red eléctrica de la Comunidad Salesiana.

Figura 2.28. Cajas térmicas de la red eléctrica de la UESDS

2. En función del punto 1 se determinan los materiales necesarios para la instalación

    a. Cable eléctrico.
    b. Toma corrientes sobrepuestos.
    c. Cinta aislante

3. Se determina el calibre del cable eléctrico: El calibre del cable eléctrico se lo determina en función de consumo de potencia de cada cámara, revisando en los datasheets que se muestran en la sección anexos se ha determinado que cada cámara consume potencias de alrededor de 8W, multiplicado por el número de cámaras se obtiene alrededor de 24W, luego se debe calcular la corriente con corrección mediante la fórmula:

$$I = \frac{Potencia}{Voltaje \cdot Factor\ de\ potencia}$$

$$I = \frac{24}{120 \cdot 0{,}9}$$

$$I = 0{,}22A$$

$$I\ con\ corrección = I * Factor\ de\ demanda$$

$$I\ con\ corrección = 0{,}22 \cdot 0{,}7 = 0{,}15A$$

Como el consumo de corriente es muy bajo basta con un cable calibre 14 AWG, además este es calibre más bajo que normalmente se puede encontrar en el mercado. [11]

4. Realizar los trabajos eléctricos necesarios para que los puntos de alimentación eléctrica (tomacorriente) estén cerca de cada cámara y de esta manera brindar alimentación eléctrica con respaldo de energía a las mismas.

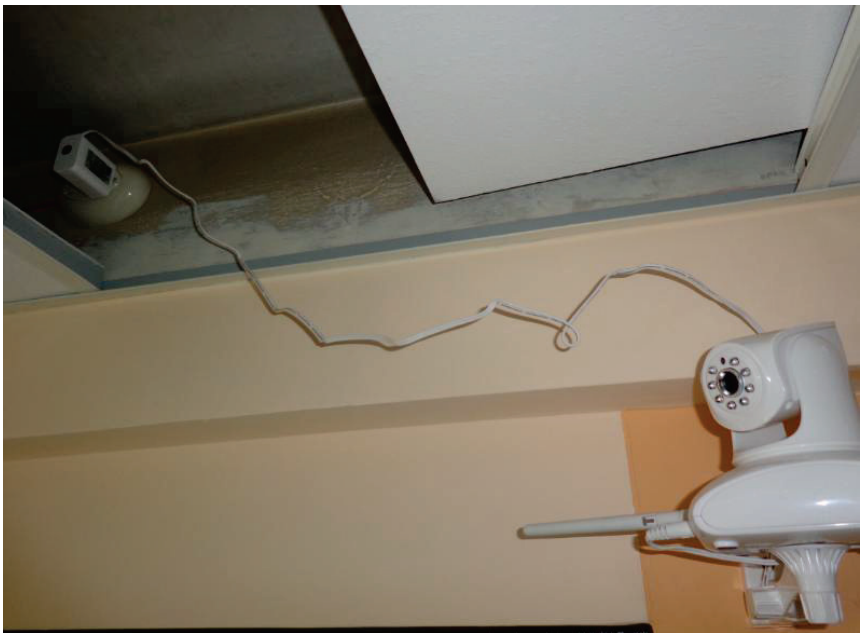


Figura 2.29. Punto de alimentación eléctrica instalado cerca de la cámara

Una vez satisfecha esta necesidad, se procede a la instalación de las cámaras y los resultados se pueden evidenciar en las figuras 2.30, 2.31 y 2.32:

Figura 2.30. Cámara de la Casa Campesina Cayambe

Figura 2.31. Secretaría de la UESDS

Figura 2.32. Entrada de la institución

2.11.4 Configuración final de cada cámara

Luego de que las cámaras se encuentran en los sitios idóneos se procede a configurar las características de cada una desde el computador de control.

2.11.4.1 Cámara Zkteco

Las cámaras ZKteco son cámaras ubicadas en interiores (Casa Campesina y Administración de la UESDS), es por este motivo que se ha considerado lo siguiente:

- Las opciones de vista previa se las colocarán de tal manera que permitan una visualización efectiva, para evitar que las imágenes se tornen lentas se ha configurado la vista previa en un video de segundo flujo **(ver figura 2.23).**

- Se ha configurado una posición preestablecida para cada cámara, esta posición se ha seleccionado buscando el mayor alcance visual y de control.

- Las opciones de audio, video y control PTZ se dejarán las mismas que vienen por default.

- En cuanto a la alarma no se realizará ninguna configuración desde la cámara, la alarma se configurará usando el software de gestión para esta cámara el cual es **ZKiVision; e**l proceso de configuración se detalla a continuación:

    1. Instalar el software en la computadora de control.

    2. Desbloquear el acceso al programa, para esto se debe ingresar una clave suministrada en el manual de este programa.

    3. En la opción configuración buscar las direcciones IP de cada cámara, mediante la opción **Search.**

Figura 2.33.- Buscar las direcciones IP de cada cámara.

4. Una vez detectadas las cámaras se debe generar una red de administración en base a las áreas donde se ubicarán las mismas, de esta manera se puede tener un control de una forma ordenada. Se crea al red UESDS y consta de dos cámaras como se muestra en la figura 2.34:

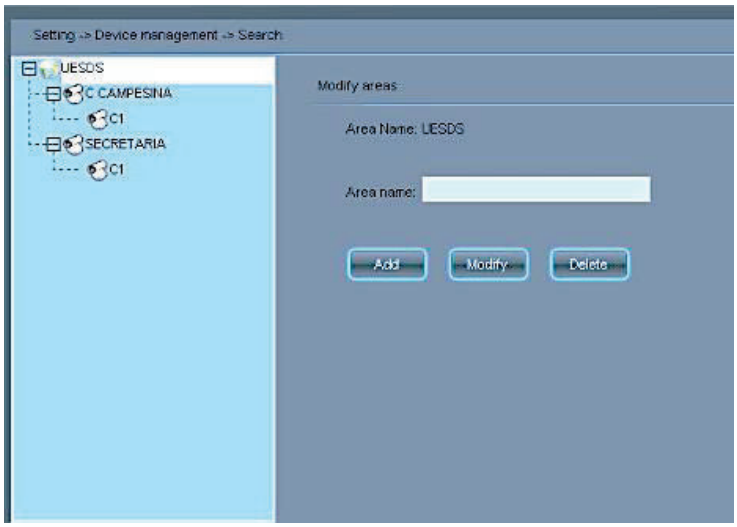


Figura 2.34. Red de administración de las cámaras

5. Para terminar el proceso de agregar las cámaras se debe ingresar los usuarios y contraseñas de acceso a cada una.
6. Luego se comprueba la visualización de cada una de las cámaras.

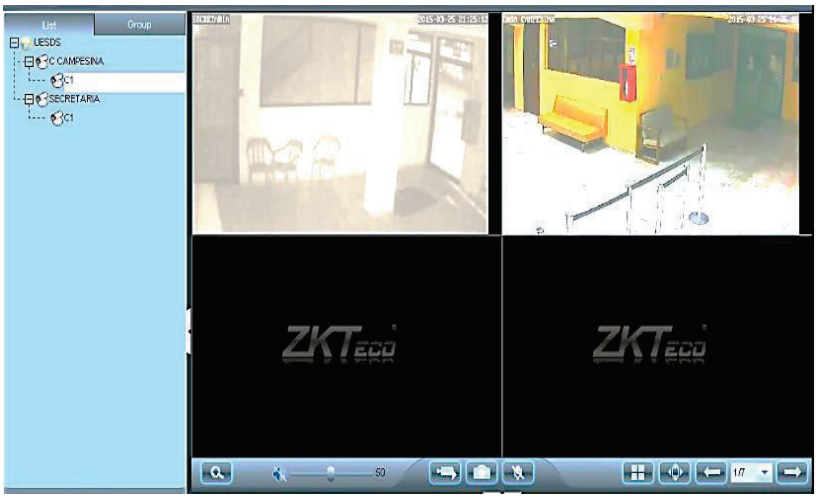


Figura 2.35. Visualización de las cámaras

7. Una vez detectadas las cámaras, se accede a configuración y luego a la opción **motion detection setting,** con esta opción se tiene la posibilidad de crear hasta cuatro ventanas de detección de movimiento y su respectiva sensibilidad. Los cuadros creados para cada cámara se pueden observar en la figura 2.36:

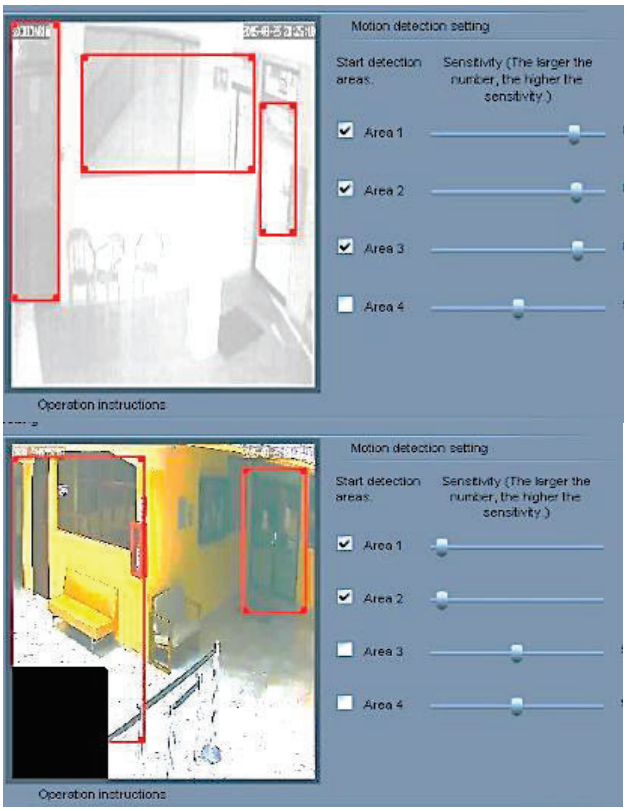


Figura 2.36. Ventanas para la detección de movimiento

8. Seguidamente se va a la opción **alarm setting,** esta opción permite configurar el tipo de alarma y las acciones que realizará al activarse la misma, se seleccionará la opción detección de movimiento y la acción a realizar es grabación de video, esta opción permite configurar los horarios de alarma.

   a. Las grabaciones accionadas por detección de movimiento serán en los horarios de menos concurrencia a la institución, en la noche y madrugada, esto con el objetivo de crear una herramienta de prevención en el caso de algún problema de inseguridad en la noche o madrugada, puesto que al accionarse la alarma se enviará un email a las autoridades.

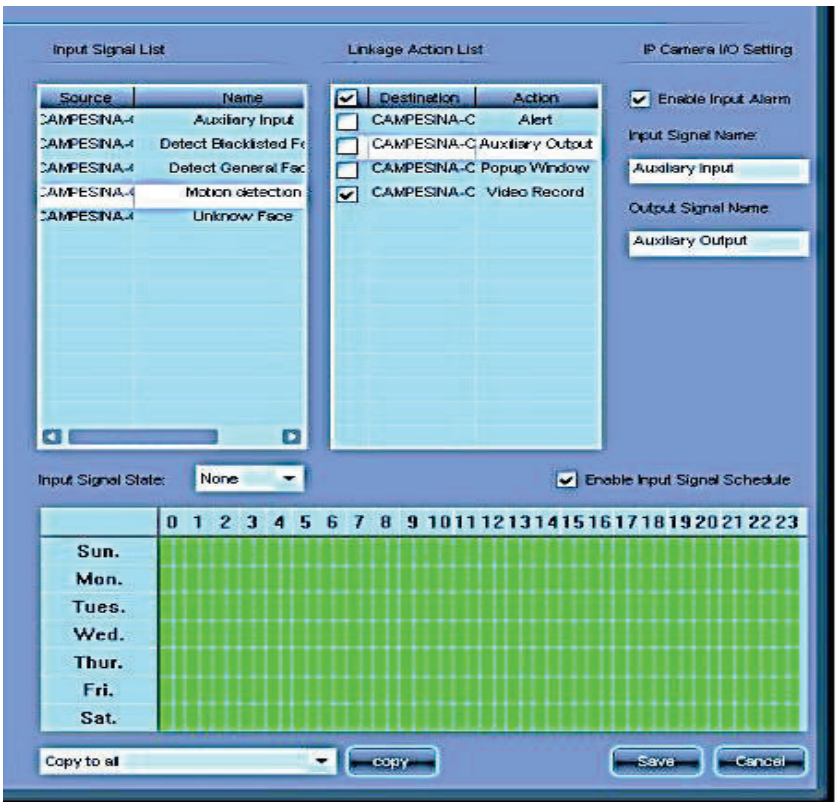


Figura 2.37. Configuración de la grabación por detección de movimiento.

