ESCUELA POLITÉCNICA NACIONAL

ESCUELA DE FORMACIÓN DE TECNÓLOGOS

IMPLEMENTACIÓN DE UNA RED DE CÁMARAS INALÁMBRICAS DE SEGURIDAD CON MONITOREO REMOTO PARA LA ESCUELA DE EDUCACIÓN BÁSICA ABELARDO MONCAYO

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

JOSÉ WENCESLAO OYANA SANGUÑA

joew_mng@hotmail.com

DIRECTOR: ING. LUIS PONCE

luis.ponce@epn.edu.ec

CODIRECTORA: ING. MÓNICA VINUEZA

Quito, Julio 2018

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por José Wenceslao Oyana Sanguña, bajo mi supervisión.

Ing. Luis Alfredo Ponce Guevara	**Ing. Mónica Vinueza**
Director del proyecto	**Codirectora del proyecto**

DECLARACIÓN

Yo, José Wenceslao Oyana Sanguña, 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 correspondiente a este trabajo, a la Escuela Politécnica Nacional, según lo establecido por la Ley de Propiedad Intelectual, por su reglamento y por la normativa institucional vigente.

José Wenceslao Oyana Sanguña

DEDICATORIA

Agradezco primero a Dios por todas las oportunidades que me ha brindado, a mis Padres José Oyana y Lucy Sanguña quienes con su apoyo, amor y comprensión a lo largo de mi vida me han ayudado a conseguir todos los objetivos que me he planteado.

A mi familia, amigos y a todas las personas que han estado siempre pendientes de mí durante el transcurso de mi vida académica, personal, y laboral.

A mi esposa Anita quien ha sido un gran apoyo y ha permanecido junto a mí en los momentos difíciles de mi vida personal y académica.

José Wenceslao Oyana Sanguña

ÍNDICE DE CONTENIDO

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

ÍNDICE DE ECUACIONES

RESUMEN

El presente proyecto consiste en el diseño e implementación de una red de cámaras inalámbricas de seguridad con monitoreo remoto para la escuela de Educación Básica “Abelardo Moncayo”. Este proyecto ha sido desarrollado para ofrecer un servicio complementario a la seguridad del plantel educativo con el objetivo de preservar los bienes materiales y la integridad de las personas que acuden a este sitio.

Este proyecto comienza con la investigación de todas las tecnologías que fueron empleadas para el desarrollo del sistema de cámaras de seguridad. En la sección de metodología se describe el levantamiento de información realizado en la institución educativa, así como la selección de los equipos que forman parte de la red inalámbrica, de acuerdo a las características más idóneas para su buen funcionamiento.

Para la implementación del proyecto se utilizó el router inalámbrico N300 Linksys E900, el cual realiza la distribución de las direcciones IP de cada cámara, así como el acceso a Internet y a la conexión inalámbrica. Se colocó un segundo equipo router en configuración de cascada para ampliar el rango de cobertura.

Se realizó la instalación de un PC servidor con un sistema operativo Windows Server 2012 R2 para controlar la aplicación *iSpy: Open Source Camera Security Software* la cual administra las cámaras. En este equipo se almacena la información obtenida por las cámaras; y también está creada la tarea programada que realiza el proceso de réplica de la misma a otro equipo, utilizando los comandos *robocopy* propios de los servidores con este sistema operativo.

Finalmente, se detalla cómo realizar el almacenamiento de información en la nube en el portal de Google Drive, así como la activación de las notificaciones a un número de celular mediante mensaje de texto, usando servicio contrato con una operadora de telefonía móvil.

Palabras clave: implementación, inalámbrico, cámaras, grabación, unidad educativa.

ABSTRACT

The present project consists of the design and implementation of a camera security wireless network with remote monitoring for the Basic Education School "Abelardo Moncayo". *This project has been developed to offer a complementary service to the security of the educational establishment, with the objective of look out and preserve the integrity of the people who come to this site.*

This project begins with the investigation of all the technologies that were used for the development of the security camera system. In the methodology section, the information collected in the educational institution is described, as well as the selection of the equipment that makes up the wireless network; according to the most suitable characteristics for a good performance.

For the implementation of the project, the wireless router N300 Linksys E900 was used, which made the distribution of the IP addresses of each camera, as well as the opening of Internet access and wireless connection. A second one was placed using the configuration cascade to extend the range of coverage.

The installation of a Server PC with operating system Windows Server 2012 R2was done to control the iSpy: Open Source Camera Security Software application for manage the cameras. Also this device storage of information that collected the cameras and the replication process to another device; for this the process of robocopy is used, which is a component that can be added to the servers with this operating system.

Finally, it details how to make the storage information in the cloud in the Google Drive portal, as well as the activation of notifications to a cell phone number by text message, using contract service with a mobile telephone operator.

Keywords: implementation, wireless, cameras, recording, educational unit.

1. INTRODUCCIÓN

En la Escuela de Educación Básica Abelardo Moncayo ubicada en el Distrito Metropolitano de Quito, parroquia de Llano Chico con la dirección Av. Carapungo E173 y Arturo Hinojosa. La institución cuenta con 649 alumnos dividido en dos jornadas de estudio matutino (442 alumnos) y vespertino (207 alumnos), en la cual se implementará una red de cámaras inalámbricas de seguridad con monitoreo remoto.

La red de cámaras inalámbricas permitirá realizar un monitoreo constante de los alrededores de la unidad educativa, así como también controlar las actividades atípicas ocasionadas por el alumnado y por las personas que ingresen al plantel educativo.

Para realizar la implementación del proyecto se procedió a la inspección del lugar y posteriormente detallar los requerimientos solicitados por el Lic. Ernesto Mora, Rector de la unidad educativa. La red está compuesta por el equipo router N300 Linksys E900 que controla la asignación de direcciones IP para las cámaras que sean necesarias; tanto para interiores, como para exteriores, en los diversos puntos seleccionados de acuerdo a su ubicación estratégica.

El router N300 Linksys E900 controla el flujo de información hacia Internet, así como el acceso remoto. Se creó un equipo PC servidor el cual tiene un sistema operativo *Windows Server* 2012 R2 en el cual se instaló la aplicación *iSpy: Open Source Camera Security Software* que controla todo el sistema de video vigilancia.

La información generada por cada una de las cámaras será almacenada en un equipo PC servidor. Se contará con un proceso de grabación en un horario establecido y habilitando la funcionalidad de grabación por detección de movimiento.

La información almacenada será copiada mediante el uso del proceso *robocopy* desde el servidor, en un horario establecido, hacia otro equipo, para garantizar que la información grabada no se pierda si falla el equipo principal.

También el equipo servidor, al estar conectado a Internet, realizará la carga de información en la nube utilizando un proceso de sincronización con la cuenta de Google Drive creada para la institución. Finalmente se planteó un prototipo para realizar el envío

de mensajes de texto hacia un número particular de las alertas recibidas de las distintas cámaras.

1.1 Tecnologías inalámbricas

Las redes de área local inalámbrica (WAN) emplean un medio de transmisión inalámbrico mediante una luz infrarroja o radiofrecuencia en lugar de una par trenzado o fibra óptica. Generalmente se usan radiofrecuencias debido a que poseen un alcance mayor, más cobertura y un mayor ancho de banda. Estas redes utilizan las frecuencias de 2.4 y 5 GHz dentro del espectro electromagnético, las cuales son reservadas en la mayoría de lugares para dispositivos sin licencia. Una de sus principales características es ofrecer flexibilidad y libertad para funcionar dentro y fuera de las edificaciones [1].

Los sistemas inalámbricos están construidos con circuitos integrados y microprocesadores conectados con sistemas LAN cableados, también los dispositivos deben ser alimentados con energía para realizar sus funciones respectivas como codificar, decodificar, transmitir, recibir las señales, por lo tanto, el sistema no es completamente inalámbrico y se lo pueden entender como una parte de una LAN cableada típica [1].

En la actualidad la tecnología inalámbrica soporta altas velocidades de trasmisión de datos y la interoperabilidad necesaria para un funcionamiento a nivel LAN, también los costos de los equipos inalámbricos se han reducido, tanto en el ambiente empresarial como doméstico, por lo que el empleo de esta tecnología resulta una opción accesible [1].

Razones y ventajas para utilizar redes inalámbricas

Existen varias razones para utilizar la tecnología inalámbrica, entre las cuales destacan las siguientes:

- Movilidad.
- Flexibilidad.
- Escalabilidad.
- Ahorro en los costos de implementación a corto y largo plazo.
- Minimiza el tiempo de implementación.
- Ventajas de instalación.

- Fiabilidad en entornos complicados.
- Utilizan una conexión de internet de banda ancha.
- Hacen frente a dificultades importantes que se presentan al instalar LAN cableadas como espacios reducidos.
- Su expansión es rápida.
- Propietarios de una empresa que necesitan tener flexibilidad frente a los constantes cambios de la infraestructura física del edificio.
- Cualquier compañía que posea limitaciones físicas y presupuestarias en su lugar de trabajo.
- Cualquier compañía que necesita ahorrar costos que se obtiene al tener un punto de conexión entre edificios por medio de una línea de visión, evitando así los procesos de soterramiento de cableado.

El uso de las WLANs resulta más económico que utilizar un ancho de banda WAN o cualquier instalación con extensos tendidos de fibra óptica. Lamentablemente este tipo de redes tienen una limitación en cuanto al área de cobertura con respecto de las redes alámbricas. En la actualidad las tecnologías inalámbricas ofrecen mejores velocidades, reducción de costos y mayor fiabilidad [1].

Desventajas de las redes inalámbricas

Entre los obstáculos e inconvenientes que implican la adopción de la tecnología WLAN se encuentran los siguientes:

- Afectación a la salud humana.
- Se puede vulnerar la seguridad de la red inalámbrica con los conocimientos adecuados.
- Administración de la energía en los puntos de acceso inalámbrico.
- Conectividad y fiabilidad, tiempos de respuesta variables.
- Inconvenientes de instalación dependiendo del diseño del lugar.
- Interoperabilidad.
- Degradación e inferencia de la señal.

Se ha expuesto varias vulnerabilidades en los mecanismos de privacidad, autenticación e integridad de los datos transmitidos en una red inalámbrica. A medida que se aumentan

las redes inalámbricas también es mayor la amenaza de los intrusos al exterior e interior de la red, dichos intrusos están continuamente escaneando la señal para beneficiarse de una red con baja seguridad [1].

El consumo de energía siempre es un inconveniente en los equipos portátiles ya que la batería que los alimenta tiene una energía limitada. Para solventar el inconveniente se debe utilizar algunas de los modos de energización existentes para los dispositivos como son: modo de activación constante (CAM), modo de ahorro de energía (PSP) o modo rápido de ahorro de energía (*Fast PSP*).

La red inalámbrica debe incluir mecanismos que les permita mejorar la fiabilidad en la trasmisión de información y que mínimo se equiparase a una red Ethernet cableada. También se debe tratar de emparejar las tecnologías de transmisión, los administradores de red deben considerar el entorno de la red ya que puede haber obstáculos que impidan la trasmisión de las señales y tomar en cuenta el ancho de banda disponible, el cual debe ser garantizado para un funcionamiento óptimo de la red.

La instalación de los equipos en cada sitio requiere de una metodología diferente dependiendo de las condiciones del área donde se implementará la red inalámbrica, existen obstáculos como: características topográficas, edificaciones, naturaleza (árboles) y la exigencia del cliente respecto a la cobertura ya que son ellos quienes principalmente determinan las necesidades que tienen que ser cubiertas en la infraestructura implementada [1].

Interferencia

Entre los retos más importantes de la WLAN está la interferencia de la señal emitida, la cual se establece porque varios dispositivos inalámbricos de diferentes redes trabajan en la misma banda de frecuencias. La interferencia no siempre se puede detectar sino hasta cuando ya se ha implementado el enlace. Una de las causas de esta interferencia es que los dispositivos inalámbricos operan con los estándares 802.11 y utilizan el espectro sin licencia lo que conlleva un riesgo dentro de la propia red inalámbrica debido a la ausencia de control y protecciones de estas frecuencias, adicionalmente la popularidad de las WLAN están en aumento lo que se genera que cada vez existan más dispositivos inalámbricos operando en la misma zona geográfica [1].

Existen algunas fuentes posibles de inferencia a las señales inalámbricas, entre las principales están las siguientes: Hornos microondas, servicio por satélite directo (DSS), cables y conectores coaxiales utilizados en algunos tipos de antenas esto si el cable tiene algún tipo de daño pueden provocar interferencias de radiofrecuencia (fuga de RF). Algunas fuentes de alimentación eléctricas externas, como líneas de alta tensión y centrales energéticas también pueden provocar interferencias. Teléfonos que operan a frecuencias de 5 GHz o 2,4 GHz, altavoces inalámbricos, cables mal aislados como conexiones de discos duros externos u otros dispositivos [2].

Existen materiales que generan obstrucciones absorbentes y reflectantes de radiofrecuencia (RF), los principales se detallan en la figura 1.

MATERIAL	EJEMPLO	INTERFERENCIA
Madera	Tabiques	Baja
Vidrio	Ventanas	Baja
Amianto	Techos	Baja
Yeso	Paredes interiores	Baja
Ladrillo	Paredes interiores y exteriores	Media
Hojas	Árboles y plantas	Media
Agua	Lluvia / Niebla	Alta
Cerámica	Tejas	Alta
Papel	Rollos de papel	Alta
Vidrio con alto contenido en plomo	Ventanas	Alta
Metales	Vigas, armarios	Muy Alta

Figura 1. Materiales absorbentes y reflectantes de señal inalámbrica [2].

Se han realizado avances tecnológicos con los que se ha conseguido disminuir el uso de la potencia en los equipos inalámbricos; dispositivos más inteligentes, sensibles y compactos; con lo que se puede generar formas de onda diseñadas para generar una menor interferencia entre redes; todo ello aumenta las posibilidades de que varias redes puedan compartir el mismo espectro [3].

1.2 Seguridad inalámbrica

Es un proceso en el cual la información digital transmitida es protegida, los objetivos que tiene este proceso son proteger la confidencialidad, mantener la integridad y garantizar la disponibilidad de la información.

También la seguridad de información se encarga de proteger los recursos y mantener los procesos de red, es decir, que se debe garantizar que los usuarios puedan ejecutar únicamente las tareas que tengan autorizadas a realizar, controlar que los mismos no puedan dañar los datos transmitidos, proteger a la red de un ataque mal intencionado, controlar los efectos de los errores de los fallos del equipo [1].

Entre los principales inconvenientes que se puede analizar con las redes inalámbricas, está el apropiamiento del ancho de banda, una situación que se presenta generalmente al no tomar las medidas necesarias, de igual forma se debe tener en cuenta que se dispone de una conexión sin cifrar, de esta forma en la red la información circulará de forma pública, con lo cual cualquier usuario dentro del espacio cubierto por la red podría interceptar la información que se está transmitiendo con el uso de algunas aplicaciones simples. Para tratar de resolver los inconvenientes de seguridad antes mencionados que se presentan en una red inalámbrica, se utiliza un sistema de cifrado que requiere cierto tipo de autenticación para poder conectarse y navegar por dicha red [4]**.**

- **Cifrado *WeB***

Fue uno de los primeros en aparecer para solventar los inconvenientes generados por las redes de comunicación abiertas. Este tipo de cifrado funciona mediante la autenticación del usuario y contraseña. De esta forma el tráfico viaja cifrado y aquel usuario que se encuentre escuchando el tráfico sólo leerá caracteres sin interpretar la información, esto sin que posea la clave para descifrar la conexión.

Está basado en el algoritmo de cifrado RC4, en donde utiliza claves de 64 o de 128 bits, las claves están conformadas de dos partes, una de ellas necesariamente debe ser configurada por el usuario en cada uno de los puntos de acceso de la red, la otra se genera automáticamente y su objetivo es obtener contraseñas diferencias para cada trama que se mueve en la red a esto se le llama vector de inicialización [4].

En este sistema las claves permanecen siempre estáticas lo cual es una gran debilidad, y por otra parte los 24 bits del vector de inicialización son insuficientes, además de transmitirse sin cifrar. Hoy en día es considerado un sistema poco seguro y no se recomienda su utilización [4].

- **Cifrado WPA**

Este sistema apareció para solventar los problemas de seguridad que presenta el sistema WEP. Para completar esta tarea hace uso de TKIP, un protocolo para gestionar claves dinámicas.

WPA realiza la autenticación de los usuarios mediante un equipo servidor donde están registradas y almacenadas las credenciales y contraseñas de los mismos. WPA permite la autenticación mediante un clave pre compartido, este sistema permite controles de acceso como la validación de usuario, contraseña o certificado digital. Algunos sistemas son:

WPA-PSK

Es el más simple después de WEP y el cual tiene el principio de funcionamiento de un sistema de clave compartida, fácil de manejar y configurar debido a esto se lo recomienda para uso en entornos familiares o empresas de bajo volumen.

Cualquier equipo que posea esta clave podrá conectarse a la red configurada. Una debilidad en este sistema es que se puede identificar la contraseña por medio del uso forzado de distintas claves hasta dar con la correcta, para remediar este percance se debe utilizar contraseñas complejas alfanuméricas [4].

WPA empresarial

Este sistema es más complejo funciona mediante la utilización de un usuario y contraseña o sistemas de certificados, generalmente se controla con equipos de gran potencia como servidores para la gestión de los usuarios o certificados.

En este sistema es posible incrementar todavía más la seguridad haciendo uso de otros mecanismos como EAP-TLS, EAP-TLLs y PEAP [4].

Cifrado WPA2

Este sistema agrega todas las características del estándar IEEE 802.11i (WAP no lo hace). Este sistema presenta dos cambios importantes respecto a WPA:

Reemplaza el algoritmo Michael por un código de autenticación conocido como el protocolo “Counter-Mode/CBC-Mac” el cual se considera criptográficamente seguro.

Reemplazo del algoritmo RC4 por el algoritmo AES, el cual es considerado actualmente como uno de los más seguros, sin embargo tiene el inconveniente de no ser compatible con el sistema WAP y que no todos los routers permiten este tipo de cifrado [4].

- **Tecnologías de seguridad**

Los administradores de la red no aplican las contramedidas disponibles en la mayoría de situaciones y debido a ello se producen los incidentes de seguridad.

Uno de los métodos a utilizar es la rueda de la seguridad WLAN, el cual es un proceso de seguridad continuo; este método ofrece probar y aplicar medidas de seguridad actualizadas de forma continua, como se aprecia en la figura 2 [1].

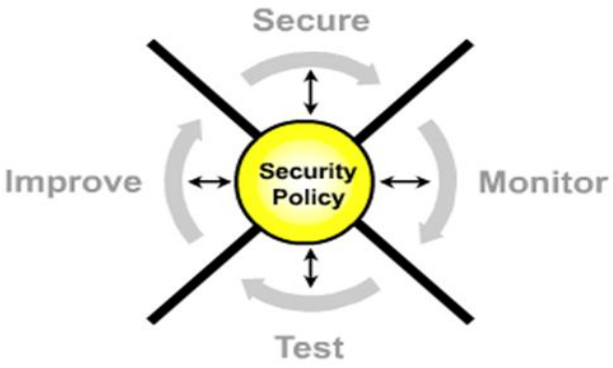


Figura 2. Rueda de seguridad WLAN [1].

Los cuatro pasos que describen este método son:

Asegurar.- Aquí se implementan las soluciones de seguridades WLAN de manera que se pueda evitar o frenar el acceso o las actividades no permitidas, para ello emplea lo siguiente:

- Autenticación (802.1x).
- Integridad (CRC MIC).
- VLAN y VPN.
- Asegurar o deshabilitar servicios.
- Filtros de tráfico.
- Control del área de cobertura inalámbrica.
- Cifrado o encriptación (WEP o AES).

Monitorizar.- Aquí se realizan las siguientes acciones:

- Detectar intrusiones en el tiempo real mediante un proceso de auditoría y llevar un registro.
- Detectar alteraciones de la política de seguridad en la WLAN.
- Validar la implementación de seguridad del punto asegurar.
- Detectar AP falsos.

Probar.- La eficiencia de la política de la seguridad WLAN se valida en este paso, mediante la auditoría realizada del sistema y la búsqueda constante de vulnerabilidades.

Mejorar.- Aquí se realizan las siguientes acciones:

- Utilizar las características de los pasos anteriores para mejorar la implementación WLAN.
- Acoplar la política de seguridad conforme se identifiquen riesgos y vulnerabilidades en el ámbito inalámbrico [1].

Autenticación

Existen dos métodos definidos por 802.11 para realizar la autenticación de usuarios en las redes inalámbricas: la autenticación abierta y la autenticación por clave compartida. El proceso de asociación se puede dividir en los siguientes elementos: sondeo, autenticación y asociación.

El método de autenticación abierta, detallado en la figura 3, es básicamente un método de autenticación nula, significa que existe una verificación del usuario o de la máquina. La autenticación abierta se puede configurar para que utilice o no WEP (*Wired Equiivalent*

Privacy). WEP es un sistema de cifrado incluido dentro del estándar IEEE 802.11 como un protocolo para redes inalámbricas el cual permite cifrar los datos que se transmite [1].

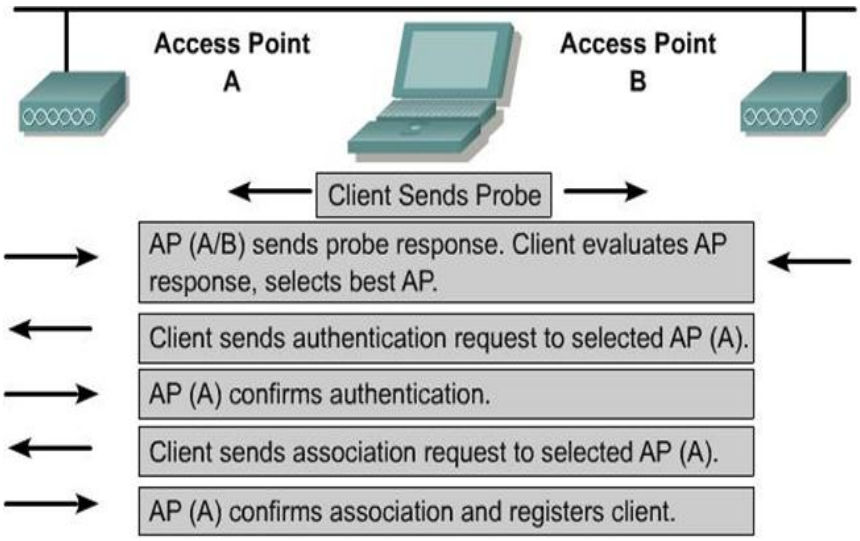


Figura 3. Autenticación abierta [1].

La autenticación por clave compartida detallada en la figura 4, funciona de una manera similar a la abierta, con una excepción ya que utiliza un cifrado WEP para realizar la autenticación. Si el cliente no posee la clave o tiene una errónea falla el proceso de autenticación [1].

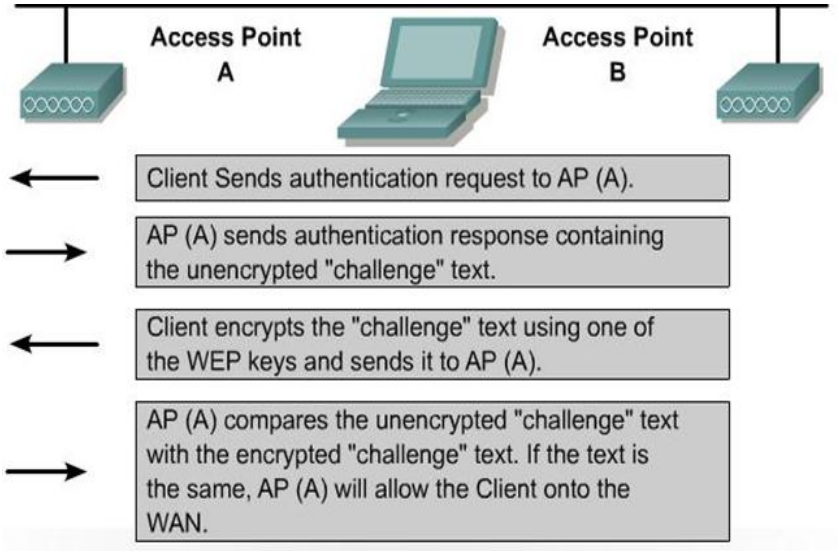


Figura 4. Autenticación por clave compartida [1].

Vulnerabilidades

En ataques especializados las WLAN son vulnerables, estos ataques exploran los puntos poco robustos de la tecnología inalámbrica, las configuraciones por defecto de algunos fabricantes son muy débiles y las contraseñas de administración se las puede obtener fácilmente. También existe vulnerabilidad a nivel de políticas ya que si no se tiene una estructura clara para la elaboración de las mismas los empleados podrían configurar sus propios dispositivos, entre las principales vulnerabilidades tenemos:

- Débil autenticación.
- Cifrado débil de los datos
- No hay integridad el mensaje.

Las vulnerabilidades de seguridad en 802.11 son un obstáculo para la implementación de WLAN a nivel empresarial [1].

Amenazas WLAN

Existen cuatro principales tipos de amenazas a la seguridad inalámbrica:

- Amenazas internas.
- Amenazas externas.
- Amenazas no estructurales.
- Amenazas estructurales.

Las amenazas internas se generan cuando se tiene acceso autorizado a una cuenta directamente en el servidor, o tiene acceso de manera física al cableado estructurado. Las amenazas externas son individuos u organizaciones que operan desde el exterior de la empresa, no tiene acceso a la red inalámbrica.

Las amenazas no estructuradas comprenden generalmente a individuos inexpertos que utilizan los programas o herramientas ya desarrollados para vulnerar la seguridad.

Las amenazas estructurales provienen de intrusos con más conocimiento y con técnicas más competentes, son personas que conocen a profundidad la vulnerabilidad de la red y pueden desarrollar programas o generar scripts que posteriormente comparten con otros intrusos de menor concomimiento [1].

Ataques contra las WLAN

Se pueden clasificar en tres categorías los métodos de ataque inalámbricos:

- Ataques de acceso.
- Ataques de reconocimiento.
- Ataques de denegación de servicio.

Ataques de acceso

Los ataques de este tipo validan la posibilidad de que un individuo no autorizado obtenga acceso a un dispositivo para el que no tiene una cuenta o una contraseña. Uno de los ataques de acceso más sencillo es emplear la ingeniería social, con esta se puede engañar al empleado para que ayuden a facilitar información valiosa. Los siguientes también son ejemplos de este tipo de ataques: explotación de contraseñas débiles o inexistentes, explotación de servicios, como HTTP, CDP, Telnet, FTP, SNMP. Algunos ejemplos de ataques son: ataque de AP (*acces point*) falso y ataques WEP [1].

Ataques de reconocimiento

Los ataques de reconocimiento, es lo que se denomina al descubrimiento, detección y esquematización no autorizadas de servicios, sistemas o vulnerabilidades. Un atacante de este tipo obtiene la mayor cantidad de información antes de comenzar el ataque en sí; utilizan comúnmente rastreadores de paquetes y analizadores de puertos.

Los atacantes utilizan herramientas de Internet para verificar el espacio de asignación de direcciones IP que estén disponibles públicamente y validar las direcciones activas de una empresa o entidad específica [1].

Ataques de denegación

Los ataques de denegación de servicios (Dos), se producen cuando un intruso deshabilitada o corrompe las redes, sistemas o servicios inalámbricos con el objetivo de denegar el servicio a los usuarios que si están autorizados para ocuparlos, generalmente este tipo de ataques emplean la ejecución de una hack, script o herramientas automatizada [1].

1.3 Circuitos Cerrados de Televisión CCTV

Un circuito cerrado de televisión tiene las siguientes funciones principales: reducir pérdidas de bienes materiales, reducir los incidentes de inseguridad alrededor de la institución, comercial u hogar. El efecto más relevante para adquirir o instalar un CCTV es mejorar la supervisión y el control del personal, alumnado, etc.

Dentro del perímetro donde se encuentre instalado. Este tipo de sistemas se han convertido en un factor fundamental para realizar la prevención y control de riesgos e incidentes. Un adecuado CCTV permite monitorear una extensa área utilizando pocos recursos humanos [5].

También en los sistemas modernos se pude automatizar diferentes procesos como son el envío de mails, alertas, llamadas automáticas a dispositivos móviles, auto iluminación, etc. Existen diferentes aplicaciones para los circuitos cerrados de televisión entre las cuales destacan las siguientes:

- Monitoreo de tráfico vehicular.
- Vigilancia en condiciones de completa oscuridad, empleando la luz infrarroja
- Vigilancia en áreas importante como negocios, hoteles, aeropuertos, etc.
- Vigilancia de los infantes en el hogar, escuelas, guarderías, parques.
- Vigilancia en estacionamiento, incluso pudiendo identificar las placas del vehículo.
- Análisis facial para identificación de personas determinadas por la autoridad como peligrosas.
- Monitoreo de procesos industriales de ensamble manual o automático.

En la mayoría de casos el CCTV debe estar complementado con la grabación de eventos que se vigilan con el objetivo de recopilar todos los movimientos importantes y reducir la vigilancia realizada por los seres humano [5].

Elementos que integran un sistema de CCTV

La cámara es el punto de generación de información de todos los sistemas de CCTV. Existen dispositivos que incluyen micrófonos, almacenamiento SD, diferentes aplicaciones y características como: imagen blanco y negro, color o duales para grabación en horarios nocturnos, resistencia a la intemperie, temperatura de funcionamiento adecuado,

iluminación necesaria, resolución en la calidad de la imagen, entre otros. En los sistemas de CCTV más sofisticados se puede adaptar el lente para obtener una mejor solución a los requerimientos, los cuales pueden variar en las siguientes características: ángulo mínimo de observación, vari focal o fijo y telefoto variable o fija [5].

Sistema simple de CCTV

El sistema más simple es instalar una cámara hacia a un monitor conectados mediante cable coaxial, RJ45 o señal inalámbrica con el suministro de la energía eléctrica respectivo, la única imagen que se muestra conforma el sistema. En sus inicios los sistemas incluían una única cámara, posteriormente comenzaron a aparecer sistemas con 2, 3 y 4 cámaras [5].

Sistemas profesionales de CCTV

Las conexiones en este tipo de sistemas permiten una mayor flexibilidad en el diseño de las redes. Cuando se requiere más de una cámara, se debe incluir una aplicación que maneje la conmutación de video. Existen en la actualidad diferentes aplicaciones que controlan las cámaras instaladas en la pantalla respectiva. La aplicación está configurada para controlar el tiempo de grabación de cada cámara [5].

Sistemas con grabación de video:

Los sistemas CCTV tienen diferentes maneras de almacenar la información, una de ellas es utilizando el principio de la funcionalidad de una VCR. La grabación se hará en forma periódica en lugar de realizarse de manera continua, en la videograbadora o en la aplicación de seguridad permite elegir los intervalos de tiempo en los se desea realizar las grabaciones, dependiendo de lo que necesite [5].

Grabadora digital - DVR:

Las videograbadoras digitales (DVRs) tienen la capacidad de transformar el video análogo de los sistemas de CCTV en sistemas digitales, con esta propiedad se puede almacenar la información recabada en dispositivos como CDs, Discos duros, USB etc.; con la ventaja de poder transmitir datos usando Internet. También brindan la posibilidad de realizar búsquedas rápidas, respaldo de información e impresión de imágenes. En la actualidad,

es posible utilizar un VCR o una DVR, de acuerdo a sus necesidades. Los sistemas DVR cubren tres funciones multiplexor, grabador y servidor IP [5].

