ESCUELA POLITÉCNICA NACIONAL

ESCUELA DE FORMACIÓN DE TECNÓLOGOS

IMPLEMENTACIÓN DE UN SISTEMA DE SEGURIDAD MEDIANTE CÁMARAS IP Y BIOMETRÍA PARA LA SALA MARCELO DÁVILA DE LA ESFOT

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

LUIS RODRIGO GUALOTUÑA TIGRE

SANTIAGO MIGUEL AUSHAY CHÁVEZ

DIRECTORA: Ing. MÓNICA VINUEZA RHOR MSc.

Quito, Septiembre 2017

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por Luis Rodrigo Gualotuña Tigre y Santiago Miguel Aushay Chávez, bajo mi supervisión.

Ing. Mónica Vinueza Rhor MSc.

DIRECTORA DE PROYECTO

DECLARACIÓN

Nosotros, Luis Rodrigo Gualotuña Tigre y Santiago Miguel Aushay Chávez, declaramos bajo juramento que el trabajo aquí descrito es de nuestra autoría; que no ha sido previamente presentado para ningún grado o calificación profesional; y, que hemos consultado las referencias bibliográficas que se incluyen en el presente documento.

A través de la presente declaración cedemos nuestros derechos de propiedad intelectual correspondientes a este trabajo, a la Escuela Politécnica Nacional, según lo establecido por la ley de Propiedad Intelectual, por su reglamento y por la normatividad institucional vigente.

Luis Rodrigo Gualotuña Tigre Santiago Miguel Aushay Chávez

DEDICATORIA

A mis padres que con gran esfuerzo y sacrificio me dieron la herencia más valiosa que es la educación, especialmente a mi madre Rosa Clementina Tigre, quién ha sido el pilar fundamental y apoyo moral constante en el desarrollo de todas mis actividades, les debo y les dedico cada uno de mis éxitos en mi vida profesional.

Luis Rodrigo Gualotuña

A mis padres Miguel Aushay y Zulema Chávez quienes fueron el motivo principal de mi formación profesional, me han permitido cumplir mis sueños y metas, les debo todo y son todo en mi vida esto es por ustedes.

Santiago Miguel Aushay

AGRADECIMIENTOS

A mis maestros por compartirme sus conocimientos y por ayudarme a fortalecer mi ética y mis valores que me ayudarán a desempeñarme correctamente en el ámbito profesional. A nuestra prestigiosa Escuela de Formación de Tecnólogos de la Escuela Politécnica Nacional de la cual me siento orgulloso y agradecido de haber pertenecido.

Luis Rodrigo Gualotuña

A mis padres por el apoyo incondicional y el esfuerzo que realizan día a día lo cual me permitió cumplir una meta más en mi vida, a mis hermanos que siempre están a mi lado con sus consejos, motivándome a ser una mejor persona. A la universidad por haberme permitido realizar mi formación profesional en ella y a mi tutor MSc. Mónica Vinueza, sus conocimientos, su manera de trabajar y sus orientaciones han sido fundamentales para mi formación académica y profesional.

Santiago Miguel Aushay

CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

Este proyecto consiste en la implementación de un sistema de seguridad en la sala Marcelo Dávila de la ESFOT, que integre video vigilancia digital a través de cámaras IP y control de asistencia por biometría. El sistema de video vigilancia digital tiene salida a internet, lo cual brinda una gran ventaja ya que su monitoreo no solamente es local sino también remoto y permite el acceso desde cualquier lugar mediante un navegador web o aplicación. Adicionalmente la información digital se puede comprimir, almacenar y transmitir a través de una red convergente con bajos costos de implementación.

El sistema biométrico de autenticación por patrón facial permite tener un registro de asistencia de los administradores de la sala Marcelo Dávila. El dispositivo se controla por software el cual arroja un reporte por plantilla de asistencia.

El almacenamiento de la información se realiza en el servidor principal de la sala Marcelo Dávila y la comunicación se realiza a través de una red cableada aplicando los estándares de cableado estructurado.

Palabras clave; video vigilancia, cámaras IP, biometría.

ABSTRACT

This project involves the implementation of a security system in the ESFOT's Marcelo Dávila room, which integrates digital video surveillance through IP cameras and biometric assistance control. The digital video surveillance system has internet access, which offers a great advantage since its monitoring is not only local but also remote and allows access from anywhere using a web browser or application. In addition, digital information can be compressed, stored and transmitted through a converged network with low implementation costs.

The biometric facial pattern authentication system allows for an attendance record of the administrators of the room Marcelo Dávila. The device is controlled by software which gives a report per attendance template.

The storage of the information is done in the main server of the room Marcelo Dávila and the communication is made through a wired network applying the standards of structured wiring.

Keywords; Video surveillance, IP cameras, biometric

1 INTRODUCCIÓN

Los primeros sistemas de video vigilancia que existieron fueron los CCTV[1] los cuales son sistemas analógicos cuya infraestructura es instalada básicamente con cable coaxial resultando tener costos de implementación muy altos; las capacidades de almacenamiento de los discos duros tienen que ser alta debido a que almacenan información analógica y se utilizan para monitoreo local de instituciones, organizaciones, etc. “La video vigilancia IP se utiliza para garantizar la seguridad de las personas y lugares, como para supervisar propiedades en instalaciones de modo remoto o retransmitir eventos en la web con imágenes y sonidos reales” [1].

La sala Marcelo Dávila de la ESFOT posee un sistema de seguridad básico que consta de sensores de proximidad para detección de movimiento distribuidos en un área dentro de la cual se presentan puntos ciegos. “Un sensor es capaz de detectar diferentes tipos de materiales, con el objetivo de mandar una señal y permitir que continúe un proceso, o bien detectar un robo dependiendo del caso que sea” [2].

Para solucionar las necesidades de la sala Marcelo Dávila se realizó un análisis con el fin de poder determinar los requerimientos del sistema de seguridad que integre video vigilancia y control de asistencia biométrico, con esta información se realizó el diseño considerando las características de las cámaras IP y del biométrico. En la implementación se tiene muy en cuenta las normas y estándares recomendados para el cableado estructurado, posteriormente se realizaron las respectivas pruebas para corroborar el correcto funcionamiento del sistema de seguridad.

[1] CCTV Circuito cerrado de TV

2 METODOLOGÍA

Este trabajo consiste en un tipo de investigación aplicada, para su desarrollo se ha dividido en varias etapas de análisis, diseño, implementación, resultados y discusión.

Para la etapa de análisis:

- Se realizó observaciones y mediciones en visitas al sitio para evaluar donde es necesario efectuar mejoras en el sistema de seguridad de la sala Marcelo Dávila. En base a investigaciones y recomendaciones de manuales de sistemas de seguridad orientados a la video vigilancia en interiores y sistemas de control de asistencia de personas.

Para la etapa de diseño:

- Mediante la recolección de datos en esta etapa se desarrollaron los respectivos planos y el dimensionamiento real de la sala Marcelo Dávila, se ubicaron los equipos en puntos estratégicos con el fin de tener cobertura total por parte de las cámaras IP y un punto idóneo para el Biométrico.

Para la etapa de implementación:

- Se revisó y sintetizó la información necesaria de los manuales técnicos correspondientes, normas y recomendaciones de cableado estructurado fundamentales para la conexión y distribución del cable UTP.

Para la etapa de resultados y discusión:

- En esta etapa se experimentó con los equipos físicamente, instalados mediante ajustes y configuraciones necesarios para lograr que el sistema de seguridad tenga un óptimo y correcto funcionamiento.

Situación actual de la sala Marcelo Dávila:

La sala de internet Marcelo Dávila actualmente cuenta con computadores con conexión a internet utilizados como herramienta de laboratorio con fines académicos para los estudiantes de la institución en general, se utiliza también para reuniones entre docentes y para dictar capacitaciones.

No cuenta con un sistema de vigilancia que permita garantizar la integridad y seguridad de los equipos allí existentes, por lo cual se plantea implementar un sistema de seguridad que permita solventar estas necesidades.

2.1 Fundamentos teóricos

Normas de cableado estructurado

En la comunicación de datos, los estándares de redes son creados para asegurar que las tecnologías de redes individuales sean compatibles. Los estándares especifican las características de varios elementos de la red como el cable, los conectores y los métodos de acceso del nodo. El sistema de cableado estructurado dentro de un campus o edificio está definido para que tenga un tiempo de duración de 10 a 15 años dentro de su diseño para el servicio de comunicaciones ya sea por red cableada o inalámbrica, por lo tanto, los organismos de estandarización describen recomendaciones y normas que se deben cumplir para alcanzar el objetivo de duración y operación de la red. Hay que tener en cuenta, protección contra corrosiones, intemperies húmedas, emisiones, ruidos, compatibilidad electromagnética, etc.

Norma TIA / EIA T568A - T568B

Esta norma define los estándares A y B para el cableado estructurado y determina que colores corresponden a los pines del conector RJ-45.

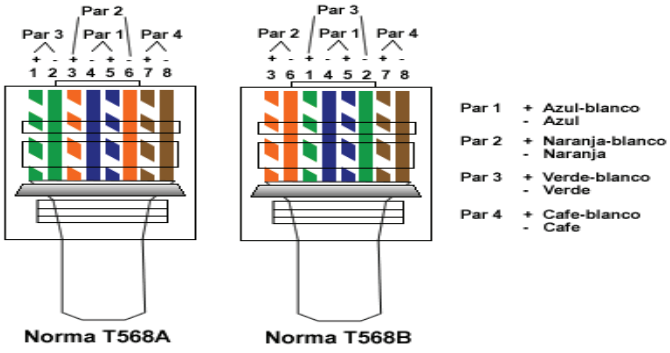


Figura 1 Norma T568-A / T568-B **[3]**

Cámaras IP

Una cámara IP es un dispositivo de red que tiene su propia dirección IP, se interconecta a la red por cable o inalámbricamente, digitaliza, procesa y codifica imágenes análogas para luego enviar esta información a otros equipos o computadores. Típicamente se puede acceder y controlar las cámaras IP por medio de un web browser: localmente o remotamente desde cualquier computador o aplicación web. Las cámaras IP son independientes de un computador, para su funcionamiento no requieren conexión directa o dedicada a un computador y pueden ser colocadas en cualquier lugar dentro de la red existente. Consisten básicamente de un lente, sensor de imagen, procesador de imagen, un SoC (sistema en chip) de compresión de video y un adaptador ethernet para la conectividad de red y transmisión de datos.

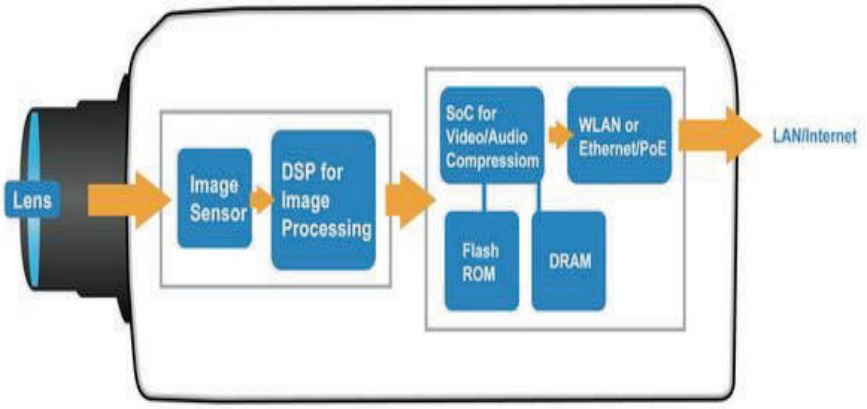


Figura 2 Componentes de una cámara IP **[4]**

Compresión

Para transmitir la información digital, los archivos audio y video componen gran cantidad de información por lo que se requiere utilizar herramientas de compresión para reducir esta cantidad de datos. Se utiliza la combinación de la compresión espacial de imágenes y la compensación de movimiento temporal. En las cámaras IP el proceso de compresión es realizado por el SoC (*System on Chip*), el mismo que está construido con un CPU RISC.