9. Para concluir se debe acceder a la ventana de visualización y en el área creada para las cámaras (UESDS), dar clic izquierdo y seleccionar la opción **All arming,** esta opción activa el monitoreo de las cámaras con las opciones antes configuradas.

Figura 2.38. Activación del monitoreo de todas las cámaras

10. Al realizar las pruebas pertinentes como: la verificación de que las grabaciones se efectúen al detectar de movimiento, verificación de grabaciones se efectúen en los horarios establecidos, acceso remoto desde un computador o smartphone y demás pruebas, se evidencia que el sistema funciona de forma eficiente, al activarse la alerta de detección de movimiento empiezan las grabaciones con una duración de 120 segundos, las grabaciones se almacenan en la unidad "D" en la carpeta "Media Record" la misma que posee carpetas de cada cámara con las fechas de cada grabación.

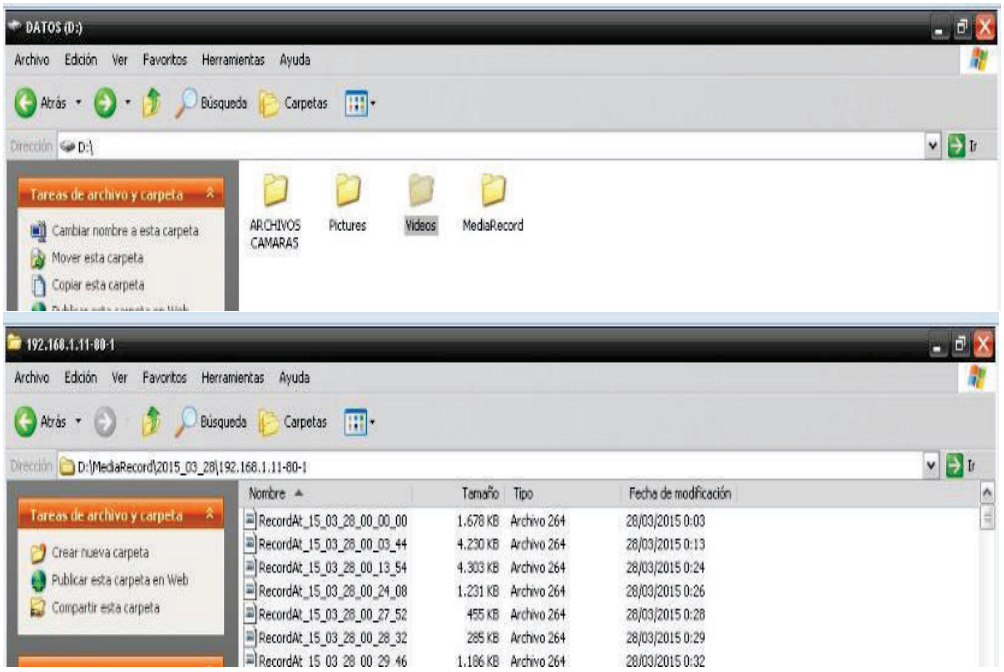


Figura 2.39. Almacenamiento de grabaciones en la unidad D

- En la configuración de red no se realiza ningún cambio puesto que toda la configuración inicial.

- En la configuración avanzada se debe realizar el proceso de configuración de envío de correos electrónicos al activarse la alarma por detección de movimiento, esta configuración tiene por objetivo crear una herramienta de prevención en el caso de presentarse alguna eventualidad de seguridad en especial en los horarios de la noche y madrugada, cabe destacar que a pesar de no ser una herramienta efectiva ayudará de alguna forma a prevenir o solucionar un problema de este tipo. El proceso de configuración se detalla a continuación:

1. Habilitar la opción de envío de correos electrónicos.

Figura 2.40. Habilitar envío de notificaciones por correo electrónico

2. Creación del correo electrónico, se ha creado el correo electrónico **camaras.alerta2014@gmail.com** desde el cual se enviarán los mensajes de notificación a las autoridades institucionales.

3. Configuración del correo en la cámara, para lograr esto se debe completar la información ahí sugerida, esta información no genera mayores inconvenientes lo único que se debe conocer es el servidor SMTP y el puerto del correo electrónico creado. En la figura 2.41 se detalla mejor esta configuración.

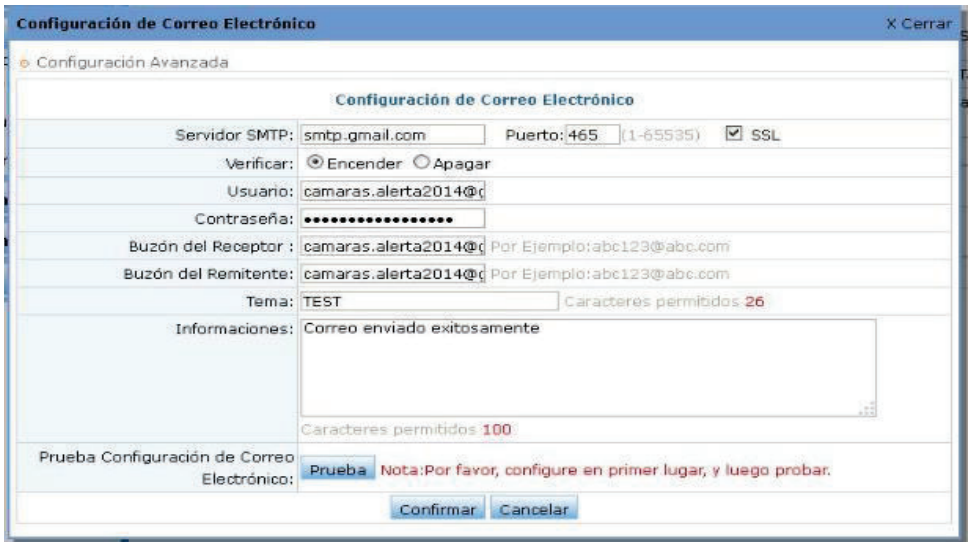


Figura 2.41. Configuración de correo electrónico de las cámaras.

Una vez confirmado el funcionamiento del envío de alertas por correo electrónico se presenta el cuadro de las personas quienes se enviarán estas notificaciones:

CÁMARA	AUTORIDAD
ZONA 2 (Casa Campesina)	Ing. Ana María Arroyo
ZONA 3 (Secretaría)	Lic. Byron Campoverde

Tabla 2.14. Autoridades que recibirán notificaciones de correo electrónico

- Las grabaciones se almacenarán por un periodo de 5 días, luego de esto las grabaciones se copiarán a dispositivos de almacenamiento externo, con la finalidad de liberar el espacio del disco duro del computador de almacenamiento.

- La configuración para grabación permanente que se realizará en los horarios de mayor afluencia a la institución es bastante sencilla y se la realiza mediante el programa de gestión, este proceso se detalla a continuación:

    1. Se debe acceder a la opción **schedule recording,** del software de control y seleccionar los horarios en los que se desee la grabación permanente.

Figura 2.42. Programación de los horarios de grabación continúa para cada cámara.

- Las pruebas realizadas evidencian el correcto funcionamiento de las grabaciones continuas, las grabaciones se almacenan en la unidad "D", para diferenciar las grabaciones continuas de las de detección de movimiento lo único que varía es el nombre del archivo.

- En sistema se debe configurar la fecha y hora, para facilitar esto se debe seleccionar la opción **sintonizar el tiempo de red con el servidor,** al seleccionar esta opción la hora se configura automáticamente.

- Otra característica a configurar son las contraseñas de cada uno de los tres usuarios que existen.

Hay que aclarar que la configuración desarrollada anteriormente es la misma para las cámaras de las zonas 2 y 3 (Casa Campesina y Administración de la UESDS)

2.11.4.2 Cámara Dericam

La Dericam es una cámara ubicada exteriormente (Entrada Principal UESDS) es por este motivo que se ha considerado la siguiente configuración:

- La calidad de video se seleccionará la opción **outdoor,** la cual es ideal al ubicar la cámara en el exterior.

- La posición de la cámara se la realiza de forma manual puesto que esta cámara no posee control PTZ.

- En la configuración de red no se realiza ningún cambio puesto que se realizó la misma al inicio.

- Como ya se había indicado la cámara grabara al detectar movimiento para ahorrar espacio de almacenamiento en el disco, esta configuración se la realiza mediante el software antes detallado para esta cámara que es el Master; el proceso de configuración se detalla a continuación:

1. Instalar el software en el computador de control.
2. Desbloquear el acceso mediante una clave, usualmente para iniciar es lo mismo que el usuario.
3. Seleccionar la opción **Add,** para detectar la dirección IP de la cámara.

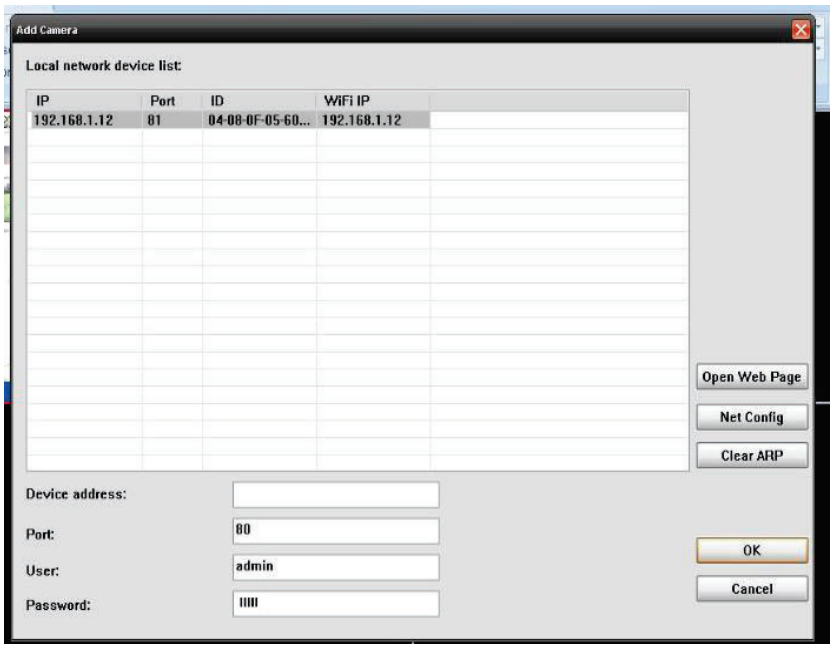


Figura 2.43. Detección de la dirección IP de la cámara.

4. Para una detección correcta se debe ingresar el usuario y la clave de acceso a la cámara.

5. Seguidamente se accede a la visualización de la cámara y se da clic izquierdo en la misma, desplegándose un menú del cual se escoge la opción **system option,** esta opción permite configurar varios parámetros, se selecciona la pestaña alarma y se habilita la grabación por alarma.