Almacenamiento de video vigilancia

La capacidad de almacenamiento es importante y fácil de malinterpretar entre los distintos criterios que afectan el valor del sistema de grabador de video digital en la video vigilancia. Debido a que las transmisiones de video ininterrumpidas son básicamente la esencia de los sistemas de video vigilancia a fin de brindar un desempeño y eficiencia, el almacenamiento para abordar tres parámetros de video fundamentales:

Almacenamiento: el plazo de tiempo en que se almacenarán las transmisiones de video.

Calidad: expresada en términos de la resolución por cuadro (por ejemplo, 1280x1024 píxeles) y cuadros por segundo (*frame per second*).

Cantidad: el número y duración de las transmisiones de video.

Se debe determinar un equilibrio específico de cantidad, calidad y almacenamiento de los datos de video para una aplicación de seguridad determinada, es sencillo calcular la cantidad de capacidad de almacenamiento que debe incluir un sistema de video vigilancia. Una forma es tener los parámetros establecidos según las siguientes figuras. La figura 5 refleja la compresión MPEG-4. Los resultados variarán en función de los formatos de compresión de video empleadas [6].

NTSC: Recording Variable: 10fps			Surveillance Hard Drive Capacity					
			1TB	2TB	3TB	4TB	5TB	6TB
176 x 120	Low Quality	# Days	694	1388	2082	2776	3470	4164
352 x 240		# Days	266	532	798	1064	1330	1596
704 x 480		# Days	86	172	258	344	430	516
1280 x 1024	High Quality	# Days	26	52	78	104	130	156

NTSC: Recording Variable: 20fps			Surveillance Hard Drive Capacity					
			1TB	2TB	3TB	4TB	5TB	6TB
176 x 120	Low Quality	# Days	346	692	1038	1384	1730	2076
352 x 240		# Days	132	264	396	528	660	792
704 x 480		# Days	42	84	126	168	210	252
1280 x 1024	High Quality	# Days	12	24	36	48	60	72

NTSC: Recording Variable: 30fps			Surveillance Hard Drive Capacity					
			1TB	2TB	3TB	4TB	5TB	6TB
176 x 120	Low Quality	# Days	230	460	690	920	1150	1380
352 x 240		# Days	88	176	264	352	440	528
704 x 480		# Days	28	56	84	112	140	168
1280 x 1024	High Quality	# Days	8	16	24	32	40	48

Figura 5. Matriz de almacenamiento de vigilancia por video.
(Se asume codificación MPEG-4) [6].

La figura 6 refleja la compresión H.264. Los resultados variarán en función de los formatos de compresión de video empleadas [6].

NTSC: Recording Variable: 10fps			Surveillance Hard Drive Capacity					
			1TB	2TB	3TB	4TB	5TB	6TB
176 x 120	Low Quality	# Days	1080	2160	3240	4320	5400	6480
352 x 240		# Days	414	828	1242	1656	2070	2484
704 x 480		# Days	134	268	402	536	670	804
1280 x 1024	High Quality	# Days	40	80	120	160	200	240

NTSC: Recording Variable: 20fps			Surveillance Hard Drive Capacity					
			1TB	2TB	3TB	4TB	5TB	6TB
176 x 120	Low Quality	# Days	540	1080	1620	2160	2700	3240
352 x 240		# Days	206	412	618	824	1030	1236
704 x 480		# Days	66	132	198	264	330	396
1280 x 1024	High Quality	# Days	20	40	60	80	100	120

NTSC: Recording Variable: 30fps			Surveillance Hard Drive Capacity					
			1TB	2TB	3TB	4TB	5TB	6TB
176 x 120	Low Quality	# Days	360	720	1080	1440	1800	2160
352 x 240		# Days	138	276	414	552	690	828
704 x 480		# Days	44	88	132	176	220	264
1280 x 1024	High Quality	# Days	14	28	42	56	70	84

Figura 6. Matriz de almacenamiento de vigilancia por video.
(Se asumen codificación H.264) [6].

Se puede utilizar una configuración básica determina según se requiera, a continuación se presenta tres casos en los que los parámetros pueden variar.

Archivado extendido

Hay muchas empresas en que las transmisiones de video de alta resolución no son exigentes. Cuando estas grabaciones pueden ser relativamente bajas, los beneficios de una mayor capacidad de HDD son fundamentales.

Para ello se puede utilizar una resolución de 10 fps/352x240 en la cual se puede transmitir información a una unidad de 6 TB durante 1596 días con compresión MPEG-4 y una cifra sorprendente de 2484 días con codificación H.264 [6].

Calidad mejorada

Los entornos más rigurosos (por ejemplo, escuelas, edificios públicos y aeropuertos) se necesitan una mayor resolución y más cuadros por segundo a fin de identificar a las personas y actividades extrañas con mayor eficacia, para ello es posible configurar una

imagen de 20 fps/704x480 puede llenar una unidad de 1 TB en solo 42 días con compresión MPEG-4 y la compresión H.264 extiende el almacenamiento de video a 66 días en este escenario [6].

Video inteligente

En este modelo se necesita un nivel de detalle que se encuentra en las transmisiones de video ininterrumpidas de alta resolución y movimiento completo (30 fps).

El uso más representativo de esta tecnología es el reconocimiento facial cuando se encuentra una coincidencia, la aplicación notifica automáticamente al personal de seguridad de una actividad sospechosa.

Para ello podemos utilizar una compresión MPEG-4, una sola transmisión continua a una resolución de 30 fps/1280x1024 agota completamente la capacidad de una unidad de 4 TB en solo 48 días, mientras que la codificación H.264 brinda aproximadamente 84 días [6].

Réplica de información usando *Robocopy*

El comando *Robocopy* es uno de los comandos más empleados y útiles en la línea de comandos de Windows. Este comando permite copiar carpetas, archivos, directorios ya sea en una equipo local o en la red, toma las propiedades de los conocidos *COPY* y *XCOPY*, y las perfecciona en su máxima expresión.

Ventajas al emplear el comando *Robocopy:*

- Acepta las interrupciones en la copia de información que pueden ser cortes eléctricos o en la conexión al destino.
- Realiza reintentos automáticos de copia si no es posible acceder a un archivo.
- Permite copiar extensas cantidades de información.
- Presenta un indicador de progreso de la copia.
- Permite copiado multi hilo.
- Copia efectivamente toda la información del documento manteniendo inalterables los permisos del archivo [7].

Modos de empleo de *Robocopy* más utilizados.

ROBOCOPY ORIGEN DESTINO /E Permite copiar de forma recursiva carpetas con subdirectorios aunque estén vacíos.

ROBOCOPY ORIGEN DESTINO /MIR modo espejo, copia de forma recursiva pero al terminar elimina archivos en el destino que ya no existen en el origen.

ROBOCOPY ORIGEN DESTINO /S Copia de forma recursiva carpetas con subdirectorios pero no los vacíos.

ROBOCOPY ORIGEN DESTINO *.* /E En este proceso solo se copiarán documentos de extensión del archivo colocado entre los asterisco [7].

Algunas opciones para emplear con *ROBOCOPY:*

- /R:n Número de reintentos en caso de algún error.
- /W:n Tiempo de espera entre reintentos.
- /MT:n Realiza copias multiproceso, n especifica el número de hilos, el valor predeterminado es 8, n debe estar comprendido entre 1 y 128.
- /MOV Mueve archivos y los elimina del origen después de ser copiados.
- */MOVE*.-Mueve archivos y carpetas y los elimina del origen después de ser copiados.
- /V Mostrar información detallada durante la copia[7].

Aplicación *iSpy: Open Source Camera Security Software*

Los usuarios pueden utilizar cámaras de video vigilancia utilizando una conexión directa o a través de direcciones IP. Un equipo de video vigilancia completamente equipado con cámaras, grabador, monitor dedicado para estos procesos es bastante costoso, por lo que una mejor opción es adquirir las cámaras por separado, para posteriormente instalar un *software* gratuito que realice las tareas de grabación y monitoreo.

Los fabricantes de cámaras ofrecen un *software* propio que permite ingresar a la configuración básica de los equipos, generalmente es sencillo y sus funciones en la mayoría de ocasiones son insuficientes para satisfacer las necesidades de los usuarios.

Existen *software* más avanzados de control, sin embargo, la mayoría de ellos son licenciados y quedan lejos del alcance de un usuario promedio, presentando limitaciones en cuanto a las marcas y modelos de cámaras compatibles [8].

iSpy es un *software* de código abierto, que permite el control de cámaras de gran nivel y permite a los usuarios administrar sus dispositivos de forma totalmente gratuita a través de una interfaz muy intuitiva.

Las principales características de *iSpy* son:

- Permite vincular cámaras, micrófonos para grabar audio y vídeo sincronizado.
- Permite vigilar tantas cámaras como se desee.
- Detecta, graba y sigue el movimiento.
- Permite capturar información usando horarios programados.
- Detección facial con reconocimiento.
- Permite grabar automáticamente a un servidor FTP.
- Reconocimiento de ciertos objetos (por ejemplo, matrículas de vehículos).
- Escucha y graba micrófonos remotos en tiempo real [9].

Los programas de video vigilancia más completos difieren en pocas características con este *software* de código abierto, por lo que es una excelente alternativa tanto para usuarios domésticos y empresas que necesiten un sistema de video vigilancia controlado localmente y a pequeña escala [9].

Entre los lugares más típicos en donde se utiliza esta aplicación son el hogar; vigilancia en la oficina, vigilancia en la empresa, vigilancia en locales comercial.

Se puede emplear para realizar automatizaciones en la aplicación *iSpy* y enviar archivos por lotes a través de Internet usando una línea de comando.

También es posible habilitar la detección de movimiento para protecciones contra robos, iSpy puede iniciarse en el arranque del sistema y comenzar a grabar usando esta función. Finalmente puede automatizar los envíos de archivos por FTP (*file transfer protocol*), correo electrónico o SMS de las imágenes capturadas [9].

2. METODOLOGÍA

Previo a la ejecución del presente proyecto fue necesario realizar el levantamiento de información de los requerimientos necesarios por parte de la Unidad Educativa. Para ello fue necesario visitar la Unidad Educativa “Abelardo Moncayo” en varias ocasiones, con el propósito de obtener la mayor cantidad de información y determinar los lugares más idóneos para colocar los equipos.

Se realizó varias inspecciones físicas y se creó los planos digitales de la Unidad Educativa a partir de algunos documentos entregados por el Sr. Rector.

Como parte de estas inspecciones se revisó la infraestructura del plantel para determinar que equipos son adecuados y cuales hacen falta para implementar el proyecto.

Para realizar el diseño se detectó que la institución no tiene un sistema de respaldo de energía, por cual es una vulnerabilidad que pueda ser neutralizada realizando otro proyecto de carácter eléctrico.

El diagrama del plantel educativo fue diseñado el programa Autocad 2018 LT. Se realizó un diagrama en donde se especificó los puntos en donde se instalaron las cámaras de la red de video vigilancia.

Se seleccionó el *software iSpy: Open Source Camera Security Software* el cual es muy apropiado para el desarrollo del proyecto por su flexibilidad y las funciones que tiene frente a aplicaciones de uso libre.

Se planteó la posibilidad de realizar el envío de mensajes de texto de alerta hacia un número de teléfono utilizando una cuenta de Exchange configurada en el pc servidor mediante un proveedor de servicios de telefonía móvil.

En la implementación de las cámaras internas y externas y los se realizó trabajos de cableado estructurado establecidos en el diseño.

Posteriormente se realizó la configuración de cada una de las cámaras y validó su funcionamiento. Los equipos routers LINKSYS E900 fueron configurados para distribuir la conexión a las diferentes cámaras asignado una IP diferente para cada una.

Para el proceso de almacenamiento y control se utilizó un equipo computacional usado como servidor el cual tiene instalado un sistema operativo Windows server 2012 R2 en el cual se instaló la aplicación que controlará los dispositivos inalámbricos y realizará el almacenamiento de información recolectada por las cámaras.

Posteriormente, se realizó la configuración para almacenar las últimas 24 horas de grabación de las cámaras más importantes a la nube, accediendo a cuentas como Google drive o en su versión de Cloud G Suite.

3. RESULTADOS Y DISCUSIONES

3.1 Contexto de la Institución

La Escuela de Educación Básica “Abelardo Moncayo” es una institución educativa ubicada en la provincia de Pichincha, en la parroquia Llano Chico del cantón Quito.

La institución está dedicada a fomentar el desarrollo académico en la juventud en dicha parroquia. Tiene una infraestructura otorgada por el gobierno, la cual tiene algunas limitaciones que son visibles, por ejemplo: aulas en estado regular, cerramiento del perímetro de la institución con poca elevación, instalaciones eléctricas en reformación, lugares con poca visibilidad para las autoridades del plantel, entre otros.

Por estos motivos y por la cantidad de personas que acuden diariamente a la institución, es conveniente instalar un sistema de seguridad de video vigilancia para salvaguardar la integridad de las personas y los bienes materiales del plantel.

La institución cuenta con 649 alumnos dividido en dos jornadas de estudio matutino (442 alumnos) y vespertino (207 alumnos).

A nivel organizacional la unidad educativa está bajo la dirección del Lic. Ernesto Mora, Rector de la Institución; quien se encarga del área administrativa, además, cuenta con 23 educadores y 1 persona para los servicios de conserjería.

Ubicación geográfica de la institución.

La Escuela de Educación Básica Abelardo Moncayo está actualmente ubicada en la provincia de Pichincha en el cantón Quito, en el centro de la parroquia de Llano Chico con

la siguiente dirección: Av. Carapungo E173 y Arturo Hinojosa, como se muestra en la figura 7 y figura 8.

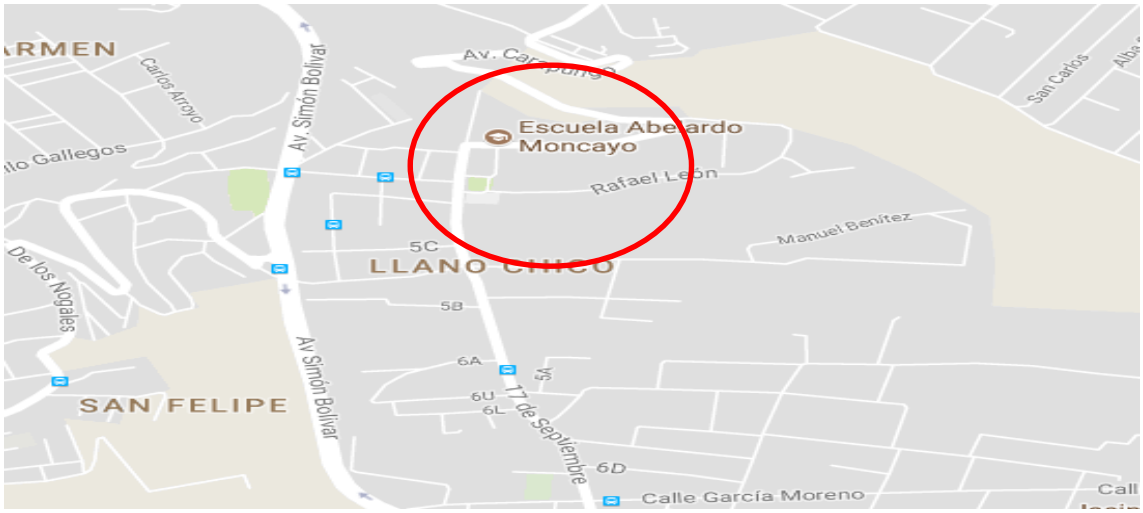


Figura 7. Ubicación de la Unidad Educativa Abelardo Moncayo.

Figura 8. Ubicación de la Unidad Educativa Abelardo Moncayo.

La Escuela de Educación Básica “Abelardo Moncayo” no tenía planos generados en forma digital, por lo cual después de realizar la inspección inicial de la institución fue necesario crear los planos en el programa AutoCad LT 2017 con las dimensiones entregas por el Rector de la institución. Las dimensiones de la institución educativa son 41,5 m de frente por 61,2 m de largo, lo cual genera un área total de 2539,8 m². Los planos detallados se muestran en la figura 9.

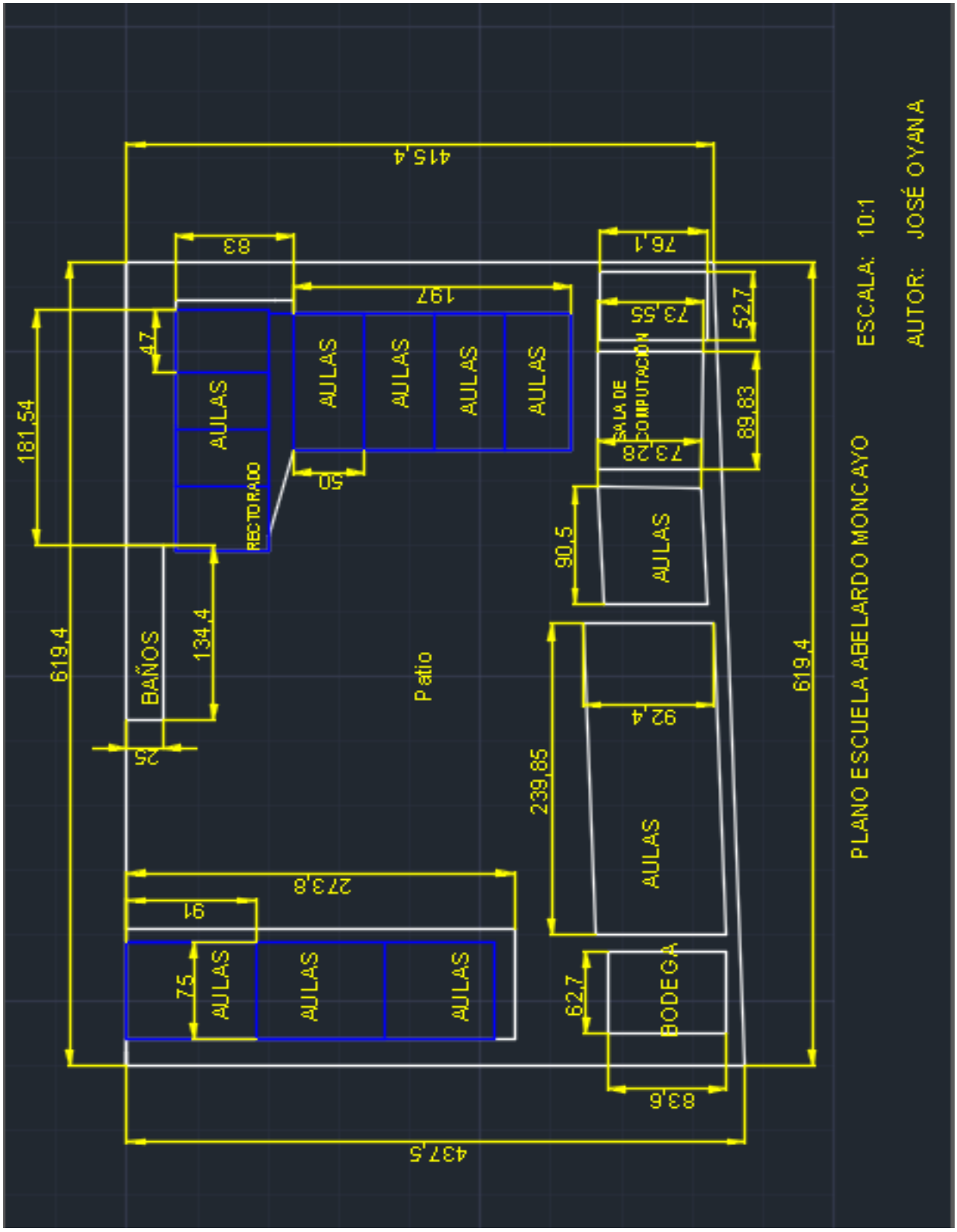


Figura 9. Planos de la Unidad Educativa Abelardo Moncayo.

3.2 Levantamiento de información

Como se puede observar en las figuras 4 y 5, la Unidad Educativa posee una amplia infraestructura, por tal circunstancia se solicitó la colaboración del Lic. Ernesto Mora, rector de la institución, para generar los requerimientos mínimos en la implementación de la red de video vigilancia, los mismos que se detallan a continuación:

- Realizar la ubicación de las cámaras externas alrededor del perímetro de la institución.
- Las cámaras no deben colocarse con vista al patio de la institución ya que se violaría el derecho a la privacidad del alumnado.
- Se deben colocar las cámaras en puntos estratégicos que permitan obtener el máximo beneficio en la supervisión y control de los alumnos y también de las personas que laboran e ingresan al plantel educativo.
- Las cámaras deben tener acceso mediante vía Web (acceso desde un celular, tablet o computador que tenga conexión a Internet).
- Las cámaras deben utilizar tecnología WIFI y soportar el estándar establecido IEEE 802.11.
- Las cámaras internas y externas deben tener sensores infrarrojos, que permitan realizar la grabación sin luz natural.
- El equipo de control debe estar conectado a una fuente de alimentación regulada, en lo posible con respaldo de energía.
- El software de gestión de la red de video vigilancia debe tener la capacidad de realizar las grabaciones y un control de autenticación para que solo pueda ingresar el personal autorizado.
- Se debe garantizar la estabilidad del sistema de video vigilancia dentro de las limitaciones de la infraestructura de la institución.
- Colocar solo dos cámaras internas.
- Instalar cuatro cámaras externas en la periferia de la institución.

Como se ha mencionado en los requerimientos anteriormente detallados el Lic. Ernesto Mora solicitó realizar una modificación en la propuesta inicial la cual consistía en cuatro cámaras internas y cuatro cámaras externas; por dos cámaras internas y cuatro cámaras externas de seguridad. Este cambio se debió, principalmente, a que en el artículo 7, literal l, de la Ley Orgánica de Educación Intercultural expresa que *“el estudiante debe gozar de*

la privacidad y el respeto a su intimidad"; por lo tanto, no se puede colocar cámaras donde haya una amplia visibilidad al alumnado como puede ser un aula. La segunda cámara interna también fue retirada debido a que el edificio no cuenta con la infraestructura necesaria para colocar la misma y tener una buena visibilidad de la parte frontal exterior de la unidad educativa [10].

Reconocimiento de la infraestructura de red actual

La unidad educativa consta con una infraestructura básica a nivel de conectividad tecnológica y computacional. Cuenta con un laboratorio de computación el cual no posee una unidad de UPS para el respaldo eléctrico de los equipos. En las distintas zonas que se van a ubicar las cámaras existe disponibilidad de una toma eléctrica cercana. El equipo que ofrece el servicio de Internet a la institución pertenece al proveedor CNT y está ubicado físicamente en el rectorado.

Determinación de las zonas de instalación de las cámaras.

Considerando los requerimientos antes mencionados y con la aprobación de las autoridades de la institución se designó las siguientes zonas para la colocación de las cámaras:

ZONA 1: Parte posterior lado oeste. Permite visualizar la parte posterior de la Unidad Educativa observando hacia el lado este, como se muestra en la figura 10.

Figura 10. Detalle zona 1 de instalación de las cámaras.

ZONA 2: Parte posterior lado este. Permite visualizar la parte posterior de la Unidad Educativa observando hacia el lado oeste, como se muestra en la figura 11.

Figura 11. Detalle zona 2 de instalación de las cámaras.

ZONA 3: Parte superior segundo piso de aulas. Permite visualizar la parte lateral externa de la Unidad Educativa observando hacia el lado este, como se detalla en la figura 12.

Figura 12. Detalle zona 3 de instalación de las cámaras.

ZONA 4: Parte lateral oeste. Permite visualizar la parte lateral externa de la Unidad Educativa observando hacia el lado oeste, mostrada en la figura 13.

Figura 13. Detalle zona 4 de instalación de las cámaras.

ZONA 5: Hall de entrada a la institución. Permite la visualización de la entrada principal desde el interior de la Unidad Educativa, mostrada en la figura 14.

Figura 14. Detalle zona 5 de instalación de las cámaras.

ZONA 6: Ingreso al laboratorio de computación. Permite la visualización del ingreso y salida al laboratorio de los equipos computacionales, mostrada en la figura 15.

Figura 15. Detalle zona 6 de instalación de las cámaras.

3.3 Diseño de la red de cámaras inalámbricas

En esta sección está representado el diseño de la red de cámaras inalámbricas de acuerdo a la toma de requerimientos acorde a la infraestructura del plantel educativo.

Especificaciones de las cámaras de acuerdo a la zona

A continuación, se detallan las cámaras que fueron seleccionadas de acuerdo a las características requeridas en el levantamiento de información. Se realizó la instalación de 4 cámaras externas y 2 internas, estas últimas están colocadas en partes exteriores, pero bajo techo cubierto. Las características de los equipos externos deben cumplir los siguientes requisitos:

1.- Realizar grabación de video en la oscuridad, para realizar la vigilancia en horas de la noche y poca luz natural.

2.- Girar en un ángulo de 90 grados. Debido a que las zonas de cobertura tienes espacios reducidos y una cámara con mayor ángulo de giro sería un desperdicio.

3.- Resistencia a la intemperie. Es necesaria esta característica debido a que las cámaras están colocadas en sitios exteriores a las edificaciones del plantel.

4.- Conectividad inalámbrica. Por facilidad de instalación en las edificaciones del plantel educativo que se encuentra en cambios de constantes de obras civiles.

5.- Calidad de video medio-alto. Se debe garantizar la calidad de la imagen al momento de realizar las grabaciones para identificar claramente los incidentes capturados por las cámaras.

6.- Recepción de señal a gran distancia. La distancia que se debe cubrir por parte de las cámaras es amplia por tal motivo debe tener suficiente recepción de la señal.

Las características de las cámaras internas deben cumplir los siguientes requisitos:

1.- Realizar grabación de corto alcance. Debido a que las cámaras están en accesos internos.

2.- Girar en un ángulo de 90 grados. Debido a que los lugares de instalación son reducidos.

3.- Protección tipo domo. Se necesita que las cámaras estén protegidas contra golpes ya que se las colocara en sitios más accesibles para el alumnado.

4.- Conectividad inalámbrica. Por facilidad de instalación en las edificaciones del plantel educativo que se encuentra en cambios de constantes de obras civiles.

5.- Calidad de video medio. Se debe garantizar la calidad de la imagen al momento de realizar las grabaciones para identificar claramente los incidentes capturados por las cámaras, sin embargo, al estar enfocadas en lugares a poca distancia la calidad de video medio es suficiente.

Selección de equipos

Antes de proceder con la compra de los dispositivos se realizó un análisis de las distintas cámaras ofertadas en el mercado en donde se observó una gran variedad de productos, así como también la diversidad de precios y funciones.

A continuación, se detallan las características de algunos equipos que fueron preseleccionados, los cuales cumplieron con los requisitos anteriormente mencionados:

Tabla 1. Especificaciones cámaras externas e internas.

Cámaras Externas:

CÁMARA	RESOLUCIÓN	ILUMINACIÓN	RANGO IR	ALIMENTACIÓN	CONEXIÓN	FUNCIONES	DIMENSIÓN PESO	PRECIO	OBS
MOTOROLA FOCUS 73	Colour CMOS 1M Pixels	0.01Lux@1.2 AGC on 0Lux	hasta 20 metros 90°	100-240V AC, 50/60Hz, 300mA	802.11 b/g/n	BLC/ HLC/	Dim: 100x140x50 mm Peso: 4750g	$180	IMPORTADA
DAHUA DH-IPC-HFW1120SN-W-0360B	1.3 Megapixel progressive scan CMOS	0.025Lux/F2.1(Color), 0 Lux/F2.1(IR on)	30 metros 90°	DC12V , PoE (802.3af)	Wifi-suppot	BLC/ HLC/DWDR	Dim: 70x167x62 mm Peso: 490 g	$125	N/A
2MP DS-2CD2020F-IW	2MP (1920x1080@30 fps)	0.01Lux@1.2 AGC on 0Lux	hasta 20 metros 90°	12 VDC +/- 10% - Consumo Max. 5,8W	Wireless 2.4 Ghz/ lan	D-WDR, 3D DNR, DWDR, BLC	Dim: 70x157x62 mm Peso: 500 g	$180	N/A

Cámaras Internas:

CÁMARA	RESOLUCIÓN	ILUMINACIÓN	RANGO IR	ALIMENTACIÓN	CONEXIÓN	FUNCIONES	DIMENSIÓN PESO	PRECIO	OBS
D-link DCS-5030 L	CMOS 1/5" progresivo 2.2 mm	Iluminación mínima 0.01 Lux / 0 Lux IR.	hasta 8 metros, 90°	12 VDC ± 10%,	Wireless IEEE 802.11n/b/g	BLC/ HLC/DWDR	Dim: Φ105 × 80 Peso: 500 g	$ 210	N/A
CHACON WIFI HD 34547	720p (1280 x 720 pixels)	0.01Lux@1.2 AGC on 0Lux	PIR 8m, 90°	12 VDC ± 10%,	Wi-Fi / Ethernet (RJ45)	BLC/ HLC/AUDIO	Dim: Φ110 × 90 Peso: 600 g	$ 80	IMPORTADA
Hikvision XC-2110F-IW	1.3 MpCMOS 1/2.8" Scan Progresivo.	Iluminación mínima 0.01 Lux / 0 Lux IR.	hasta 30 metros, 90°	12 VDC ± 10%, PoE (802.3af).	Wireless 2.4 Ghz/ lan	BLC/ HLC/DWDR	Dim: Φ111 × 82 Peso: 500 g	$ 140	N/A

De acuerdo al cuadro de especificaciones de los equipos preseleccionados que cumplen con las características ideales además de tener un precio asequible para realizar la implementación en la red de video vigilancia se consideraron los siguientes:

Cámara interna: Hikvision XC-2110F-IW

Figura 16. Cámara Hikvision XC-2110F-IW [11].

Cámara externa: DAHUA DH-IPC-HFW1120SN-W-0360B

Figura 17. Cámara DAHUA DH-IPC-HFW1120SN-W-0360B [12].

Router

El equipo seleccionado fue el router LINKSYS E900 el cual está colocado para obtener la mayor área de cobertura posible. Este equipo es ideal para administrar redes *Wireless* LAN a mediana escala. En la figura 18 se muestra las características del equipo seleccionado [13].

Características router Linksys E900

- Especificaciones
- Nombre del modelo: Linksys E900
- Estándares de red:

    - IEEE 802.11b
    - IEEE 802.11a
    - IEEE 802.11g
    - IEEE 802.11n
    - IEEE 802.3
    - IEEE 802.3u

- Bandas de radiofrecuencia: 2,4 GHz
- Puertos: 1 10/100 WAN, 4 10/100 LAN
- Indicadores LED: Alimentación, WLAN, Ethernet (1-4), Internet
- Compatibilidad con plataformas:
    - Windows XP
    - Windows Vista 32/64
    - Windows 7 32/64
    - Windows 8 32/64
    - Windows 8,1 32/64
    - Mac OS X 10.5.8 Leopard
    - Mac OS X 10.8 Mountain Lion
    - Mac OS X 10.9 Mavericks

Figura 18. Router LINKSYS E900 [13].

PC servidor

El equipo PC servidor tiene instalado el sistema operativo *Windows Server* 2012 R2. En el cual utilizando los parámetros de configuración propia del sistema operativo y adicionando los componentes necesarios, se instaló el software de control y monitoreo iSpy: (*Open Source Camera Security Software*). El equipo PC servidor tiene una memoria RAM de 4 GB, disco de almacenamiento de 500 GB con espacio físico para instalar otro disco duro interno, características suficientes para gestionar toda la red de video vigilancia. Se ha colocado el nombre de video vigilancia SERVER_UEAM_VID mostrado en la figura 19.