Compresión de video

La compresión de video (imágenes en movimiento) puede realizarse con un margen de pérdida o sin pérdida de información. Si no hay pérdida la imagen permanece idéntica, es decir que los pixeles no fueron alterados después de haber realizado la compresión, la reducción de información en este caso es limitada por ejemplo el formato GIF, así este formato resultaría inadecuado para utilizarlo en la transmisión de información desde un sistema de video vigilancia IP ya que se debe transmitir grandes cantidades de imágenes por segundo. Por lo tanto, se han desarrollado varios estándares de compresión con pérdida de información, con el objetivo de aumentar la relación de compresión a medida que el ojo humano no pueda percibir esta variación.

Compresión de imágenes con pérdidas

Cuando se utiliza el estándar de compresión con pérdidas. Al procesar la reconstrucción de la imagen comprimida, esta difiere y presenta menor calidad en comparación con la imagen original, se emplea cuando la información es redundante en una imagen, la cual puede ser reducida. La reducción se realiza mediante técnicas de codificación que se basan en la fuente de la imagen.

Estándares de compresión de video

- **M-JPEG:** *Motion* JPEG estándar utilizado comúnmente en sistemas de vídeo IP.
- **H.263:** Transmite tasas de bits fijas en video.
- **MPEG:** Compara dos fotogramas de referencia y envía las partes de las siguientes imágenes, se basa en la imagen de referencia y las diferencias de imágenes**.**
- **MPEG-1:** Diseñado para una tasa de bits de destino de aproximadamente 1,5 Mbps con resolución CIF (Common Intermediate Format).
- **MPEG-2:** se utiliza en vídeo digital de alta calidad, TV digital de alta definición (HDTV).
- **MPEG-4:** Es la actualización de MPEG-2 reduce la tasa de bits y lograr cierta calidad de imagen.
- **H.264 - MPEG-4 (Parte 10):** Compresión de datos elevada ofrece calidad de video óptima a tasas de bits reducidas en comparación con los estándares anteriormente mencionados.

En la figura 3 se puede observar la relación entre los distintos formatos de compresión en donde H.264 ocupa menor ancho de banda y puede reducir hasta 20 veces la capacidad ocupada por MJPEG.

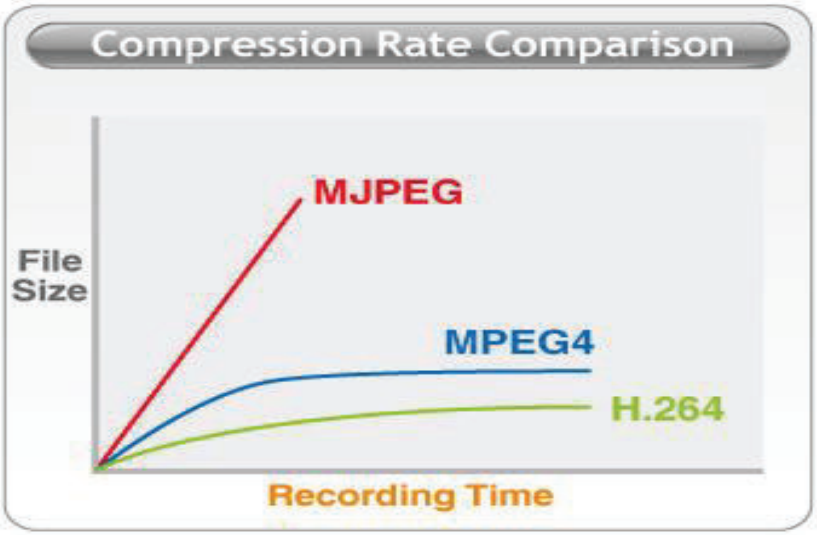


Figura 3 Formatos de compresión de video **[5]**

Tipos de cámaras IP

Las cámaras IP están diseñadas para exteriores e interiores y se clasifican como:

- CÁMARAS IP FIJAS (tipo cubo); Estas cámaras trabajan con sensor CMOS, donde el campo de visualización es fijo.

Figura 4 Cámara IP fija (tipo cubo) **[6]**

- CÁMARAS IP FIJAS (tipo caja): Utilizada para monitorear áreas específicas, tiene un lente fijo que apunta en una sola dirección, en la carcasa se incluye los LEDs IR (infrarrojos) para poder observar ambientes nocturnos.

Figura 5 Cámara IP fija (tipo caja) **[6]**

- CÁMARAS IP FIJAS (tipo domo): Tiene una forma de cúpula invertida, diseñada para instalación en interiores y exteriores, posee un lente no cambiable y no visible al espectador.

Figura 6 Cámara IP fija (tipo domo) **[6]**

- CÁMARAS IP PTZ (paneo, inclinación, zoom) Y PTZ TIPO DOMO: Puede planearse, inclinarse y realizar *zoom in/out* a través de mandos en un navegador web para controlar el ángulo óptimo de visualización de video en vivo. Todos los comandos PTZ son enviados a través de la red IP, a diferencia de las tradicionales cámaras análogas PTZ que requieren cables RS-485 adicionales y un teclado de control.
    - Paneo: Expande el área de visualización a un rango más amplio en ángulo horizontal.
    - Inclinación: Expande el área de visualización a un rango más amplio en ángulo vertical.
    - Zoom digital: Aumenta una imagen al magnificar los pixeles en una posición seleccionada.
    - Zoom óptico: Un lente especifico de motor puede identificar imágenes detalladas más claramente que el zoom digital.

Figura 7 Cámaras IP PTZ **[6]**

Características de las cámaras

- Sensor de imagen tipo (CMOS o CCD): CCD se utiliza en cámaras análogas, mientras que CMOS se utiliza en cámaras IP.
- HD (*High Definition*): Resolución en Mega pixeles, velocidad de cuadros por segundo (fps).
- Ultra HD (*High Definition*): Tecnología 4K mayores detalles en más gamas de colores.
- Líneas de resolución (TVL): Resolución de imágenes para cámaras análogas, la calidad de imagen depende de las líneas de TV.
- Luminosidad de la cámara: Es la cantidad mínima de luz que se requiere para producir una imagen legible.
- BLC (*Back light compensation*): Compensa la contraluz cuando existe mayor intensidad de luz detrás de un objeto.
- Lente Vari focal: Ajusta manualmente el ángulo de cobertura y profundidad focal.
- Lente auto iris: Controla la cantidad de luz automáticamente para dar una mejor imagen.
- Cámaras infrarrojas: Visión nocturna, se puede observar en ambientes con bajo niveles de iluminación, utiliza tecnología de iluminación con Leds, la cantidad de Leds en una cámara infrarroja determina hasta que distancia la cámara puede enfocar.

Equipos biométricos

Un equipo biométrico realiza la función de medir los rasgos físicos de una persona (biometría estática) o medir los rasgos de diferentes comportamientos de una persona (biometría dinámica) y con esta referencia poder autenticar. La palabra biometría proviene del griego bios de vida y metrón de medida. “El término biometría clásicamente se aplica de forma general a la ciencia que se dedica al estudio estadístico de las características cuantitativas de los seres vivos: peso, longitud, etc.” [7].

Mediante las técnicas biométricas se puede medir las características físicas o de comportamiento de las personas para poder establecer o conocer su identidad. En la figura 8 se puede observar las características físicas y dinámicas de un sistema de identificación biométrico.

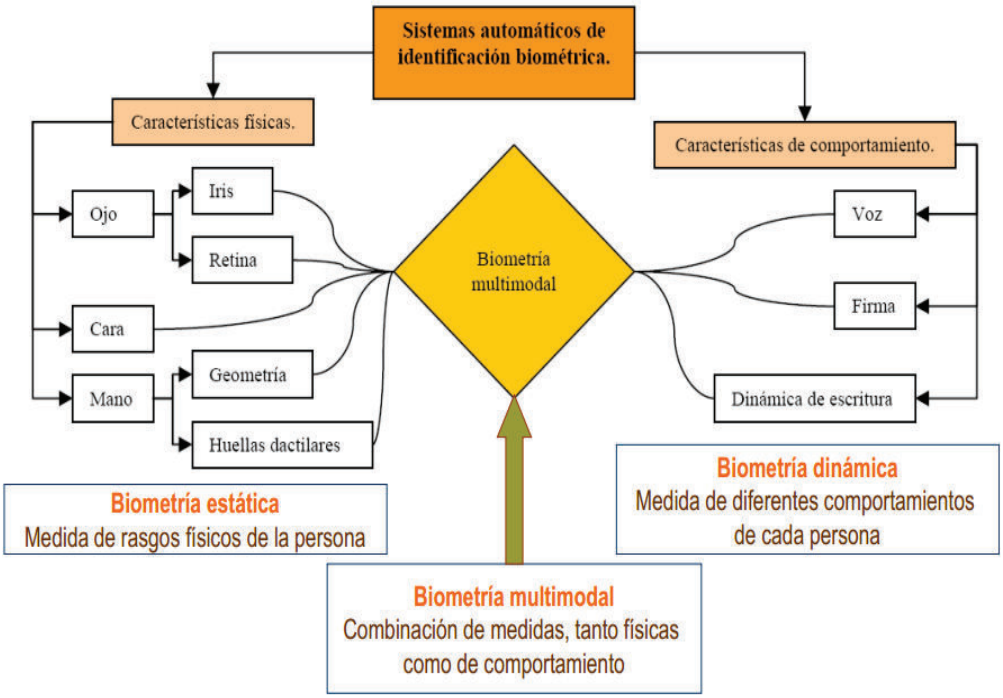


Figura 8 Sistema de identificación biométrico **[8]**

Técnicas biométricas

ESTÁTICAS:

- Características de ojo, iris y retina.
- Huella Dactilar.
- Geometría de la mano.
- Reconocimiento facial.
- Líneas de la mano.

DINÁMICAS:

- Composición química del olor corporal.
- Escritura manuscrita.
- Voz.
- Tecleo.
- Gesto y movimiento corporal.

Rasgos comunes en las técnicas biométricas

Un sistema se define como biométrico si cumple con los requisitos y parámetros de identificación y clasificación, una característica biométrica debe cumplir ciertas condiciones.

- Permanencia: esta característica no puede variar con el tiempo.
- Cuantificable: debe poder ser medida cualitativamente.
- Universalidad: Debe ser común en todas las personas.
- Unicidad: Características que no se pueden repetir en más de una persona.

Funcionamiento de los sistemas biométricos

La mayoría de los sistemas biométricos funcionan con un modelo general que consiste en el registro, almacenamiento del modelo y verificación o identificación.