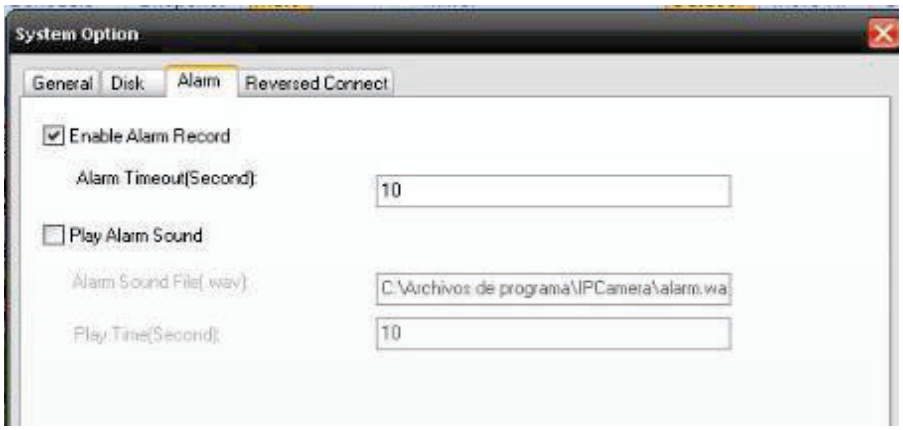


Figura 2.44. Habilitación de las grabaciones accionadas por la alarma.

6. De igual forma que las otras cámaras se habilitará la grabación por detección de movimiento de forma permanente, a excepción de los horarios de mayor recurrencia a la institución, esta configuración se debe realizar desde la cámara.

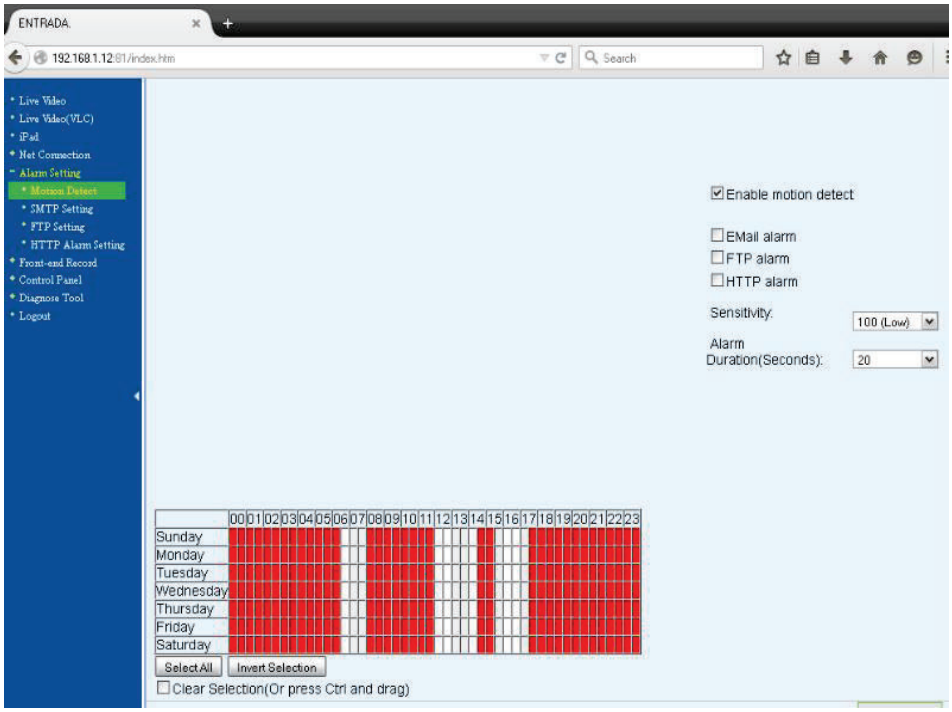


Figura 2.45. Horarios para la detección de movimiento, programado desde la cámara.

7. Una vez guardadas todas las configuraciones realizadas, se ha probado la funcionabilidad de las mismas y se ha podido evidenciar que las grabaciones se realizan de forma adecuada por un lapso de 60 segundos en la unidad "D" en la carpeta "video", los archivos están organizados en carpetas por fechas como se muestra en la figura 3.14.

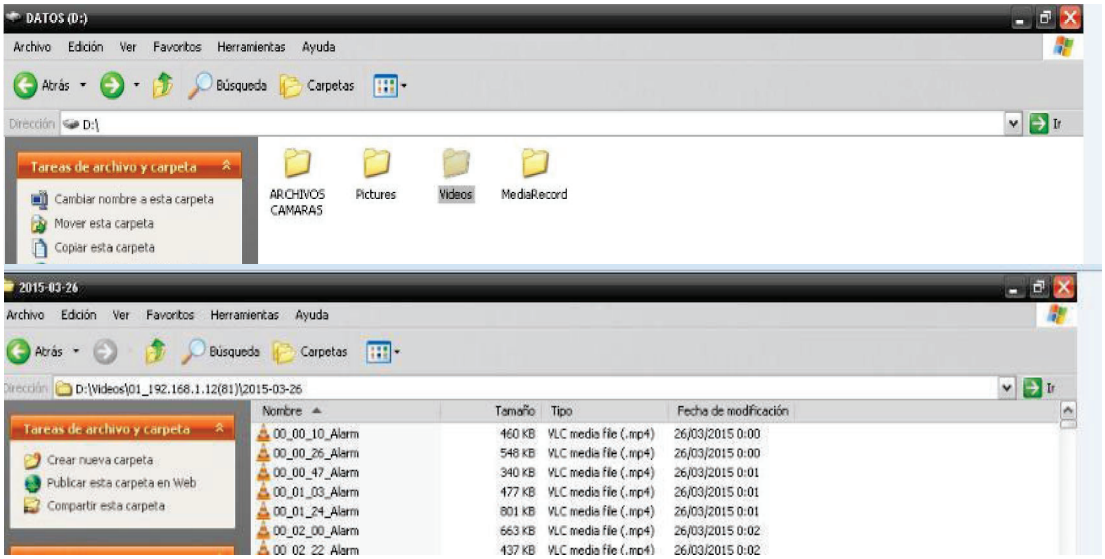


Figura 2.46. Almacenamiento de las grabaciones

- En el inicio y fin de las grabaciones se configura de las misma forma que la cámara ZKTeco es decir considerando la opción Schedule recording y se programa los horarios de grabación permanente.
- En esta cámara no se activará el envío correos electrónicos al activarse la alarma por detección de movimiento puesto que es una cámara exterior y las alertas pueden resultar falsas y ocasionaría problemas.
- En el panel de control no se hacen mayores cambios, lo que se debe considerar es la creación de usuarios, para un mejor control son los mismos de las cámaras Zkteco (**Ver tabla 2.13**) y sus respectiva contraseñas.
- Es importante la configuración de fecha y hora, para facilitar esta configuración solo basta con seleccionar la opción de sintonizar con el servidor NTP.

Una vez terminada la configuración de todas las cámaras se procede a realizar pruebas para verificar su correcto funcionamiento, estas pruebas se desarrollarán en el capítulo tres de este proyecto.

2.12 Resumen general de la red implementada

A continuación se muestra un resumen de los distintos parámetros de configuración de la red.

N° CÁMARA	MARCA CÁMARA	ZONA DE UBICACIÓN	DIRECCIÓN IP CÁMARA	PUERTO CÁMARA	PUERTO EXTERNO (ACCESO REMOTO)
CÁMARA 1	ZKTeco	ZONA 2	192.168.1.10	80	10001
CÁMARA 2	ZKTeco	ZONA 3	192.168.1.11	80	10002
CÁMRA 3	Dericam	ZONA 1	192.168.1.12	81	10003

Tabla 2.15. Resumen de las direcciones IP de cada cámara.

N°CÁMARA	MARCA CÁMARA	DETECCIÓN DE MOV.	ALMACENAMIENTO
CÁMARA 1	ZKTeco	SI	Al detectar movimiento y permanente en cierto horario
CÁMARA 2	ZKTeco	SI	Al detectar movimiento y permanente en cierto horario
CÁMARA 3	Dericam	SI	Al detectar movimiento y permanente en cierto horario

Tabla 2.16. Resumen de la configuración de cada cámara.

3 PRUEBAS, RESULTADOS Y COSTOS

3.1 Introducción

En el presente capítulo se realizarán varias pruebas, con la finalidad de verificar el correcto funcionamiento de las cámaras, en base a los resultados se tomarán los correctivos necesarios. Otro punto a tomar en cuenta es la elaboración de un manual para el manejo adecuado de las cámaras. Para terminar se presentarán los costos requeridos para implementar este proyecto.

3.2 Pruebas

Las pruebas que se realizarán serán las siguientes:

- Alcance de visualización de las cámaras.
- Acceso remoto vía Internet y atributos de usuario.
- Grabaciones al detectar movimiento.
- Envío de emails de alerta.
- Amenazas a la red

3.2.1 Alcance de visualización

Una parte importante de este proyecto de titulación es el alcance de visualización que tienen las cámaras, cuyo objetivo es evitar puntos ciegos y maximizar la eficiencia del sistema de cámaras. En las figuras 3.1, 3.2 y 3.3 se muestran las posiciones preestablecidas de cada una de las cámaras:

ZONA 1:

Figura 3.1. Alcance de visualización de la cámara exterior, entrada de la institución.

ZONA 2:

Figura 3.2. Visualización de la cámara en la Casa Campesina Cayambe.

ZONA 3:

Figura 3.3 Visualización de la cámara en la Secretaría de la UESDS.

3.2.1.1 Correctivos en el alcance de visualización

Las imágenes no evidencian puntos ciegos y en el caso de haberlos las cámaras de la zona 1 y 2 tienen opción de movimiento con lo que se puede solucionar esta limitación.

3.2.2 Acceso remoto vía Internet y atributos de usuario

Una de las utilidades propuestas al instalar las cámaras, es el acceso a las mismas de forma remota, para esto únicamente es necesario un equipo (PC, Smartphone o tablet) que tenga acceso a Internet.

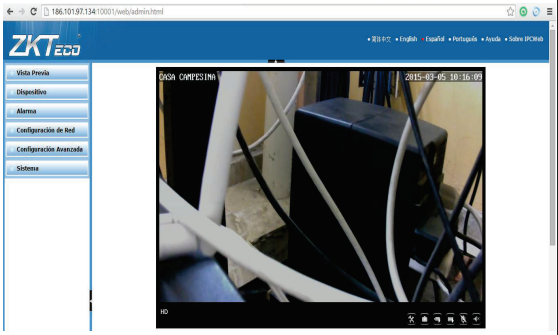
Por motivos de seguridad se han creado usuarios, los cuales se detallan a continuación:

- Admin
- User
- Guest

Cada uno con sus atribuciones las cuales se detallan en la **tabla 2.13** del capítulo dos.

Para acceder a las cámaras, cada usuario debe conocer la dirección IP de acceso la cual es **186.101.97.134** además del puerto respectivo para cada cámara, esto se detalla de mejor manera en la **tabla 2.12** del capítulo dos.

En la siguiente tabla se visualizarán las pruebas de acceso a las cámaras con los distintos usuarios y en dos tipos de equipos (PC y Smartphone).