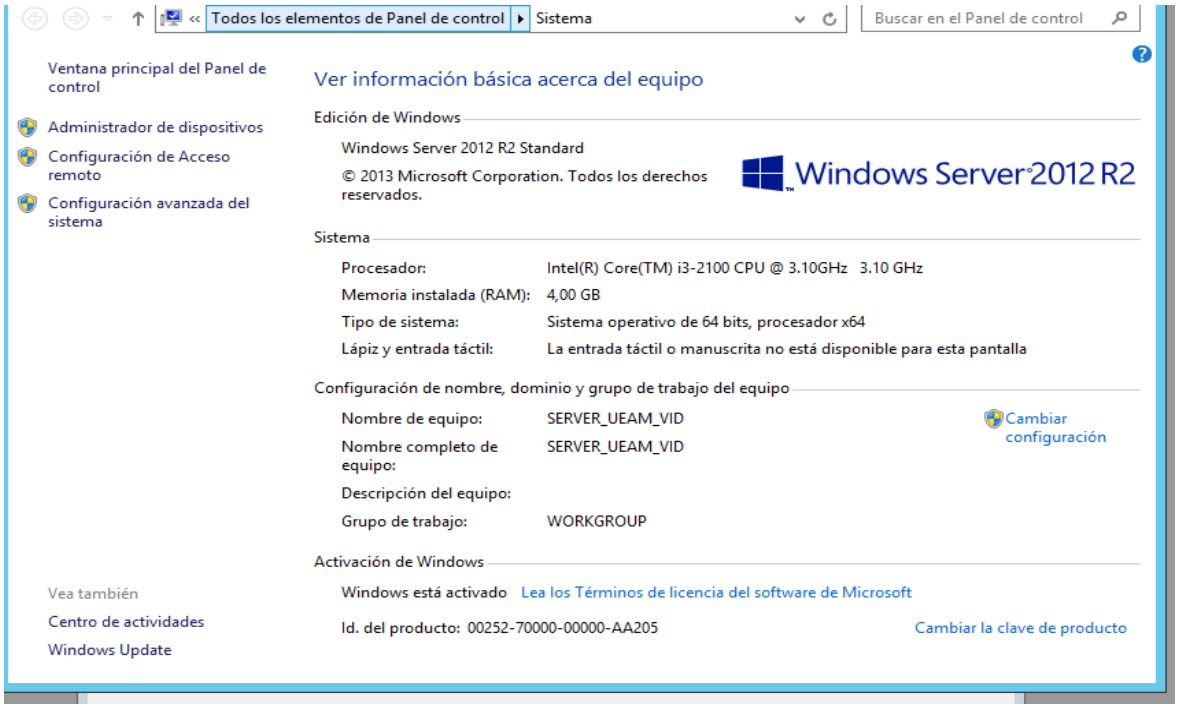


Figura 19. Servidor video vigilancia UEAM.

3.4 Esquema de la red inalámbrica

De acuerdo a los procedimientos que se detallaron en la sección de metodología, el diseño de la red inalámbrica mostrado en la figura 20, detalla la forma en la que están interconectados los equipos en la red de video vigilancia y su conexión de Internet.

El router uno administra toda la red y entre sus funciones principales están: generar la red inalámbrica con la autenticación WPA- 2 personal y conectar las cámaras a la misma, también se realiza la reserva de direcciones IP de cada cámara.

Las cámaras tienen configurada una dirección IPV4 fija identificada para acceder remotamente a las mismas y poder validar las configuraciones respectivas. El router dos está configurado en modo puente para que únicamente haga la función de repetidor de señal hacia las cámaras de la parte posterior de la unidad educativa.

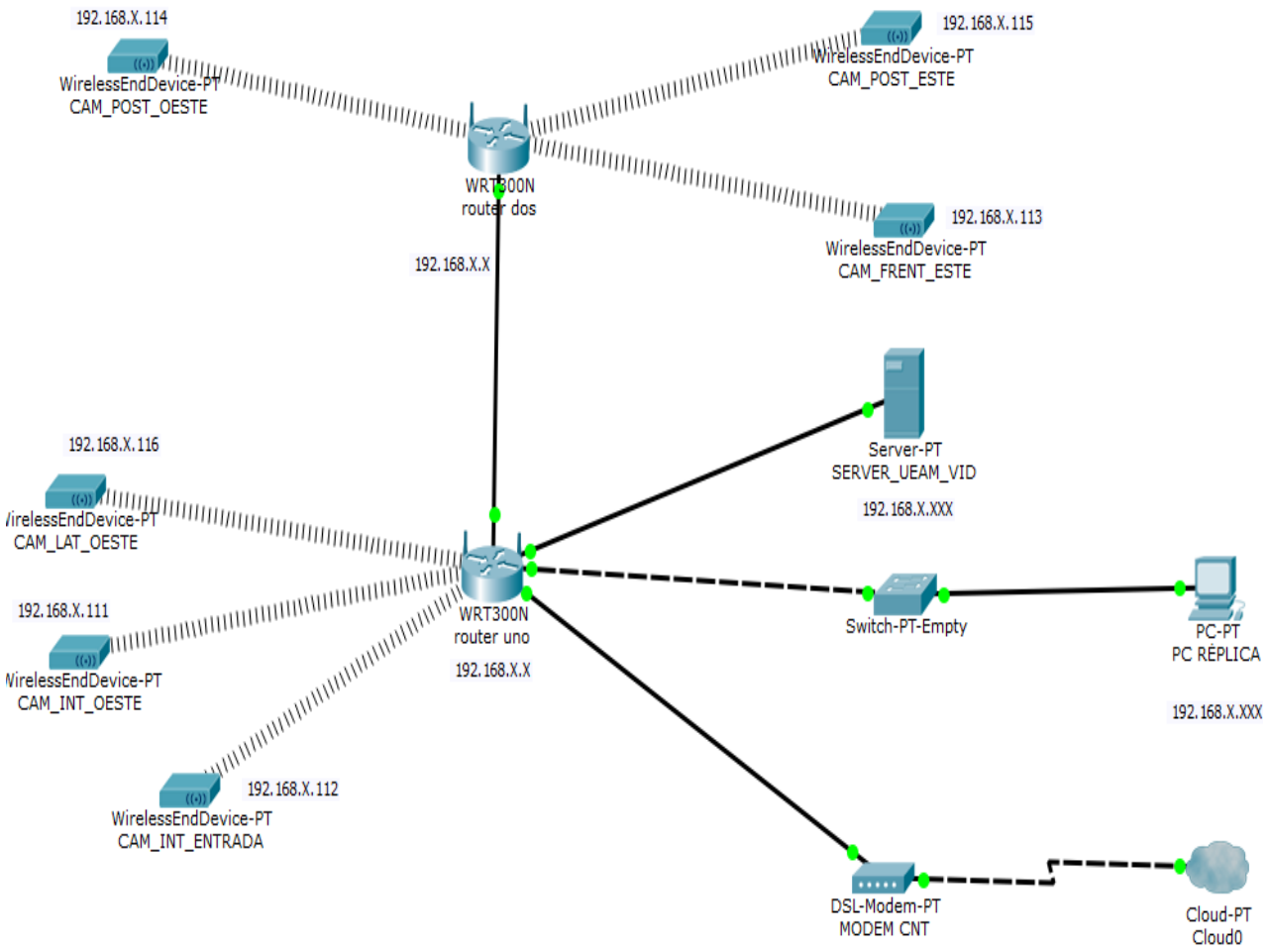


Figura 20. Diseño de la red de video vigilancia.

El router inalámbrico Linksys E900 ofrece un direccionamiento de IPv4 con direcciones privadas en el rango 192.168.x.0 a 192.168.x.255, para utilizarlas dentro de una red privada o doméstica. El direccionamiento de las IP utilizadas está configurado a partir de la dirección 192.168.x.100 en adelante. Los routers y el servidor están interconectados a través de un switch por medio de una conexión LAN Ethernet. El router uno proporciona la salida de Internet por que está conectado directamente hacia el modem del ISP (Proveedor de servicios de internet) CNT.

Ubicación de los equipos.

Las cámaras están ubicadas en los lugares en donde se tenga una mayor visibilidad, campo de visión amplio y una señal adecuada para un funcionamiento óptimo. Los routers están colocados en puntos adecuados para brindar una señal óptima a los equipos, en la figura 21 se muestra el plano de la institución educativa donde se hizo el análisis para instalación de los equipos.

Figura 21. Plano de la Institución Educativa.

Selección de los puntos idóneos para la ubicación de las cámaras

Para que los equipos sean una herramienta útil en la vigilancia, el control y la supervisión; fueron ubicados de forma adecuada en cada una de las zonas designadas con anterioridad, en las siguientes figuras se muestra el plano de la unidad educativa y los lugares más idóneos donde se ubicaron los equipos. Para cada zona se indican los posibles puntos analizados para colocar las cámaras.

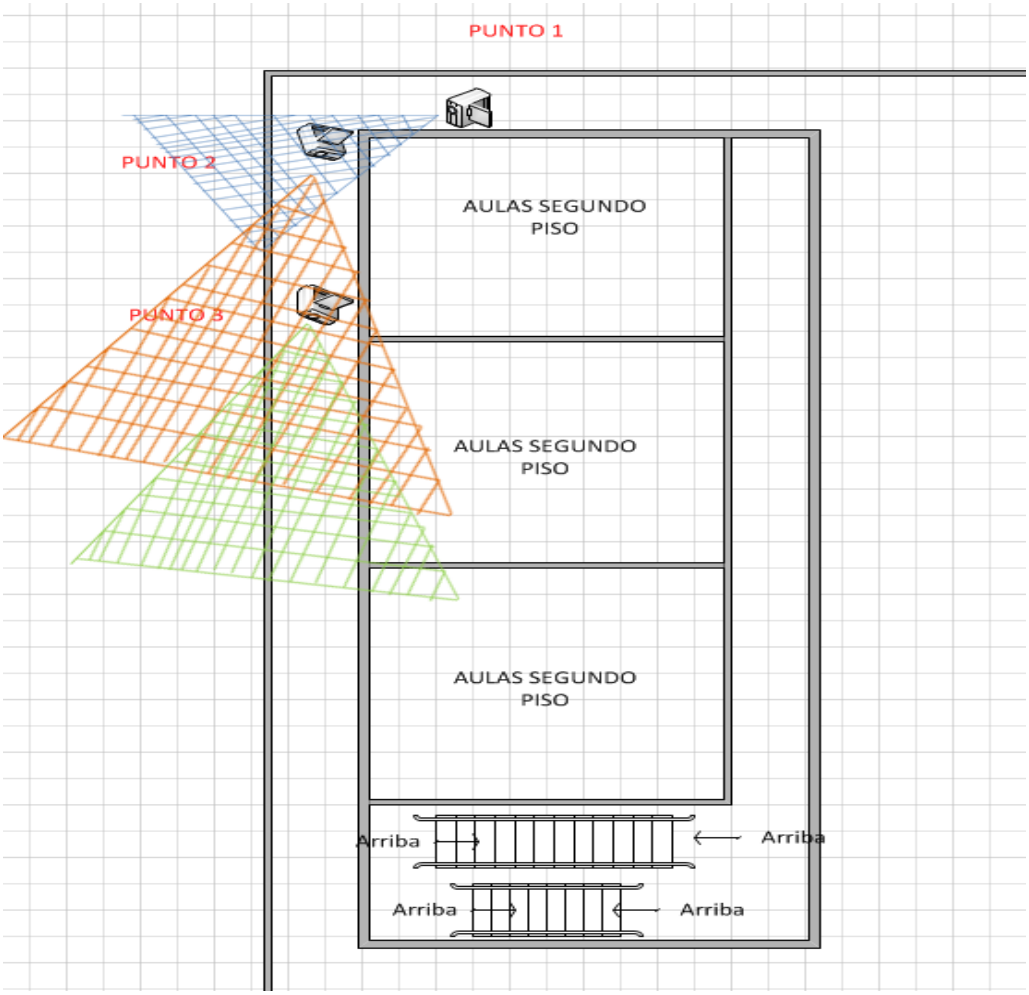


Figura 22. Puntos de colocación posibles cámara zona 1.

Para determinar la ubicación de la cámara de la zona 1, representada en la figura 22, se tomó en cuenta que el objetivo es visualizar la parte posterior de la institución, controlar el acceso y salida ilícita del alumnado o de alguna persona ajena al plantel, debido principalmente a que el cerramiento no tiene una altura adecuada y es relativamente sencillo ingresar o salir de la institución.

Se descartó el punto número uno ya que se observa parcialmente el cerramiento de la Unidad Educativa y el campo de visión de la cámara estaría desperdiciado. El punto número tres no visualiza la parte inferior de la esquina del cerramiento y no tiene una toma eléctrica cerca para realizar la conexión, siendo esta parte importante de vigilancia. El punto número dos es el ideal ya que permite visualizar toda la parte posterior incluido el cerramiento y el pasillo posterior.

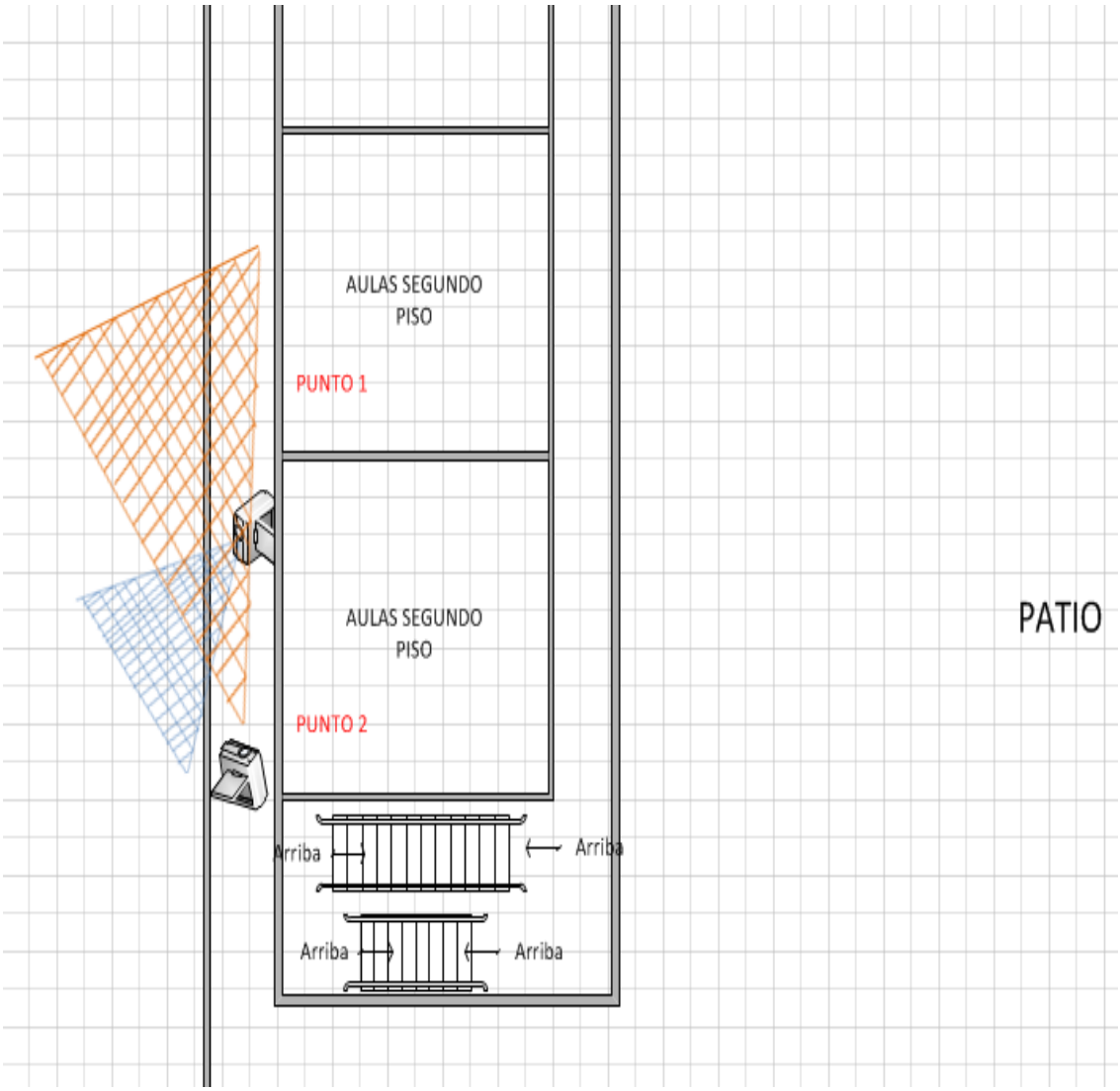


Figura 23. Puntos de colocación posibles cámara zona 2.

Para determinar la ubicación adecuada de la cámara de la zona 2, representado en la figura 23, se analizó la posibilidad de obtener un mayor ángulo de visualización del cerramiento posterior de la unidad educativa. Se descartó el punto uno debido a que no

es posible visualizar el cerramiento posterior en su totalidad y la infraestructura del edificio no permite colocar la cámara en este punto. El punto dos es el ideal ya que se tiene el mayor ángulo de visibilidad a la parte posterior del plantel y la conexión eléctrica a una distancia cercana.

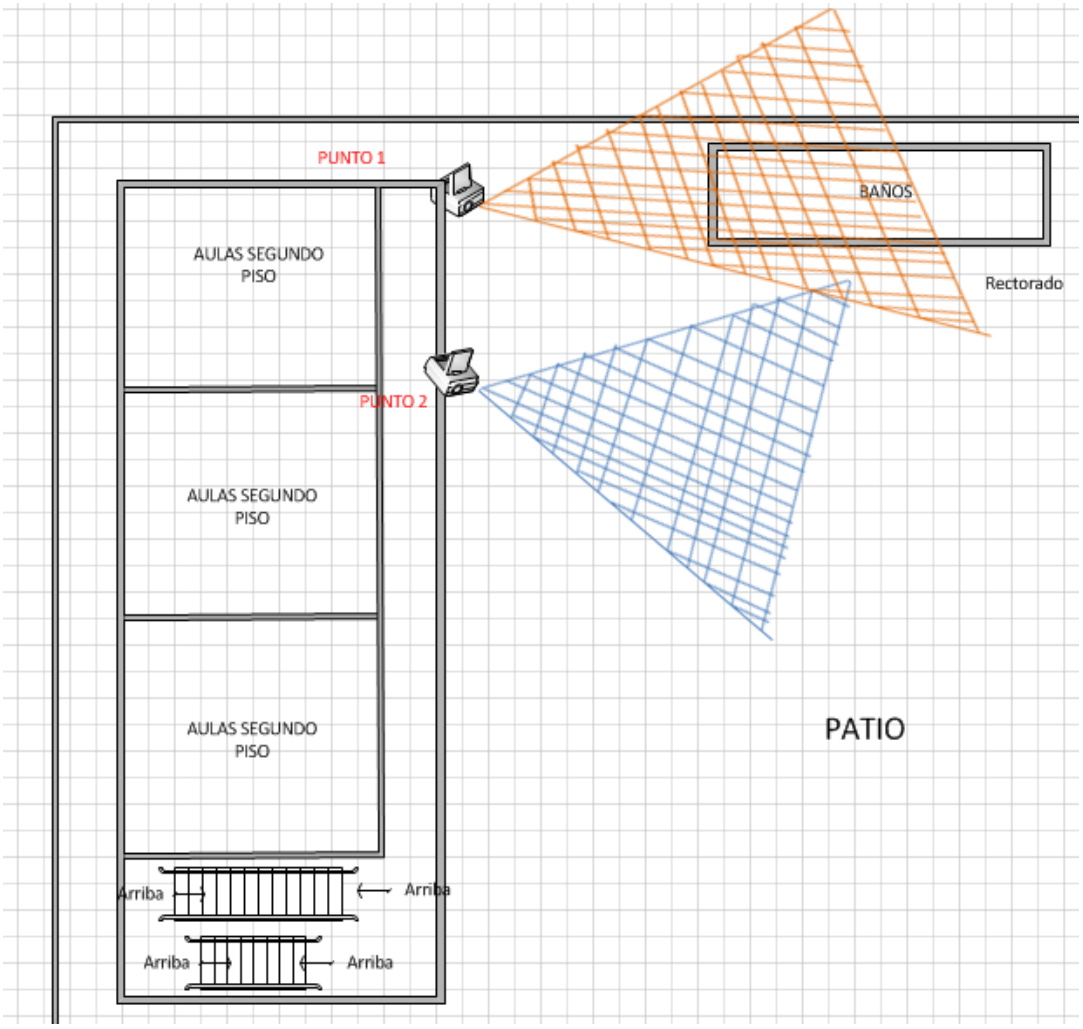


Figura 24. Puntos de colocación posibles cámara zona 3.

Para determinar la ubicación idónea de la cámara de la zona 3, representada en la figura 24, se tomó en cuenta que el objetivo de visualización es observar todo el cerramiento lateral, incluida la entrada de acceso de los vehículos. Se descartó el punto dos debido a que se observa gran parte del patio y como se mencionó anteriormente se estaría violando el derecho de privacidad del alumnado. El punto uno es el ideal ya que se tiene una visibilidad de todo el cerramiento lateral de la zona este y también la entrada de los vehículos.

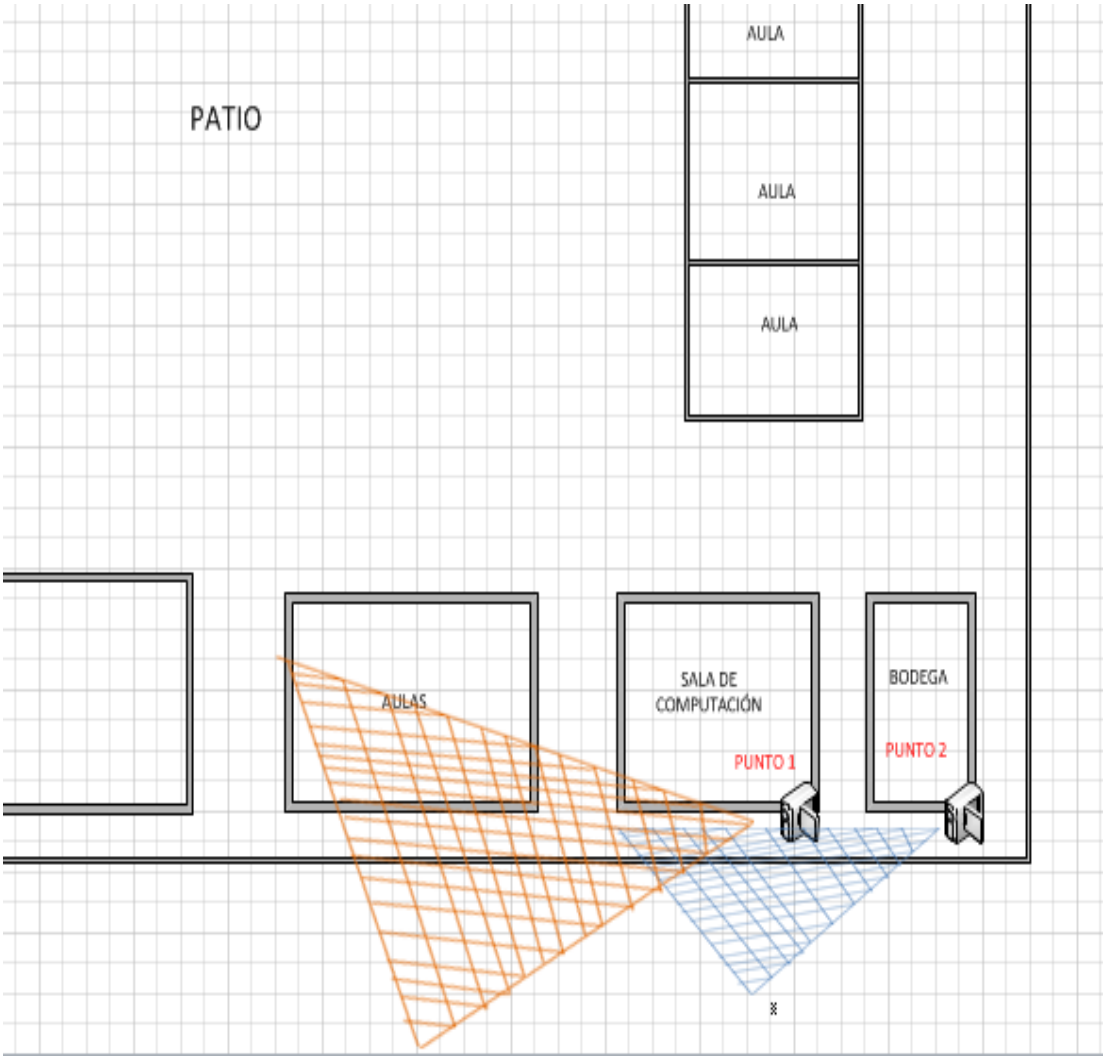


Figura 25. Puntos de colocación posibles cámara zona 4.

Para determinar la ubicación idónea de la cámara de la zona 4, representando en la figura 25, se analizó la posibilidad de tener la mayor visualización en el corredor oeste del plantel; tomando en cuenta que no se dispone de una edificación con una altura adecuada para colocar el dispositivo.

Se descartó el punto dos debido a existen muchos objetos que bloquean la señal que emite el router. El punto uno es el ideal ya que se tiene una visibilidad de todo el corredor lateral oeste y al mismo tiempo recibe una señal apropiada para el funcionamiento de la cámara.

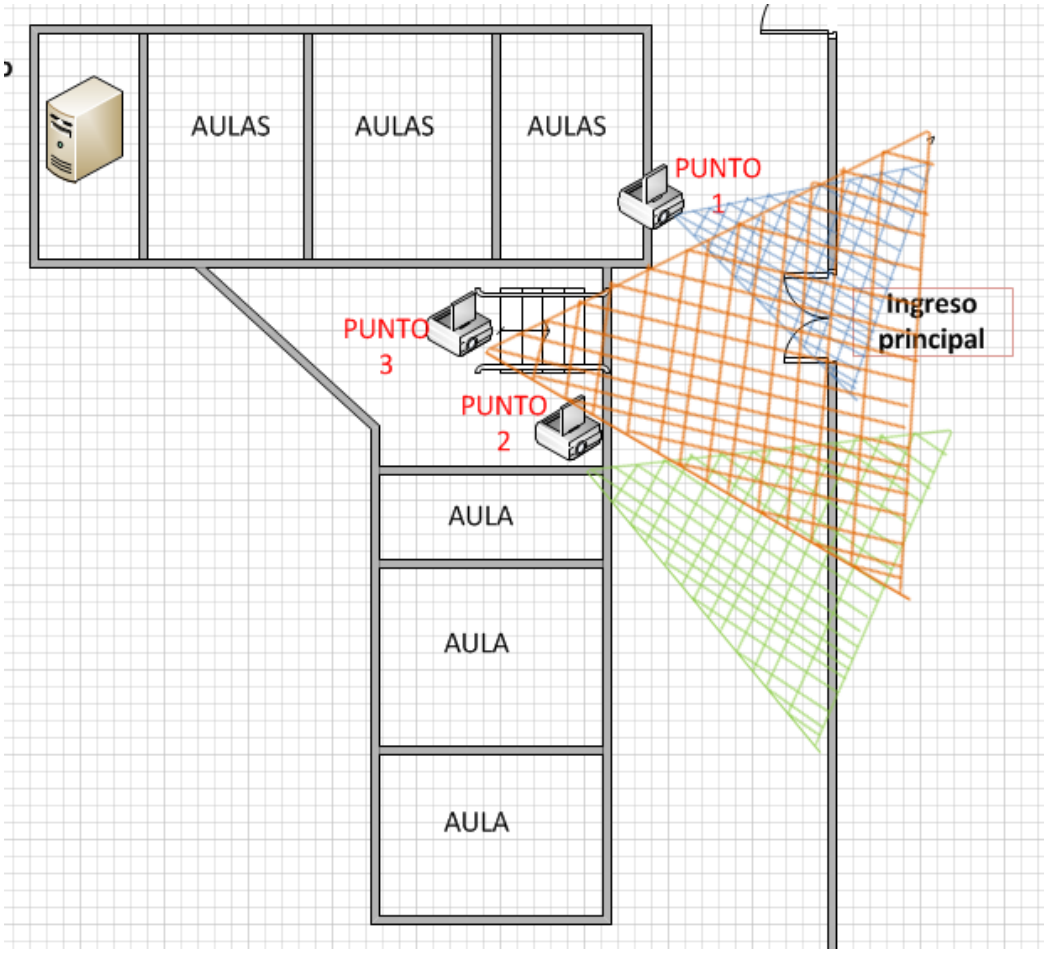


Figura 26. Puntos de colocación posibles cámara zona 5.

Para determinar la ubicación de la cámara de la zona 5, representada en la figura 26, se tomó en cuenta que el objetivo de este dispositivo es visualizar la entrada principal para controlar el acceso de las personas que ingresan al plantel educativo, adicionalmente debe visualizarse el cerramiento de la parte frontal.

Por estos motivos se han considerado los puntos uno, dos y tres para la instalación del equipo. Se descartó el punto 1 debido a que no se podía visualizar el cerramiento de la unidad educativa y la edificación no ofrece un espacio adecuado para colocar el equipo.

Se descartó el punto número dos debido a que se observa claramente el ingreso al plantel, sin embargo, el cerramiento aparece de manera parcial. El punto tres es el ideal ya que tiene una visibilidad de toda la puerta de entrada y el cerramiento de la parte frontal.

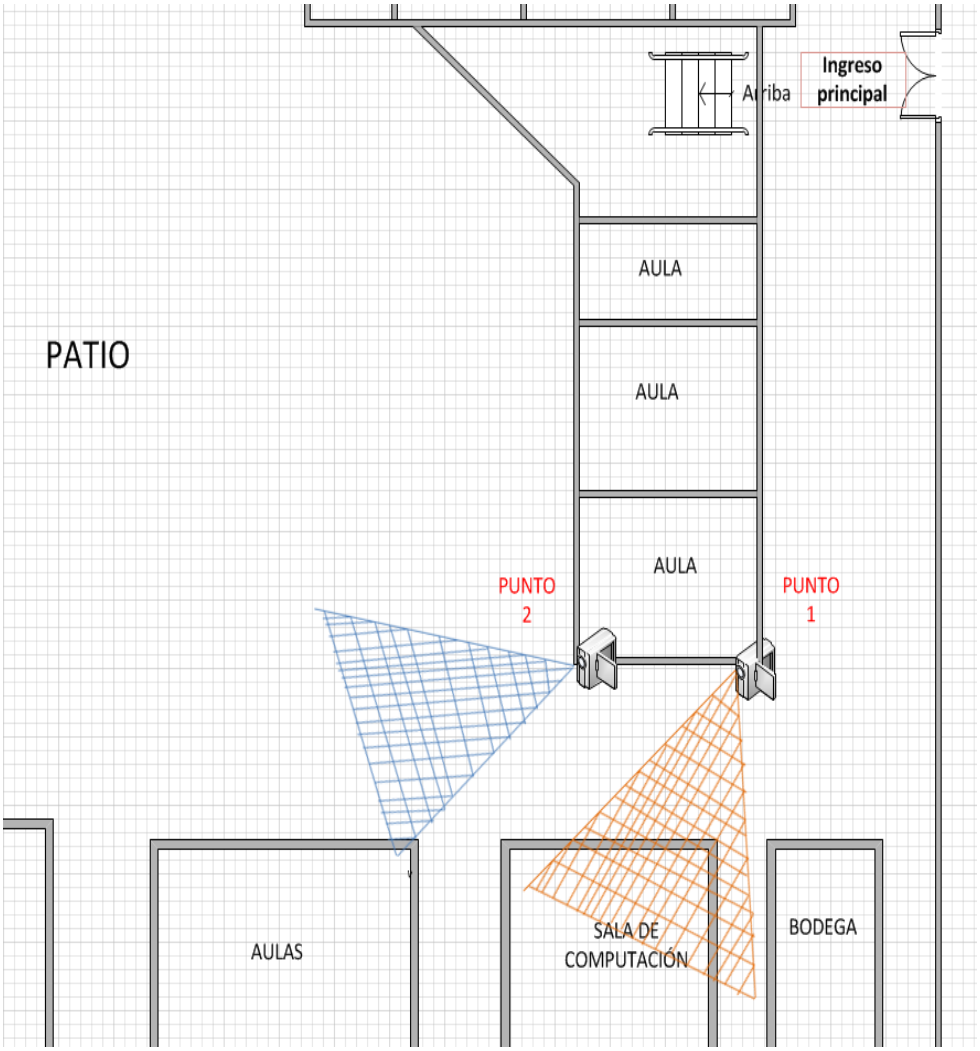


Figura 27. Puntos de colocación posibles cámara zona 6.