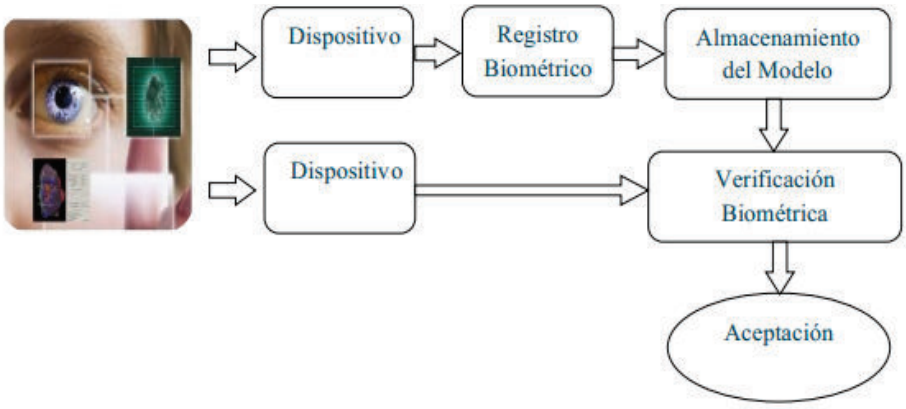


Figura 9 Funcionamiento de un sistema biométrico **[8]**

Primero: Se realiza el registro de la persona en el sistema, después se captura el rasgo característico de la persona y se lo procesa para generar una representación electrónica a la cual se la llama modelo de referencia.

Segundo: El sistema biométrico puede verificar la identidad de una persona o identificar a una persona de acuerdo a lo siguiente:

- **Verificación:** A través de una tarjeta de identificación o pin se le informa al sistema cuál es la identidad, después el sistema captura el rasgo biométrico de la persona y realiza una correlación con el modelo de referencia existente en su base de datos, si la correlación es positiva se realiza una verificación exitosa caso contrario es fallida.
- **Identificación:** El sistema desconoce la identidad, captura el rasgo o patrón biométrico y compara con un conjunto de modelos de referencia para poder determinar la identidad de la persona.

Direccionamiento en redes TCP/IP

El direccionamiento IP es una de las más importantes herramientas para administrar redes *LANs* y *WANs*. Es un tipo de direccionamiento lógico que provee a los *hosts* en la red una identificación única, estas identificaciones hacen posible enviar mensajes a *hosts* específicos. [9]

El direccionamiento IP usa el sistema de numeración binario con el cual las computadoras están diseñadas para entender, basado en el sistema binario los bits pueden estar en *on/off*, los datos digitales están representados en la misma forma, una señal eléctrica o un pulso de luz puede estar en *on/off.*

Todas las direcciones IPV4 están compuestas de 4 octetos binarios los que significan 32 bits, estos octetos están separados por un punto. Cuando una dirección IP es creada los octetos de la izquierda identifican a la red, mientras que los octetos de la derecha identifican un host, juntos los octetos conforman una dirección IP completa. La identificación de la red (*Network ID*) es fijada dentro de una red específica. Mientras que la identificación de un host (*host ID*) son únicas para cada host, las dos IDs juntas conforman una dirección única.

Reglas específicas se aplican a las *network ID* y al *host ID* para lograr un direccionamiento IP más racionalizado.

Las reglas para *Network ID* son:

- El primer octeto en una dirección IP nunca puede ser 127.
  El número 127 es reservado para utilizar como dirección de *loopback*, por ejemplo, para hacer test en la red 127 es utilizado como primer octeto en una dirección IP, en este caso la computadora está siendo probada comunicándose consigo mismo.
- Los bits de una *Network ID* para un host nunca pueden ser todo unos.
  Las identificaciones de red consistentes únicamente de unos son usadas para *broadcast.*
- Los bits de una *Network ID* para un host nunca pueden ser todo ceros.
  Las identificaciones de red consistentes de solo ceros son usadas para identificar los hosts de una red local.
- Cada red IP debería tener una única *Network ID.*
  Todos los segmentos de red dentro de una red más amplia tienen su propia identificación de red.

Las reglas para *Host ID* son:

- Las identificaciones de *Hosts* nunca pueden ser establecidas todo unos, porque esta dirección es reservada para *broadcast.*
- Las identificaciones de *Host* nunca pueden ser establecidas todo cero porque esta dirección identifica a una red.
- Todas las identificaciones de *Hosts* dentro de una red deberían ser únicas en esa red.

Clases de direcciones IPv4

Las direcciones IP son agrupadas dentro de clases para proveer tantas opciones sean posibles mientras se mantiene un sistema de direccionamiento estándar. El sistema de clases se conoce como (*classful sytem*).

Si solo el primer octeto o más de un octeto se utilizan para la identificación de la red depende de si la dirección cae en clase A, clase B, clase C, clase D o clase E. Cada clase cubre un rango específico de direcciones como se muestra en la tabla 1 y tabla 2.

Tabla 1 Rango de clases de direcciones IPv4

CLASE	DESDE	HASTA	MÁSCARA
A	0.0.0.0	127.255.255.255	255.0.0.0
B	128.0.0.0	191.255.255.255	255.255.0.0
C	192.0.0.0	223.255.255.255	255.255.255.0
D	224.0.0.0	239.255.255.255	No definido
E	240.0.0.0	255.255.255.255	No definido

- En clase A el primer bit siempre se pone 0. Esto significa que el valor del primer octeto en clase A nunca puede ser más alto que 127, un valor de 128 significa que el valor del bit inicial no está en cero.
- En clase B los dos primeros bits de izquierda a derecha deben ser puestos 10 respectivamente creando un valor decimal de 128, por lo que el valor decimal del primer octeto en clase B es 128 o mayor.
- En clase C los tres primeros bits de izquierda a derecha son puestos 110 por lo que el valor del primer octeto en la dirección debería ser entre 192 y 223.

Tabla 2 Clases de direcciones IPv4

CLASE		Bits del primer octeto	Valor decimal	Número de redes	Número de Hosts
A	Desde	00000000	0	128	16´777214
	Hasta	01111111	127		
B	Desde	10000000	128	16384	65534
	Hasta	10111111	191		
C	Desde	11000000	192	2´097152	254
	Hasta	11011111	223		

Tabla 3 Clases de direcciones IPv4 reservadas

D	Desde Hasta	**1110**0000 **1110**1111	224 239	Clase usada solamente para direcciones *multicast*.
E	Desde Hasta	**1111**0000 **1111**1111	240 255	Clase experimental para uso futuro.

Direcciones IPv4 privadas

Todos los dispositivos que se comunican dentro de una red TCP/IP necesitan tener una dirección IP única conocida como dirección IP privada, el rango de estos bloques de direcciones se muestra en la tabla 4.

Tabla 4 Direcciones privadas IPv4

Desde	Hasta	Bits para Host	Máscara de subred
10.0.0.0	10.255.255.255	24	255.0.0.0
172.16.0.0	172.31.255.255	20	255.240.0.0
192.168.0.0	192.168.255.255	16	255.255.0.0

Si una red no requiere comunicación saliente con una *WAN* como internet, esa dirección IP puede ser única dentro de la organización LAN; sin embargo, si los dispositivos de red tienen que comunicarse globalmente sus direcciones IP tienen que ser únicas globalmente esto significa que dos dispositivos en el mundo no pueden compartir la misma dirección IP.

La comunidad de Internet crece globalmente por lo que se necesita conservar las direcciones IP públicas, los administradores de red deberían tratar de conservar, documentar y reservar las direcciones IP para uso futuro.

Direcciones IPv4 públicas

La gran mayoría de direcciones IPv4 son públicas y sirven para enrutar a nivel global los routers de los ISP (proveedores de servicio de internet) están diseñadas para tener acceso público desde Internet, en el rango de direcciones IPv4 existen otros rangos designados para fines específicos.

Direccionamiento IPv6

Aunque el sistema de direccionamiento IP con clase ha sido un éxito y útil en sus inicios, gradualmente estas direcciones empezaron a agotarse, debido a que el número de usuarios de internet continúa creciendo exponencialmente según pasan los años, para superar este problema de direcciones insuficientes, se crea un nuevo sistema IP versión 6 (IPv6) que resuelve el problema de la falta de direcciones IP disponibles y que provee una mejor estructura jerárquica en comparación con IPv4.

La primera y más notable diferencia entre los dos sistemas es que IPv6 consiste de 128 bits en lugar de 32 bits, debido a que 128 bits en notación binaria pueden llegar a ser tediosas y abrumadoras las direcciones IPv6 se escriben en notación hexadecimal.

En lugar de necesitar 128 bits binarios para notar una dirección IP. En sistema hexadecimal se requiere de 32 Hexadecimales, así este sistema se hace mucho más fácil de entender y de leer. En la figura 10 se muestra su representación.

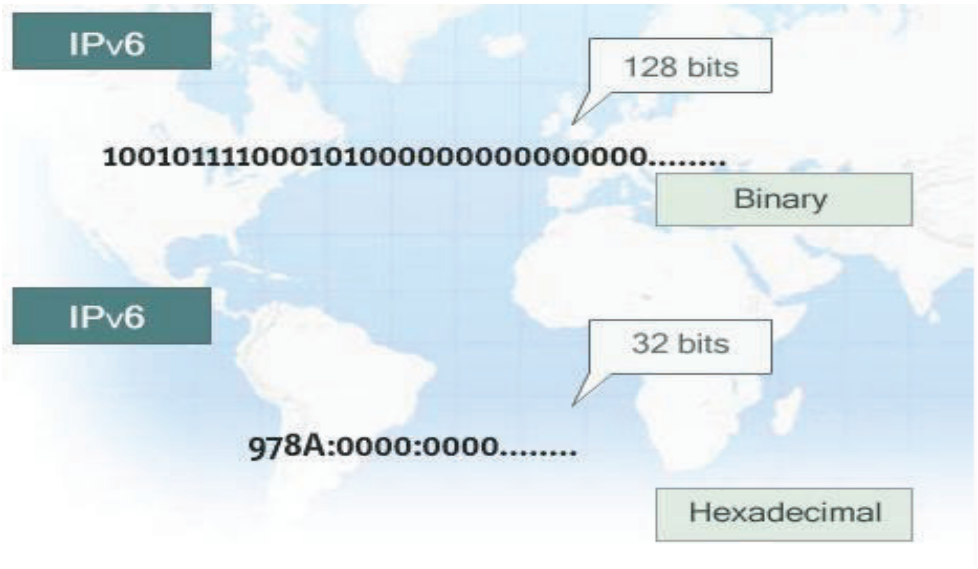


Figura 10 Notación IPv6 **[9]**

Dos convenciones adicionales hacen que el direccionamiento IPv6 sea incluso más pequeño y fácil de leer. Se usan dos puntos (:) en lugar de un punto (.) para separar el grupo de bits que conforman una dirección IP.

- Los ceros iniciales en secuencias de 16 bits pueden ser excluidos.
- Permite que las cadenas de ceros sean representadas por doble dos puntos.

Ancho de banda

El ancho de banda representa la velocidad de un canal de transmisión, es la cantidad de información que puede transmitirse en un segundo por un medio de transmisión. [10]

Fórmula del ancho de banda en video, expresado en bps:

BW = Velocidad x Tamaño de cada imagen en promedio x % de actividad.

• Velocidad de las imágenes: cantidad de cuadros y se expresa en *frames* por segundo (fps).

• Tamaño promedio de cada imagen: se expresa en Bytes.

• Resolución: píxeles por cuadro.

• Algoritmos de Compresión: característica de la cámara.