EQUIPO	USUARIO	IMAGEN	DETALLE
PC	admin		Al acceder desde una PC, primero se debe instalar los controladores de la cámara y acceder mediante la opción “vea el video”. Como se ve en la imagen no se tiene ningún inconveniente al acceder a la cámara vía Internet. Al acceder como administrador se tiene acceso a todas las opciones de configuración

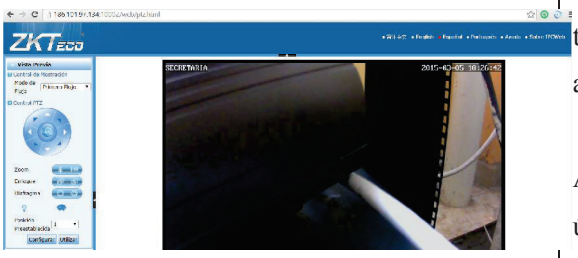
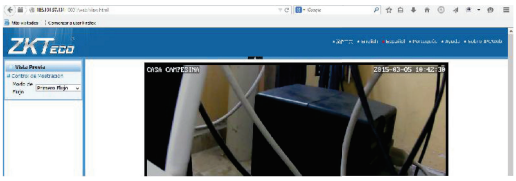
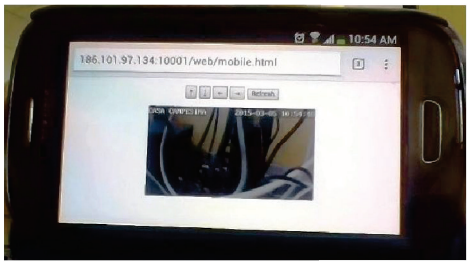
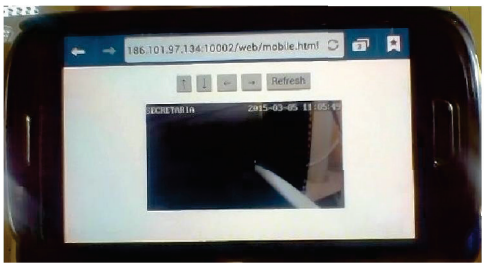
	user		Como se ve en la imagen no se tiene ningún inconveniente al acceder a la cámara vía Internet. Al acceder como usuario únicamente se tiene acceso al control PTZ de la cámara.
	guest		Como se ve en la imagen no se tiene ningún inconveniente al acceder a la cámara vía Internet. Al acceder como invitado únicamente se tiene acceso a la vista previa.
SMARTPHONE	user		Al acceder desde un Smartphone o tablet es importante seleccionar la opción “de vigilancia móvil”, puesto que esta opción muestra un video de baja resolución ideal para equipos móviles. Como se ve en la imagen no se tiene ningún inconveniente al acceder a la cámara por medio de Smartphone o tablet. Al acceder como usuario se permite el control PTZ como atributo
	guest		Como se ve en la imagen no se tiene ningún inconveniente al acceder a la cámara por medio de Smartphone o tablet. Al acceder como invitado solo se tiene acceso al video, en la imagen se puede ver los controles PTZ pero estos no realizan ninguna acción.

Tabla 3.1. Acceso vía Internet en distintos dispositivos y atribuciones de usuario

3.2.2.1 Correctivos en el acceso remoto a las cámaras

Se ha comprobado que se puede acceder a las cámaras sin ningún inconveniente y además las atribuciones de usuario son correctas.

El problema que se presentó fue al acceder recurrentemente, el navegador de Internet (en ciertas ocasiones) borra las opciones iniciales de acceso. La solución para este problemas es limpiar el historial de navegación y luego acceder a la cámara.

Otro problema que se podría presentar es que el video se vea lento o que los comandos de movimiento PTZ no funcionen adecuadamente, esto se debe a la velocidad de la conexión a Internet.

En el caso de no poseer una conexión a internet de alta velocidad, se soluciona este problema accediendo a las cámaras con la opción "de vigilancia móvil" puesto que presenta un video de menor calidad.

3.2.3 Grabaciones al detectar movimiento

La detección de movimiento y las grabaciones que efectúan cada cámara en estas condiciones funcionan de forma correcta sin ningún problema el único inconveniente es la limitada memoria RAM y el poco espacio de almacenamiento del PC de control.

Este problema se ha socializado con las autoridades y supieron manifestar que no hay más presupuesto para el mejoramiento de estos limitantes, es por esto que se ha solicitado dar una solución efectiva a este problema con los recursos ya existentes.

Al realizar pruebas se evidenció un problema relacionado con la sensibilidad de los detectores de movimiento, puesto que hay muchas grabaciones realizadas en horas de la madrugada que no presentan ningún movimiento aparente o evidenciable lo cual carga al disco duro de almacenamiento de grabaciones inservibles.

3.2.3.1 Correctivos en la detección de movimiento

Para solventar el problema de los detectores de movimiento se ha bajado la sensibilidad de los mismos ubicándolos en un valor menor que el 50% del total, para nuestro caso se operará a una sensibilidad de 25, esto se realiza en la opción de creación de las ventanas de detección de movimiento del software de gestión como se evidencia en la figura 2.36 del capítulo dos del presente proyecto.

En cuanto al almacenamiento se debe liberar el espacio de grabaciones en el plazo establecido de 5 días en forma rutinaria, considerando que las grabaciones están configuradas para realizarse al detectar movimiento se pueden realizar la liberación de disco hasta cada 8 días, además hay que considerar que en el caso de suscitarse un evento en cuanto a la seguridad institucional se debe informar al encargado del control del sistema de forma oportuna para almacenar las grabaciones de dichos eventos en discos externos.

3.2.4 Envío de email de alerta

Se han realizado varias pruebas y el detalle de las mismas se presenta a continuación:

1. Para realizar esta prueba se debe habilitar la detección de movimiento y simplemente generar movimiento por las ventanas habilitadas, luego se accede al correo electrónico del receptor (por ser una prueba se ha enviado al mismo email) y evidenciar que el email se ha enviado exitosamente. Esto se apreciar mejor en la siguiente imagen.

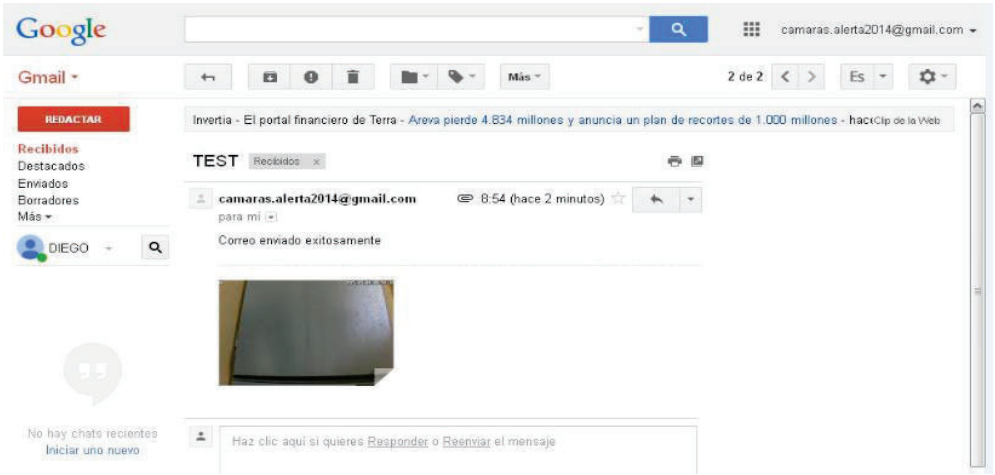


Figura 3.4. Email recibido desde las cámaras al detectar movimiento

Como se puede evidenciar en la figura 3.4 los correos electrónicos se envían de forma adecuada lo único que se debe realizar es la modificación de destinatarios basados en la tabla 2.14 para que así los correos electrónicos se remitan a las autoridades competentes.

3.2.4.1 Correctivos para el envío de correos electrónicos

Al realizar las pruebas del envío de correos electrónicos se presentó un problema, el cual consistía en que la cuenta Gmail creada bloqueaba el acceso a la cámara para el envío de los correos de alerta, puesto que consideraba que se estaba accediendo a la cuenta de Gmail de una forma fraudulenta. El equipo de Gmail manda un mensaje advirtiendo que se ha accedido a la cuenta y preguntan si el usuario es el dueño de la cuenta, caso contrario, la cuenta será bloqueada.

Para corregir este inconveniente se deben tomar las siguientes acciones en la configuración de la cuenta:

- Responder el email remitido por el equipo Gmail, confirmando que quien ha accedido a la cuenta es el dueño.
- Acceder a la cuenta y configurarla con las siguientes características:

    - Habilitar correos de tipo POP y POP 3
    - Deshabilitar los filtros.
    - Permitir aplicaciones consideradas como peligrosas.

Luego de realizar los pasos antes mencionados se solventa el inconveniente presentado.

3.2.5 Amenazas a la red

En esta prueba se considera dos tipos de amenazas: físicas o informáticas. Las físicas hacen referencia a posibles daños que pueda sufrir la red implementada de forma estructural es decir cortes de energía eléctrica ocasionados, vandalismo en las cámaras, daños accidentales.

En cuanto a las amenazas informáticas se hace referencia a ataques de hackers que deseen tener acceso a las cámaras.

En la tabla 3.2 se presentan las posibles amenazas que puede presentar la red de cámaras de seguridad implementadas.

AMENAZA	DETALLE DE AMENAZA	LINEAMIENTO A SEGUIR
FÍSICA	Corte intencional de energía eléctrica	• Ubicar las cámaras en un lugar de difícil acceso para su manipulación. • Conectar las cámaras a un circuito eléctrico con respaldo de energía, para este caso se ha conectado a un generador que brinda energía al momento de ocasionarse un corte eléctrico.
	Vandalismo	A esta amenaza no se le puede dar una solución definitiva, se podría considerar la ubicación de las cámaras como solución o incluso el hecho de que las cámaras almacenan todas las grabaciones, pero el vandalismo en el caso de suscitarse no tiene solución efectiva.
	Daños accidentales	Tampoco habría mayores correctivos a realizar puesto que un accidente no es corregible pero si evitable, para esto último considerar: • Ubicación idónea de las cámaras. • Instalaciones eléctricas bien realizadas. • Para el sistema implementado se evidencia una amenaza en la cámara exterior(zona 3), pues a pesar de que sus características le permiten estar a la intemperie, el agua es un factor ambiental que no soporta, motivo por el cual se ha colocado una visera sobre la cámara para garantizar que no sufra un daño accidental por esta causa, esto se evidencia en la figura 2.32

INFORMÁTICA	Hackers	La red debe ser implementada de forma independiente, para este sistema de cámaras se generó una nueva red muy aparte de la red institucional. Limitar el acceso de usuarios a la red mediante las opciones del Router, en esta red se ha limitado el acceso a la red a cinco usuarios como se muestra en la figura 2.15. Crear claves de acceso consideradas seguras que cuenten con caracteres alfabéticos, numéricos y de ser posible símbolos. Configurar el router con un cifrado WPA o WPA2 que son considerados seguros, en el presente sistema se consideró el cifrado WPA2 como se puede evidenciar en las figuras 2.17 a 2.19 En el caso de ser necesario configurar en el router las direcciones MAC de los equipos que pueden acceder a la red.

Tabla 3.2. Amenazas a la red

Cada una de las amenazas antes mencionadas como se indica en la tabla 3.2 han sido solventadas para el correcto funcionamiento del sistema, todos estos detalles han sido probados y funcionan de forma correcta.

Todas las pruebas realizadas en los puntos anteriores evidencia la eficiencia de la red de cámaras de seguridad implementada puesto que garantizan una correcta configuración y funcionamiento de la red, ahora bien todos los problemas presentados se han solventado de forma puntual, pero eso no garantiza que se presenten nuevos inconvenientes los mismos que deben irse solventado en el caso de que estos se susciten por personal calificado.

3.3 Manual de Usuario

Como se ha mencionado anteriormente se han creado tres usuarios (admin, user y guest) los cuales pueden acceder a las cámaras, para el correcto uso de las mismas se detallarán varios parámetros y normas las cuales serán socializadas a las autoridades institucionales.

3.3.1 Sistema

El sistema de cámaras instalado consta de tres cámaras, dos interiores y una exterior, cuya implementación se basa en la necesidad de crear una herramienta de control y prevención en cuanto a las necesidades de seguridad de la Comunidad Salesiana de Cayambe, en particular a de la Unidad Educativa Salesiana "Domingo Savio" y la Casa Campesina Cayambe.

El sistema realiza acciones de videovigilacia y almacenamiento de grabaciones de forma periódica, detecta movimiento y envía alertas tempranas en caso de eventualidades a correos electrónicos, además permite la visualización de video en vivo desde PC´s o Smartphones de forma remota con una conexión a Internet.

Para acceder a cada una de las cámaras se debe conocer la dirección IP de acceso y el puerto correspondiente a cada cámara, además de usuario y clave de acceso.

3.3.2 Usuarios

Los usuarios son las personas que pueden acceder a las cámaras con su respectiva clave de autentificación, estos usuarios puede ser de tres tipos:

3.3.2.1 Administrador

Es la persona encargada de implementar, configurar, mantener, monitorizar, documentar y asegurar el correcto funcionamiento de un sistema de cámaras implementado. El administrador posee acceso a todas las opciones de configuración de la cámara.