Para determinar la ubicación de la cámara de la zona 6, representado en la figura 27, se tomó en cuenta que se necesita visualizar la entrada al laboratorio de computación, para controlar el acceso de las personas, por tal motivo se ha considerado los puntos uno y dos para la instalación del equipo.

Se descartó el punto dos debido a que no se podía visualizar la puerta de ingreso en su totalidad. El punto uno es el ideal ya que se tiene una visibilidad de toda la puerta de la sala de computación y las condiciones del edificio son las ideales para la instalación del equipo.

Finalmente se observa cómo se han distribuido las cámaras en toda la Institución Educativa en la figura 28.

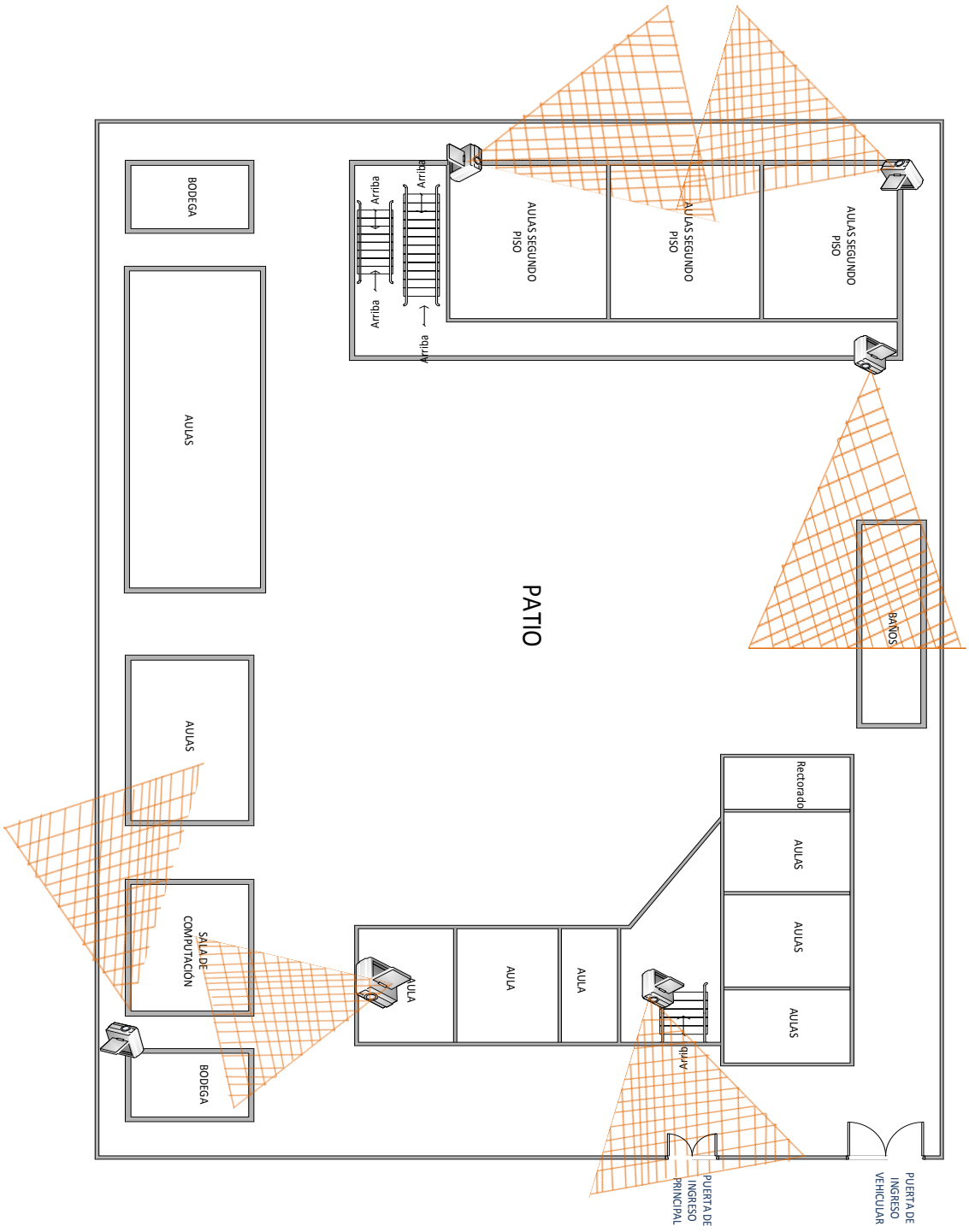


Figura 28. Ubicación del lugar de instalación de las cámaras en el plano.

3.5 Implementación de las cámaras de seguridad

A continuación, se evidencia la instalación realizada de cada una de las cámaras internas y externas en los lugares designados anteriormente. En las siguientes figuras se visualizan las cámaras ya instaladas desde la toma eléctrica y con el cajetín respectivo. Zona 1, figura 29.

Figura 29. Cámara instalada zona 1.

Zona 2, figura 30.

Figura 30. Cámara instalada zona 2.

Zona 3, figura 31.

Figura 31. Cámara instalada zona 3.

Zona 4, figura 32.

Figura 32. Cámara instalada zona 4.

Zona 5, figura 33.

Figura 33. Cámara instalada zona 5.

Zona 6, figura 34.

Figura 34. Cámara instalada zona 6.

Se realizó la configuración de los parámetros respectivos de cada cámara para conectarlas a la Red de Video UEAM creada en el router uno.

A continuación, se presenta la configuración de una cámara la red de video vigilancia:

1.- Se debe conectar la cámara a la Red de Video UEAM detallada anteriormente con la autenticación WPA2-Personal con la clave respectiva, como se muestra en la figura 35:

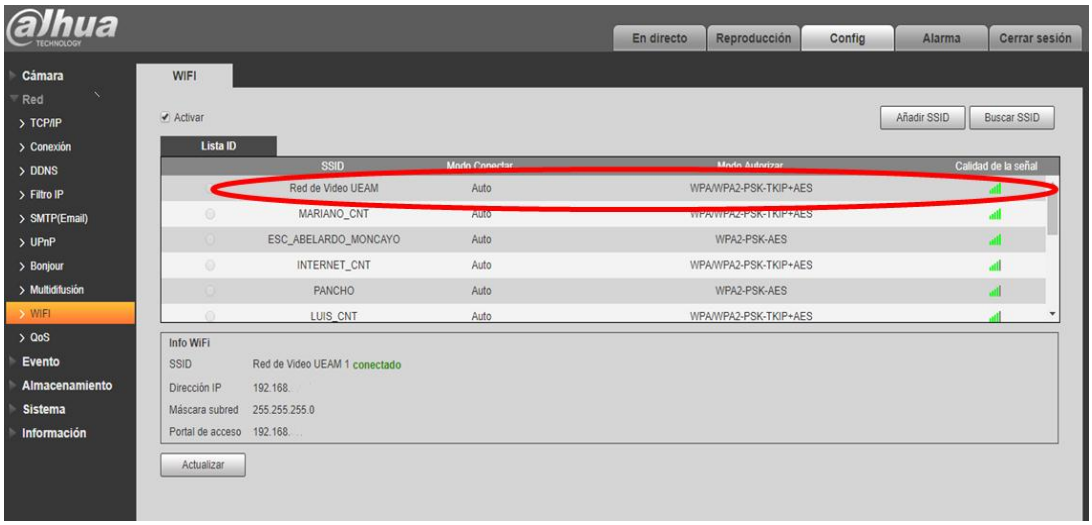


Figura 35. Conexión a la Red de Video UEAM.

Configuración IP de las cámaras externas, figura 36:

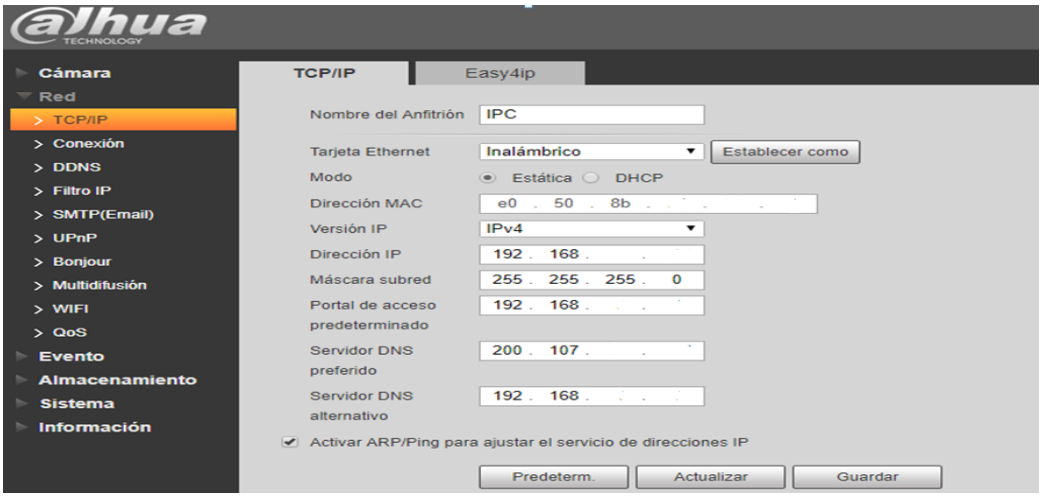


Figura 36. Configuración IP de las cámaras externas.

Configuración IP de las cámaras internas, figura 37:

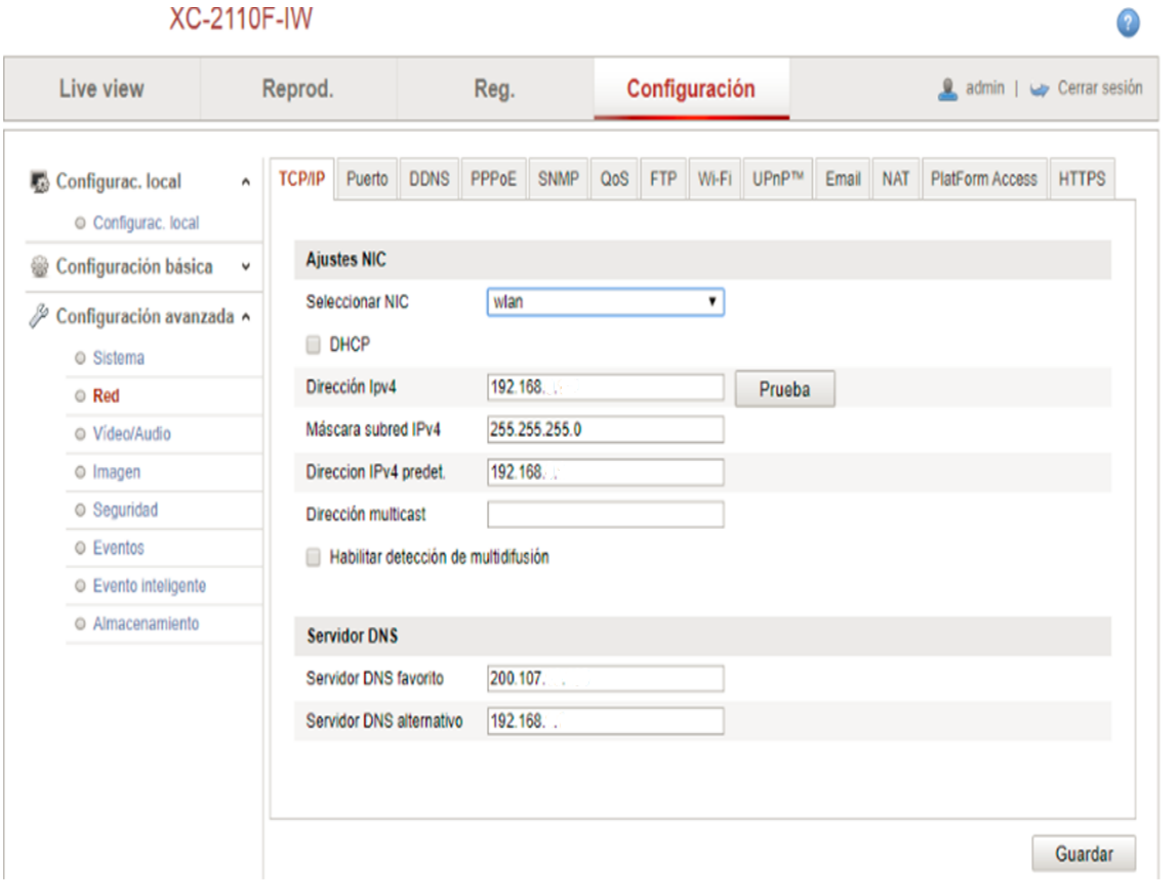


Figura 37. Configuración IP de las cámaras internas.

La cámara interna tiene un margen de funcionalidad de señal de S/N Ratio -50dB [17]. La cámara externa también tiene un margen de funcionalidad de S/N Ratio -50dB [18]. Datos obtenidos del datasheet de los equipos.

Instalación de router Linksys E900

Para abarcar toda el área de la Unidad Educativa fue necesario utilizar dos equipos router Linksys E900 explicado en la sección anterior. El router uno es quien administra toda la red y donde se han configurado las direcciones IP de cada cámara así como también la dirección IP del router dos y del pc servidor que maneja la aplicación.

A continuación se muestra la configuración de la red y la salida a Internet, detallado en la figura 38.

Figura 38. Configuración router administración.

En la figura 39 se detalla cómo se realizó la reservación de la dirección IP de cada una de las cámaras que conforman el sistema de monitoreo con los nombres asignadas a cada dispositivo.

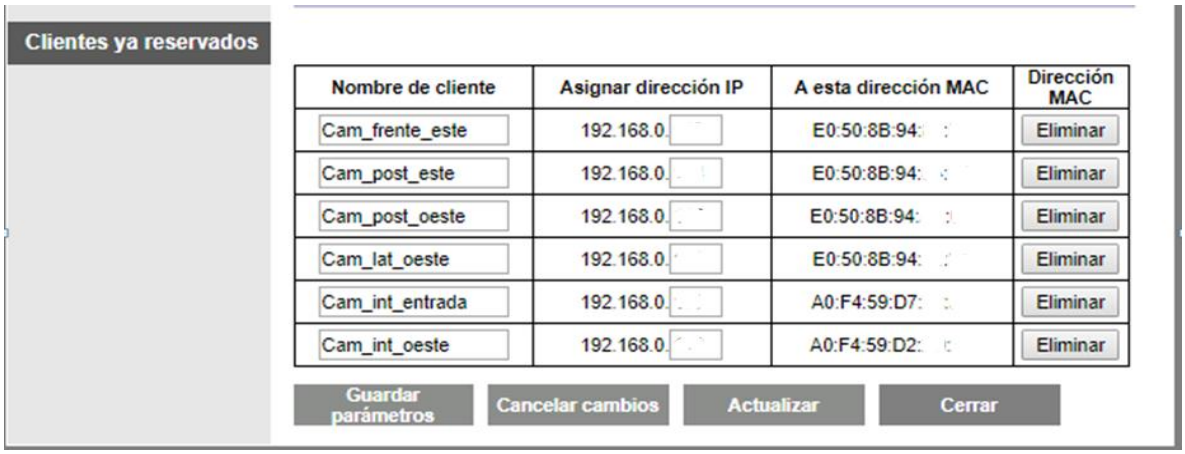


Figura 39. Reservación de direcciones IP de las cámaras.

Cálculo del tiempo de almacenamiento de información

Al emplear este cálculo se puede identificar aproximadamente la cantidad de información que registran las cámaras y el espacio de almacenamiento, entre los detalles que se necesita tomar en cuenta son: cantidad de cámaras y las horas de grabación.

Las cámaras fueron configuradas a 30 cuadros por segundo con una resolución de 720P (1280x720) igual a 0,9 Megapíxeles, tiene una compresión en H264 normalmente valores entre 32kbps y 10 Mbps [17].

$$BW\ Cámara = \left(\frac{240kbits}{s}\right) * \left(\frac{1byte}{8bit}\right) = 0{,}03\ Mbytes\ /s$$

Ecuación 1. Ancho de banda de cámara con compresión de 240 kbps.

Por lo tanto, para una compresión de 240 kbps se tiene con una un ancho de banda por cada cámara de 0,03 Mbyte/s.

Las cámaras se configuraron para realizar grabaciones de forma continua durante 10 horas.

$$Cantidad\ de\ información\ por\ cámara = BW * tiempo$$

Ecuación 2. Cantidad de información por cámara.

$$Cantidad\ de\ información\ por\ cámara = 0{,}03\frac{Mbytes}{s} * \left(\frac{3600s}{1\ hora}\right) = 106\frac{Mbytes}{hora}.$$

$$Cantidad\ de\ información\ por\ cámara = 106\ \frac{Mbytes}{hora} * 24\ horas$$

$$Cantidad\ de\ información\ por\ cámara = 2560\ Mbytes\ diarios$$

$$Cantidad\ de\ información\ por\ cámara = 2560\ Mbytes * 6\ cámaras$$

$$Cantidad\ de\ información\ por\ cámara = 15\ GB\ diarios$$

Considerando la capacidad de almacenamiento de 500 GB

$$Días\ de\ almacenamiento = \frac{capacidad\ de\ alamacenamiento}{informacion\ diaria}$$

Ecuación 3. Cálculo de días de almacenamiento de información.

$$Días\ de\ almacenamiento = 500\ GB\ /15\ GB$$

$$Días\ de\ almacenamiento = 33{,}3\ días$$

Por lo tanto, las grabaciones se deben almacenar por un tiempo promedio de 33,3 días antes de que se sature el disco duro con la información.

3.6 Configuración del sistema de seguridad inalámbrico

Instalación del sistema operativo y software de control.

Se realizó la instalación del programa iSpy en el servidor de la red de video vigilancia. En la figura 40 se muestra la pantalla principal del programa.

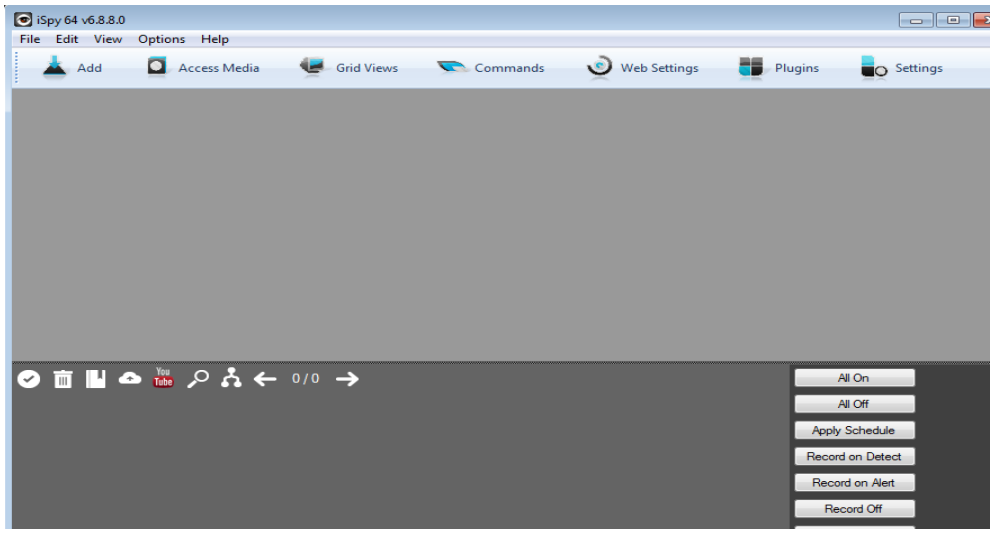


Figura 40. Pantalla del programa *iSpy.*

Para realizar la configuración de las cámaras se eligió la opción agregar una cámara con el asistente, se seleccionó el modelo del equipo y posteriormente se designó un canal. Para la autenticación se completa el campo nombre, usuario y contraseña que se ha establecido con anterioridad a la cámara para acceder vía web al equipo.

En la sección de configuración IP se seleccionó el puerto y la dirección IP, que se asignó a cada cámara, al realizar esta acción la aplicación genera varios links. Se seleccionó uno de los mismos según el formato de video que desee tener en las grabaciones.

Al seleccionar uno de los links, la cámara aparece en la pantalla principal y se puede empezar a configurar las características necesarias como almacenamiento, horario de grabación, etc. Las configuraciones se muestran en las siguientes figuras:

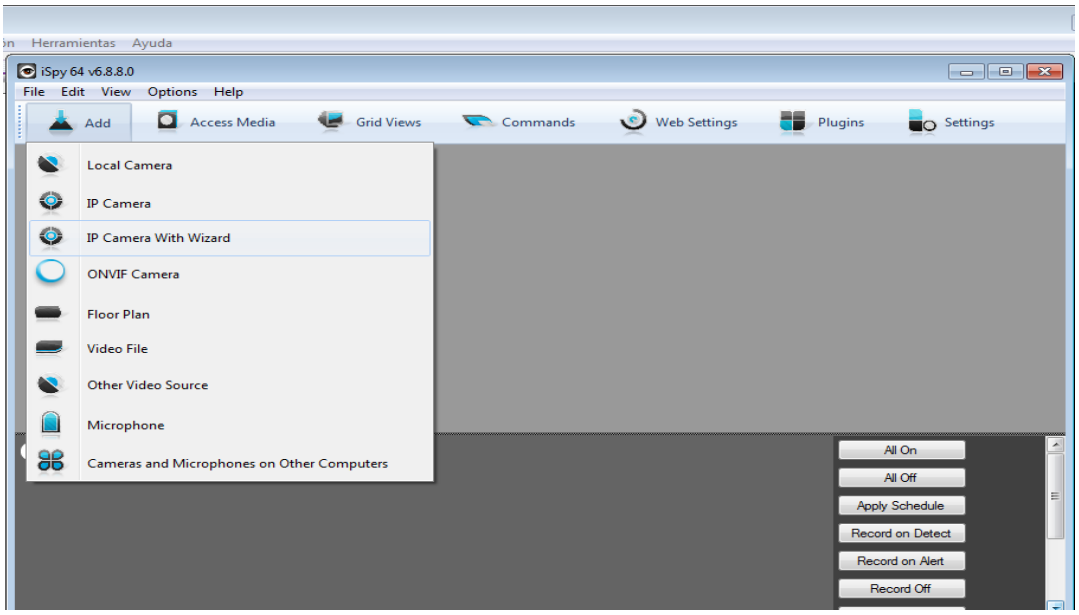


Figura 41. Configurar cámara con el asistente.

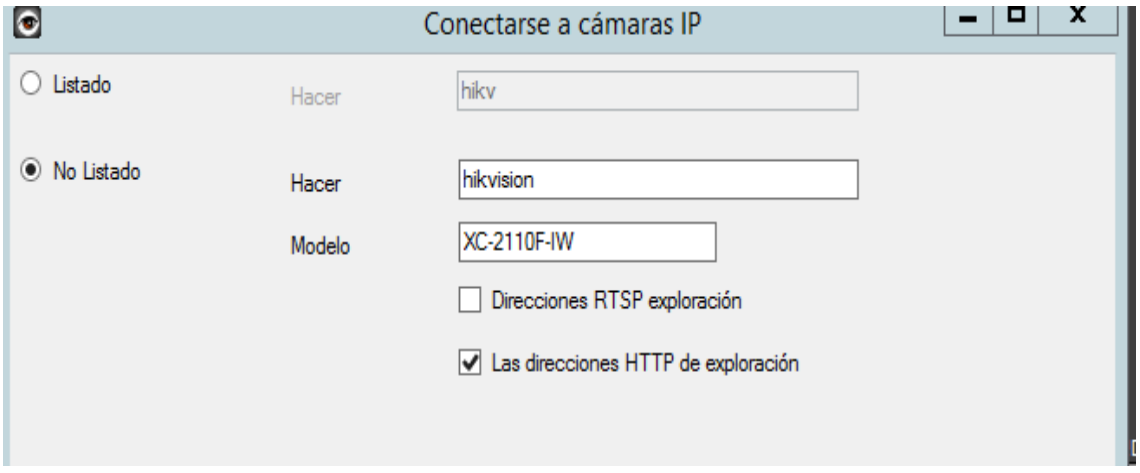


Figura 42. Selección de modelo y marca de la cámara.

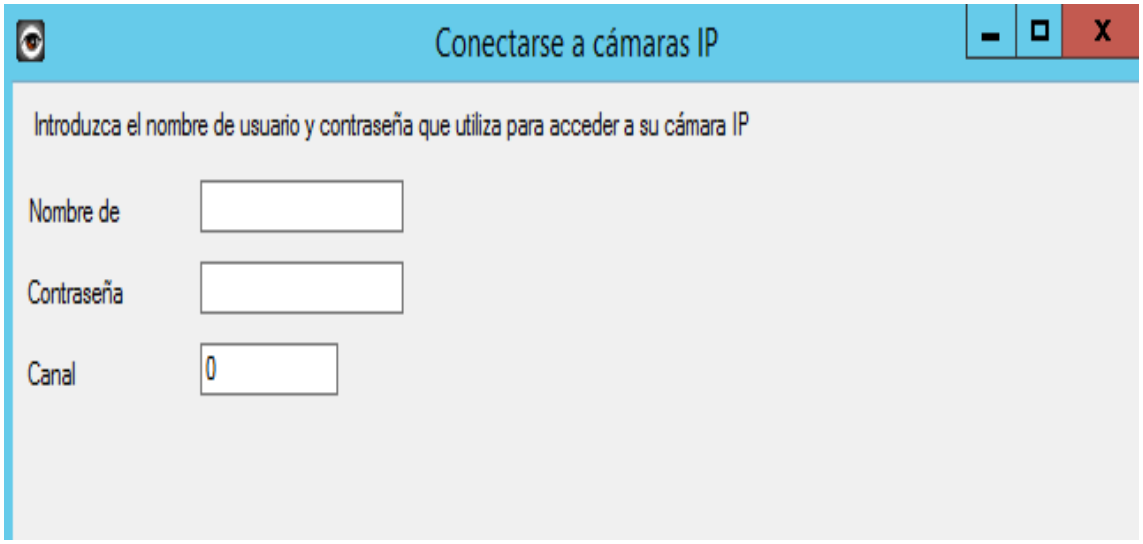


Figura 43. Configuración de la autenticación y canal de trasmisión.

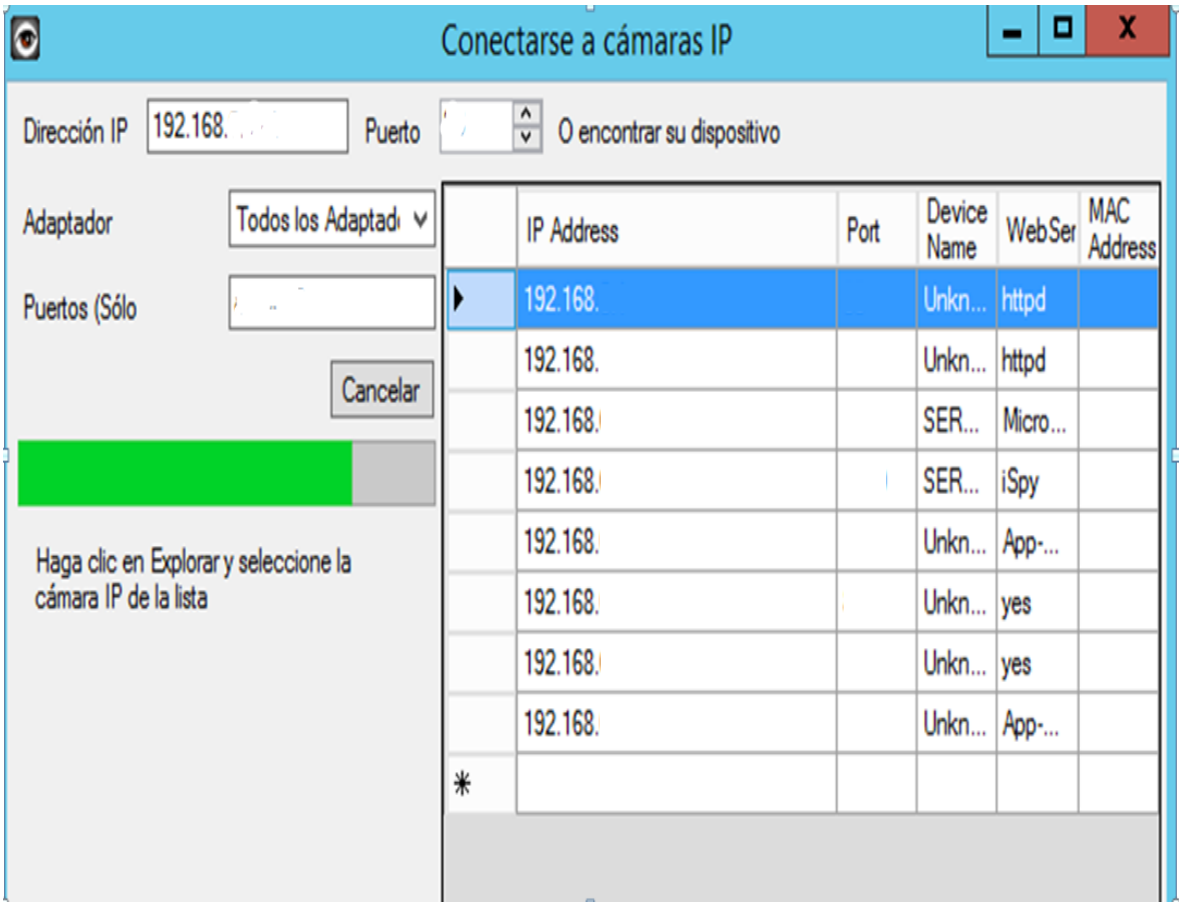


Figura 44. Selección del equipo por dirección IP.

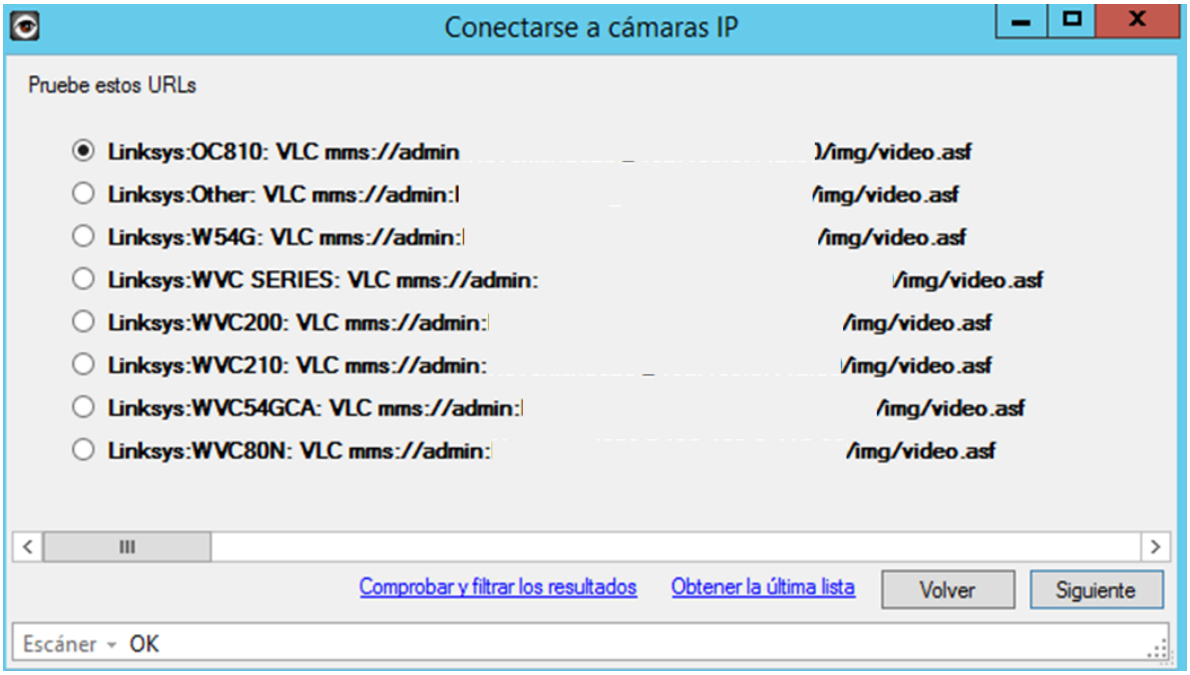


Figura 45. Selección del link de conectividad.