2.2 Requerimientos del sistema

Cámaras IP

Las cámaras IP existentes en el mercado actual están orientadas a varios tipos de servicios según sea su requerimiento, existen varios tipos y modelos, por lo cual para este proyecto se tomará en cuenta varios aspectos fundamentales y se considerará que son para monitoreo interno, que tengan un ángulo de visión que cubra el área o cobertura de la sala Marcelo Dávila en su totalidad, capacidad de almacenamiento local, capacidad de visualización nocturna, capacidad de monitoreo de forma local y de forma remota a través de Internet. [11]

Se considera ubicar en la sala Marcelo Dávila dos cámaras IP tipo domo en puntos estratégicos que permita cubrir las zonas de mayor interés, posición frontal y/o angular y posición enfocada en el área de ingreso y salida general.

Resolución de imagen

La resolución análoga y digital son parecidas, pero existen algunas diferencias sobre su definición, en video analógico una imagen consta de líneas o líneas de TV, en un sistema digital una imagen está formada por píxeles cuadrados. [12] Las cámaras de red adecuadas que se van a utilizar para la implementación, tienen que captar video en detalle y una óptima calidad de imagen, por lo que una de sus características tendrá que ser resolución en Megapíxeles, es decir, más de un millón de pixeles por imagen para poder visualizar con claridad toda el área de cobertura ya sea en el día o en la noche.

- Resolución mínima requerida 1,3 Megapíxeles (1280 x 960), 1280 pixeles por línea (resolución horizontal), 960 líneas activas (resolución vertical).
- Sensor de imagen CMOS o CCD.

Compresión de video

La compresión reduce la cantidad de información de tal manera que se facilita su almacenamiento y transmisión, esto ocasiona que exista pérdida de información es decir a mayor compresión mayor pérdida de información por lo que la calidad de imagen se deteriora según el nivel de compresión, para la compresión y descompresión se utiliza varios algoritmos que codifican y decodifican toda la secuencia de video. [13]

Es muy importante considerar el tipo de compresión que ofrecen las cámaras, ya que de esto depende la cantidad de información que se puede almacenar, los formatos más comunes en compresión de video digital son MPEG, H.264 (MPEG-4 parte10).

El algoritmo de compresión debe ser H.264 ya que ofrece tasas binaras de transmisión notablemente inferiores a los estándares anteriores MPEG con una elevada calidad de video, es óptimo que las cámaras trabajen con compresión H.264 lo cual aumenta la capacidad de almacenamiento del disco duro que se utilice en el servidor instalado.

Visión nocturna

Las cámaras IP dedicadas al monitoreo local interno deben tener visión nocturna a través de enfoque con luz infrarroja lo cual también es una característica fundamental a considerar como funcionamiento del sistema.

Conexión a la red

Para el correcto funcionamiento todas las cámaras deberían estar dentro del mismo segmento de red con salida a internet configuradas con direcciones IP estáticas, cada dispositivo se conectará por red cableada con cable UTP.

Conexión a Internet

La cámara principal debe tener salida a internet para poder monitorear remotamente la sala Marcelo Dávila desde cualquier lugar en donde se tenga acceso a un dispositivo inteligente o computador conectado a Internet, los cuales permitan utilizar un navegador web o aplicación compatible. “En realidad internet no es una red, sino una enorme colección de distintas redes que utilizan ciertos protocolos y proveen ciertos servicios comunes. Es un sistema inusual en cuanto a que nadie la planeó y nadie la controla”. [14]

Seguridad de las cámaras

Las cámaras IP pueden ser manipuladas o reconfiguradas a través de un navegador web por protocolo HTTP, es decir se tiene acceso a la configuración únicamente conociendo su dirección IP, para la mayoría de equipos de informática en general el usuario y contraseña por defecto es conocido o es fácil de consultar en internet únicamente conociendo el modelo o marca del equipo.

Como medida de seguridad se cambia las contraseñas por defecto y se documenta de manera adecuada, permitiendo tener el control y administración, evitando en muchos de los casos fuga de información o reconfiguración no autorizada de equipos.

Equipo biométrico

Existen varios equipos de autenticación e identificación biométrica específicamente para este proyecto se va a utilizar un dispositivo de autenticación por reconocimiento de patrón facial, el cual registra el acceso mediante rasgos biométricos del rostro, los cuales previamente ya están registrados en la base de datos del dispositivo, “el control de asistencia tiene por objeto registrar el acceso a las instalaciones, centros de trabajo y oficinas de una entidad pública o privada por motivos de seguridad y para protección de bienes y personas”. [15]

Cableado estructurado

Para el cableado estructurado horizontal se requiere la fabricación de distintas longitudes de cables UTP con terminales RJ45, cada uno de los requerimientos y procesos de implementación se realizan siguiendo las normas y estándares T568-A / T568-B.

Ubicación de los equipos

Los equipos deben estar ubicados lejos de fuentes de interferencias electromagnéticas como; transformadores, motores, rayos x, inductores, etc., área seca libre de humedad, geográficamente en puntos estratégicos con su respectiva carcasa de protección.

Cable UTP

Para la implementación se requiere tender el cableado horizontal desde el panel de comunicaciones principal de la sala Marcelo Dávila hasta los dispositivos finales. La categoría de cable considerada será Cat 6, par trenzado de cobre, 100 Ohm, parámetros de transmisión especificada para frecuencias de hasta 250 MHz a una velocidad de trasmisión de 1Gbps, los componentes de conexión están basados en un ancho de banda de hasta 100 MHz. La norma que se utiliza para la terminación de cable UTP es T568B, identifica y corresponde a la asignación de pines en los cables de 8hilos y 100 Ohm.

Topología

El cableado estructurado se implementa siguiendo topología estrella, por lo que cada estación de trabajo o dispositivo final debe ser conectado hacia el panel de comunicaciones directamente, tal como lo menciona la norma; sin puentes, ni derivaciones o empalmes en todo el tendido del cableado. Se debe considerar su mínima proximidad con el cableado eléctrico que genera altos niveles de interferencia electromagnética y cuyas limitaciones se encuentran en el estándar ANSI/EIA/TIA 569. La máxima longitud permitida independientemente del tipo de medio de transmisión utilizado es 100m equivalente a: 90 m (máximo de recorrido de cableado horizontal) + 3 m (*patch cord* hacia el usuario) + 7 m (*patch cord* hacia el panel).

3 RESULTADOS Y DISCUSIÓN

3.1 Esquema del sistema de seguridad

Para la conectividad de las cámaras se utilizó un *switch* al que se conectan mediante cable UTP la cámara 01, cámara 02, el biométrico y el servidor local, este *switch* se conecta al principal el cual tiene salida a internet.

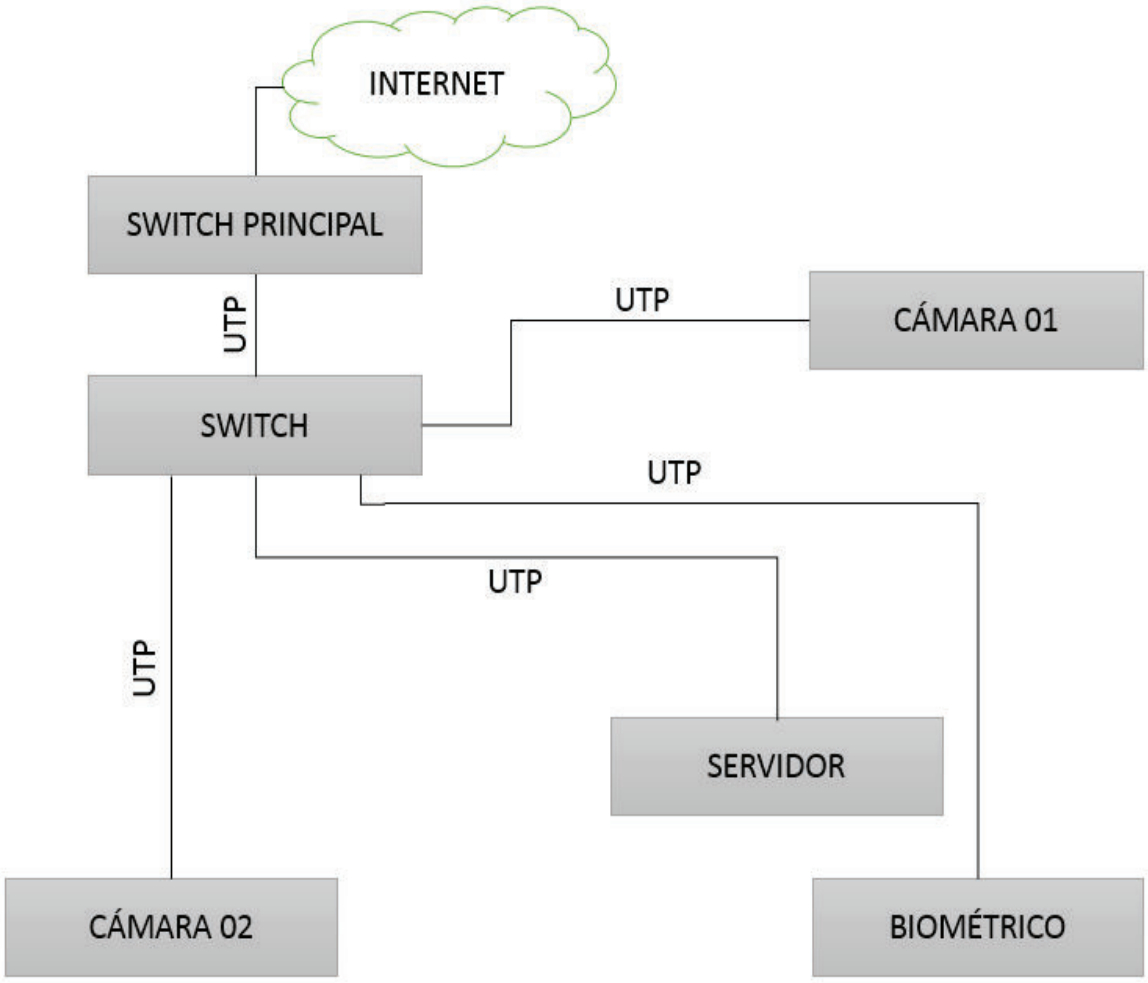


Figura 11 Esquema del sistema

Mediante el uso del programa AutoCAD y las dimensiones reales tomadas de la sala Marcelo Dávila es decir longitud, ancho y altitud se dimensiona el plano real y se obtiene las perspectivas necesarias por simulación. Como se puede ver en la figura 12 se considera los sitios adecuados de las cámaras y se espera que la cobertura de la cámara 01 sea total y se solape con la cobertura de la cámara 02 cuyo objetivo es enfocar la puerta principal de ingreso a la sala Marcelo Dávila.