3.3.2.2 Usuario

Es la persona que puede acceder a la cámara pero solo tiene acceso a la visualización en vivo de la cámara y el control de movimiento de la misma.

3.3.2.3 Invitado

Es la persona que únicamente tiene acceso a la visualización del video en vivo de las cámaras.

3.3.3 Acceso a las cámaras

Para acceder a las cámaras ya sea desde una PC o Smartphone se debe abrir un navegador de Internet e ingresar la siguiente dirección **186.101.97.134: puerto.** El puerto por cada cámara se detalla en la tabla 3.4.

CÁMARA	PUERTO
ZONA 1 (ENTRADA PRINCIPAL)	10003
ZONA 2 (CASA CAMPESINA)	10001
ZONA 3 (SECRETARÍA UESDS)	10002

Tabla 3.3. Cámaras con su respectivo puerto de acceso

Ejemplo:

Figura 3.5. Forma de ingresar la dirección IP de acceso.

Luego de ingresar la dirección IP aparece un cuadro de diálogo el cual solicita ingresar usuario y contraseña.

Ejemplo:

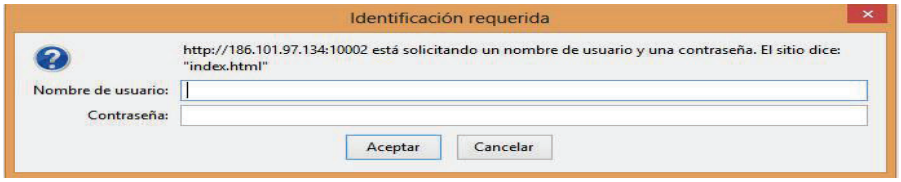


Figura 3.6. Cuadro de diálogo para ingreso de usuario y contraseña

A continuación se verá una ventana de inicio la cual muestra tres opciones:

- **"Vea el video":** Permite acceder a todas las opciones de configuración y control de la cámara.

- **"De vigilancia móvil":** Muestra un video de baja calidad el cual es idóneo para accesar desde un Smartphone.
- **"Instale software (primer uso)":** Esta opción permite descargar e instalar el software de visualización de cada cámara, esta opción se usa la primera vez que se accede a una cámara desde un computador.

Ejemplo:

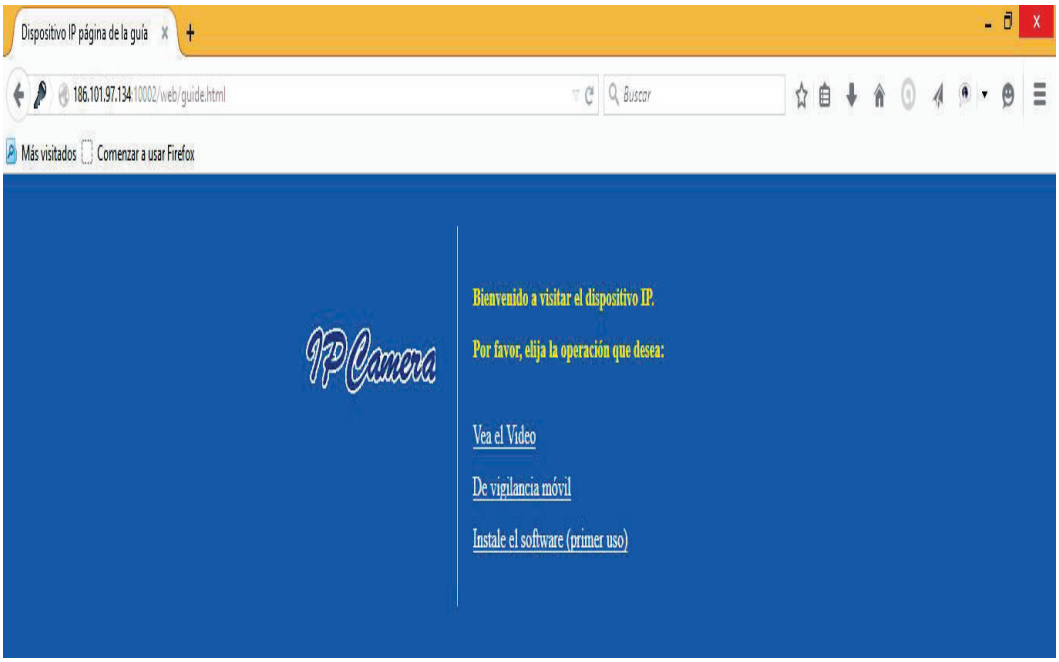


Figura 3.7. Ventana inicial con las opciones de acceso.

Finalmente se selecciona la opción conveniente según el equipo por el cual se está accediendo a las cámaras y se podrá visualizar el video con los atributos de acuerdo al usuario con el que se ha ingresado a las cámaras.

3.3.4 Cerrar sesión

Es muy importante que antes de cerrar la sesión se deje la cámara en la posición preestablecida inicial (en el caso de haber ingresado como administrador o usuario y haber movido las cámaras), para garantizar este particular se debe dar clic en el botón **utilizar,** el mismo que se encuentra al final de la barra de herramientas, de esta manera la cámara automáticamente regresará a la posición original.

Figura 3.8. Botón UTILIZAR para regresar la cámara a la posición preestablecida.

Una vez ubicada la cámara en la posición original solo basta con cerrar el navegador de internet.

NOTAS:

1. En el caso de no poseer Internet de una buena velocidad, se puede acceder a las cámaras con la opción **"De vigilancia móvil"** desde un computador y se evitan inconvenientes.
2. Al acceder recurrentemente a las cámaras, suele suceder, que luego de ingresar el usuario y contraseña la ventana inicial aparece sin las opciones descritas anteriormente. Para solucionar este inconveniente solo basta con borrar el historial del navegador web y volver a cargar la página.

3.4 Análisis de costos

Con la finalidad de tener una noción del costo de implementación del presente proyecto se realizará un estudio con los costos de los equipos utilizados y los gastos que genera la operación del mismo.

Para determinar los costos que conlleva realizar el proyecto, es necesario saber de manera aproximada el beneficio que se tendrá con la implementación del mismo, para esto se debe conocer los costos directos e indirectos ligados al proyecto y estimar los beneficios que genera la ejecución del proyecto.

3.4.1 Costos directos

Los costos directos que intervienen en este proyecto son:

- Costo de equipos (una sola vez)
- Costo de elementos de instalación (una sola vez)
- Costos de mensuales para la funcionalidad de la red
- Costos de mejoramiento del sistema (una sola vez)

El detalle de estos costos se realiza a continuación:

3.4.1.1 Costo de equipos

Los equipos que se adquirieron para la implementación fueron las cámaras y el router. El computador fue reutilizado del departamento de software por lo que no se considera para este cálculo.

PRODUCTO	CANTIDAD	VALOR UNITARIO	VALOR TOTAL
Cámara ZKTeco, modelo ZKPT531	2	119,00	238,00
Cámara Dericam modelo H216W	1	107,00	107,00
Router LINKSYS modelo E900	1	49,11	49,11
		SUBTOTAL	394,11
		IVA 12%	47,29
		TOTAL	441,40

Tabla 3.4. Costo total de los equipos

3.4.1.2 Costo de los elementos de instalación

Como se detalló en el capítulo dos, se realizaron instalaciones eléctricas para brindar alimentación electica de 110V para las cámaras, los costos se detallan a continuación:

PRODUCTO	CANTIDAD	VALOR UNITARIO	VALOR TOTAL
Cable flexible 14AWG	30 metros	0,40	12,00
Toma corrientes sobrepuestos	3	1,92	5,76
Canaletas	1	1,07	1,07
Cinta aislante	1	0,54	0,54
		SUBTOTAL	19,37
		IVA 12%	2,32
		TOTAL	21,69

Tabla 3.5. Costo total de elementos para la instalación eléctrica

3.4.1.3 Costo mensual del mantenimiento

Se han considerado dos pagos mensuales que son el servicio de internet y el consumo eléctrico, esto último se detalla a continuación:

- **Costo mensual del consumo eléctrico del sistema:**

  Para realizar este cálculo se debe conocer la potencia eléctrica de los equipos que operan el sistema: 3 cámaras, router y computador.

  - Cámaras en promedio consumen alrededor de 8W.[7]
  - Router en promedio consume alrededor de 8W.[8]
  - Computador en promedio consume alrededor de 200W.[9]

[7] Revisar anexos B y C
[8] Revisar anexo A
[9] Trucopei Blog, obtenido de "*https://juantrucupei.wordpress.com/2011/08/16/64/*"

Por lo tanto la potencia eléctrica total de sistema sería de 232W. Seguidamente debemos calcular el consumo de energía del sistema mediante la fórmula:

$$E = Potencia(KW) \cdot Tiempo(h)$$
$$E = 0{,}232\ KW \cdot 24h$$
$$E = (5{,}568\ KWh\ /\ día) \cdot 30\ días$$
$$E = 167{,}04 KWh\ /mes$$

El costo del consumo eléctrico se lo realiza consideramos el precio actual del consumo de energía en (KWh) en el Ecuador el cual es de 9,33ctv por lo tanto:

$$Costo\ de\ consumo\ eléctrico\ mensual = 167{,}04 KWh/mes \cdot 0{,}0933\ \$/KWh$$

$$Costo\ de\ consumo\ electrico\ mensual = 15{,}58\ \$\ /mes$$

PRODUCTO	CANTIDAD	VALOR UNITARIO	VALOR TOTAL
Servicio mensual de Internet	1	26,79	26,79
Consumo eléctrico	1	15,58	15,58
		SUBTOTAL	42,37
		IVA 12%	3,22
		TOTAL	45,59

Tabla 3.6. Costos mensuales del proyecto

3.4.1.4 Costos de mejoramiento del sistema

Hay que considerar que para este proyecto no consta la adquisición de un computador de mejores características, un UPS y una memoria externa de almacenamiento, puesto que estos equipos fueron facilitados por la institución.

Para tener una idea clara del costo real de un proyecto de estas características, se ha considerado el costo en el mercado de los equipos antes mencionados

EQUIPO	VALOR
COMPUTADOR BÁSICO	600,00
UPS	100,00
DISCO EXTERNO DE 1 TERABYTE	100,00
TOTAL	800,00

Tabla 3.7. Costos adicionales de proyecto

La sumatoria de los costos directos antes detallados da como resultado el total de costos directos cuyo valor es de **1 308,68 $**

3.4.2 Costos indirectos

Este tipo de costos son intangibles y difíciles de calcular por ende, no dan efectividad en cuanto a su apreciación por lo que no se considerarán en el presente análisis de costos.

3.4.3 Costo estimado del proyecto

La sumatoria de los costos directo e indirecto permiten conocer los costos estimado de muestro proyecto, dicho costo es de **$ 1 308,68**

3.4.4 Estimación de beneficios

Este cálculo no es tan fiable pero da una idea clara de los beneficios que brindará la implementación del proyecto, para ello se han considerado:

BENEFICIO	ESTIMACIÓN MONETARIA
Confianza en todo el personal que labora en la UESDS por lo que no se requiere contratar empresas de seguridad grandes, basta con un guardia y el conserje de la institución.	$ 7 200

Evitar y controlar el mal uso de los bienes institucionales como son los vehículos, logrando ahorro de combustible y mantenimiento de los mismos	$ 800
Controlar daños realizado en contra de la infraestructura de la institución logrando una ahorro en el mantenimiento de la misma.	$ 500
Controlar que los trabajadores de la UESDS y la Casa Campesina Cayambe cumplan con las 8 horas de trabajo	$ 500
MONTO DE BENEFICIOS TOTALES	**$ 9 000**

Tabla 3.8. Monto de beneficios totales al implementar el sistema

3.4.5 Decisión final

La decisión final se la realiza comparando los beneficios contra los costos y como se puede evidenciar los beneficios superan por mucho los costos del proyecto, cabe destacar que los beneficios son estimados, por lo tanto el proyecto: diseño e implementación de una red de cámaras de seguridad inalámbricas para la Unidad Educativa Salesiana “Domingo Savio” es viable y una gran decisión.