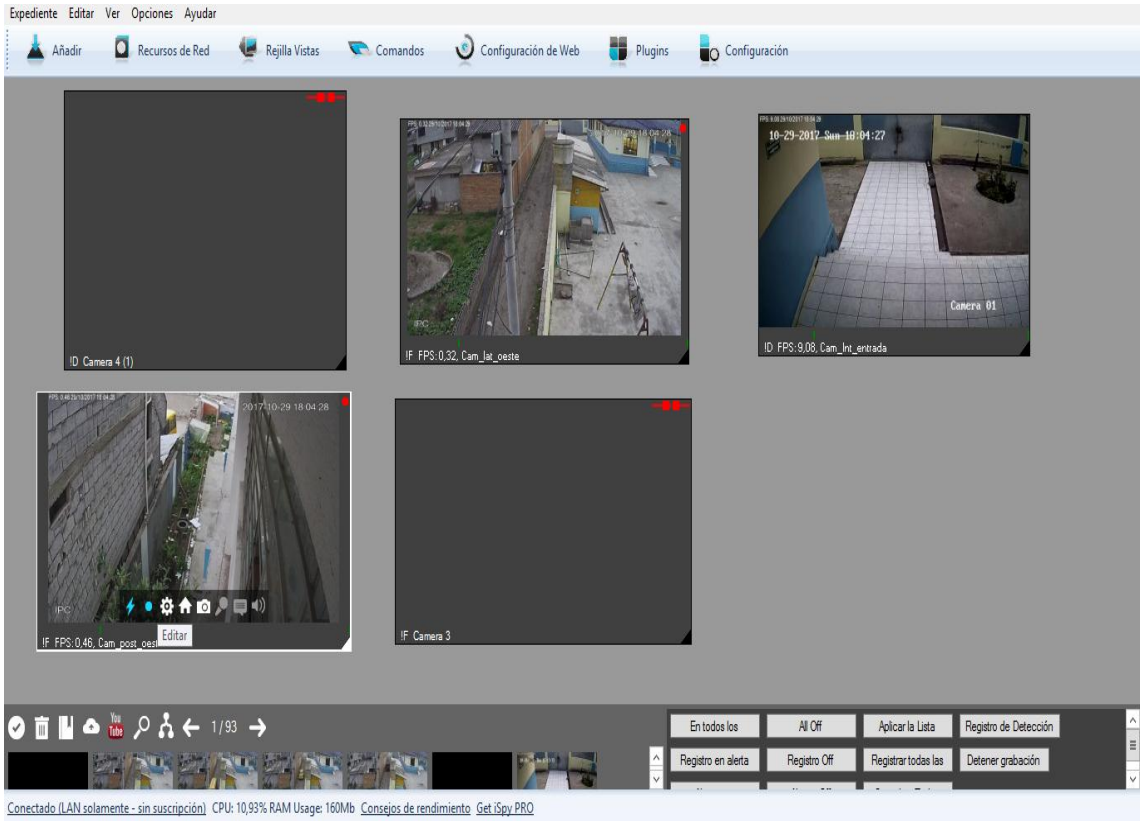


Figura 46. Vista de las cámaras en la aplicación.

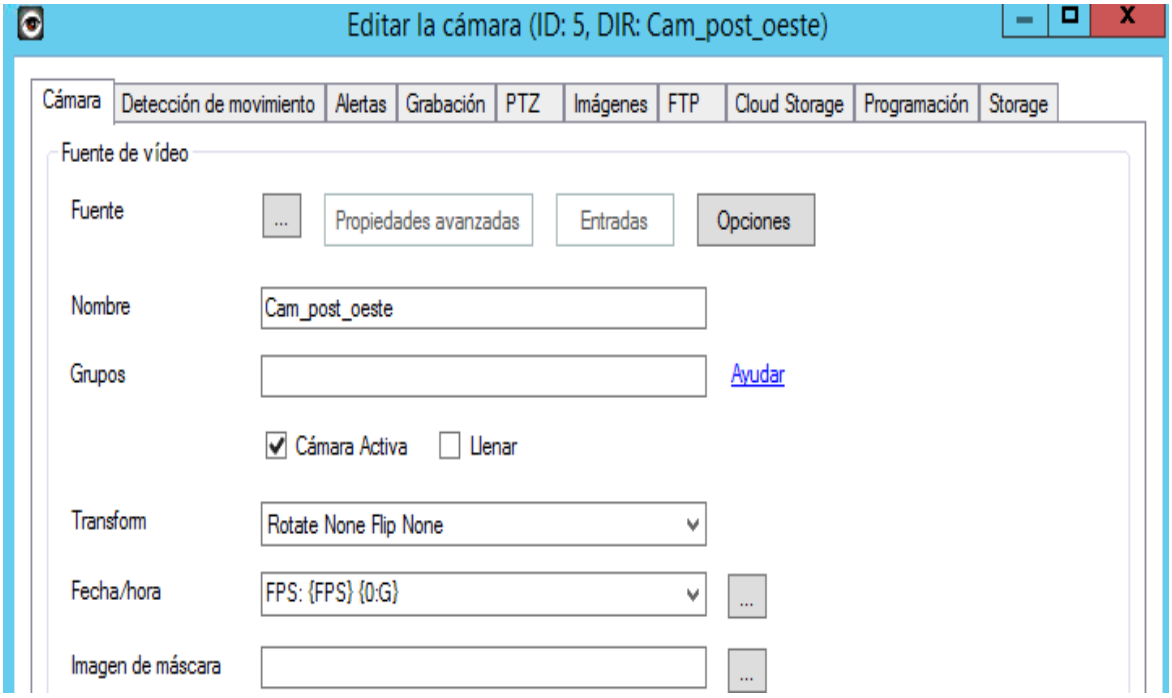


Figura 47. Editor de la configuración de las cámaras.

Configuración de notificación vía correo electrónico.

Para la configuración del correo electrónico se habilitó el complemento SMTP en el sistema operativo del servidor de la red de video vigilancia.

Al realizar este proceso se habilitaron los parámetros para realizar la salida de información a Internet en el servidor de video vigilancia (IP 192.168.x.xxx) y el puerto xx.

También se creó la cuenta de correo redvideoueam@example.com para realizar el proceso de notificación.

Posteriormente en la configuración de cada cámara se completan los siguientes datos:

- De Dirección: dirección desde donde se enviarán los correos.
- Nombre de la cuenta de correo.
- Contraseña de la cuenta de correo.
- Y el servidor configurado previamente el cual tiene salida a internet detallada en la figura 48.

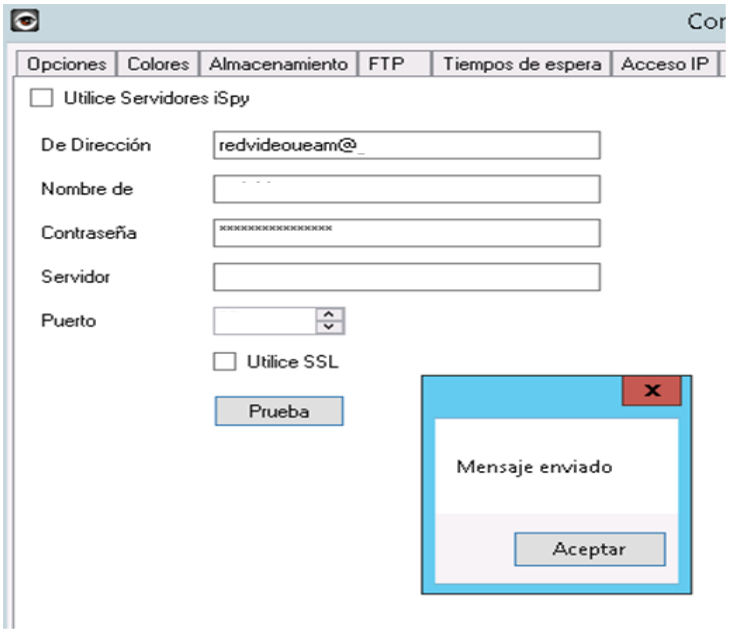


Figura 48. Configuración de salida SMTP y envío de correo electrónico.

Configuración almacenamiento de información.

Para configurar el respaldo de información, se utilizaron los parámetros de almacenamiento (*storage*) asignando una ruta en el equipo en donde se guarda los datos generados por cada dispositivo. En este caso se almacena la información en el equipo local en la ruta: C: User\Aministrador\Video\RedVideoVigilanciaUEAM\Videos, se creó una carpeta para cada cámara y realizar el almacenamiento de información, como se muestra en la figura 49.

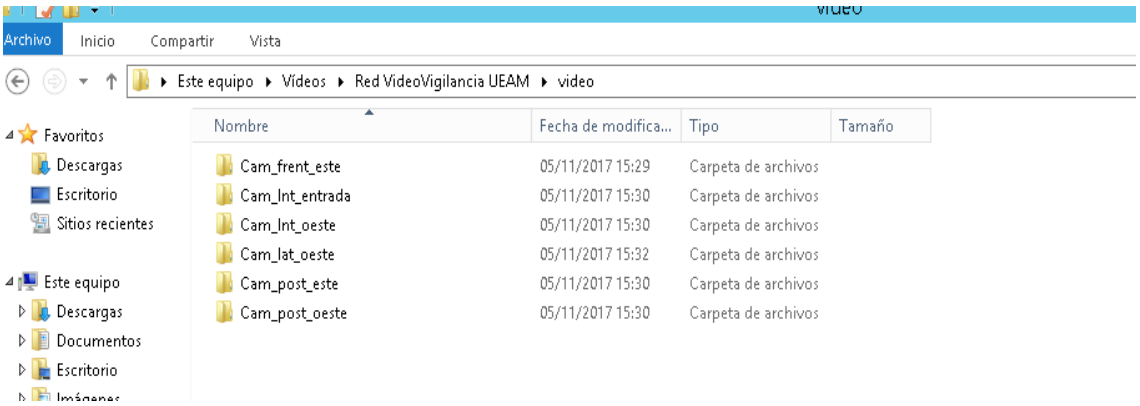


Figura 49. Configuración del repositorio de información.

Las cámaras fueron configuradas para realizar grabaciones en diferentes horarios según lo solicitado por el señor director Ernesto Mora. En la aplicación se selecciona las carpetas creadas y luego se configuró los horarios y diferentes acciones que se pueden realizar con los dispositivos, adicional también fue posible configurar estos horarios de grabación en el software propio de la cámara y en la aplicación se puede asociarlos seleccionando la pestaña horario de la cámara como se muestra en la figura 50 y 51.

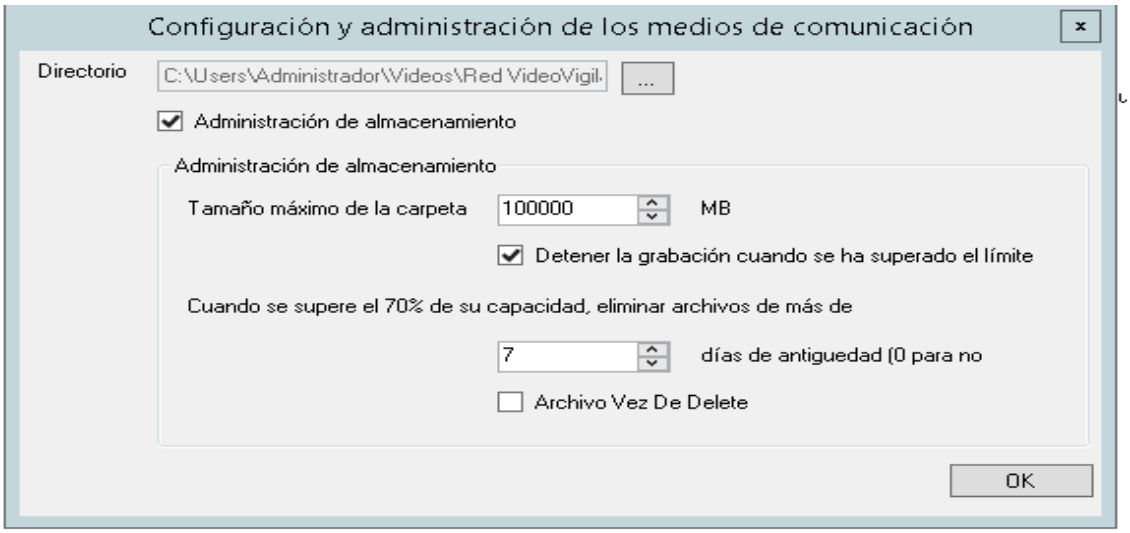


Figura 50. Selección de carpetas para respaldo de información.

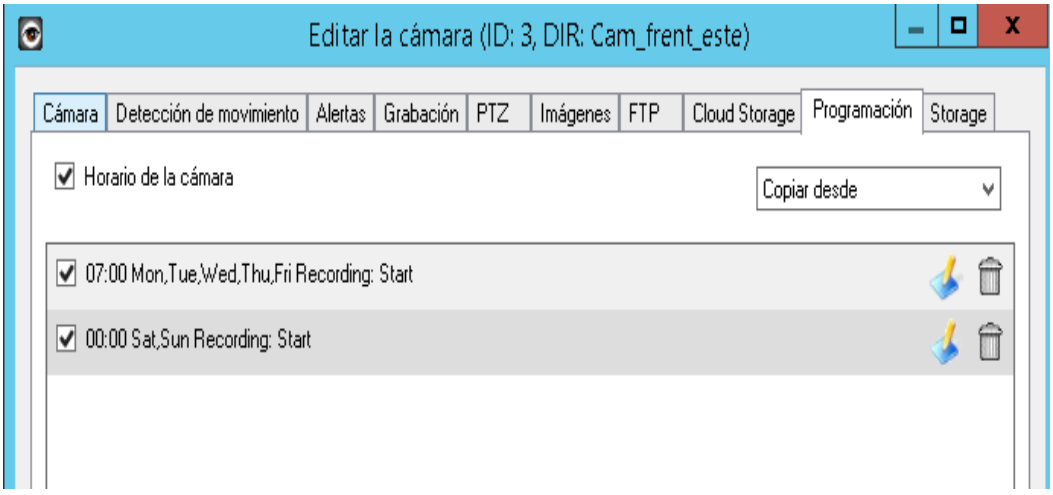


Figura 51. Horario de grabación.

La representación gráfica de como seleccionar el horario de grabación de una cámara se muestra en la figura 52.

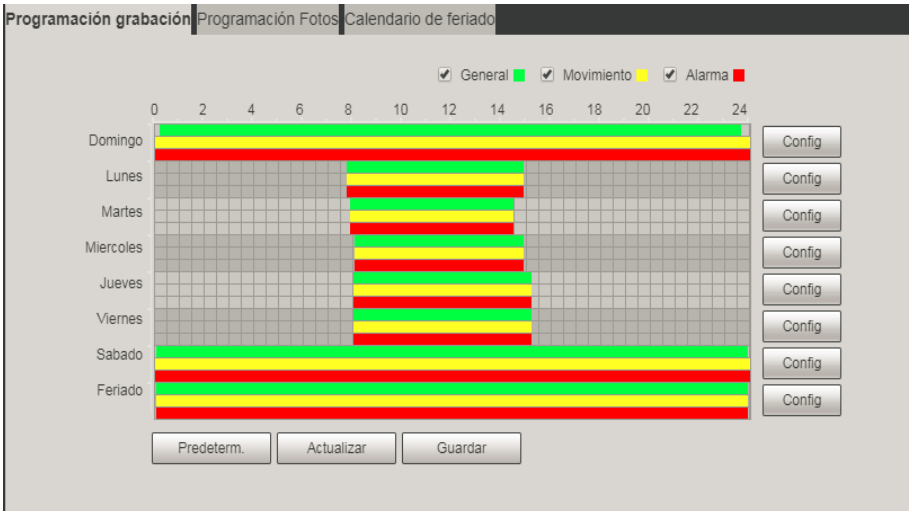


Figura 52. Representación gráfica horario de grabación.

También se puede parametrizar la cámara para que realice o no las grabaciones es las fechas establecidas como feriados en el año, según se observa en la figura 53.

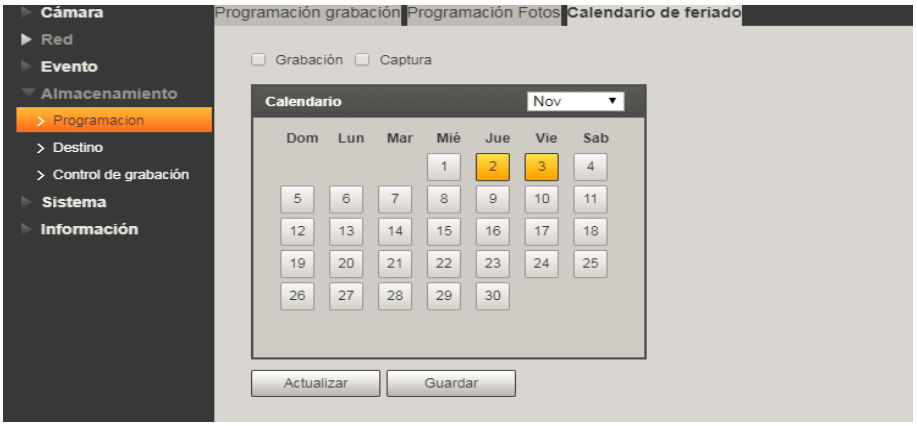


Figura 53. Selección de fechas para realizar las grabaciones.

Réplica de información

Para realizar la réplica de información previamente fue necesario configurar una dirección IP fija (192.168.x.2) en el equipo destino (IES-EXAMPLE) propiedad de la institución Educativa ya que de esto depende la funcionalidad del comando *robocopy*.

También se creó una carpeta compartida en el equipo destino con todos los permisos habilitados de lectura y escritura que es en donde se almacenará la información. En la figura 54 se observa la configuración de la carpeta compartida en el equipo destino.

Figura 54. Carpeta compartida para la réplica de información.

En el equipo destino se crearon carpetas con el mismo nombre de repositorio origen, donde se copian as grabaciones después de ejecutarse la tara programada en el servidor, mostrado en la figura 55.

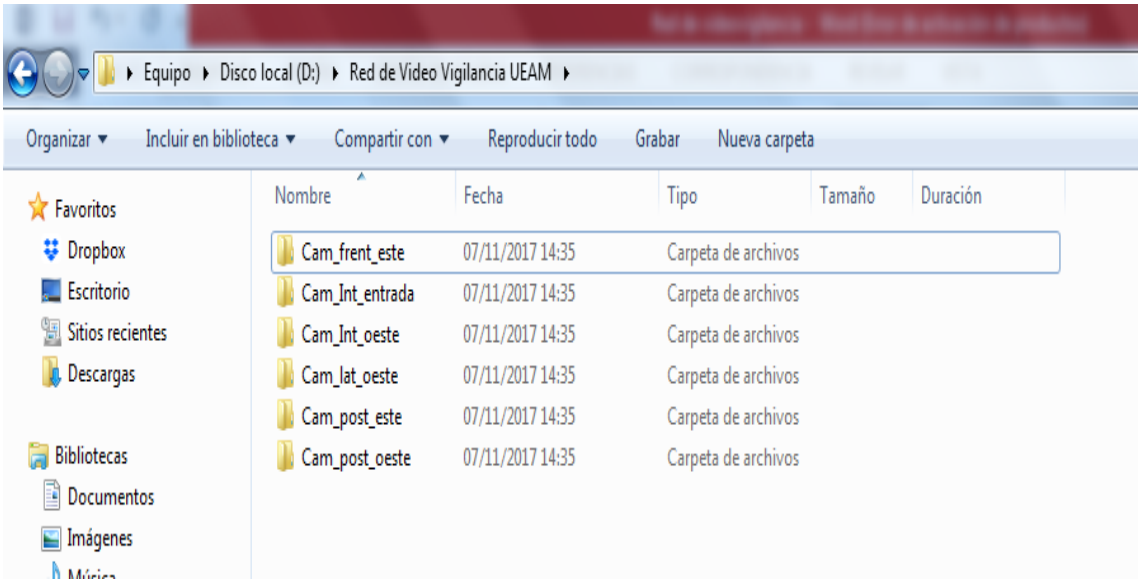


Figura 55. Estructura de las carpetas en el equipo destino.

Para el proceso de réplica de información se utiliza el comando *ROBOCOPY ORIGEN DESTINO /MIR* MIR modo espejo, este comando copia y luego elimina archivos en el destino que ya no existen en el origen. Para cada cámara se genera un archivo .bat con este formato de comando mostrado en la figura 56 y 57.

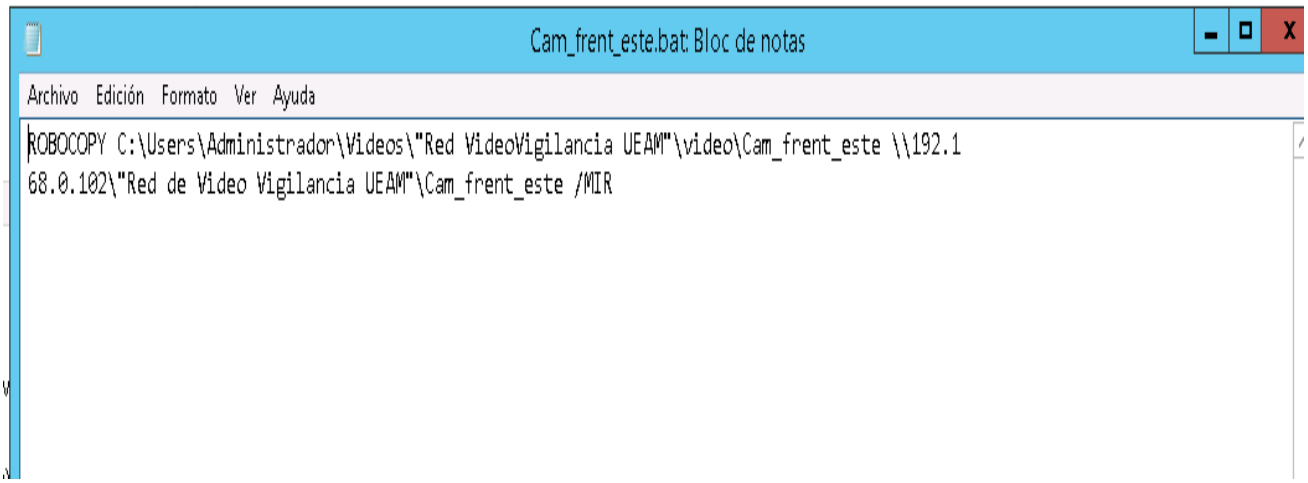


Figura 56. Archivo .bat del proceso de copia.

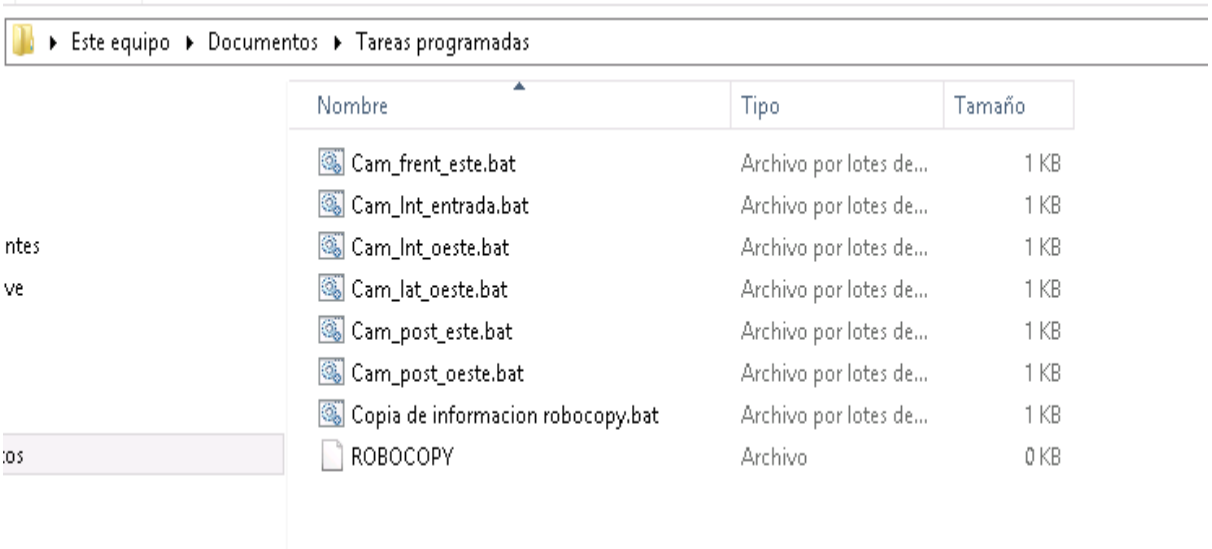


Figura 57. Archivos .bat creados para cada cámara.

Después de crear los archivos, se creó la tarea programada en el equipo servidor en la sección de biblioteca de tareas programadas en la consola de administración del equipo servidor.

En la figura 58, 59, 60 se muestra la configuración de la tarea programada, se colocan datos generales como el nombre de la tarea, en desencadenadores se coloca la hora de ejecución y en acciones se solicita que se ejecute el archivo .bat respectivo de cada cámara.

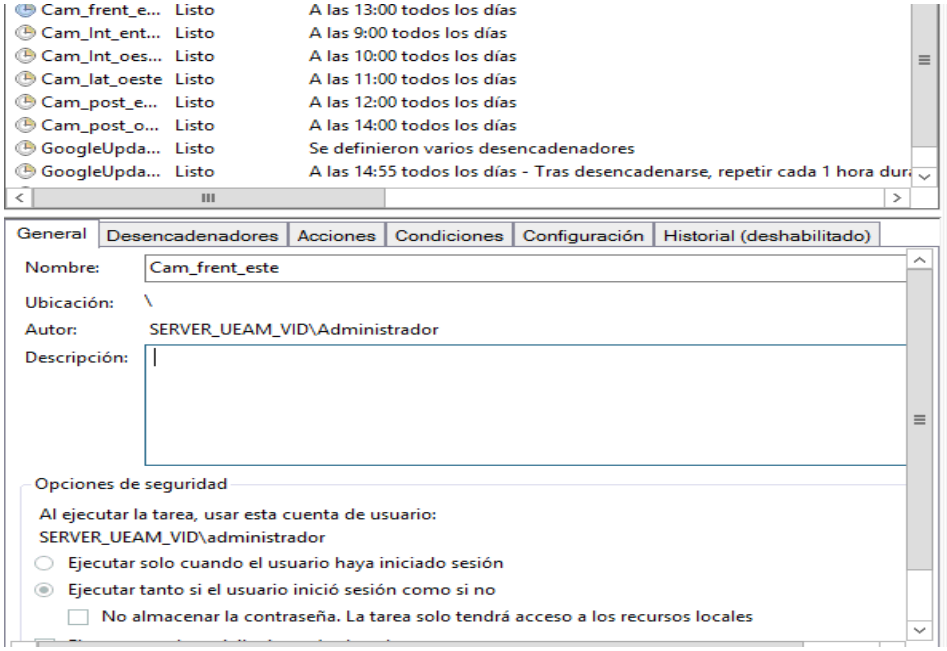


Figura 58. Creación de la tarea programada para copia de información.

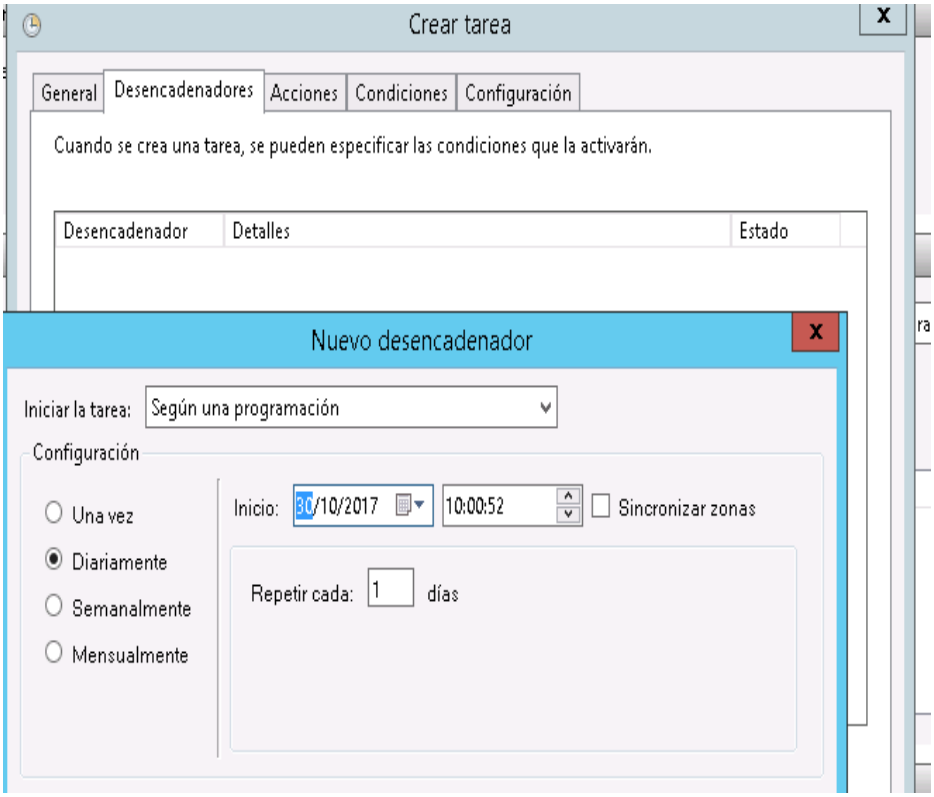


Figura 59. Configuración del horario de la réplica de información.

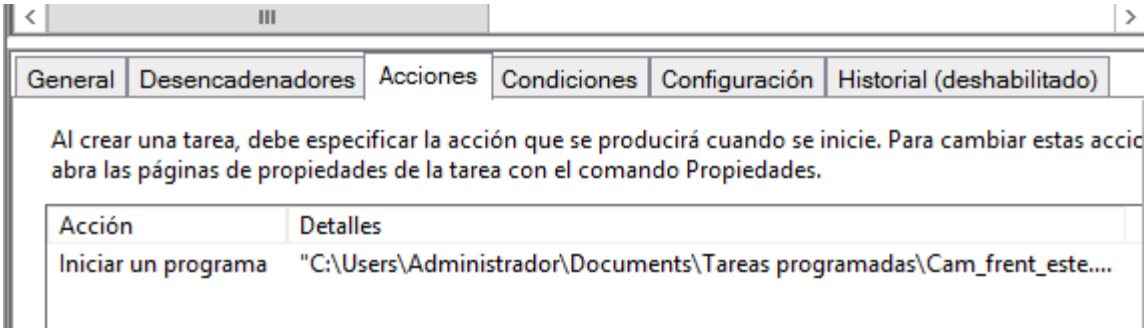


Figura 60. Selección de los archivos .bat para la ejecución de la tarea programada.