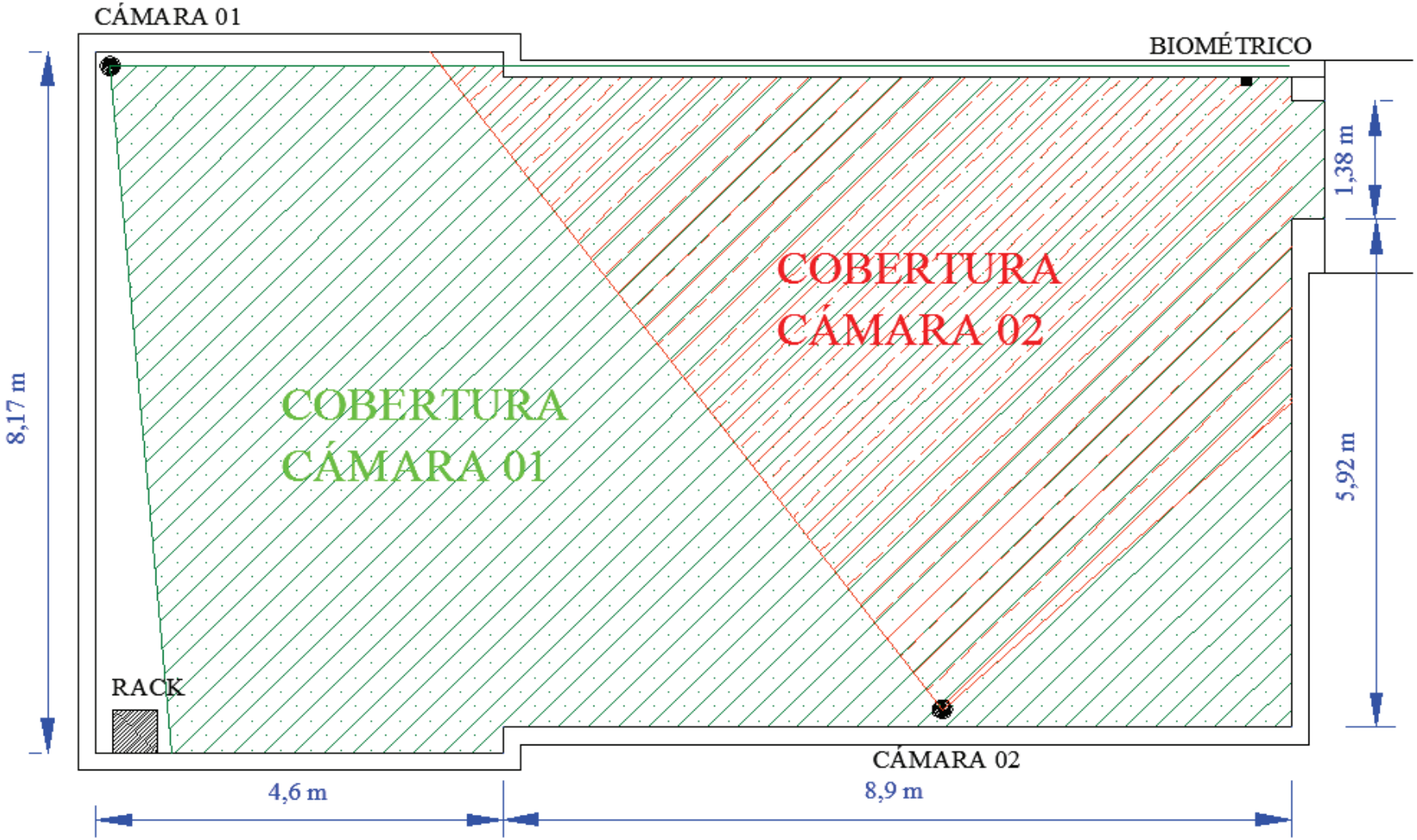


Figura 12 Plano de planta

3.2 Disposición de cámaras IP

La ubicación óptima de las cámaras como se muestra en la figura 13 es una en la esquina derecho y otra lateral izquierda, desde su perspectiva frontal, con el que se logra cubrir en su totalidad la sala de Internet. El dispositivo de autenticación biométrico se ubica en la entrada principal en donde no se tiene reflexión de luz solar. Las cámaras IP, el biométrico y el servidor están conectados mediante red cableada de topología estrella hacia el *switch* ubicado en *rack* principal de comunicaciones de la sala Marcelo Dávila en donde se conectan y tiene salida a Internet.

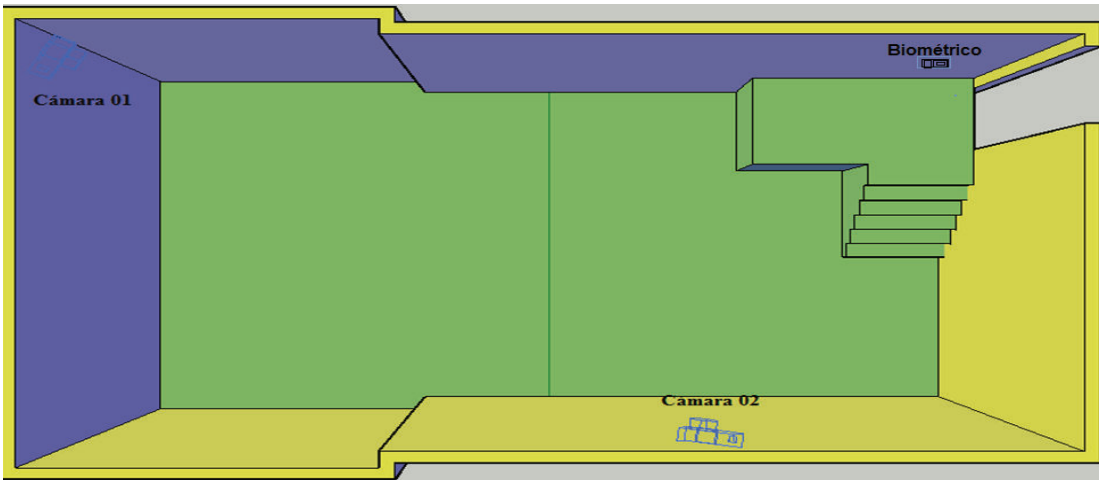


Figura 13 Disposición de cámaras IP

3.3 Simulación de visualización cámara 01

La ubicación de la cámara 01 como se puede identificar en la figura 14 cubre gran parte de la sala Marcelo Dávila.

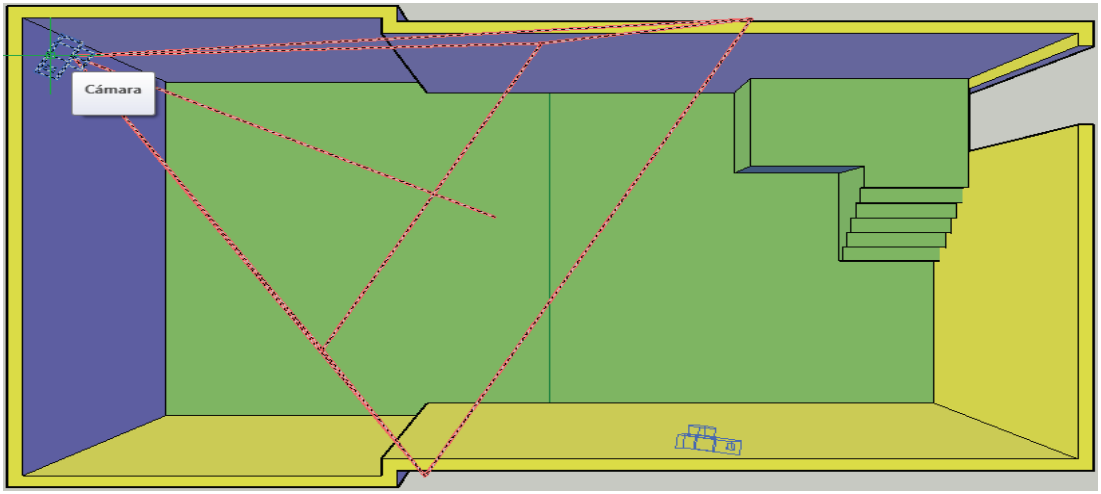


Figura 14 Visualización cámara 01

3.4 Simulación de visualización cámara 02

La ubicación de la cámara 02 como se puede identificar en la figura 15 cubre la entrada principal de la sala Marcelo Dávila.

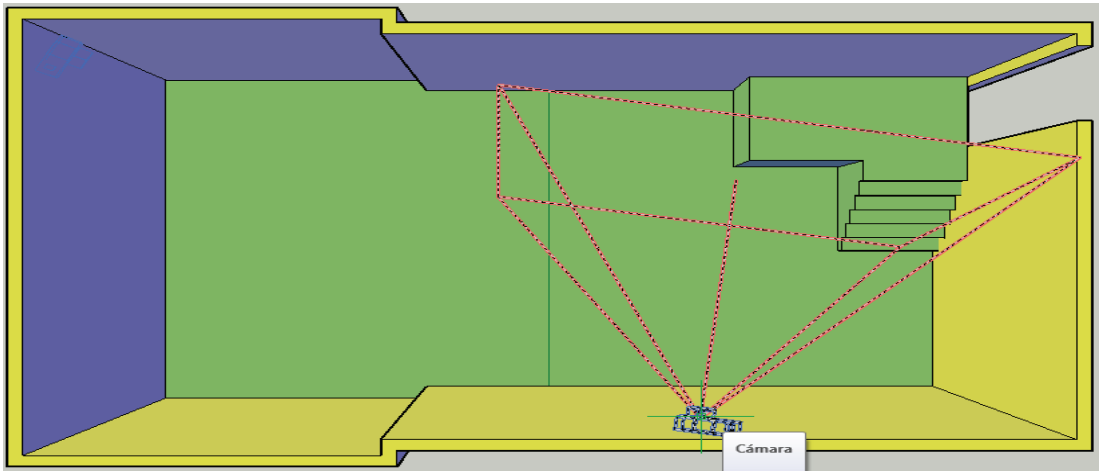


Figura 15 Visualización cámara 02

3.5 Diseño de red

El diseño de la red se realiza en función de las direcciones IP disponibles en la sala Marcelo Dávila, toda la red está dentro de un mismo segmento.

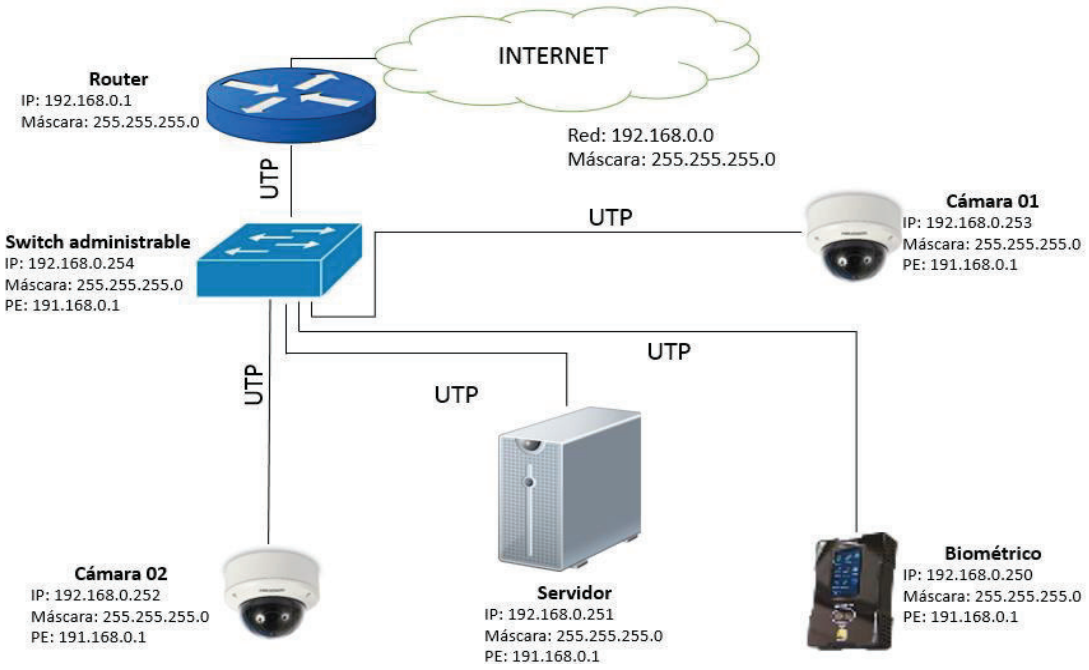


Figura 16 Diseño de la red

3.6 Direccionamiento IP

Para el direccionamiento real se utilizó el segmento de red establecido en la sala Marcelo Dávila el cual consta de una dirección IP de clase B privada. Demostrativamente se utilizará una dirección IP clase C: 192.168.0.1, máscara 255.255.255.0 que se encuentra distribuida para los equipos de la siguiente manera:

RED: 192.168.0.0/24
PUERTA DE ENLACE: 192.168.0.1/24

Tabla 5 Direccionamiento IP de la red del sistema

DISPOSITIVOS	IP ASIGNADA	MÁSCARA	PUERTA DE ENLACE
SWITCH	192.168.0.254	255.255.255.0	192.168.0.1
CÁMARA 01	192.168.0.253	255.255.255.0	192.168.0.1
CÁMARA 02	192.168.0.252	255.255.255.0	192.168.0.1
SERVIDOR	192.168.0.251	255.255.255.0	192.168.0.1
BIOMÉTRICO	192.168.0.250	255.255.255.0	192.168.0.1

3.7 Ancho de banda

Es importante calcular el ancho de banda requerido con el fin de asegurar y contar con la capacidad de red suficiente según los cálculos, asegurando que se tendrá un sistema que trabaje de manera eficiente y no cause frustraciones en un futuro.