4 CONCLUSIONES Y RECOMENDACIONES

4.1 Conclusiones

- Los sistemas de video vigilancia son una herramienta de seguridad muy útil, puesto que satisfacen necesidades primordiales de todo negocio, empresa u hogar, las cuales son: salvaguardar bienes y generar una herramienta de prevención y control.

- La Comunidad Salesiana Cayambe utilizará este sistema de video vigilancia para generar una herramienta de seguridad que permita monitoreo, control, detección oportuna de eventualidades y almacenamiento de las mismas para la toma de decisiones, sin que se instale un centro de control permanente del sistema.

- Las cámaras utilizadas en la implementación del presente proyecto: ZKTeco y Dericam son herramientas que permiten un abanico inmenso de prestaciones para operar un sistema de seguridad sin la necesidad adquirir un software compatible para las dos marcas, el software de cámara brinda todas las opciones necesarias para hacer de dos simples cámaras todo un sistema de seguridad eficiente.

- La oferta de cámaras de seguridad en el mercado es inmensa, con cámaras de variadas características, las cámaras seleccionadas ZKTeco y Dericam son de un nivel medio, pero basta este nivel para cumplir características requeridas para el sistema, al final lo que va a mandar en la selección de un equipo siempre será la capacidad adquisitiva de la persona o empresa que va a implementar la cámara.

- El acceso remoto vía web incorporado al sistema facilita las acciones de control de las autoridades de la Comunidad Salesiana Cayambe, puesto que basta con tener un dispositivo tecnológico tan común como una PC o un smartphone con acceso a Internet y teclear la dirección IP de acceso remoto con su respectivo puerto, para poder visualizar puntos de interés, los cuales permiten monitorear y controlar las labores del personal.

- El acceso remoto mediante el reenvío de puerto único configurado en este proyecto facilita la configuración inicial de las cámaras con lo cual se consiguen dos aspectos importantes: 1) Evita la modificación de los puertos de fábrica; 2) Permite acceso vía Internet hacia los dispositivos de vigilancia sin la necesidad de modificar los puertos de fábrica.

- Al configurar el envío de correos electrónicos por detección de movimiento en la zona de la secretaria de la Unidad Educativa Salesiana "Domingo Savio" y en el hall de la Casa Campesina Cayambe se logra que el sistema funcione como una herramienta que evite robos, claro está que esta herramienta por sí sola no cumple con este cometido, como se ha mencionada varias veces la infraestructura institucional es de primer nivel y zonas de interés como las mocionadas cuentan con alarmas por detección de movimiento que se han sido potencializadas con las instalación de las cámaras y la opción de envío de correos electrónicos.

- Los sistemas de video vigilancia actuales presentan gran cantidad de beneficios y prestaciones, es por este motivo que este proyecto tendrá gran acogida en el medio externo, al satisfacer de forma eficiente los problemas relacionados con la seguridad.

- En sistemas de video vigilancia digital basados en IP, los componentes indispensables para la implementación son: cámaras, router e Internet. El computador, por lo general es común en toda empresa u hogar, el almacenamiento se lo puede realizar hacia la nube mediante un servidor FTP, de esta manera se logra reducir costos.

- El uso del programa Inssider da una clara idea que cual es el estado previo de las señales inalámbricas en la zona de secretaria de la UESDS y la Casa Campesina Cayambe, los resultado arrojados por el programa permiten tomar decisiones relevantes en la implementación del proyecto como es la ubicación del router y los canales en los cuales debe operar la señal inalámbrica a implementar para que no haya interferencia con otras señales.

- Es muy importante realizar cálculos aproximados de la distancia de cobertura del router implementado utilizado los datos técnicos de cada equipo (datasheet), la distancia calculada para este proyecto fue de alrededor de 75 metros pero esto en la práctica no es real puesto que la señal debe atravesar muros y en la zona hay gran cantidad de equipos que trabajan en la banda de frecuencia de 2,4GHz lo que genera interferencias, por los que las distancia de cobertura real disminuye, en este proyecto la distancia más lejana es de alrededor de 10 metros.

4.2 Recomendaciones

- Se recomienda que las autoridades que tengan acceso a las cámaras de forma remota tengan limitación de atributos puesto que pueden generar problemas en la administración del sistema de cámaras de seguridad, esto se logra asignando usuarios de tipo invitado.

- Es recomendable que el almacenamiento de las grabaciones se organice de tal manera que se logre aprovechar al máximo la capacidad de almacenamiento de nuestro sistema, es decir, grabando de forma continua en horarios de interés y el resto de tiempo al detectarse movimiento, además las grabaciones se deben almacenar por un tiempo prudencial para liberar el sistema de grabaciones innecesarias.

- Es una recomendación prioritaria realizar la adquisición de un disco de mayor capacidad de almacenamiento además de una memoria RAM de mayor capacidad puesto que son limitantes en este sistema y pueden generar serios inconvenientes.

- Se recomienda que este proyecto se use como una guía para el proceso de implementación de un sistema de cámaras de seguridad, mas no como una regla específica, puesto que existe gran cantidad de sistemas de video vigilancia de distintas marcas.

- Se recomienda realizar una adecuada planificación entre técnicos y autoridades antes de implementar sistemas de video vigilancia, puesto que en ella se determinan los sitios de mayor importancia para la ubicación de las cámaras, se analizan todos los escenarios posibles de acuerdo a la realidad institucional, permitiendo una configuración adecuada de las herramientas de control de cada cámara y lo más importantes garantiza el correcto funcionamiento del sistema.

- Al configurar la detección de movimiento desde el software de gestión se recomienda garantizar que la detección de movimiento esté habilitada desde las herramientas de la cámara, caso contrario no se detectará movimiento.

- A pesar de que los software de gestión multimarca son de gran utilidad y ayudan a la escalabilidad de una red, se recomienda, en lo posible, trabajar con una misma marca de cámaras y así usar un software de gestión exclusivo, esto agilita y facilita el proceso de configuración, evita gastos de adquisición de software con licencia además de los problemas y limitaciones genera un software libre.

- Es importante garantizar el flujo continuo e ininterrumpido de energía eléctrica, en este proyecto se ha solventado esta necesidad puesto que la Comunidad Salesiana Cayambe cuenta con un generador, el cual garantiza el flujo eléctrico en el caso de haber cortes de energía. En el caso de no garantizar esta cuestión se recomienda la adquisición de un UPS de respaldo.

- La seguridad de la red de datos de toda institución es muy importante, es por este motivo que se recomienda implementar proyectos de estas características de forma independiente a la red institucional, es decir el acceso a las cámaras desde Internet debe ser mediante una dirección IP distinta a la de la red institucional.

- Es recomendable que al configurar el software de gestión se habilite la opción de arranque del programa inmediatamente después de inicializado el computador, esto en el caso de que se interrumpa el flujo eléctrico y que la máquina se reinicie, de esta manera se evitará que el programa deje de grabar.

- Considerando el derecho a la privacidad de cualquier persona y para evitar problemas de índole legal, es de mucha importancia ubicar carteles informativos en los cuales se advierta a las personas que están siendo grabadas.

- Para reducir costos es adecuado reusar equipos que no se estén utilizando, garantizando que cumplan con características mínimas que permitan el correcto funcionamiento del sistema de video vigilancia.

- Para incrementar las seguridades a la red es recomendable el uso del protocolo https, además de las opciones ya detalladas en el proyecto.

5 BIBLIOGRAFÍA

Artículo Web

[1] LÓPEZ GUERRERO, J. A. (MAYO de 2007). *UNIVERSIDAD AUTÓNOMA DEL ESTADO DE HIDALGO."Redes Inalámbricas Wireless LAN"* Recuperado el 22 de MAYO de 2014, de http://www.uaeh.edu.mx/docencia/Tesis/icbi/licenciatura/documentos/Redes%20inalambricas%20wireless%20LAN.pdf

[2] ACOSTA, J. (26 de ENERO de 2005). *DEPARTAMENTO DE INFORMÁTICA UNIVERSIDAD DE VIGO."Topologpia de Redes LAN"* Recuperado el 27 de MAYO de 2014, de http://www.lsi.uvigo.es/lsi/jdacosta/documentos/apuntes%20web/Topologia%20de%20redes.pdf

[3] Dericam. (19 de 04 de 2013). Network Camera. *"User Manual"* Recuperado de http://www.dericam.net/Support.asp?i=1&a=3&typeid=28&typpid=47

[4] Docentes de la Universidad de la Republica de Uruguay. (11 de Abril de 2014). *Facultad de Ingeniería de la Universidad de Uruguay.* "*Señales Wireless"* Obtenido de Facultad de Ingeniería de la Universidad de Uruguay: https://eva.fing.edu.uy/

[5] Mifsud Talón, E., & Lerma-Blasco, R. V. (s.f.). *"Despliegue de Redes Inalámbricas"* Recuperado el 16 de 06 de 2014, de http://serviciosenred2012inma93.files.wordpress.com/2012/03/diapositivas-u-t-9.pdf

Libro Digital

[6] PEÑA MILLAHUAL, C. A. (2012). "*Redes wi-fi en entornos windows".* BUENOS AIRES: FOX ANDINA; DÁLAGA S.A.

[7] PONCE, E., MOLINA TORTOSA, E., & MOMPÓ MAICAS, V. (15 de 05 de 2001). *"Redes inalámbricas: IEEE 802.11".* Recuperado el 10 de 06 de 2014, de http://www.freelibros.org/libros/redes-inalambricas.html

[8] SALVETTI, D. (2011). "R*edes wireless".* BUENOS AIRES: FOX ANDINA; DÁLAGA.

[9] TELECOMMUNITY. (26 de MAYO de 2009). "*Redes Inalámbricas"*. Recuperado el 22 de MAYO de 2014, de http://www.telcommunity.com/wp-content/uploads/pdf/redes_wireless.pdf

Página Web

[10] ZKT. (16 de 10 de 2013). ZKPT531-Series.

[11] InformáticaModerna. (2008). Informática Moderna.com. Obtenido de http://www.informaticamoderna.com/Cable_calibre.htm

[12] AXIS. (15 de 02 de 2002). CÁMARAS AXIS. Obtenido de: http://www.axis.com/files/datasheet/2120/2120ds.pdf

[13] GalcaNetworks. (28 de 09 de 2015). *COMPRAWIFI*. Obtenido de http://www.comprawifi.com/index.php?act=calculo.

6 ANEXOS

ANEXO A

Data Sheets

Especificaciones técnicas Router Lynksys E900

ANEXO B

Date Sheets

Especificaciones técnicas cámara ZKTeco- 531 Series

ANEXO C

Data Sheets

Especificaciones técnicas cámara Dericam H216W

ANEXO D

Proformas

Proformas recibidas para la cotización de las cámaras de seguridad.

ANEXO A

Data Sheets

Especificaciones técnicas Router Lynksys E900

Especificaciones

Linksys E900

Nombre del modelo	Linksys E900
Descripción	Router Wireless-N
Número de modelo	E900
Estándares	802.11n, 802.11g, 802.11b, 802.3u
Puertos	Power (Alimentación), Internet y Ethernet (1-4)
Botones	Reset (Reinicio), Wi-Fi Protected Setup™
Luces	Configuración de alimentación/Wi-Fi protegida, Internet, Ethernet (1-4)
Tipo de cableado	CAT 5e
Potencia de transmisión	802.11n (20 MHz): 15,0 ± 1,5 dBm a CH6, MCS 0~4, MCS 8~12 13,5 ± 1,5 dBm a CH6, MCS 5~7, MCS 13~15 802.11n (40 MHz): 14,0 ± 1,5 dBm a CH6, MCS 0~4, MCS 8~12 13,5 ± 1,5 dBm a CH6, MCS 5~7, MCS 13~15 802.11g: 14,5 ± 1,5dBm a CH6, todas las velocidades 802.11b: 16,5 ± 1,5dBm a CH6, todas las velocidades
Ganancia de la antena	≤2,0 dBi, ≤4,0 dBi (2 antenas)
UPnP	Compatible
Seguridad inalámbrica	Wi-Fi Protected Access™ 2 (WPA2), WEP, filtrado de direcciones MAC inalámbrico
Bits de clave de seguridad	Encriptación de hasta 128 bits

Condiciones ambientales

Dimensiones	188,7 x 151,7 x 31,2 mm (7,43" x 5,97" x 1,23")
Peso de la unidad	202,0g (7,13 onzas)
Alimentación	12 V, 0,5 A
Certificaciones	FCC, UL/cUL, ICES-003, RSS210, CE, Wi-Fi (IEEE 802.11b/g/n), WPA2™, WMM®, Wi-Fi Protected Setup, Windows 7
Temperatura de funcionamiento	De 0 a 40 °C (de 32 a 104 °F)
Temperatura de almacenamiento	De -20 a 60 °C (de -4 a 140 °F)
Humedad de funcionamiento	10% a 80%, sin condensación
Humedad de almacenamiento	5% a 90%, sin condensación

NOTAS

Para obtener información sobre la garantía, la normativa y las especificaciones, consulte el CD incluido con el router o visite Linksys.com/support.