El resultado de la copia de información realizada por la tarea programada se observa en la figura 61.

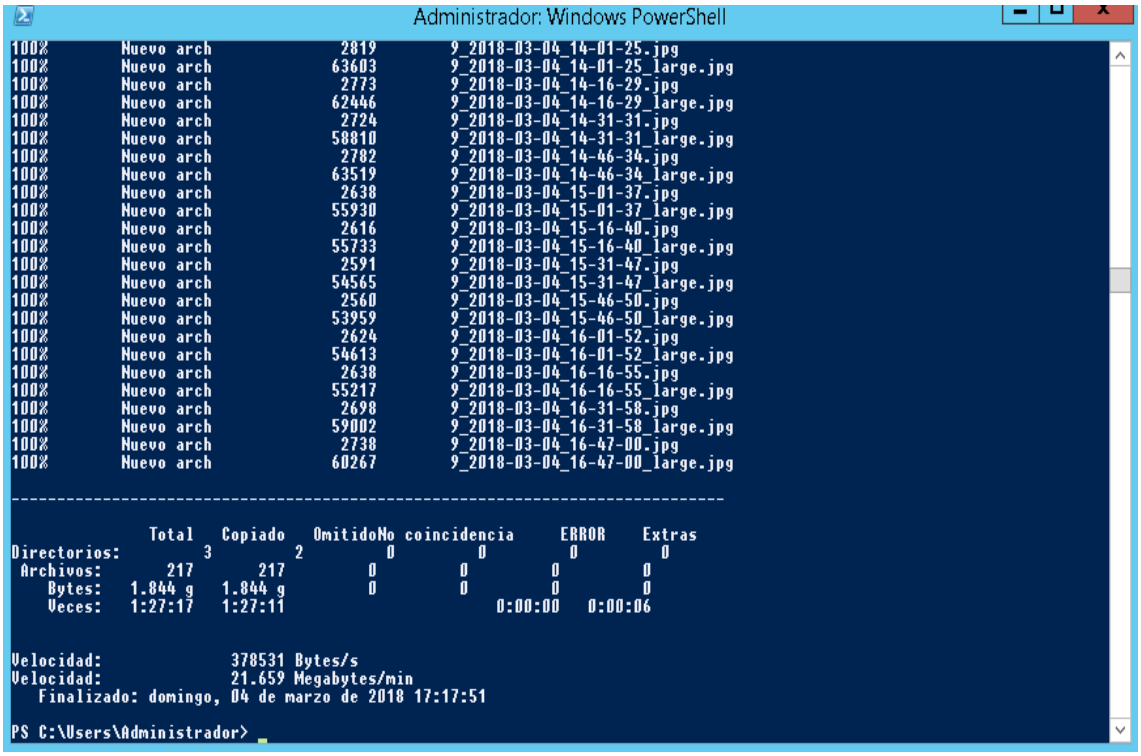


Figura 61. Resultado del proceso de réplica de información.

Configuración de acceso remoto desde Internet hacia las cámaras.

Después de completar la configuración de las cámaras, se procedió a realizar la habilitación del acceso remoto a través de Internet. Para ello se utilizó la opción de configuración de reenvío de puertos único con se detalla en la figura 62.

Esta funcionalidad permite acceder al router de manera remota a través de un puerto único, que el dispositivo se encarga de re direccionar hacia la IP que tiene cada cámara dentro de la red de video vigilancia.

El puerto de cada cámara se lo evidencia en la configuración básica de cada equipo, también se lo puede obtener revisando los parámetros de conexión de los dispositivos en la aplicación de video vigilancia.

Al realizar un escaneo con la aplicación todos los equipos están asociados al puerto 80. En la siguiente tabla se describe el puerto utilizados para cada cámara.

Tabla 2. Especificación de los puertos

CÁMARA	PUERTO EXTERNO	PUERTO INTERNO
Cámara zona 1	10001	80
Cámara zona 2	10002	80
Cámara zona 3	10003	80
Cámara zona 4	10004	80
Cámara zona 5	10005	80
Cámara zona 6	10006	80

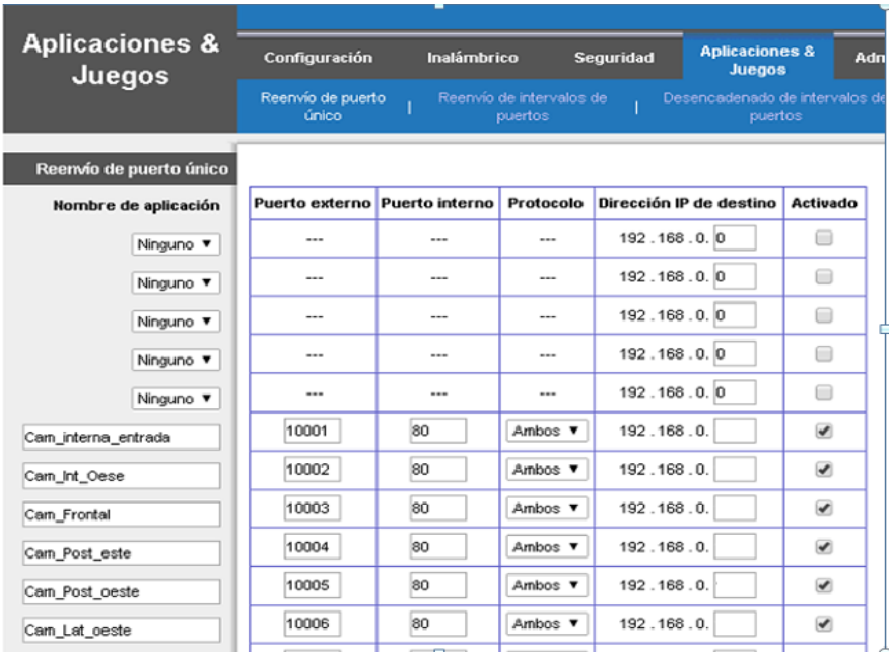


Figura 62. Configuración de reenvío de puerto único.

Configuración de acceso a la nube

Para la configuración de conexión a la nube de Google Drive se realiza el proceso de copia de seguridad y sincronización en el equipo PC servidor con la cuenta redvideoueam@example.com; en la configuración inicial realizó la selección la carpeta donde están los videos que se necesita tener un respaldo las últimas 24 horas. Las cámaras seleccionadas para este proceso son: Cam_frente_este, Cam_Int_entrada, como se muestra en la figura 63 y 64.

La capacidad de almacenamiento en la nube es de 15 GB lo cual nos permite almacenar información de las últimas 24 horas según lo antes calculado.

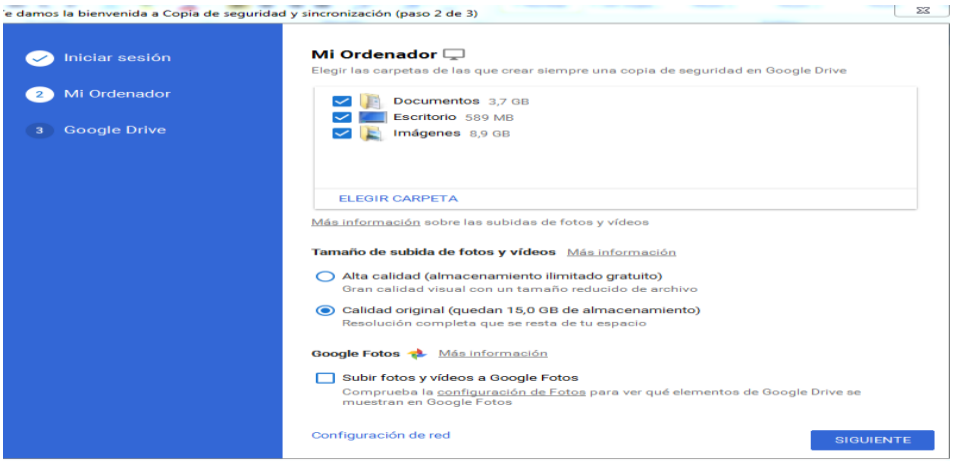


Figura 63. Aplicación Copia de seguridad y Sincronización

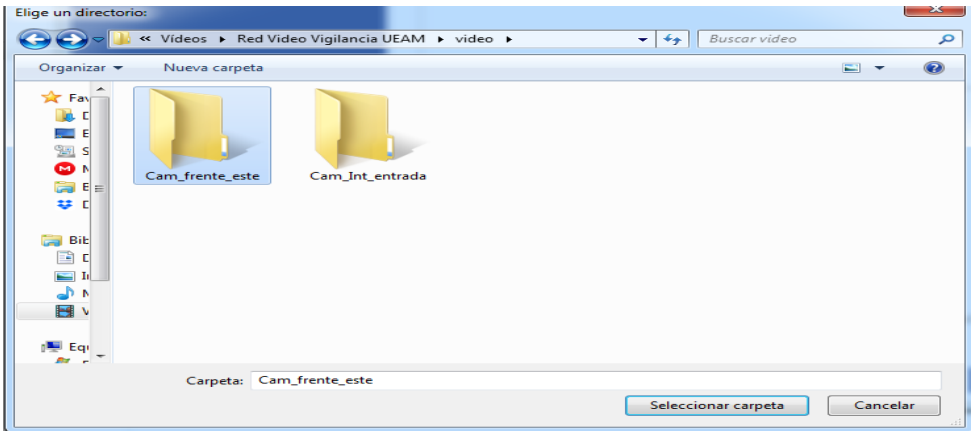


Figura 64. Selección de la ruta de respaldo de información

En la sección de parámetros se configuró el ancho de banda sin limitaciones en la velocidad de descarga y subida de información para un rendimiento óptimo, se muestra el detalle en la figura 65.

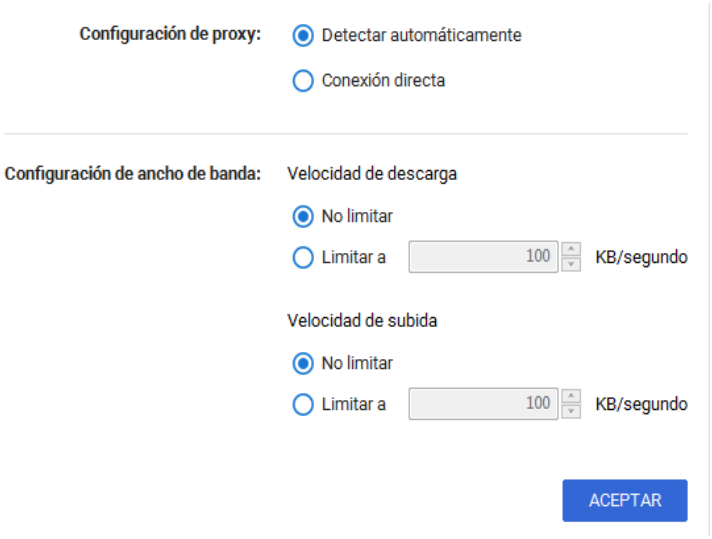


Figura 65. Configuración del ancho de banda

La información que se ha respaldado en la nube de Google Drive de la cuenta creada para la institución educativa se muestra en la figura 66.

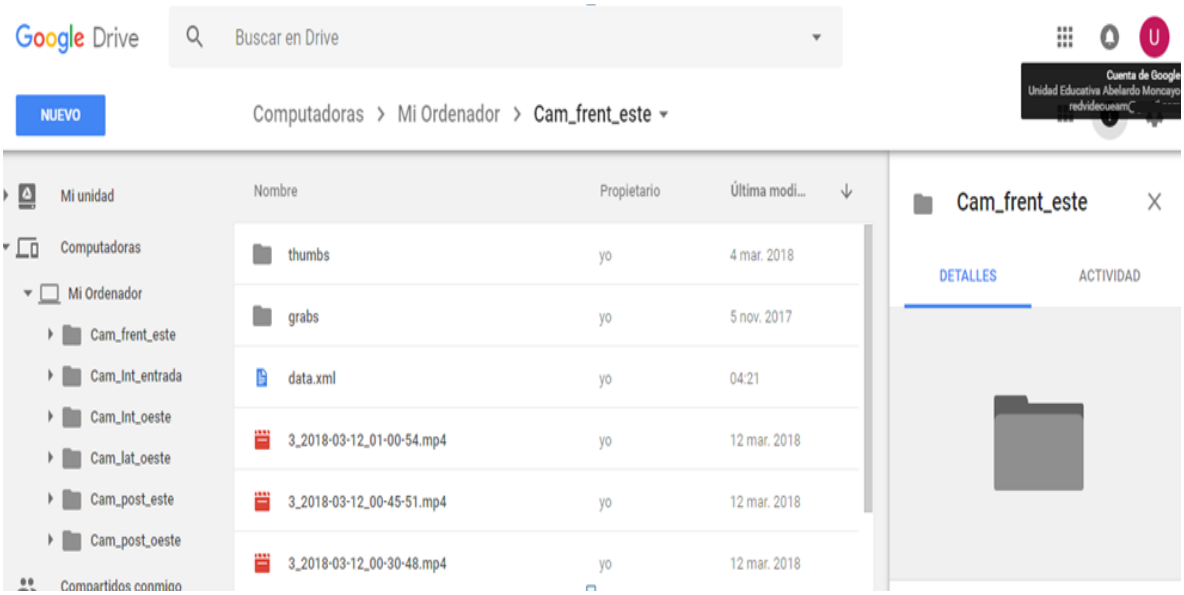


Figura 66. Información respaldada en la nube.

Prototipo de notificaciones vía SMS.

Para este proceso lo que se debe realizar es la configuración del correo de gmail (redvideoueam@gmail.com) en la cuenta Outlook en el equipo PC servidor, como se muestra en la figura 67 y 68.

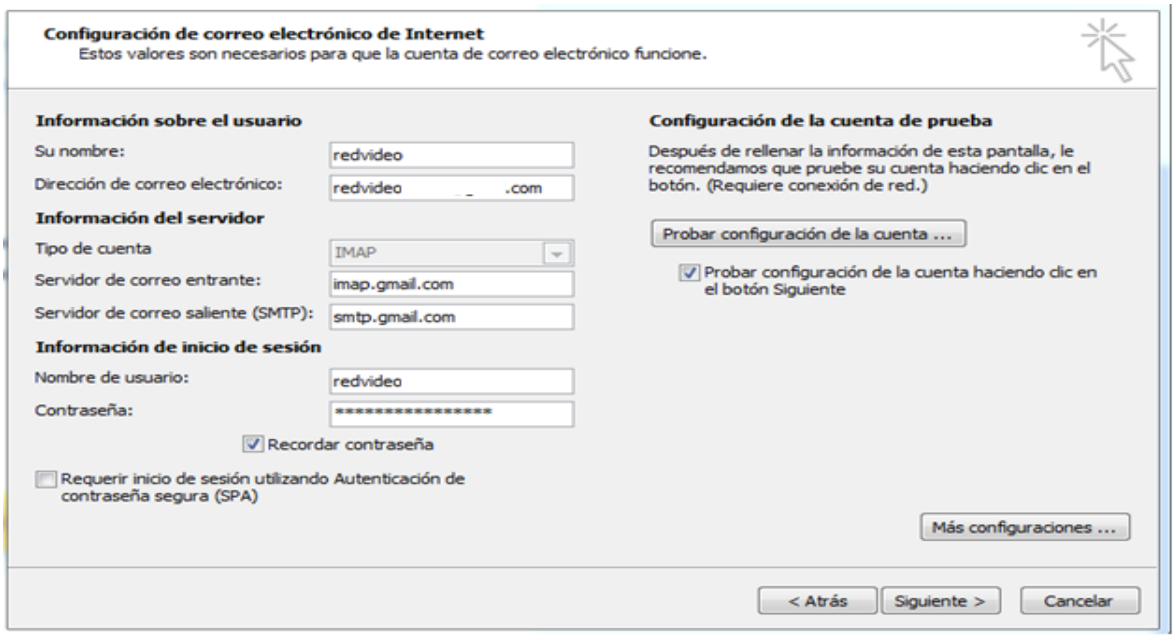


Figura 67. Configuración de cuenta de correo en Outlook.

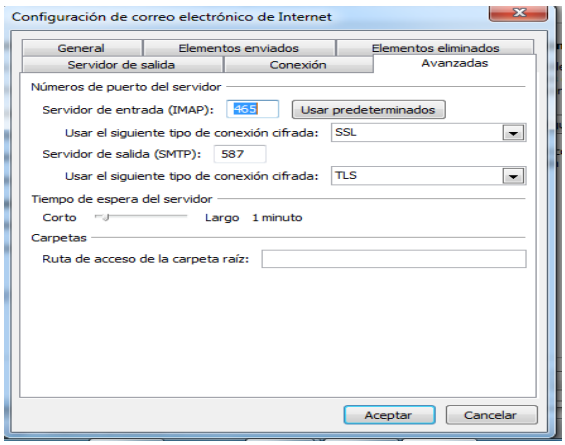


Figura 68. Habilitación de puertos para envío y recepción de mensajes.

Se debe contratar un servicio de hosting compatible para las operadoras telefónicas del país para realizar el envío de SMS disponibles para Outlook como: SureM Co. Ltd. IntelliSoftware redcoal Pty Ltd Red Oxygen, Textburst, Bulletin.net Inc, ZapitSMS, MessageMedia [20].

En este caso se utilizará intellisoftware; se debe ingresar el URL del proveedor de servicios (https://www.intellisoftware.co.uk/account/UserDetails.aspx) para realizar la subscrición a este servicio detallada en la figura 69.

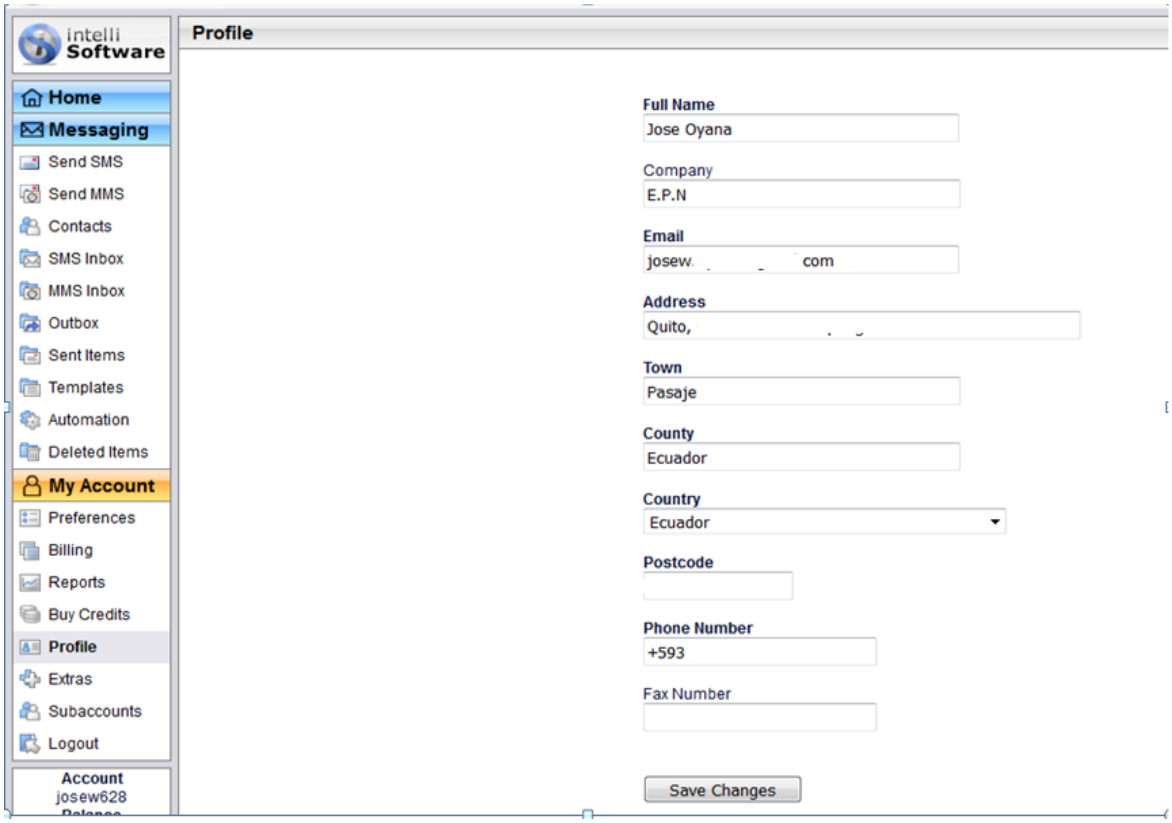


Figura 69. Subscripción al servicio de Intellisoftware.

Con el usuario y la contraseña asignados se ingresa los valores en Outlook al portal detallado en la figura 70 y 71, donde se muestra el cuerpo del mensaje de texto y el destinatario.

Finalmente se crea una regla que realice el reenvío del email de notificación de alertas hacia el número de celular que se deseado, mostrado en la figura 70.

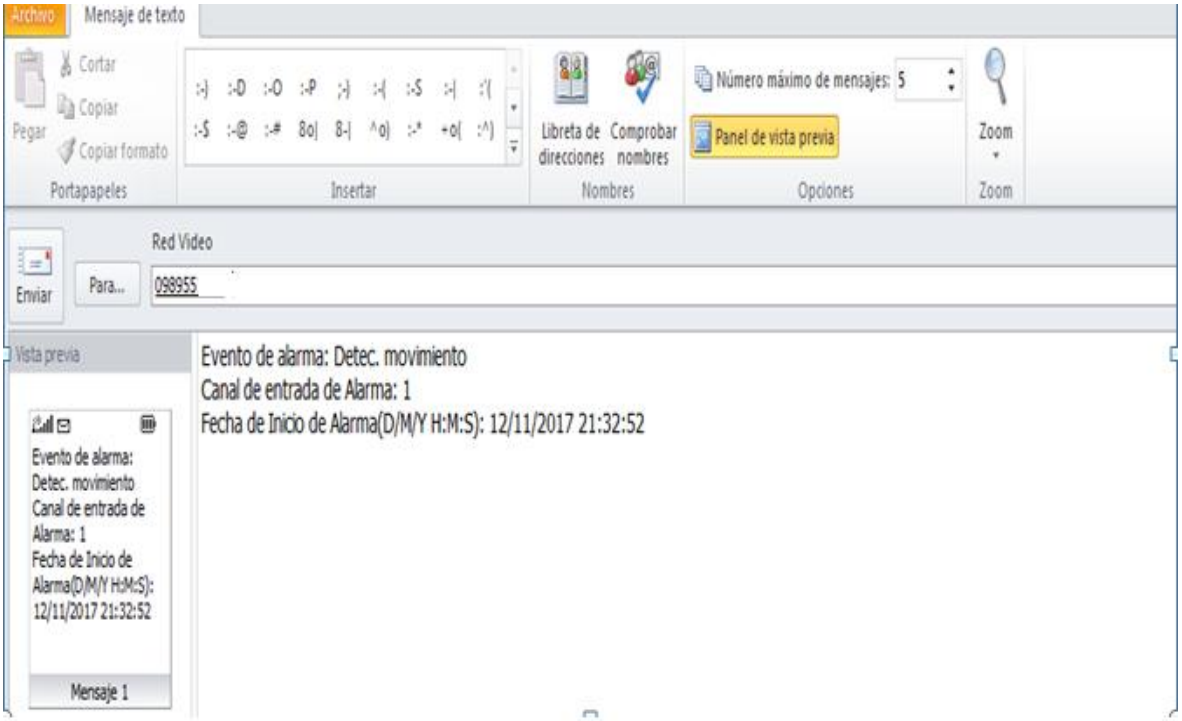


Figura 70. Configuración del proveedor de servicios de SMS.

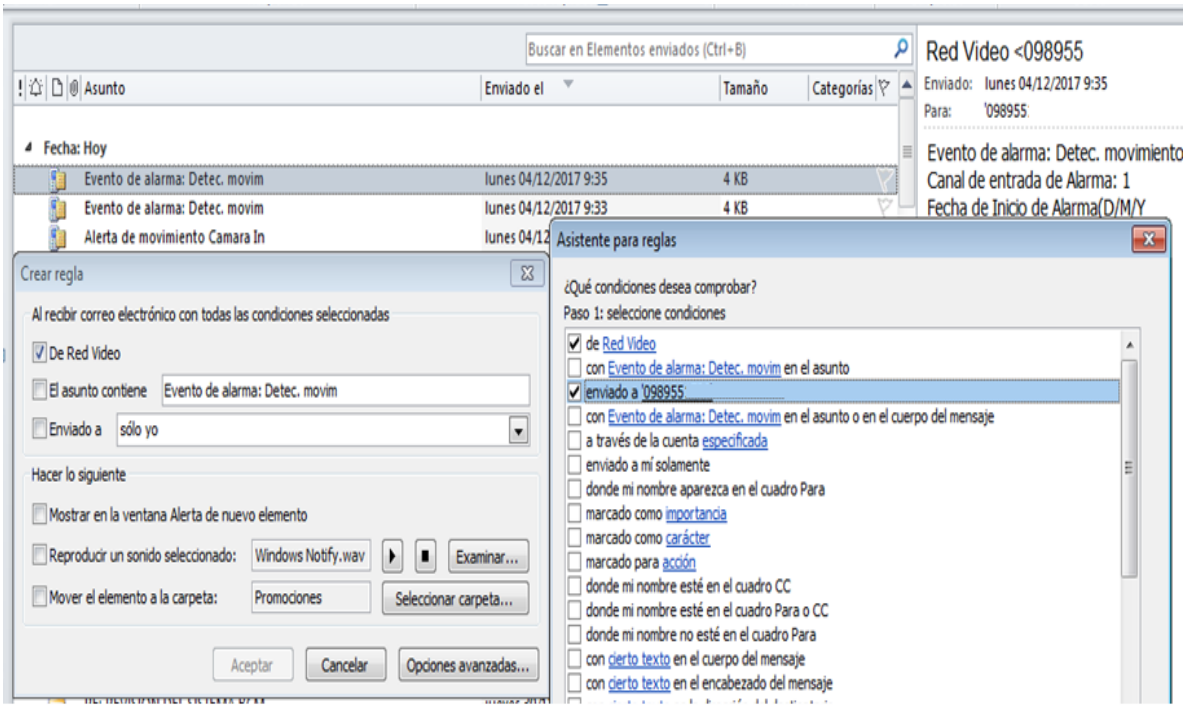


Figura 71. Creación de la regla de envió de mensaje en Outlook.

Figura 72. Mensaje de texto enviado.

3.7 Pruebas del sistema de seguridad inalámbrico

Software de control *iSpy*

En la figura 73, se observa la aplicación funcionando con todas las cámaras ya operativas y grabando información, dependiendo de la zona las cámaras se configuraron para realizar grabaciones continuas o con detección de movimiento.

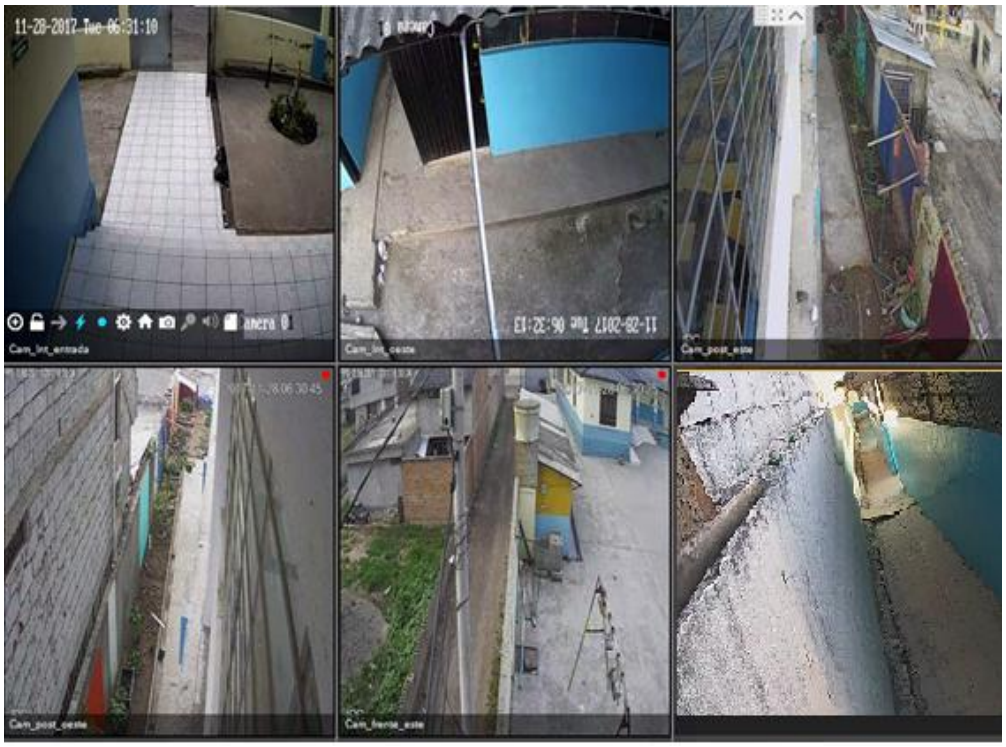


Figura 73. Vista de paneles en la aplicación iSpy.

Configuración de notificación vía correo electrónico.

Posterior a las configuraciones de correo y la habilitación de la salida SMTP, se evidencia envío de correo electrónico para el remitente josew.oyana@gmail.com de las alertas envidas por los equipos, mostrada en la figura 74.

Figura 74. Notificaciones vía correo electrónico

Configuración de almacenamiento y réplica de información.

En esta sección se observa como se ha generado la información de una cámara que está realizando las grabaciones de forma continua las 24 horas. En promedio en la práctica a diario obtiene una cantidad de información de 2,93 GB como se muestra en la figura 75.

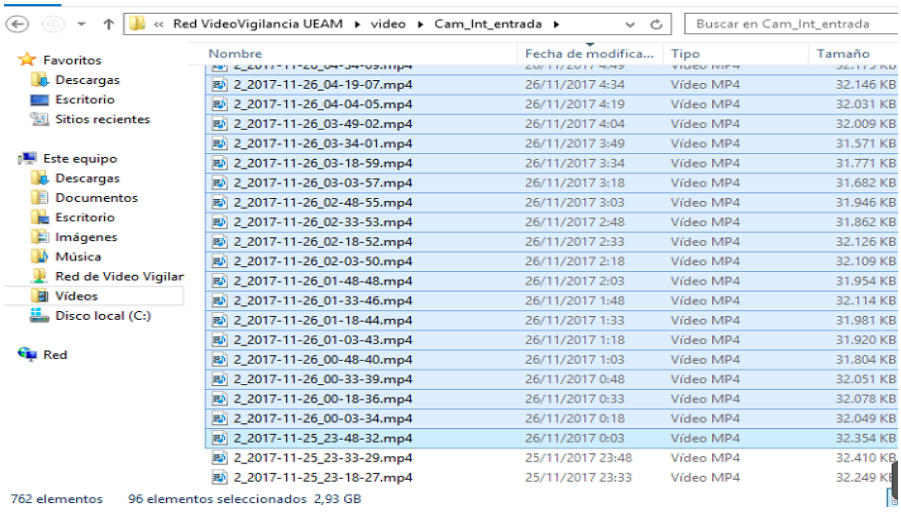


Figura 75. Almacenamiento de información.

En la figura 76 se observa las réplicas de información realizadas en el equipo destino después de ejecutarse la tarea programada en el equipo servidor.