El ancho de banda requerido para el sistema de seguridad a implantarse en la sala Marcelo Dávila, se calcula de acuerdo a las especificaciones técnicas de las cámaras que se van utilizar.

Factores a considerar:

- Velocidad de grabación (FPS).
- Resolución, algoritmo de compresión utilizado (tamaño de cuadro de video en promedio).
- Porcentaje de actividad de la escena (indica en cuanto cambia un cuadro respecto al consiguiente).

Se aplica la fórmula y se obtiene el espacio requerido para 1 segundo de video (bps).

$$\boldsymbol{Espacio\ para\ 1\ seg\ de\ video = FPS\ x\ video\ bit\ rate\ x\ \%\ de\ actividad}$$

Datos de las cámaras:

- 60Hz: 20 fps (1280x960)
- Video Bit rate: 32 kbps
- Actividad: 15 %

$$Espacio\ para\ 1\ seg\ de\ video = 20\ x\ 32000\ bps\ x\ 0,15$$

$$AB = 96\ Kbps$$

$$AB\ total = 96\ Kbps\ x\ 2\ cámaras$$

$$AB\ total = 192\ Kbps$$

Este valor corresponde al ancho de banda efectivo del sistema en un segundo, calculado para las dos cámaras IP.

3.8 Almacenamiento de la información

Para el cálculo del almacenamiento se considera de igual manera el ancho de banda total del sistema, en este caso expresado en días; En la práctica se utiliza grabación por detección de movimiento para optimizar la capacidad de almacenamiento.

$$Información\ por\ cámara = 96000\ \frac{bits}{\cancel{seg}}\ x\ \frac{3600\ \cancel{seg}}{1\ \cancel{h}}\ x\ \frac{24\ \cancel{h}}{1\ día} = 8,2944\ Gb/día$$

$$Información\ total = 192000\ \frac{bits}{\cancel{seg}}\ x\ \frac{3600\ \cancel{seg}}{1\ \cancel{h}}\ x\ \frac{24\ \cancel{h}}{1\ día} = 16,5888\ Gb/día$$

Tabla 6 Cálculo de almacenamiento de información

Dispositivo	Cantidad	Ancho de banda	Almacenamiento diario
Cámara 1	1	96 kbps	8,2944 Gb/día
Cámara 2	1	96 kbps	8,2944 Gb/día
TOTAL, DIARIO		192 kbps	16,5888 Gb/día

Este cálculo corresponde al ancho de banda real según las especificaciones técnicas del equipo, es muy importante considerar que las cámaras trabajan con compresión H.264 lo que reduce una cantidad importante de la información.

3.9 Características de los equipos

En esta sección se define todo el hardware y software requerido para el proyecto con el fin de satisfacer las necesidades planteadas en el análisis y cumplir con el objetivo principal del proyecto. Se menciona todos los componentes de hardware y software que se utilizan incluyendo su modelo, características técnicas de los dispositivos y el espacio o área en el que se instalaron.

- **Infraestructura física (hardware)**

En la tabla 7 se enlista los materiales físicos requeridos para la implementación del proyecto:

Tabla 7 Lista de elementos físicos utilizados

Hardware	Cantidad	Características	Función
Cámara IP marca: HIKVISION modelo: DS-2CD2132F-I	2	Cámara IP tipo domo, resolución 3 Megapíxeles, lente de 2,8 mm, visión nocturna Infrarrojo, anti vandálica, estándar IP66, tipo de compresión h.264	Monitoreo local y remoto
FT- QUAD	2	Fuente de alimentación para cámaras 110//12VDC-1Amp.	Fuente de alimentación eléctrica para 12V 1 Amp.
HDD -1TB DVRWD	1	Disco Duro 1 Terabyte, especial DVR WD *Purple*	Almacenamiento
Asistencia y acceso AZface+ID Reconocimiento facial	1	Biométrico reconocimiento facial 800 rostros, RFID, pantalla de color táctil 3", TCP/IP	Dispositivo de control de asistencia
Router DD-WRT 4 puertos	1	*Router* DD-WRT Dir600 4 puertos	Dispositivo de red intermedio, interconexión de dispositivos
Cable UTP	80 m	Cat 6 / UTP azul	Cableado horizontal
Tubo corrugado flexible	20 m	Tubo corrugado flex ¾ plg amarillo	Tubería para tendido de cable UTP por cielo falso
Canaletas	10m	Canaleta adhesiva de 1 plg	Canalización de UTP
Conectores RJ-45 categoría 6	10	Terminal macho de cable de red	Interfaz física del cable de red
Jack hembra RJ-45	4	Terminal hembra de cable de red	Interfaz física del cable de red
Toma de corriente	2		Terminal de alimentación eléctrica (hembra)
Enchufe	2		Terminal de alimentación eléctrica (macho)

- **Infraestructura lógica (software)**

En la tabla 8 se enlista los programas requeridos para la implementación del proyecto:

Tabla 8 Lista de programas utilizados

Software	Cantidad	Características	Función
SADP tools HIKVISION	1	Software de implementación y configuración inicial	Permite el reconocimiento de cámaras en red
IVMS 4200 v 2.4	1	Paquete de software para PC	Interfaz gráfica de monitoreo y configuración de PC
IVMS 4500	1	Paquete de software para dispositivos móviles	Interfaz de monitoreo de dispositivos móviles
IVMS 4200 PCNVR v 1.3	1	Paquete de software para gestión de almacenamiento de información	Almacenamiento de información en el servidor
ZK Time-Net Lite	1	Paquete de software para administración del biométrico	Interfaz gráfica de configuración del biométrico
Windows 7	1	Sistema Operativo de 32 bits	Sistema operativo del servidor.

3.10 Implementación del sistema

En esta sección se señala los procesos de implementación del sistema de video vigilancia y del sistema biométrico incluyendo datos técnicos de los sistemas instalados, software de implementación, infraestructura de equipos y complementos.

3.10.1 Implementación del cableado estructurado

Los materiales requeridos para la implementación del cableado horizontal incluyen: tubería, canaletas, cables, tornillos, tacos *Fisher* y amarras. Que son necesarios para fijar el cableado a la estructura de la manera más adecuada y bordear con tubería la trayectoria del cableado estructurado según las normas de implementación de cableado. La canalización horizontal conecta las 2 cámaras IP, el equipo biométrico y el servidor con el *switch* principal. El material necesario para la canalización es; cable UTP cat 6, tubería para exteriores, sunchos, canaletas, tacos *Fisher*, tonillos tirafondo y seguro de empotrado.

Figura 17 Material para el cableado horizontal

La opción para canalización horizontal según el diseño de la sala Marcelo Dávila permite tender el cableado sobre el cielo falso para las cámaras IP y por las bandejas multicanal ya alojadas para la canalización hacia el dispositivo biométrico y hacia el servidor. Para la canalización sobre el cielo falso acatando la norma de cableado estructurado ANSI/TIA/EIA-569-A, se utiliza tubería de ¾ de pulgada empotrada a la pared a 45 cm del cielo falso, por su interior se tiende el cable UTP hacia la interfaz física de cada una de las cámaras como se muestra en la figura 18.

Figura 18 Tubería sobre cielo falso hacia las cámaras

3.10.2 Instalación de cámaras

Para la conexión de las cámaras IP y de todo el sistema de cableado estructurado, se utiliza el estándar T568-B con el cual se va a conectar los terminales o conectores RJ-45 a su respectiva cámara. Mediante el estándar mencionado, se conecta la interfaz física (conector) incluida en el equipo, con el cable para su respectiva unión a las cámaras tal como muestran las figuras 19 y 20.

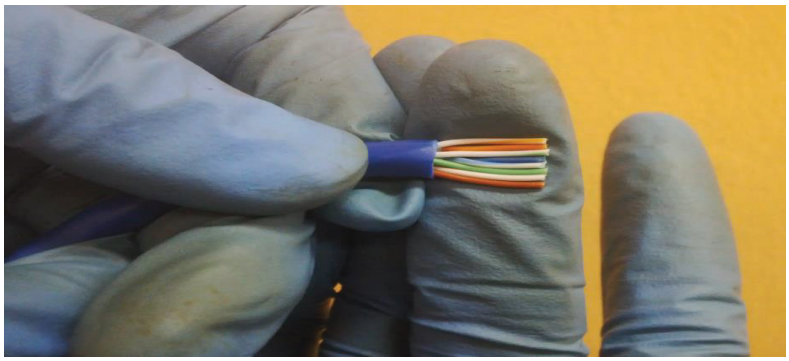


Figura 19 Disposición física de cables según norma T568-B

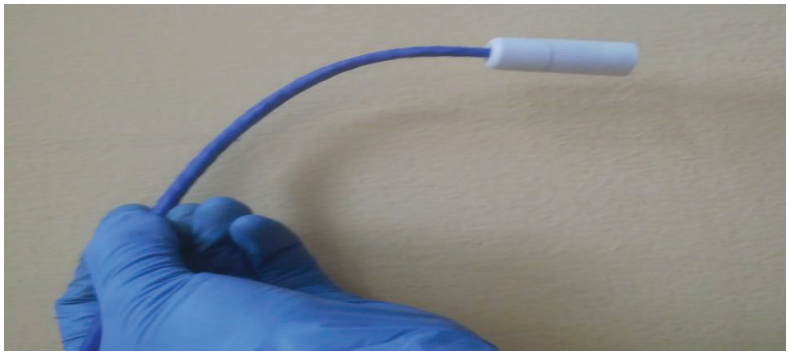


Figura 20 Ponchado con conector para cámaras IP

Una vez realizado el ponchado y colocado el seguro de tensión de cada una de las cámaras se procede a conectarlas. Mediante el software incluido en el equipo se puede asignar una dirección IP para poder configurarlas remotamente desde una estación de trabajo.

Figura 21 Conexión final de las cámaras

Una vez configuradas las cámaras, asignadas una dirección IP, máscara de subred y puerta de enlace se ubica físicamente en el lugar que corresponden.

Figura 22 Ubicación física de la cámara 01

Figura 23 Ubicación física de la cámara 02

3.10.3 Configuración de cámaras

La aplicación SADP[2] es una herramienta que ayuda a reconocer que dirección IP se asignó por DHCP a la cámara. También se puede conectar la cámara punto a punto hacia un computador en el cual se fija en el adaptador de red una dirección IP que este dentro del segmento de 192.168.1.x y máscara 255.255.255.0. Se conecta directamente vía web Browser con la IP: 192.168.1.64 (la marca establece esta dirección IP por defecto) para el caso se utilizará el software SADP.