Las especificaciones pueden cambiar sin previo aviso.

Rendimiento máximo según lo establecido en las especificaciones de la norma IEEE 802.11. El rendimiento real puede variar y la capacidad de red inalámbrica, el índice de producción de datos, el alcance y la cobertura pueden disminuir. El rendimiento depende de muchos factores, condiciones y variables, entre ellos, la distancia desde el punto de acceso, el volumen de tráfico de la red, la fabricación y materiales, el sistema operativo utilizado, la combinación de productos inalámbricos utilizados, las interferencias y otras condiciones adversas.

ANEXO B

Data Sheets

Especificaciones técnicas cámara ZKTeco- 531 Series

ZKTeco

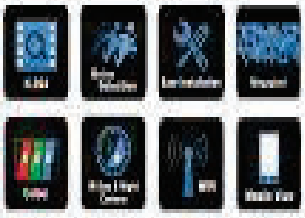
ZKPT531

PT IP Camera

• H.264 • 1 Megapixel • IR Illuminators • Easy Installation

Features:

- Super video quality, HD up to 720P
- Multiple H.264 streams
- Day & Night function
- WIFI standard
- ONVIF protocol
- Support mobile preview



Product Description

ZKPT531 supports 1 megapixel (1280*720) resolution, delivering super H.264 compression image quality up to 25fps. It is an all-in-one solution that meets a wide variety of needs for indoor surveillance.

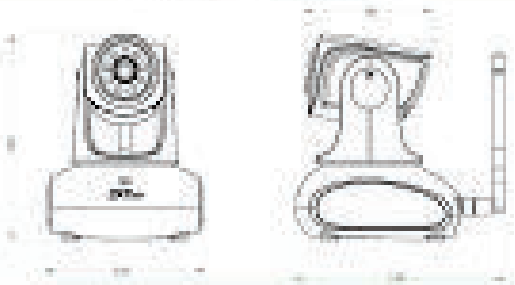
ZKPT531 series also can support WIFI function as standard. You can install this camera in applications locations like corridors, stairs, baby rooms, and offices. Compare to other cameras, it is a cost effective choice for civil used application.

ZKPT531

Technical Specifications

	Product Model	ZKPT531
	Product Name	PT Network Camera
Camera Performance	Image Sensor	1/4" Megapixel progressive CMOS
	Image Resolution	1280*720
	Minimum Illumination	0.5 Lux / F2.0 (IR Off), 0 Lux (IR on)
	Day/Night Mode	Automatically IR-cut filter
	Lens Type	2.8mm
	IR Distance	5~10 meters
Video & Audio	System	LINUX
	Video Compression	H.264/M-JPEG
	Audio Compression	G711A/G711
	Video Resolution	Main stream：1280x720 / Second stream：640x352 / Third stream：320x176
	Image streaming	20fps/s ~ 512Kbit/s adjustable
	Video Frame Rate	PAL：1-25fps，NTSC：1-30fps
	Image settings	Brightness, contrast, saturation, sharpness , Shutter
Function & Port	Audio Input	Built-in microphone / Audio jack input
	Audio Output	Built-in speaker / Audio jack output
	Reset	Yes
	Motion Detection	4 Motion detection areas editable
	Alarm Event	Email snapshot notification, FTP snapshot upload, Event record to TF card
	Supported Protocols	TCP/IP、HTTP、TCP、UDP、ARP、SMTP、FTP、DHCP、DNS、3GPP、MTP、UPnP、RTSP、Onvif
	Network Interface	10Base-T/100Base-TX Ethernet interface / Wi-Fi 802.11 b/g/n wireless network
	Storage	TF card local storage maximum 32G
Pan & Tilt	Motor	Built-in motor
	Rotation Angle	Horizontal：355°，Vertical：120°
	Preset	8
Working Environment	Power Supply	DC5V / 2A
	Operating temperature	-10℃~50℃
	Operating humidity	10%~80%
	Dimension	Item size: 148x148x185mm (5.8"x5.8"x7.3") / Package size: 175x175x215mm (6.9"x6.9"x8.5")
	Weight	N.W.：300g (0.66lb) / G.W.：550g (1.21lb)

Camera Dimensions



ANEXO C

Data Sheets

Especificaciones técnicas cámara Dericam H216W

Dericam

User Manual

Model: H216W

Outdoor 720P HD IP Camera

Ver. 1.2

1. Product Introduction

Welcome to use Dericam wired/wireless IP Camera. IPCAM is electronic equipment which can transmit dynamic video stream to all over the world through the network. The user can always monitor the place anywhere, as long as he can connect to Internet.

Dericam IP camera works based on the TCP/IP standard. A WEB server is integrated inside which can support Internet Explorer or other major browsers. And this feature can help you to accomplish online management and maintenance on your device simply, such as remote configuration, remote start-up and firmware upgrade.

You can use the IPCAM monitoring homes, offices, factories, stores, nurseries and etc, simply, conveniently and real-time.

1.5 Product features:

1.5.1 Simple Installation: It is very simple to install IP cameras. If you choose wired networking solution, you only need to prepare power and networks connection. If you want to use WIFI wireless connection, only power is need.

1.5.2 Scope of applications: Apply to homes, offices, enterprises, supermarkets, schools and other public places.

1.5.3 Supporting multiple protocols: Embedded operation system supports the TCP / IP, SMTP (simple mail protocol), HTTP, UPnP, etc.

1.5.4 Simple configuration: Standard Web browser GUI can help users to control and manage the IP cameras through LAN or Internet.

1.5.5 Video Watching and Video Record: Provide concise GUI for user to watch re-

al-time video stream from anywhere networking connection is available. And the video segments can be recorded on your computer or SD Card.

1.5.6 Alarm Monitoring: When alarm of camera is triggered, the alarm information can be sent to your e-mail or ftp server. Especially, user can activate motion detection function to detect any movement in the selected area. If any illegal invasion happens, alarm will be realized. Simultaneously, the captured images will be sent to email address specified by user.

1.5.7 Support dynamic DNS: Support Dynamic DNS. Users can access IP cameras easily through DDNS despite that the camera IP changes frequently.

1.5.8 Simple User Authority Management: Setting USER and PASSWORD of the system can help user to protect privacy effectively, meanwhile, users can be authorized with different permission levels to operate the IP camera.

1.5.9 Real-time Monitor through Intelligent Mobile Phone: With the assistance of professional client software **IPMaster Viewer**, user can access any online IP Camera anywhere through intelligent mobile phone, iPhone or Android-OS (Operation System) based mobile phone and run routine PTZ operations. User can download this app from CD delivered in package box to your intelligent mobile phone. Please confirm your mobile phone has iPhone OS or Android-OS and choose the correct software version.

1.6 Packing list:

- •HD Outdoor IP Camera x 1
- •CDROM x 1 (include user guide, control, IP search tool)
- •Quick Installation Guide x 1
- •Power adapter x 1

Shenzhen Dericam Technology Co., Ltd H218W User Manual

- •Net Cable x 1
- •Bracket x 1

ANEXO D

Proformas

Proformas recibidas para la cotización de cámaras.

I

Quito 26 de Mayo del 2014

RUC 1710690049001

COTIZACIÓN

Proforma No **PROF56000456**

RAZÓN SOCIAL: UNIDAD EDUCATIVA SALESIANA "DOMINGO SAVIO"

RUC: 1791749626001

DIRECCIÓN: CAYAMBE

TELF: 022361490

De mi consideración.

Estimado cliente, en atención a su solicitud; me permito enviarle la cotización correspondiente a los productos y servicios de su interés.

N°	DETALLE DEL PRODUCTO O SERVICIO	PRECIO UNIT.	SUB. TOTAL
2	Cámara interior Ip. **Polaroid** Vision Nocturna , Wifi.	133,93	267,86
1	Cámara de exterior **EasyN**, robotica, Wi-Fi vision Nocturna	259,38	259,38
		SUB. TOTAL	527,24
		IVA 12%	63,27
		TOTAL	590,51

Quito, Avenida de los pinos y Zaldunvide Sector Kennedy

Telefonos: 5144858 - 0980125332

TELF.: 2362-008 / 2363-646 / 09 9842-365 Cayambe – Ecuador e-mail oscarguana@yahoo.com
RUC: 1710202167001
DIR: Sucre y Rocafuerte (Centro Comercial Vendedores Autónomos Local #90)

PROFORMA L0001007

CLIENTE: U.EDUCATIVA SALESIANA DOMINGO SAVIO
ATENCION: ING.DIEGO CEVALLOS
CIUDAD: CAYAMBE
FECHA: 16 de jun de 15

CAN.	DESCRIPCION	P. UNI.	TOTAL
2	**DCS-942L MM720DLN73 Cámara de red Wireless N**	189.50	379.00
	Home con luz infrarroja		-
	IR - microSD		-
	H.264 - microfono		-
1	**UNIDAD IMB-V13MPW Cámara IP**	187.90	187.90
	Línea Milenium tipo bala de 1.3 MP		
	Lente varifocal 2.8-12mm,		
	Con sensor 960P HI 3518E+AR0130 IR-CUT		-
	con WDR, POE		-
	GARANTIA 12 MESES		
	PROFORMA VALIDA 15 DIAS		
	ENTREGA INMEDIATA		
		SUB TOTAL	566.90
		12% IVA	68.03
		TOTAL	634.93

Atentamente,

Srta; Lucia Ushiña
PROSYSTEM
comuniquese a:
msn:ventas1@prosystem.ec
msn:ventas3@prosystem.ec

SALUDOS
EN LA PROFORMA ADJUNTO EL LINK DE LOS DETALLES DE LAS CAMARAS SOLICITADAS COMO LE COMENTE ANTES NO LAS TENGO LOS ITEMS DE ESTAS EN EL SISTEMA POR LO CUAL NO ADJUNTO PROFORMA DE LA EMPRESA PERO AHI ESTAN LOS PRECIOS INCLUIDO EL IVA

CAMARA DLINK DCS-932A INTERNET WIRELESS ·$229.00
CAMARA DLINK DCS-7010L IP Outdoor PoE Infrarrojo MicroSD HD $699.00

VER LINK

http://www.dlinkla.com/dcs-932l

DCS-932L

Cloud IP Camera, Cube, Wireless 11N with IR Leds - Day&Night Vision and mydlink support

225.94$ ICLUIDO IVA

CARACTERÍSTICAS PRINCIPALES

Período de Garantía: 36 meses
Conectividad Wireless N
Sensor CMOS de 1 lux que permite captura de video en entornos de baja luminosidad
IR LED que entrega 5 metros de luminosidad en ambientes sin luz
Soporte de stream de video MJPEG para una alta calidad de imagen
Detección de movimiento para activar la grabación y enviar alertas al E-Mail
Monitoreo y Grabación de video remoto, Software de monitoreo D-ViewCam 2.0 incluido
Soporta UPnP y WPS para una fácil instalación y configuración de la Red
Acceda rápidamente a las cámaras registradas a través de la página web mydlink

La cámara de red DCS-932L Wireless N de día y noche para el hogar es la solución perfecta de vigilancia 24 horas. Cuenta con LEDs infrarrojos integrados que permiten el monitoreo en condiciones de baja o nula luminosidad. Con el nuevo servicio gratuito mydlink ™, el

monitoreo del hogar es más fácil que nunca, ya que le permite vigilar a sus hijos o incluso sus mascotas en el hogar. A través de un portal web intuitivo o de una aplicación gratuita en su iPhone, Android o Tablet, mydlink ™ le permitirá visualizar el lugar que desee, a cualquier hora del día y los 7 días de la semana, incluso cuando se encuentra de viaje.