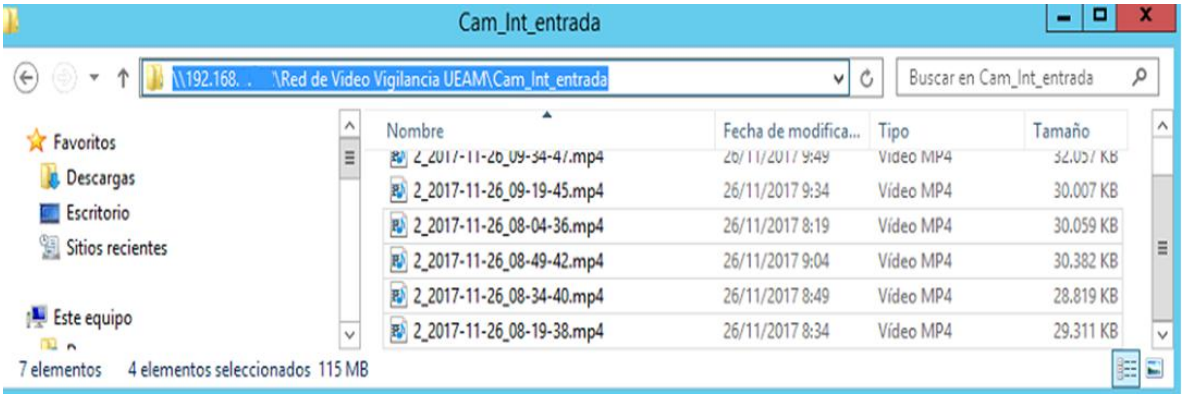


Figura 76. Información creada con la réplica de datos.

Configuración de acceso remoto desde Internet hacia las cámaras.

Al ingresar la dirección establecida se debe conocer la IP de acceso remoto la cual es 181.112.xxx.xxx y el reenvió único de puerto (10001-10006) a la cámara que sea necesaria. Para autenticarse se utiliza el usuario administrador asignada a cada cámaras en las configuraciones básicas de los dispositivos. En la figura 77 se observa la conexión a la cámara frontal este desde Internet.

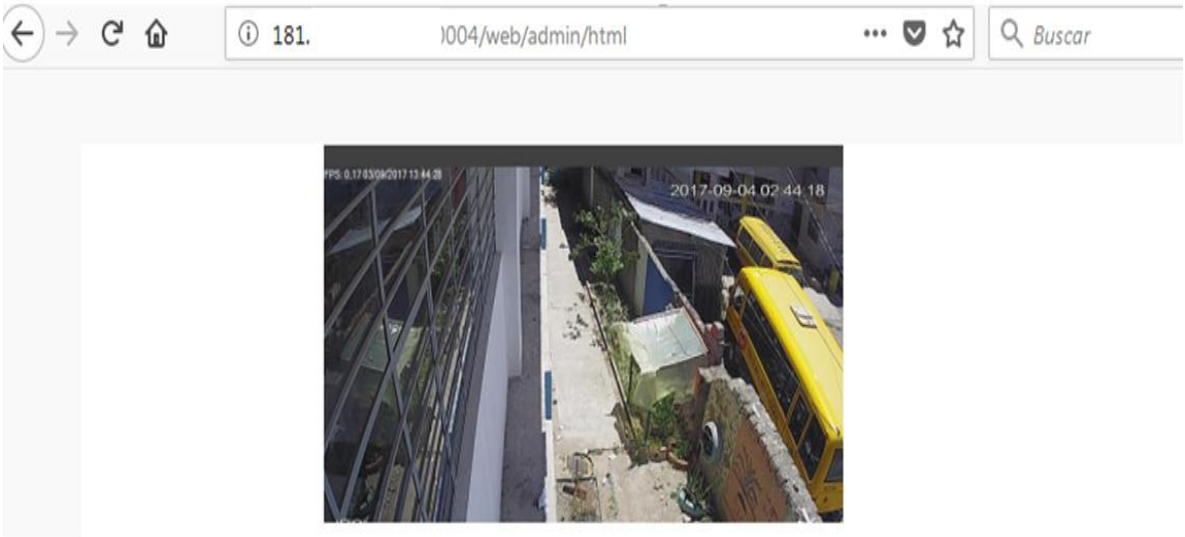


Figura 77. Conexión de acceso remoto.

Configuración de acceso a la nube.

Para este proceso se observa en la figura 78, que los videos son almacenados en la carpeta creada en la nube de Google Drive. La capacidad de almacenamiento de la nube es de 15GB con lo que es posible en la práctica almacenar hasta 3 días de dos dispositivos diferentes ya que el promedio de cantidad de información recolectada es de 2.93 GB por dispositivo al día grabando todas las 24 horas.

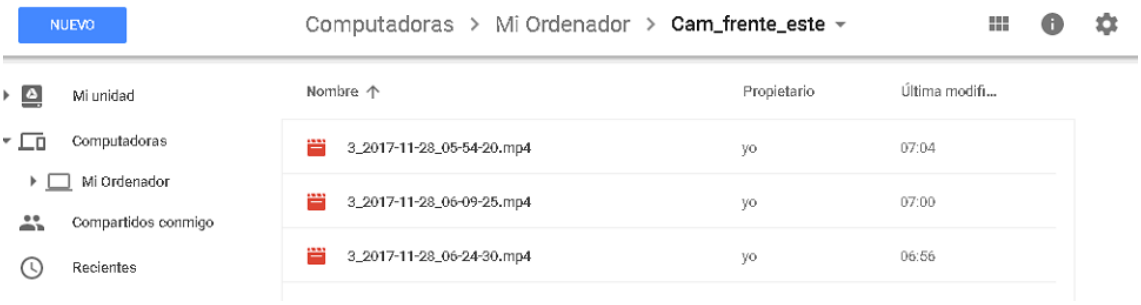


Figura 78. Información almacenada en Google Drive.

4. CONCLUSIONES Y RECOMENDACIONES

4.1 Conclusiones

- Los sistemas de video vigilancia en general son muy útiles como herramienta de seguridad debido a que satisfacen los requerimientos primordiales de todo tipo de negocio, institución, hogar o empresa en cuanto a temas de seguridad para salvaguardar el bienestar de las personas y los bienes materiales.

- La Unidad Educativa Abelardo Moncayo utilizará el sistema de video vigilancia como herramienta para obtener la posibilidad de tomar decisiones oportunas ante cualquier eventualidad y almacenando cada uno de los eventos presentados en los alrededores de la institución, minimizando el impacto generado a los bienes materiales y al alumnado.

- Los sistemas de video vigilancia pueden ser sencillos o avanzados. Para instituciones grandes generalmente los objetivos son mayores, y necesitan conseguir más beneficios, motivo por el cual invierten en mejores equipos. Para poder aprovechar todos los beneficios posibles de un sistema de seguridad, es importante cooperar con un proveedor profesional y así poder prevenir, controlar riesgos y pérdidas, ya estos proveedores que tiene la experiencia requerida para este proceso.

- Los dispositivos utilizados en la instalación del sistema de video vigilancia como son las cámaras Hikvision y Dahua ofrecen un amplio margen de servicios de forma individual, también ofrecen la ventaja de poder integrarse a un software genérico de seguridad.

- El acceso remoto utiliza la característica de reenvío de puerto único configurado en el router uno con lo que se obtiene la ventaja de acceder desde Internet a los dispositivos sin la necesidad de modificar los puertos de fábrica.

- Al realizar la configuración de los avisos mediante correos electrónicos por cada movimiento registrado por las cámaras, se creó una herramienta de prevención ante cualquier siniestro, sin embargo, esta herramienta por sí sola no puede cubrir toda la demanda de eventualidades, para ellos la Unidad Educativa consta con un sistema de emergencia el cual se complementa perfectamente con las cámaras.

- El sistema de video vigilancia realiza un almacenamiento de información de alrededor de 2,6 GB por cada cámara en el modo de grabación continua, el disco duro de almacenamiento tiene una capacidad de 500 GB lo que permite almacenar información de hasta 33 días utilizando el máximo de uso de cada equipo.

- La señal recibida por cada una de las cámaras esta alrededor de los – 50 y -80 dB lo cual es aceptable para tener una conectividad adecuada según lo especifica la hoja de características (*datasheet*) hacia los *routers* inalámbricos.

- Al realizar la instalación de las cámaras inalámbricas fue necesario configurar las IPs de manera fija y adicional se debe guardar cada configuración en la memoria de las cámaras para evitar el volver a configurar todo durante un corte de energía inesperado.

- Debido a las limitaciones de infraestructura en el plantel educativo para este tipo de proyectos, se realizaron trabajos de cableado eléctrico para la colocación de las cámaras, cableado estructurado para la instalación de los puntos de datos usados para la conexión del equipo computacional que controla el sistema de video vigilancia y los *routers* LINKSYS E900, necesarios para la conexión de las cámaras.

- Al realizar la instalación de las cámaras se observó que no fue posible colocar cableado Ethernet en algunas zonas, debido principalmente a que la infraestructura de la institución está cambiando debido a obras civiles para mejora de la misma.

- Al no contar con un sistema de respaldo de energía en el plantel educativo, la red de video vigilancia tiene cierta vulnerabilidad a los cortes eléctricos, se planteó la posibilidad de realizar un sistema eléctrico con respaldo de energía en la institución, sin embargo en la institución no tiene el presupuesto necesario para realizar dicho proyecto, posteriormente se puede migrar las fuentes de energía a este sistema.

- La aplicación *iSpy*, permite configurar cámaras adicionales (sin limitaciones) en el software de control, el diseño de la red tiene una escalabilidad para colocar 4 equipos adicionales sin tener inconvenientes con la señal emitida por los equipos inalámbricos. También es posible realizar un proceso de cableado estructurado para colocar un equipo inalámbrico adicional en modo puente para ampliar el rango de cobertura.

- El equipo PC servidor tiene un puerto SATA disponible para colocar un disco duro interno adicional y aumentar la capacidad de almacenamiento a 60 días.

4.2 Recomendaciones

- Los sistemas de video vigilancia en la actualidad presentan múltiples beneficios, por lo cual su implementación se ha ido expandiendo en los diferentes negocios, instituciones y hogares, por estos motivos el proyecto tendrá una gran acogida para cumplir con las necesidades primordiales de seguridad para el plantel.

- Es recomendable realizar el mantenimiento de las cámaras cada dos meses debido a que los dispositivos se encuentran en exteriores, el equipo servidor PC debe apagarse durante 30 minutos cada quince días, y realizar un mantenimiento preventivo cada seis meses.

- Los routers inalámbricos deben ser revisados cada dos meses y obtener un respaldo de las configuraciones de cada uno de los equipos, con esto se garantiza la operatividad de la red de video vigilancia.

- Se recomienda a la institución educativa realizar la gestión para obtener el sistema de respaldo de energía en todo el plantel, no sólo por las cámaras de seguridad sino por preservar el buen funcionamiento de los dispositivos electrónico conectados a la red eléctrica.

5. BIBLIOGRAFÍA

[1] CISCO, SYSTEMS, INC, Fundamentos de redes inalambricas, Madrid: Pearson Educación, S.A, 2006.

[2] www.google.com, «seguridadwifis,» 2014. [En línea]. Available: https://sites.google.com/site/seguridadwifis/interferencia-y-atenuacion. [Último acceso: 10 Abril 2018].

[3] apcorg, «APCORG,» 2008. [En línea]. Available: https://www.apc.org/sites/default/files/APC_RedesInalambricasParaElDesarrolloLAC_20081223.pdf. [Último acceso: 10 Abril 2018].

[4] acens.com, «Redes de seguridad,» Julio 2012. [En línea]. Available: https://www.acens.com/wp-content/images/whitepaper-redes-seguridad-acens-julio-2012.pdf. [Último acceso: 15 Abril 2018].

[5] rnds, «Componentes y características de un sistema de CCTV,» rnds, 14 Noviembre 2007. [En línea]. Available: http://www.rnds.com.ar/articulos/037/RNDS_140W.pdf. [Último acceso: 13 Octubre 2017].

[6] seagate.com, «seagate.com,» 2015. [En línea]. Available: https://www.seagate.com/la/es/tech-insights/how-much-video-surveillance-storage-is-enough-master-ti/. [Último acceso: 16 Abril 2018].

[7] microsoft.com, «microsoft.com,» microsoft.com, 14 Agosto 2015. [En línea]. Available: https://msdn.microsoft.com/es-es/library/dn495044(v=ws.11).aspx. [Último acceso: 14 Octubre 2017].

[8] redeszone.net, «redeszone.net,» 13 Septiembre 2014. [En línea]. Available: https://www.redeszone.net/2014/09/13/ispy-el-software-de-videovigilancia-opensource-mas-completo/. [Último acceso: 14 Octubre 2017].

[9] ispyconnect.com, «ispyconnect.com,» 14 Agosto 2015. [En línea]. Available: https://www.ispyconnect.com/. [Último acceso: 15 Octubre 2017].

[10] G. A. Medina, «educaciondecalidad,» Septiembre 2016. [En línea]. Available: http://educaciondecalidad.ec/ley-educacion-intercultural-menu/ley-educacion-intercultural-texto-ley.html. [Último acceso: 16 Agosto 2017].

[11] hikvision.com, «hikvision.com,» [En línea]. Available: http://oversea-download.hikvision.com/uploadfile/doc/20141015/DS-2CD2110F-I.pdf. [Último acceso: 24 Agosto 2017].

[12] alphatronics, «alphatronics dahua tecnology,» 2011. [En línea]. Available: https://www.alphatronics.nl/media/wysiwyg/PDF/Video/IPC-HFW1120S-W.pdf. [Último acceso: 25 Agosto 2017].

[13] Linksys, «Linksys,» linksys.com, 05 Mayo 2016. [En línea]. Available: http://www.linksys.com/ec/p/P-E900/. [Último acceso: 20 Febrero 2017].

[14] dahuasecurity, «dahuasecurity.com,» Agosto 2015. [En línea]. Available: http://www1.dahuasecurity.com/products/ipc-hfw1120s-w-5601.html. [Último acceso: 10 Septiembre 2017].

[15] hikvision.com, «hikvision.com,» 17 Agosto 2016. [En línea]. Available: http://oversea-download.hikvision.com/uploadfile/doc/20141015/DS-2CD2110F-I.pdf. [Último acceso: 15 Septiembre 2017].

[16] officeredir.microsoft, «officeredir.microsoft,» Microsoft, 12 Junio 2015. [En línea]. Available: http://officeredir.microsoft.com/r/rlidOMSSP2?clid=&ver=14&app=outlook.exe&lidhelp=0C0A&liduser=300A&lidui=0C0A. [Último acceso: 20 Noviembre 2017].

[17] A. S. Tanenbaum, Redes de Computadoras, Mexico: Pearson Education, 2003.

[18] Tutorialspoint, «Tutorialspoint simplyeasylearning,» Tutorialspoint, 04 Enero 2017. [En línea]. Available: https://www.tutorialspoint.com/computer_fundamentals/computer_networking.htm. [Último acceso: 5 Mayo 2017].

[19] J. J. L. H. S. M.-R. Carmen de Pablos, INFORMÁTICA Y COMUNICACIONES EN LA EMPRESA, Madrid: ESIC, 2004.

[20] IST La Recoleta, «IST La Recoleta,» IST La Recoleta, 20 Enero 2003. [En línea]. Available: http://ual.dyndns.org/Biblioteca/Redes/Pdf/Unidad%2003.pdf. [Último acceso: 10 Mayo 2017].

[21] J. B. C. F. G. V. Manual Álvarez-Campana, TECNOLOGÍAS DE BANDA ANCHA Y CONVERGENCIA DE REDES, Madrid: Ministerio de Industria, Turismo y Comercio, 2005.

[22] Eyca, «eyca.com,» Eyca Total Security, Enero 2011. [En línea]. Available: http://www.eyca.com.mx/funcionamiento-cctv. [Último acceso: 13 Octubre 2017].

[23] Novenca Security System, «Novenca Security System,» 21 Septiembre 2011. [En línea]. Available: http://www.novenca.com/site/index.php?option=com_content&view=article&id=98&It

emid=88. [Último acceso: 14 Octubre 2017].

[24] Jorge_Hernandez-Constante, «researchgate.ne,» Marzo 2014. [En línea]. Available: https://www.researchgate.net/profile/Jorge_Hernandez-Constante/publication/309591673_Calculo_de_Radio_Enlace_Terrestre/links/5818cf7008ae6378919e73db/Calculo-de-Radio-Enlace-Terrestre.pdf. [Último acceso: 30 Octubre 2017].

6. ANEXOS

ANEXO A: *Datasheet* cámara Hikvision ds-2cd2110f-i.

HAIKON
By Hikvision Digital Technology

datasheet

DS-2CD2110F-I Indoor / Outdoor IR Fix Dome Camera, 1.3Mp, H.264, Day/Night

Key Features

- Up to 1.3 Mp (1280 X 960) @ 30 fps Resolution
- Built-in Smart IR Led, up to 30mt
- True Day Night, IR Cut Filter
- Dual Stream
- Built-in Smart Video Analysis
- ROI (Region of Interest)
- Backlight Compensation (BLC)
- D(ital WDR
- Digital Noise Reduction
- IP66
- Vandal-Proof

Low-Bit Stream Transmission : With the advanced codec algorithm, HAIKON 2-line Smart IPC can realize an efficient encoding, and further minimize the system's load and storage requirement. For example: at a very low bitrate streaming condition, 2Mbps at 720p resolution, **2-line** camera could increase the image quality up to 30%

Dual Streams : 2 streams gives much more flexibility to use different data stream for each independent purpose: Main stream: full resolution, Sub stream: low resolution .

Smart IR : The improved Smart IR function allows to auto adjust the IR strength to have a better visibility.

ROI : Based on user-defined ROI **(Region of Interest)**, camera can decrease a non-ROI's image quality to save maximum bandwidth and storage, also for having a better image quality of target ROI area under the same bitrate stream condition.

Intrusion Detection : Intrusion detection is very useful for defined area protection. when an intruder been detected, alarm or event recording will be directly triggered. With its auto analyze for the intruder's dimension ratio, the latest algorithm can effectively reduce the false alarm rate.

Line Crossing : Line crossing is very important application for border security. When the some attach come from border or any specific area that you selected, alarm or event recording will be directly triggered

DS-2CD2110-I Indoor / Outdoor Fix Dome Camera Technical Specification

Image Sensor	1/3" Progressive Scan CMOS
Min. Illumination	0.01 Lux @ (F1.2, AGC ON), 0 lux with IR
Shutter Speed	1/25s to 1/100,000 s
S/N Ratio	50dB
Lens	4mm@ F2.0 (2.8mm, 6mm, 12mm optional)
Day & Night	IR cut filter with auto switch
Digital Noise Reduction	3D DNR
Wide Dynamic Range	DWDR
Video Compression	H.264 / MJPEG
H.264 Type	Main Profile
Video Bit Rate	32 Kbps ~ 16 Mbps
Dual Stream	Support
Max. Resolution	1280 X 960
Frame Rate	50 Hz: 25 fps (1280 X 960), 25 fps (1280 x 720), 25 fps (704 x 576), 25 fps (640 x 480) 60 Hz: 30 fps (1280 X 960), 30 fps (1280 x 720), 30 fps (704 x 576), 30 fps (640 x 480)
BLC	Support
Image Setting	Rotate mode, Saturation, Brightness, Contrast adjustable by client software or web browser
ROI	Support
Network Storage	NAS (Support NFS,SMB/CIFS)
Smart Video Analysis	Line Crossing, Intrusion Detection, Motion detection, Dynamic analysis, Tampering alarm, Network disconnect , IP address conflict, Storage exception
Protocols	TCP/IP,ICMP,HTTP,HTTPS,FTP,DHCP,DNS,DDNS,RTP,RTSP,RTCP, PPPoE,NTP,UPnP,SMTP,SNMP,IGMP,802.1X,QoS,IPv6,Bonjour
General	One-key reset, Flash-prevention, dual stream, heartbeat, mirror, password protection, privacy mask, watermark, IP address filtering, Anonymous access
Standard	ONVIF Profile S, PSIA, CGI, ISAPI
Communication Interface	1 RJ45 10M/100M Ethernet port
IR Range	Approx. 10 to 30 meters
Impact Protection	IEC60068-275Eh, 50J; EN50102, up to IK10
Ingress Protection	IP66
Operating Conditions	-30 °C ~ 60 °C (-22°F ~ 140 °F) humidity 95% or less (non-condensing)
Power Supply	12 V DC ± 10%, PoE (802.3af)
Power Consumption	Max. 5 W (Max. 7 W with IR cut filter on)
Dimensions	Φ111 X 82 (4.4" X 3.2")
Weight	500 g
Certification	CE EN 55022(CLASS B),EN50130-4,EN61000-3-2,EN 61000-3-3,EN60950-1 FCC CFR 47 FCC Part 15 subpart B(CLASS B) C-TICK AS/NZS CISPR 22:2009 (CLASS B) UL&cUL UL 60950-1, CSA C22.2 No. 60950-1-07 RoHS 2011/65/EU REACH No1907/2006 WEEE 2012/19/EU

ANEXO B: *Datasheet* cámara dahua dh-ipc-hfw1120sw.

DH-IPC-HFW1120S-W

1.3MP IR Mini-Bullet Wi-Fi Network Camera

- 1/3" 1.3Megapixel progressive CMOS
- H.264& MJPEG dual-stream encoding
- 25/30fps@1.3M(1280×960)
- DWDR, Day/Night(ICR), 3DNR, AWB, AGC, BLC
- Multiple network monitoring: Web viewer, CMS(DSS/PSS) & DMSS
- Wi-Fi support
- 2.8 mm fixed lens (3.6mm optional)
- Max IR LEDs Length 30m
- IP67

System Overview

The IR Megapixel Fixed Mini-Bullet camera delivers 1.3MP resolution with a choice of 2.8mm or 3.6mm lens options. The camera's elegant blend of aesthetics combined with its compact form factor provides an excellent choice for a variety of small to mid-size, indoor/outdoor applications at an affordable price

Functions

True Day/Night
A day/night mechanical IR cut filter makes this camera ideal for applications with fluctuating lighting conditions, delivering color images during the day and automatically switching to monochrome as the scene darkens

Regions of interest
Regions of Interest (ROI) is a user defined feature that allows the operator to monitor specific areas of a scene while still maintaining overall situational awareness of less important areas

Smart IR
With IR illumination, detailed images can be captured in low light or total darkness. The camera's Smart IR technology adjusts to the intensity of camera's infrared LEDs to compensate for the distance of an object. Smart IR technology prevents IR LEDS from whiting out images as they come closer to the camera. The camera's integrated infrared illumination provides high performance in extreme low-light environments up to 30m (98ft).

Image flip
Capturing unnecessary data such as surrounding hallway walls can increase storage requirements without any added value. The image flip feature allows the camera's image to be rotated in 90° increments for better video optimization.

Protection
Supporting ±10% input voltage tolerance, this camera suits even the most unstable conditions for outdoor applications. Its 6KV lightning rating provides protectection against the camera and its structure from the effects of lightning.

Interoperability
The camera conforms to the ONVIF (Open Network Video Interface Forum) specifications, ensuring interoperability between network video products regardless of manufacturer

Technical Specification

Camera

Image Sensor	1/3" 1.3Megapixel progressive CMOS
Effective Pixels	1280(H) x960(V)
RAM/ROM	256MB/16MB
Scanning System	Progressive
Minimum Illumination	0.1Lux/F2.0(Color), 0Lux/F2.0(IR on)
S/N Ratio	More than 50dB
IR Distance	Distance up to 30m(98ft)
IR On/Off Control	Auto/ Manual
IR LEDs	24

Lens

Lens Type	Fixed
Mount Type	Board-in
Focal Length	2.8 mm (3.6 mm optional)
Max. Aperture	F2.0/F2.0
Angle of View	H:92°/72°, V:55°/55°
Focus Control	Fixed
Close Focus Distance	N/A

PTZ

Pan/Tilt Range	Pan:0° ~360° ;Tilt:0° ~90° ;Rotation:0° ~360°

Video

Compression	H.264/H.264B/H.264H/MJPEG
Streaming Capability	2 Streams
Resolution	1.3M(1280*960)/720P(1280*720)/VGA(640*480)/ QVGA(320*240)
Frame Rate	1.3M (1 ~ 25/30fps) VGA(1 ~ 25/30fps)
Bit Rate Control	CBR/VBR
Bit Rate	H264:32K ~ 10Mbps
Day/Night	Auto(ICR) / Color / B/W
BLC Mode	BLC / HLC / DWDR

White Balance	Auto/Natural/Street Lamp/Outdoor/Manual
Gain Control	Auto/Manual
Noise Reduction	3D DNR
Motion Detection	Off / On (4 Zone, Rectangle)
Region of Interest	Off / On (4 Zone)
Electronic Image	Support
Smart IR	Support
Digital Zoom	16x
Flip	0°/90°/180°/270°
Mirror	Off / On
Privacy Masking	Off / On (4 Area, Rectangle)

Audio

Compression	N/A

Network

Ethernet	RJ-45 (10/100Base-T)
Wi-Fi	Wi-Fi(IEEE802.11b/g/n),30m(open field)
Protocol	HTTP;HTTPs;TCP;ARP;RTSP;RTP;UDP;SMTP;FTP;DHCP;DNS;DDNS;PPPOE;IPv4/v6;QoS;UPnP;NTP;Bonjour ;802.1x;Multicast;ICMP;IGMP;
Interoperability	ONVIF, P2A, CGI
Streaming Method	Unicast / Multicast
Max. User Access	10 Users/20 Users
Edge Storage	NAS(Network Attached Storage),Local PC for instant recording, 128GB
Web Viewer	IE, Chrome, Firefox, Safari
Management Software	Smart PSS, DSS,Easy4ip
Smart Phone	iPhone, iPad, Android Phone

Certifications

Certifications	CE (EN 60950:2000) UL/cUL60950-1 FCC: FCC Part 15 Subpart B

Interface

Video Interface	N/A
Audio Interface	N/A
RS485	N/A
Alarm	N/A

Electrical

Power Supply	DC12V
Power Consumption	4.5W

Environmental

Operating Conditions	-10° C ~ 60° C (14° F ~ 122° F) / Less than 95% RH
Storage Conditions	-10° C ~ 60° C (14° F ~ 122° F) / Less than 95% RH
Ingress Protection	IP67
Vandal Resistance	N/A

Construction

Casing	Metal+Plastic
Dimensions	Ø70mm×154.7mm(2.76"×6.49")
Net Weight	0.45Kg (0.99lb)
Gross Weight	0.52Kg (1.15lb)

Ordering Information

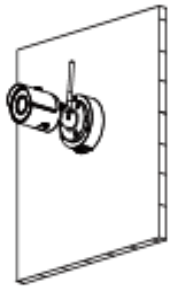
Type	Part Number	Description
1.5MP camera	DH-IPC-HFW1120SP-W-0360B	1.5MP IR Mini-Bullet Wi-Fi Network Camera, 2.8mm, PAL
	DH-IPC-HFW1120SN-W-0360B	1.5MP IR Mini-Bullet Wi-Fi Network Camera, 2.8mm, NTSC
	IPC-HFW1120SP-W-0360B	1.5MP IR Mini-Bullet Wi-Fi Network Camera, 2.8mm, PAL
	IPC-HFW1120SN-W-0360B	1.5MP IR Mini-Bullet Wi-Fi Network Camera, 2.8mm, NTSC
	DH-IPC-HFW1120SP-W-0560B	1.5MP IR Mini-Bullet Wi-Fi Network Camera, 3.6mm, PAL
	DH-IPC-HFW1120SN-W-0560B	1.5MP IR Mini-Bullet Wi-Fi Network Camera, 3.6mm, NTSC
	IPC-HFW1120SP-W-0560B	1.5MP IR Mini-Bullet Wi-Fi Network Camera, 3.6mm, PAL
	IPC-HFW1120SN-W-0560B	1.5MP IR Mini-Bullet Wi-Fi Network Camera, 3.6mm, NTSC
Accessories (optional)	PFA134	Junction Box
	PFA150	Pole mount

Accessories

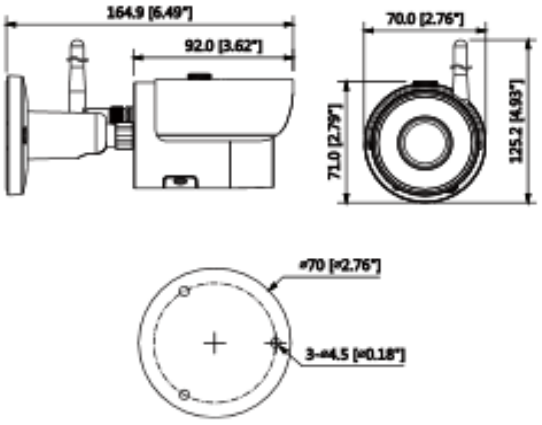
Optional:

PFA134
Junction Box

PFA150
Pole Mount

Junction Mount	Pole Mount
PFA134	PFB134 + PFA150
	

Dimensions (mm/inch)



ANEXO C: Especificaciones router inalámbrico N300 linksys E900.

ROUTER INALÁMBRICO N300 LINKSYS E900

ESPECIFICACIONES TÉCNICAS

Nombre de modelo:
Linksys E900
Estándares de red:
- IEEE 802.11b
- IEEE 802.11a
- IEEE 802.11g
- IEEE 802.11n
- IEEE 802.3
- IEEE 802.3u

Bandas de radiofrecuencia:
2,4 GHz
Puertos:
1 10/100 WAN, 4 10/100 LAN
Luces LED:
Electricidad, WLAN, Ethernet 1-4, Internet
Botones:
1 botón de Reset (Reinicio)
Temperatura de funcionamiento:
Entre 0 y 40°C
Temperatura de almacenaje:
De -20 a 70 °C
Humedad de funcionamiento:
10 a 80 % sin condensación
Tasa de enlace máxima:
300 Mbps
Compatibilidad con plataforma:
- Windows XP
- Windows Vista 32/64
- Windows 7 32/64
- Windows 8 32/64
- Windows 8,1 32/64
- Mac OS X 10.5.8 Leopard
- Mac OS X 10.6.1 Snow Leopard
- Mac OS X 10.7 Lion
- Mac OS X 10.8 Mountain Lion
- Mac OS X 10.9 Mavericks

ANEXO D: Certificado Escuela de Educación básica Abelardo Moncayo.

CERTIFICADO

Quito, 05 mayo 2017

Ingeniera Subdirectora

Mónica Vinueza

SUBDIRECTORA DE LA ESFOT

Presente.

Señora Subdirectora:

Por medio de la presente certifico que el Sr. José Wenceslao Oyana Sanguña, con cédula de identidad 1716210099 estudiante de la escuela de formación tecnológica (ESFOT) de la Escuela Politécnica Nacional, solicitó realizar el proyecto **DISEÑO E IMPLEMENTACIÓN DE UNA RED DE CÁMARAS INALÁMBRICAS DE SEGURIDAD CON MONITOREO REMOTO PARA LA ESCUELA DE EDUCACIÓN BÁSICA ABELARDO MONCAYO** el cual se encuentra aprobado para su realización, señalando que no se ha implementado un proyecto parecido en esta institución.

Por la atención que se sirva a brindar a la presente le anticipo mis agradecimientos.