Se conectan las cámaras a un punto de red existente dentro de la LAN y se encienden. Luego se Instala en el computador el software incluido en el equipo SADP setup.

[2] SADP (Search Active Devices Protocol) Software que permite detectar el dispositivo en red.

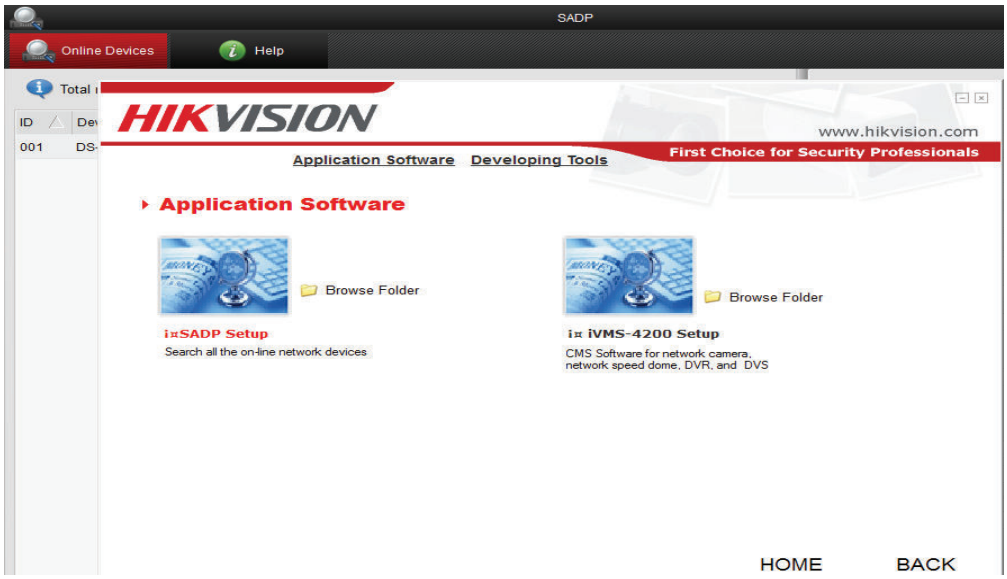


Figura 24 SADP HikVision

Una vez instalado SDAP, se crea un icono en el escritorio y se ejecuta la aplicación que indica cuantos dispositivos HIKVISION están en red, y la dirección IP asignada.

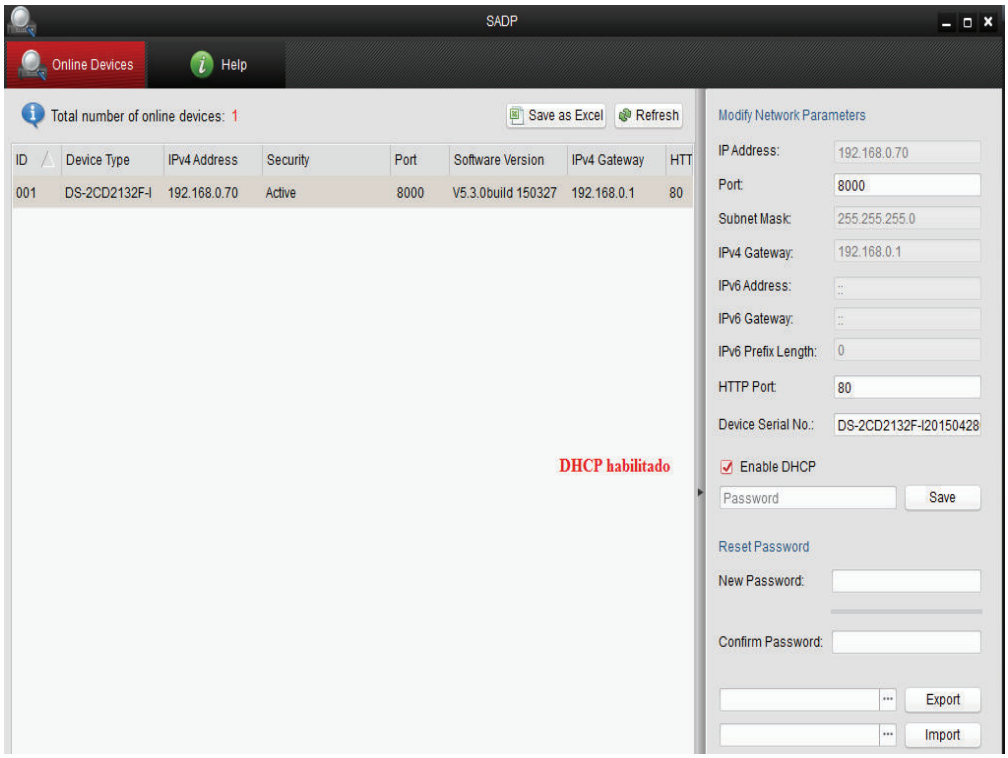


Figura 25 Configuración SADP

Configuración de cámaras vía web browser

Una vez conocidas las direcciones IP de las cámaras (a través de SADP) se puede acceder vía web Browser. En el primer acceso el equipo solicita que se fije un usuario y contraseña de administrador.

- **Nombre de Usuario:** usuario
- **Contraseña:** **********

A través de Internet Explorer (de preferencia) se accede a la interfaz del dispositivo, como medio de seguridad el sistema siempre va a solicitar el nombre de usuario y contraseña establecido anteriormente.

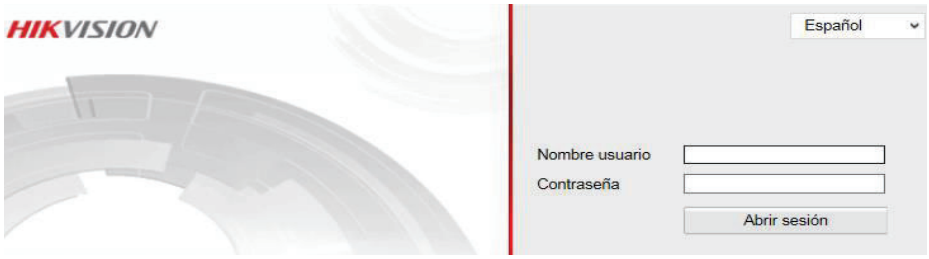


Figura 26 Acceso vía web browser

Configuración de direcciones IP de las cámaras

Después de establecer la conexión con las cámaras, en la pestaña configuración se asigna las direcciones IP correspondiente a las cámaras.

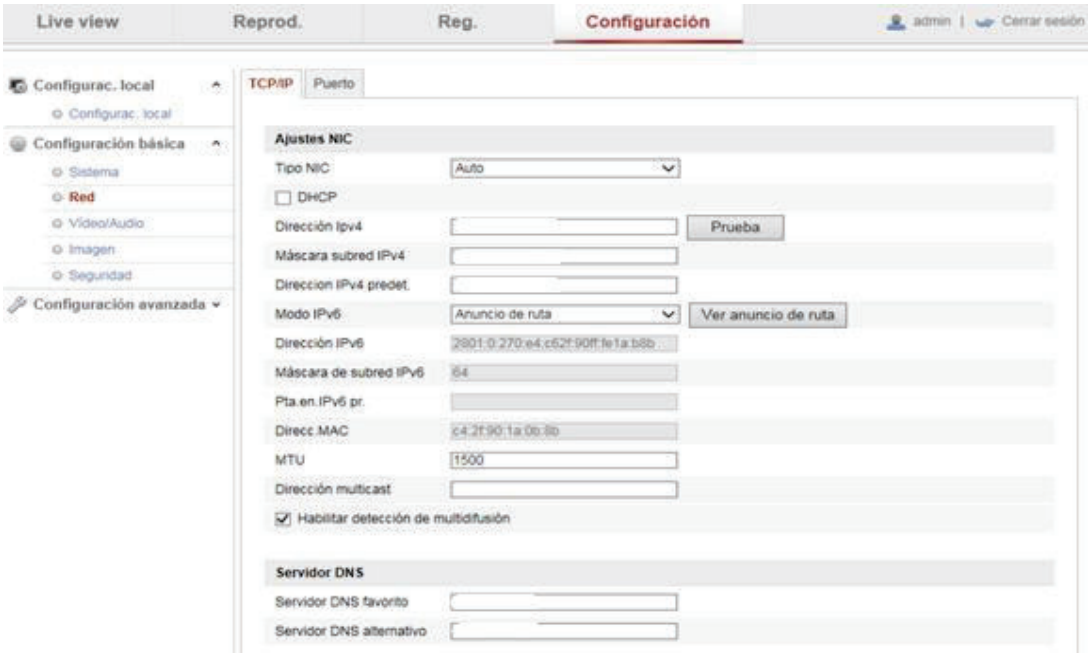


Figura 27 Configuración de IP cámara 01

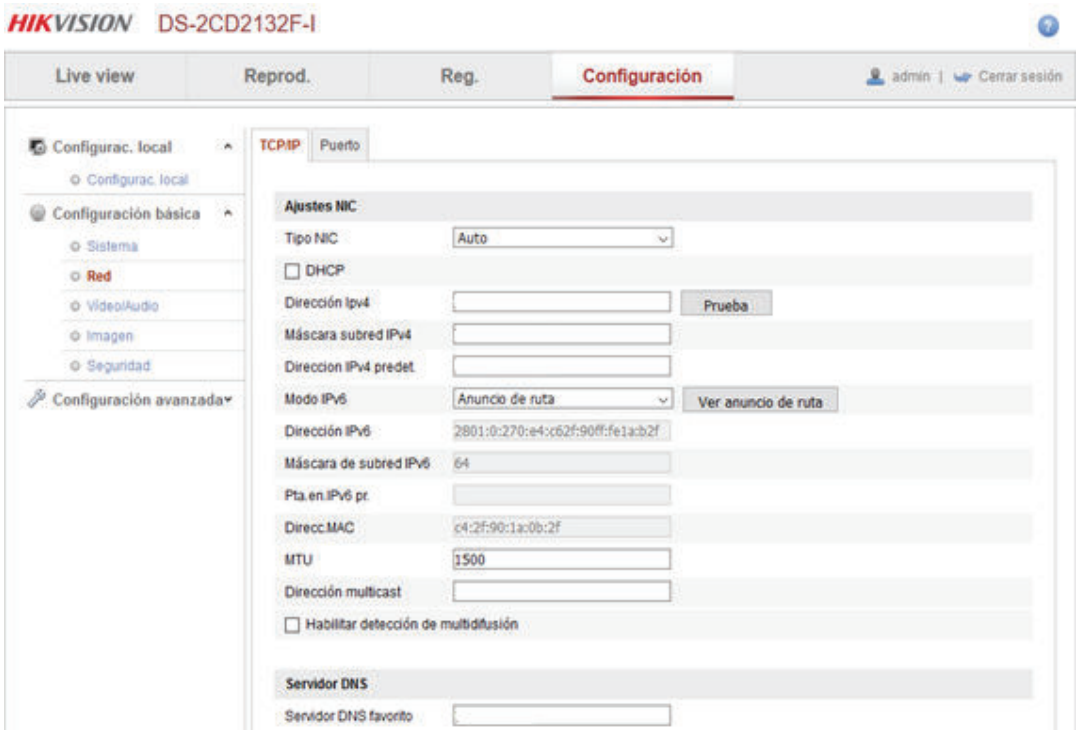


Figura 28 Configuración de IP cámara 02

Luego de la configuración de las direcciones IP y de la autenticación con usuario y contraseña ya se puede tener acceso localmente a las cámaras vía web browser.