VISIÓN NOCTURNA

La cámara de red Wireless N de día y noche para el hogar cuenta con LED infrarrojos integrados que permiten un monitoreo continua, incluso cuando la oscuridad es total. La distancia de iluminación de 5 metros la hace muy adecuada para vigilar lo que realmente le importa: el bebé en su habitación o la oficina durante la noche.

UN SISTEMA DE VIGILANCIA COMPLETO

La DCS-932L incluye detección de movimiento y alertas por correo electrónico a través de la interfaz de usuario, lo que convierte a esta cámara en un sistema de vigilancia para el hogar muy completo. Mediante la interfaz de usuario de la cámara podrá crear fácilmente un área de detección (por ejemplo, una ventana o una puerta del garaje), y configurar que se le envíe un correo electrónico para avisarle cuando se detecte movimiento.

VER LINK

http://www.dlinkla.com/dcs-7000l

DCS-7000L

Wireless AC Day/Night HD Mini Bullet Cloud Camera

- **$ 696.72 INCLUIDO IVA**

DESCRIPCIÓN

La cámara mini bullet DCS-7000L es una cámara de vigilancia IP que cuenta con tecnología Wireless AC, graba videos en HD y se puede conectar al servicio en la nube mydlink, permitiéndole monitorear las 24 horas del día. La tecnología AC incorporada le entrega un streaming de video mejorado y aumenta la confiabilidad. Ya que es un dispositivo compatible con mydlink, usted puede monitorear directamente desde su dispositivo móvil.

VIGILANCIA HD 24/7

La cámara DCS-7000L incorpora un sensor de imágen HD para entregarle fotografías de alta calidad y videos con una resolución de hasta 720p HD, lo que da como resultado imágenes nítidas de alta resolución y videos ricos en detalles. No pierda de vista los pormenores con ePTZ, el cual le permite hacer zoom y moverse dentro de la imágen para vigilar fácilmente áreas extensas. La DCS-7000L cuenta con un filtro de corte infrarrojo removible, el que bloquea la luz infrarroja durante el día para mejorar la calidad de la imagen. De noche, este filtro cesa su efecto para dejar pasar toda la luz posible, mejorando la imagen en condiciones de baja luminosidad y, junto a un potente LED infrarrojo con 8 metros de alcance, esta cámara es capaz de monitorear incluso en completa oscuridad.

HIKVISION

epcom SYSCOM

MaxiGroup
TELECOMUNICACIONES Y VIDEOVIGILANCIA

Cotización CÁMARAS IP

Unidad Educativa Salesiana "Domingo Savio"

CUALQUIER DUDA O REQUERIMIENTO ADICIONAL ESTAREMOS GUSTOSOS DE ATENDERLO

Atentamente,

Jefferson Guevara

Ingeniero de Proyectos

MaxiGroup
TELECOMUNICACIONES Y VIDEOVIGILANCIA

Av. Amazonas N14-29 y Colon Edif. España of. 26,27,28
Quito - Ecuador
Telefonos: +593 2 223 744 / 2239 713
Celular: +593 984041140
e-mail: Jefferson.Guevara@grupomaxi.com.ec
www.grupomaxi.com.ec

Responsabilidad

Aunque se han hecho todos los esfuerzos para asegurar la precisión de la información aquí contenida en éste y en los documentos asociados, ello no debe considerarse como un compromiso por parte de MaxiGroup, y la responsabilidad de MaxiGroup sobre los errores u omisiones, está limitada a la corrección de los mismos. MaxiGroup agradece cualquier comentario de mejora recibido.

La información contenida en adelante ha sido concebida para su uso por parte de personal cualificado, y está destinada al propósito del acuerdo bajo el que se suministra esta información. El usuario de dicha información asume la completa responsabilidad sobre su uso, y en ningún caso** MaxiGroup **será responsable por daños directos o indirectos relacionados o como consecuencia del uso de esta información.

La información o las afirmaciones expresadas en este documento relativas a la idoneidad, capacidad o características del mencionado software o hardware no pueden ser consideradas como un compromiso, y deberán ser definidas particularmente en el acuerdo realizado entre MaxiGroup y el cliente.

MaxiGroup se reserva el derecho de revisar este documento y de realizar cambios decontenido en cualquier momento sin aviso previo.

Copyright

Ni el conjunto ni extractos de la información aquí contenida o de los documentos asociados pueden ser copiados, distribuida o transmitida por medio alguno a terceros sin previa autorización escrita por parte de MaxiGroup. La distribución de este documento puede estar protegida mediante NDA (acuerdo de confidencialidad) entre MaxiGroup y el receptor.

La información contenida en algunas partes de estos documentos puede estar protegida por derechos de patente.

Este documento, los documentos asociados y el producto descrito se consideran protegidos por Copyright de acuerdo a las leyes aplicables.

Quito, 27 de Mayo del 2015

Estimados,

Luego de un cordial saludo, permítame introducirle al conjunto de empresas que conforman nuestro prestigioso grupo:

MaxiGroup
TELECOMUNICACIONES Y VIDEOVIGILANCIA

- El Grupo Maxi está formado por las empresas **MAXIDISTRIBUCIONES CÍA LTDA, Radiocomunicaciones de los Andes RACOMDES**, y **DALTRON Cia. Ltda.**, la primera empresa fue fundada en el año 2001 y como su nombre lo indica, fue creada con fines deser un canal de distribución de tecnología y productos electrónicos en el Ecuador.
  Actualmente mantenemos el contrato de distribución exclusiva de la marca KENWOOD para el territorio ecuatoriano, y gozamos de la distribución de EPCOM para los sistemas de **seguridad, accesos** y **video vigilancia**.

- La segunda empresa ha sido fundada en la década de los 90 como un **Operador de Sistemas Troncalizados** en la banda de 800 MHz, para lo cual tiene la licencia del Estado Ecuatoriano para brindar servicios de radio troncalizado en todo el país. En el año 2009esta empresa pasó a formar parte del grupo.

- La tercera empresa fue fundada para ser un canal de integración de tecnología en soluciones de **Comunicaciones Unificadas,** siendo distribuidor de soluciones reconocidas en el mercado como YEALINK, Elastix, XORCOM, YEASTAR.

Nuestro portafolio de productos es amplio, permitiéndonos brindar a nuestros clientes una gama de productos diversos de alta calidad y variedad que se ajusten a los requerimientos de cada proyecto, y en todas las áreas de comunicaciones, seguridad y vigilancia. Además, nuestros ingenieros especializados pueden integrar el sistema de telefonía IP (VoIP) para que se integre al Circuito Cerrado de Televisión CCTV.

COTIZACIÓN CÁMARAS

CANT	CODIGO	IMAGEN	DESCRIPCION	V/UNID.	V/TOTAL
2	Modelo: DS2CD2132I Marca: HIKVISION		**CARACTERÍSTICAS DE LA CÁMARA:** • CMOS 1/3" Scan Progresivo. • Iluminación mínima 0.01 Lux / 0 Lux IR. • Lente fijo 4 mm@F1.2. 18 LEDs IR (hasta 20 m de visión). • Resolución: 1280 x 960 pixeles (1.3 Megapixeles). • Resolución Full HD 1080p (2048 x 1536). (3 Megapixeles). • Hasta 15 IPS@1.3MPixeles/30IPS@720p (DS-2CD2112-I). • Hasta 15 IPS@3MPixeles/30IPS@1080p (DS-2CD2132-I). • Compresión H.264/MPEG4/MJPEG. Funciones Generales: • Protección por usuario y contraseña. • Det.de mov. con notificación en Software Cliente. • Acceso remoto por Internet Explorer y Software Cliente.	$ 232.00	$ 464.00
1	Modelo: DS2CD2120FIW Marca: HIKVISION		**CARACTERÍSTICAS DE LA CÁMARA:** • CMOS 1/3" Scan Progresivo. • Iluminación mínima 0.01 Lux / 0 Lux IR. • Lente fijo 4 mm@F1.2. 18 LEDs IR (hasta 30 m de visión). • Función Día y Noche Real con Filtro ICR. • Shutter electrónico automático. • WiFi con alcance de 50 m (dependiendo del entorno) • Resolución: 1920 x 1080 pixeles (2 Megapixeles).	$ 237.00	$ 237.00

			• Hasta 30 IPS @ 1.3 MP • Compresión H.264/MJPEG. Funciones Generales: • Protección por usuario y contraseña. • Det.de movimiento con notificación en Software Cliente. • Acceso remoto por Internet Explorer y Software Cliente.		
				SUBTOTAL	$ 701.00
				IVA	$ 84.12
				TOTAL	$ 785.12

Nota:

- **Los costos de instalación NO están incluidos.**
- **Pago:** 70% de anticipo y 30% contra entrega.
- **Tiempo de entrega:** 15 a 20 días a partir de la orden de compra
- **Garantía:** 1 año contra defectos de fábrica en todos los productos.
- **Validez de la Cotización:** 60 días

MaxiGroup
TELECOMUNICACIONES Y VIDEOVIGILANCIA

CUALQUIER DUDA O REQUERIMIENTO ADICIONAL ESTAREMOS GUSTOSOS DE ATENDERLO

Atentamente,

Jefferson Guevara

Ingeniero de Proyectos

MaxiGroup
TELECOMUNICACIONES Y VIDEOVIGILANCIA

Av. Amazonas N14-29 y Colon Edif. España of. 26,27,28
Quito - Ecuador
Telefonos: +593 2 223 744 / 2239 713
Celular: +593 984041140
e-mail: Jefferson.Guevara@grupomaxi.com.ec
www.grupomaxi.com.ec

Moreno Villacis Andres Guillermo
RUC: 0101834596001
Obligado a llevar Contabilidad

Centro de Negocios Kaufer, Oficina 7
Ph: (593) 3-319-717 / 099-496-1173
Quito - Ecuador

ID CONSULTA NTS / DACTRADING CORP.

ventas@idconsultants.us

www.idconsultants.us

PROFORMA # 13345

Cliente: Diego Andrés Cevallos Guerra

Dirección:

Rep. MVP

Términos Contado

RUC

Fecha: 25/08/2014

Vencimiento 25/08/2014

Telf.:

Jefe de Cuenta MARCO

CANTIDAD	DESCRIPCION	PRECIO UNIT.	VALOR TOTAL
2	ZK TECO CAMARA IP PROFESIONAL TIPO PT ZKPT531, MOVIMIENTO VERTICAL , HORIZONTAL, CMOS, 1 MEGAPIXEL, DETECTOR DE MOVIMIENTO, IE WEBSERVER, ICR-CUT , WIFI	119.00	238.00
1	DCR CAMARA IP SEMI-PRO DRC-H216W, Tipo Bala, 1/3CMOS, 1 Megapixel alta resolucion con Compresion H.264 , F=8MM LENTE, WIFI, 64 CANALES SOFTWARE, 30METROS, 36 IR-LEDS,EXTERIORRES, CON FILTRO DE NO DISTROSION DE COLOR, 90 DIAS SOPORTE Y GARANTIA (COMPATIBLE CON H502W)	107.00	107.00

AUTORIZADO

16/VII/2014

SACAR U. FACTURA

Subtotal: $345.00

IVA (12.0%) $41.40

Total: $386.40

Formas de Pago

Transferencia Bancaria - Banco Pichincha Cta.
Cte. a nombre de Andrés Moreno Villacis # 3036579104

Tarjeta de crédito internacional

Pago Electrónico PayPal

Envios y Entregas

Firma Cliente