Atentamente,

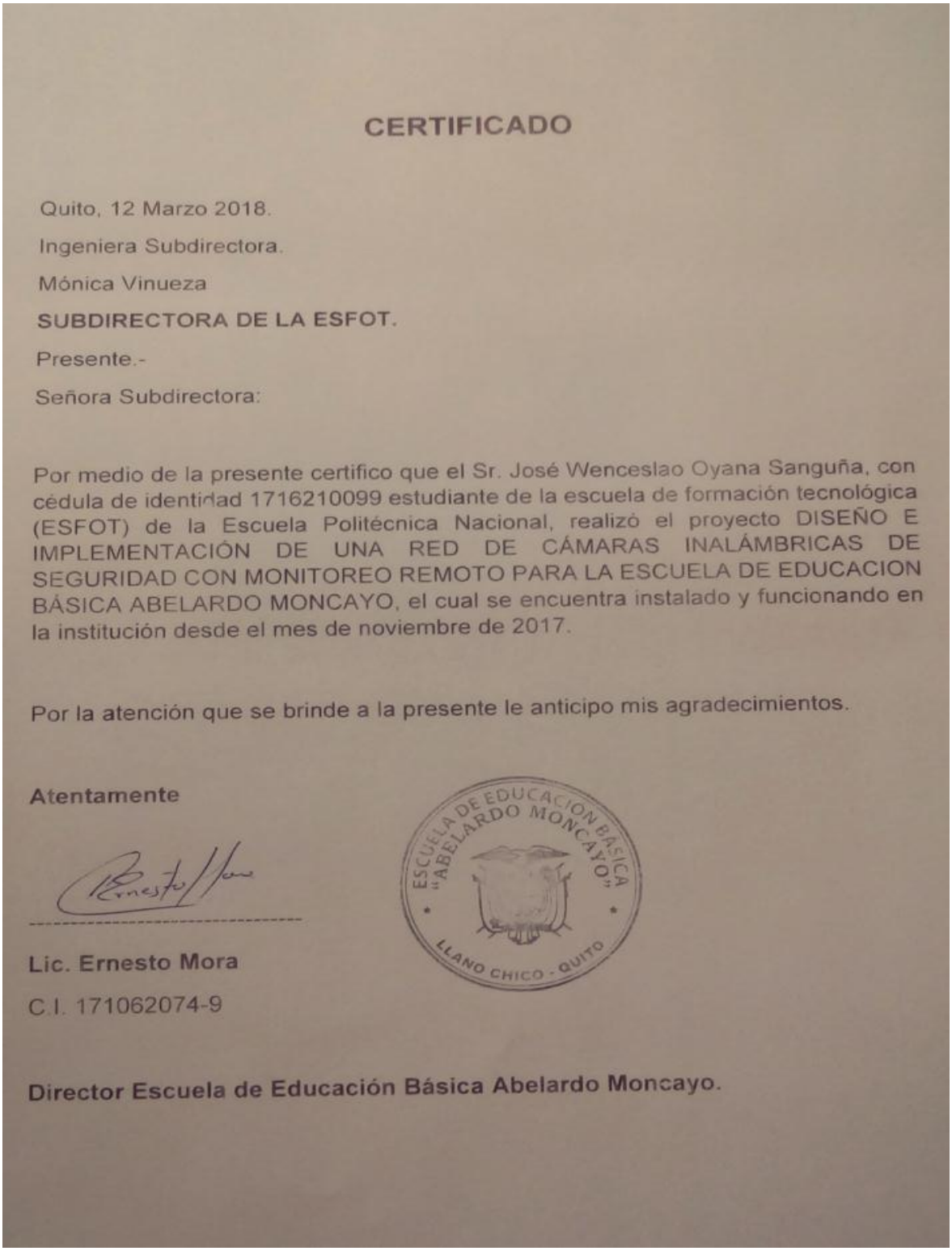
ESCUELA DE EDUCACION BASICA ABELARDO MONCAYO
ANO CHICO - QUITO

Lic. Ernesto Mora

C.I. 1710620710-9

Rector Escuela de Educación Básica Abelardo Moncayo.

ANEXO E: Certificado de funcionamiento del proyecto emitido por la Escuela de Educación básica Abelardo Moncayo.



CERTIFICADO

Quito, 12 Marzo 2018.

Ingeniera Subdirectora.

Mónica Vinueza

SUBDIRECTORA DE LA ESFOT.

Presente.-

Señora Subdirectora:

Por medio de la presente certifico que el Sr. José Wenceslao Oyana Sanguña, con cédula de identidad 1716210099 estudiante de la escuela de formación tecnológica (ESFOT) de la Escuela Politécnica Nacional, realizó el proyecto DISEÑO E IMPLEMENTACIÓN DE UNA RED DE CÁMARAS INALÁMBRICAS DE SEGURIDAD CON MONITOREO REMOTO PARA LA ESCUELA DE EDUCACION BÁSICA ABELARDO MONCAYO, el cual se encuentra instalado y funcionando en la institución desde el mes de noviembre de 2017.

Por la atención que se brinde a la presente le anticipo mis agradecimientos.

Atentamente

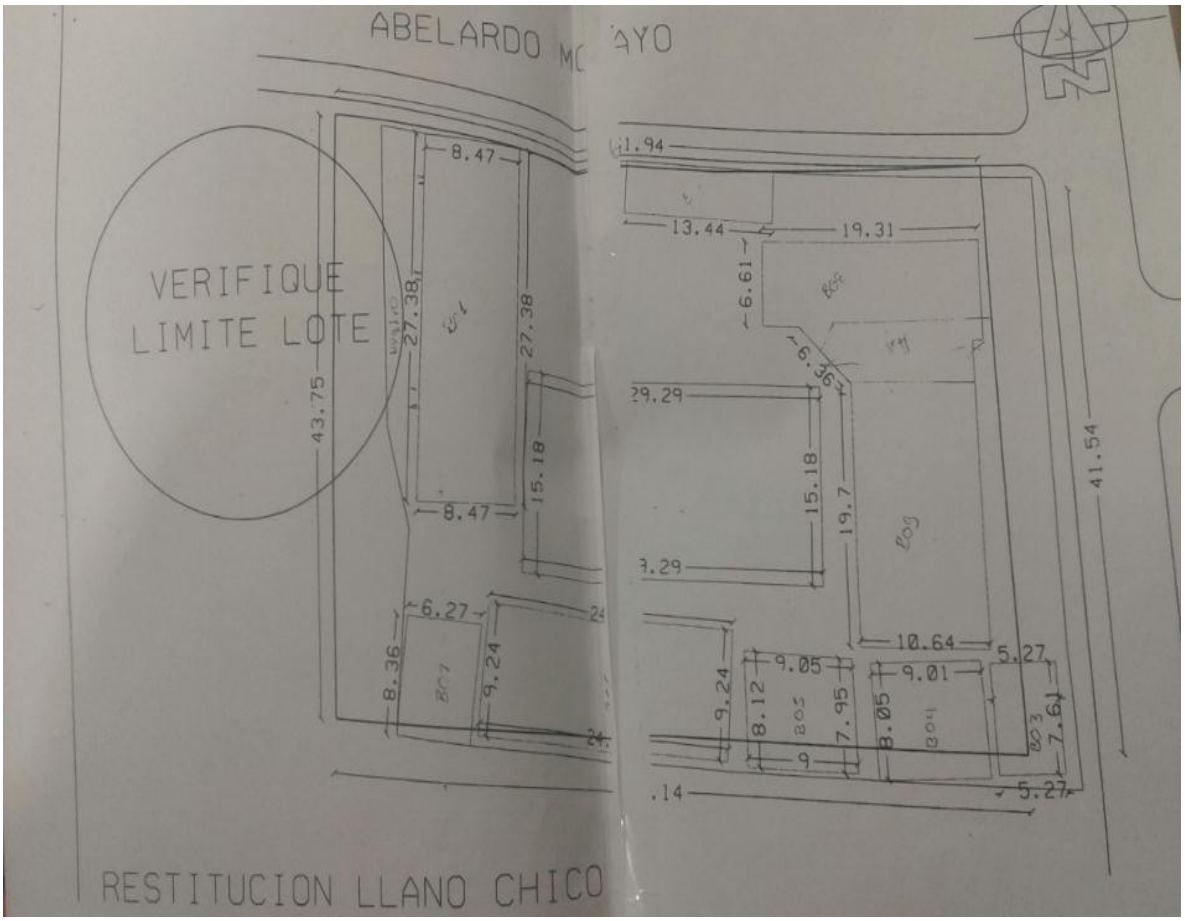
ESCUELA DE EDUCACION BÁSICA "ABELARDO MONCAYO" LLANO CHICO - QUITO

Lic. Ernesto Mora

C.I. 171062074-9

Director Escuela de Educación Básica Abelardo Moncayo.

ANEXO F: Planos originales de la escuela de Educación Básica Abelardo Moncayo.

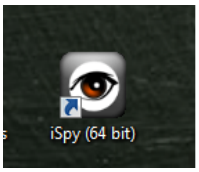


ANEXO G: Detalle de los equipos adquiridos.

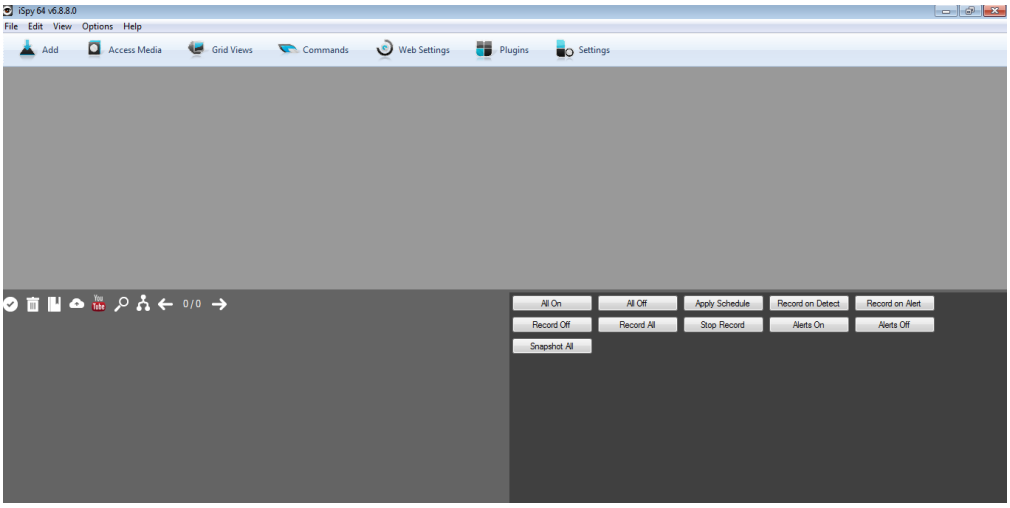
DESCRIPCIÓN	CANTIDAD	V. UNITARIO	SUBTOTAL
Cámara Dahua	4	125	500
Cámara Hikvision	2	145	290
Adaptador eléctrico de cámara 12 V	6	4,5	27
Router Linksys E900	2	65	130
Cable de red para exteriores	40 m	35	35
Cable de red para interiores	10 m	13	13
Switch de escritorio	1	10	10
PC Servidor	1	280	280
Cableado eléctrico	40 m	50	50
Caja de protección para cámaras en exteriores	6	2,5	15
			1350

ANEXO H: Manual de usuario de la aplicación *iSpy.*

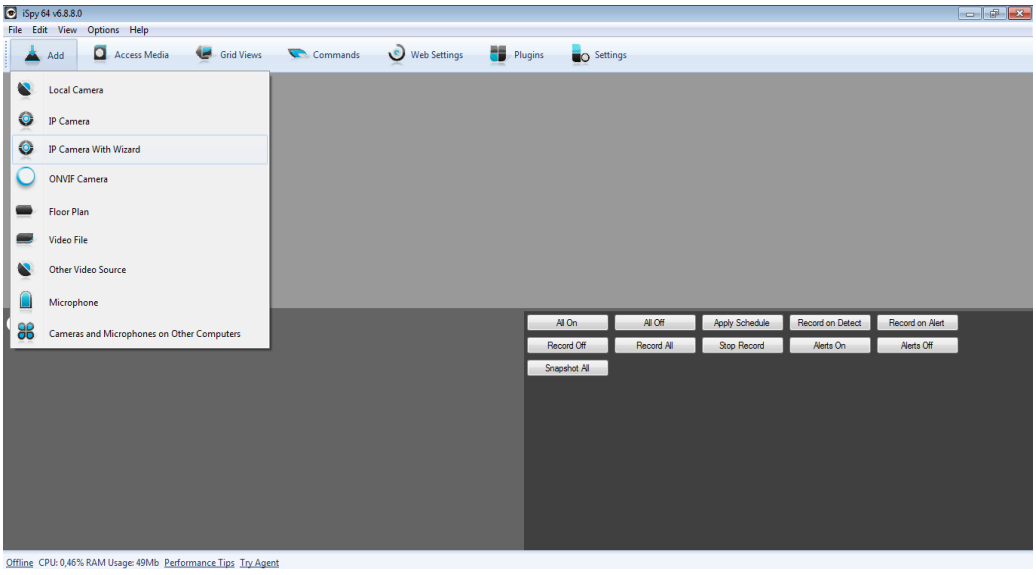
1.- Para ingresar a la aplicación realizar click en el siguiente ícono.



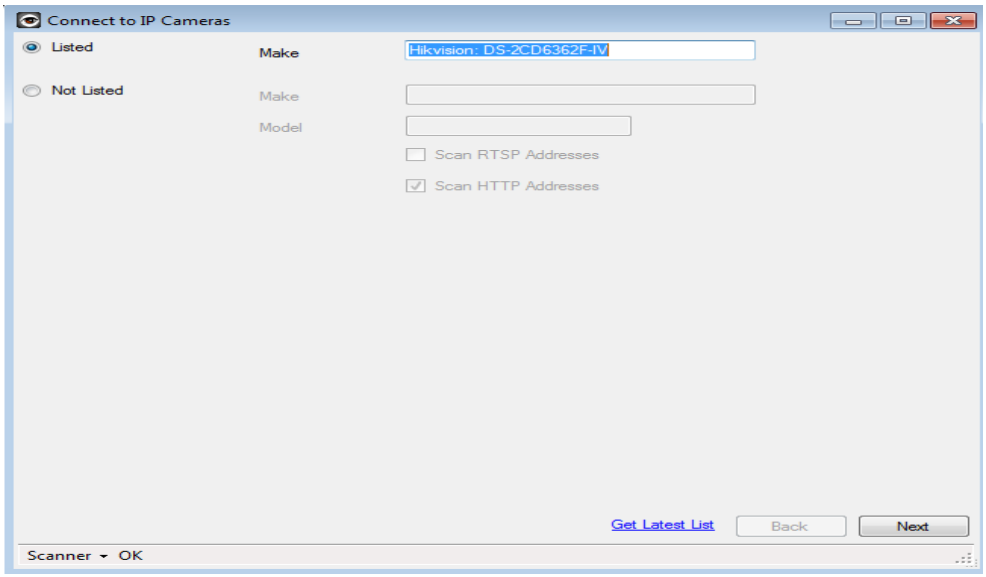
2.- Inicia la interfaz de la aplicación *iSpy.*



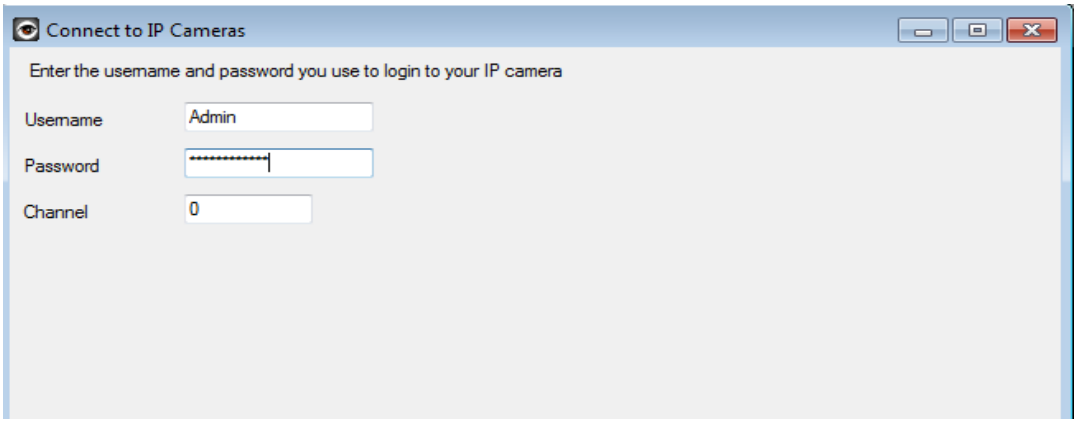
3.- Para agregar una cámara nueva, seleccionamos cámara IP con el asistente.



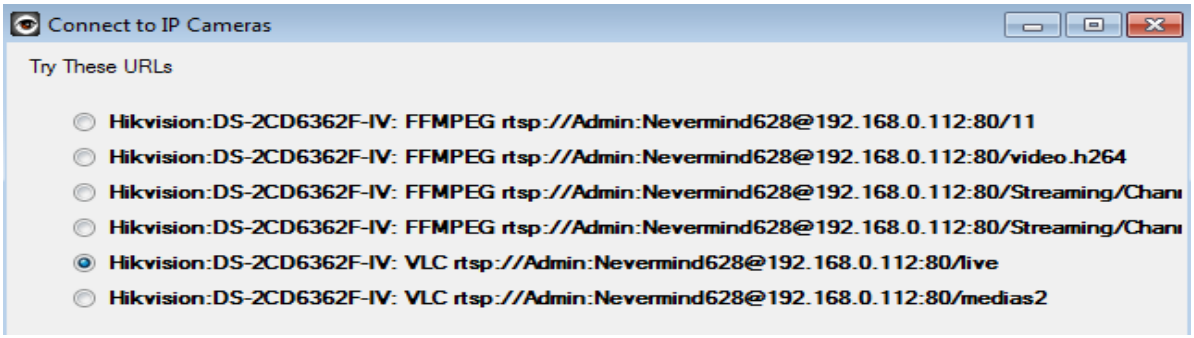
4.- Seleccionar el modelo de la cámara.



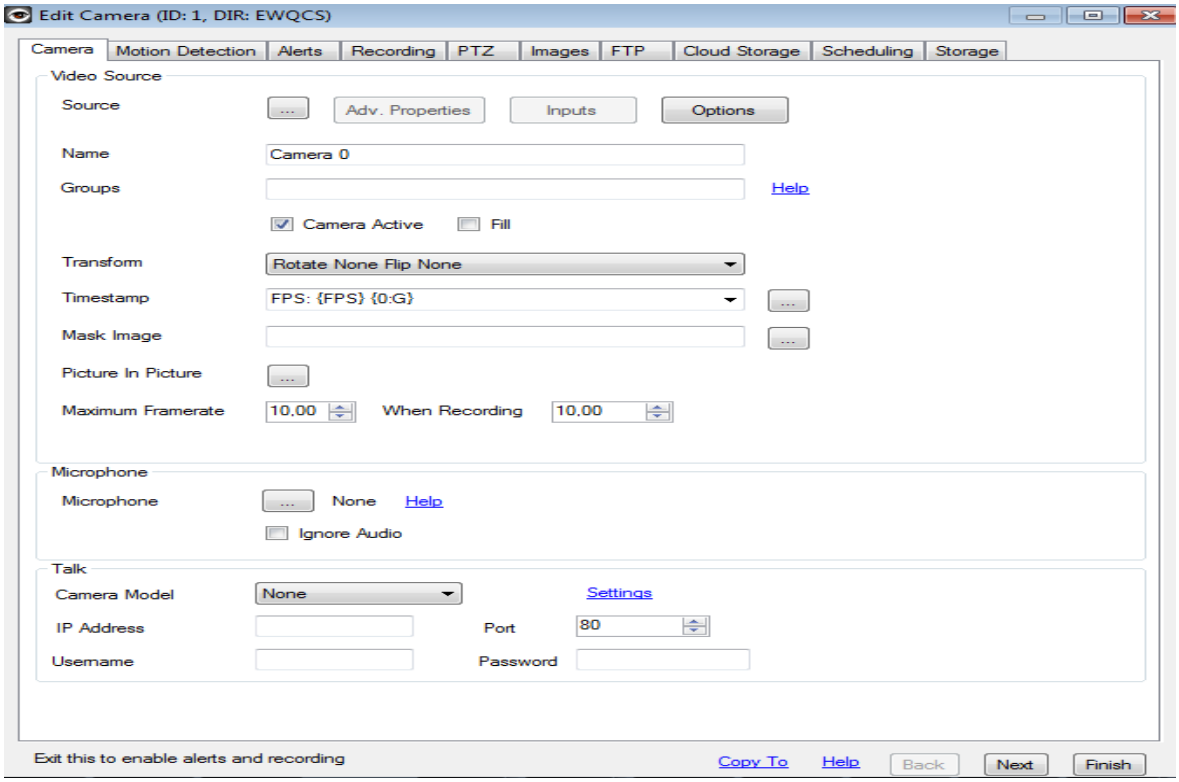
5.- Colocar el usuario y la contraseña de cada cámara. Para todas las cámaras se definió el usuario admin y la contraseña asignada.



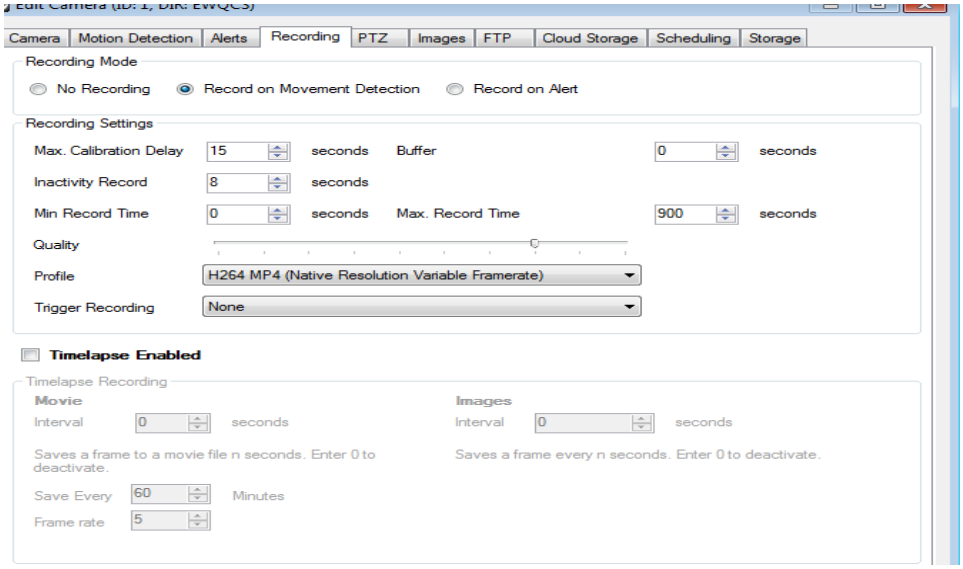
6.- Seleccionar unos de los links que aparecen del modelo de la cámara.



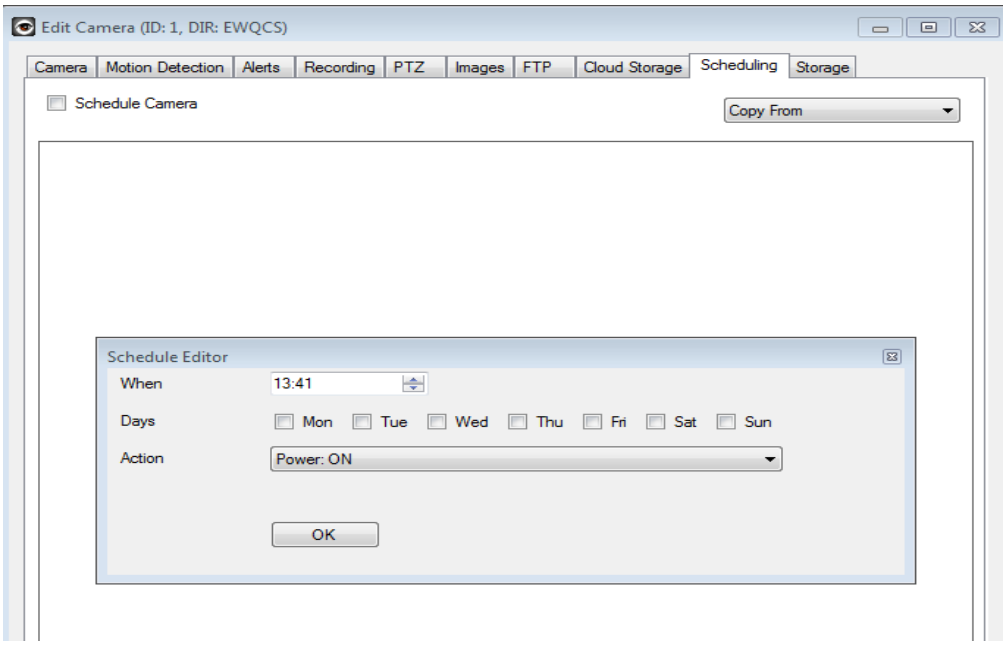
7.- En los parámetros de edición seleccionar el puerto, la IP, y si se desea invertir la imagen de las cámaras.



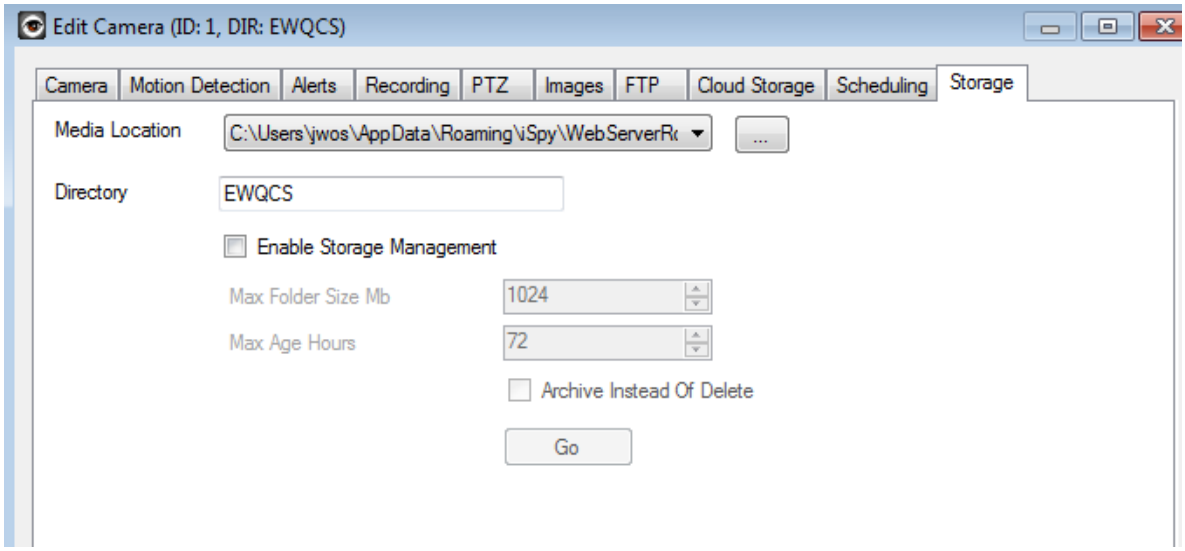
8.- En los parámetros de grabación seleccionar la norma de compresión del formato de video para almacenar información y los tiempos que se necesite que dure la misma. Adicional seleccionar la opción de grabación por detención de movimiento.



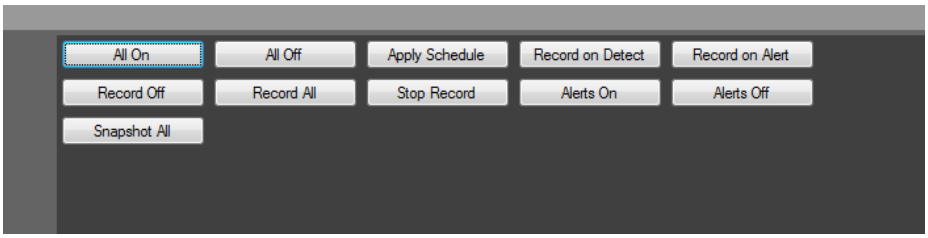
9.- En la sección de horario seleccionar la hora, día y la acción que se necesita realizar en cada cámara, entre estas acciones están: iniciar grabación, detener grabación, envío de alertas, etc.



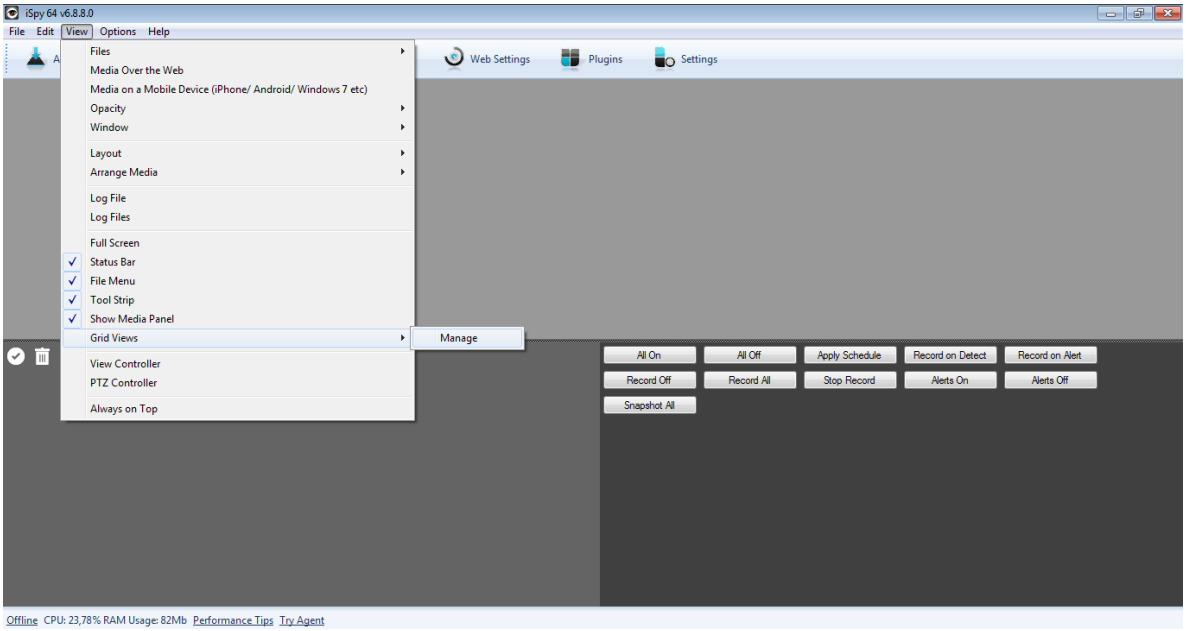
10.- En la sección de almacenamiento, configurar la ruta donde se guardarán las grabaciones realizadas y el nombre del directorio. También es posible determinar el tamaño máximo del contenedor, así como el máximo de horas de grabación.

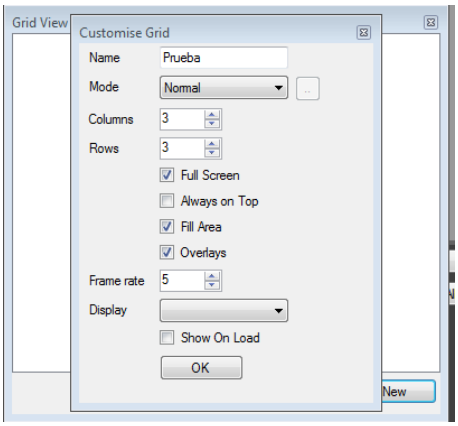


11.- En la vista principal de la aplicación se observa un panel de comandos rápidos que permite, encender las cámaras, apagarlas, iniciar grabaciones enviar alertas de todos los equipos a la vez.



12.- En la sección de vista es posible crear vistas de cuadrillas para todas las cámaras. Es necesario colocar en la configuración de la grilla los números de filas y columnas para generar la vista.





13.- Finalmente seleccionar cada cámara para ir colocando en cada una de la grillas y de esta forma permanezcan en esta vista de manera fija las imágenes emitidas por las cámaras.