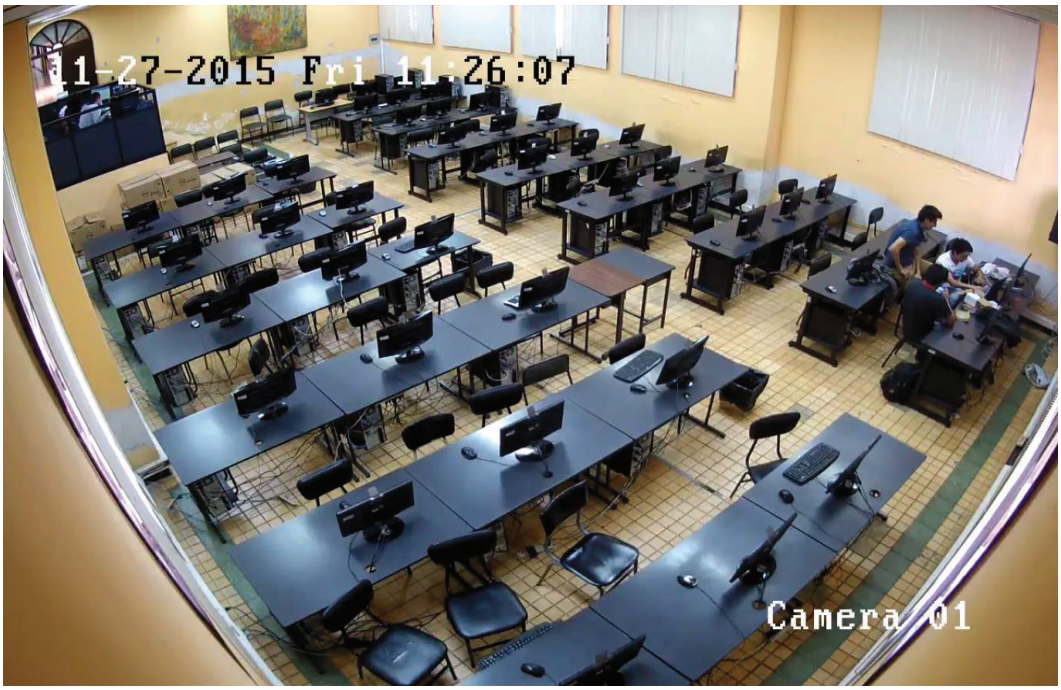


Figura 29 Monitoreo local cámara 01

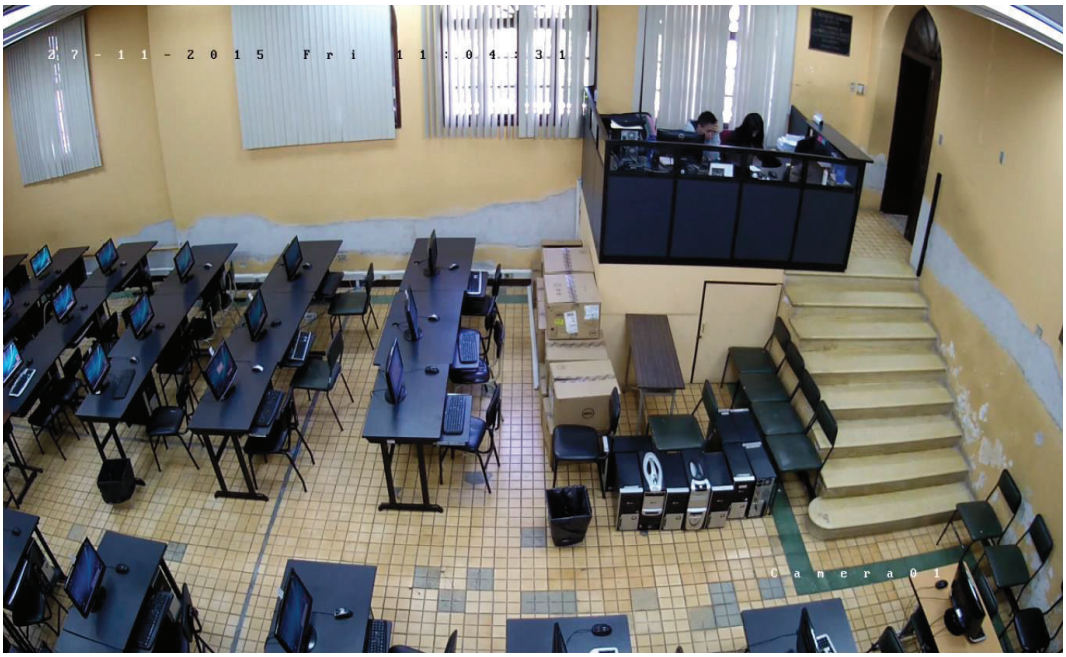


Figura 30 Monitoreo local cámara 02

3.10.4 Instalación del equipo biométrico

Para la instalación del equipo biométrico se empotra las platinas del dispositivo a la pared con tornillo y taco Fisher. La ubicación está situada en el área menos afectada por reflexión de luz solar, para la correcta operación del equipo.

Figura 31 Empotrado de plantilla del biométrico

Para el cableado del equipo biométrico AZ-Face 400 se utiliza cable UTP cat 6 tendido dentro de una canaleta desde el dispositivo ubicado alado de la puerta principal hacia el *switch* ubicado en el rack de comunicaciones, por recomendación del fabricante, el equipo se encuentra ubicado a 1,20m de altura y en la entrada principal de la sala Marcelo Dávila.

3.10.5 Configuración del equipo biométrico

El equipo biométrico se maneja a través del software ZKTIMENET el cual se obtiene de la página web del proveedor del producto: http://www.idconsultants.us/descargas.html. Es el asistente ZKTIMENET con su correspondiente instalador.

Figura 32 Asistente de instalación ZKTIMENET

El software se instala en el equipo Windows 7 de 32 bits de la sala Marcelo Dávila, se selecciona los componentes a instalarse y se ejecuta la instalación.

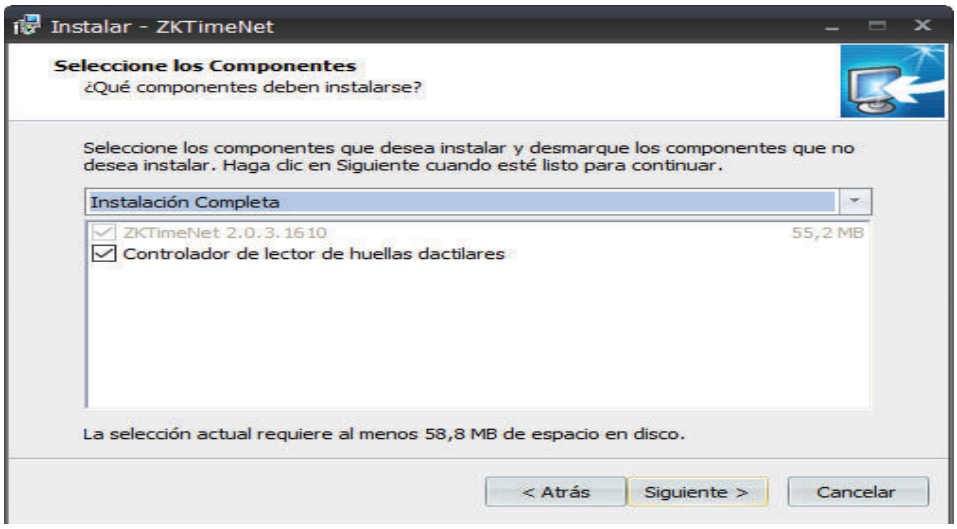


Figura 33 Componentes instalados ZKTIMENET

3.10.6 Configuración de ZKTIMENET

Para la configuración del equipo se ejecuta el programa instalado, al inicio se debe establecer un nombre de usuario y una contraseña.

- USUARIO: usuario
- PASSWORD: *******

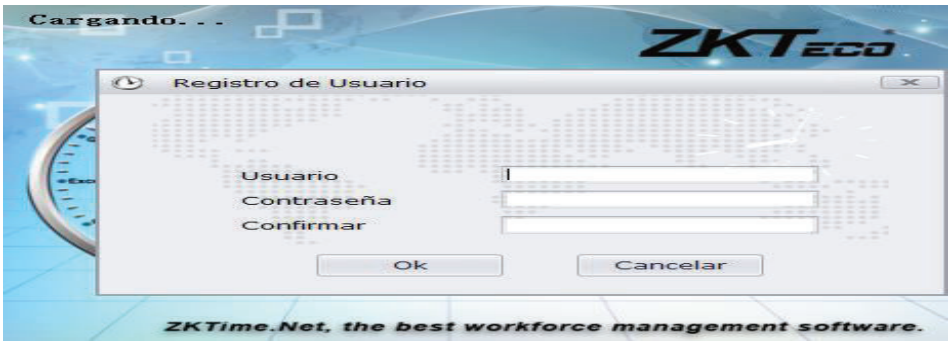


Figura 34 Configuración usuario y contraseña ZKTIMENET

Después de establecer el usuario y contraseña el asistente de configuración permite configurar:

- Dispositivos: Se agrega nombre y dirección IP del dispositivo.
- Empresa: Establece un perfil, nombre para la organización.
- Horarios: Establece los periodos de tiempo registrados por jornada laboral.
- Turnos: Establece los días de trabajo y horarios de la jornada laboral.
- Departamentos: Asignación de varias áreas o departamentos para el registro.
- Empleados: Registro de usuarios de la organización.

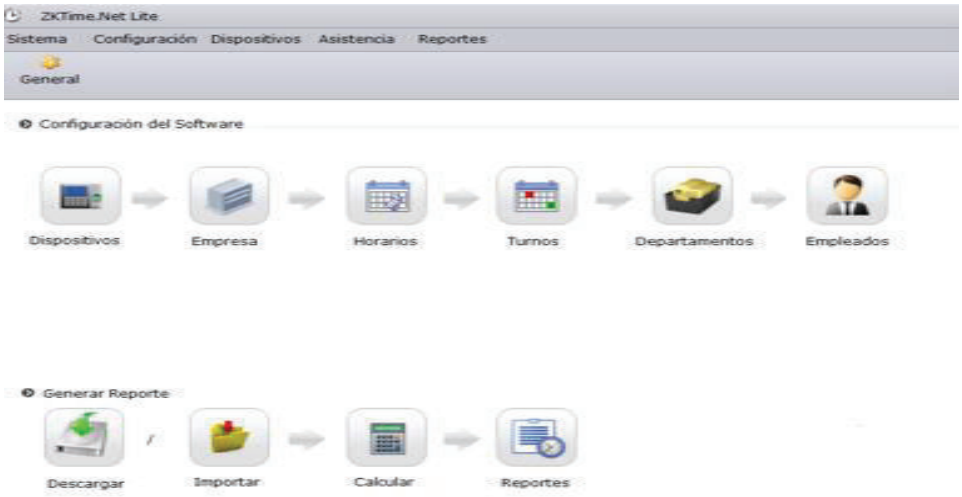


Figura 35 Asistente de configuración ZKTIMENET

Después de realizar la configuración siguiendo el asistente, se sincroniza con el dispositivo biométrico, para cargar toda la información.

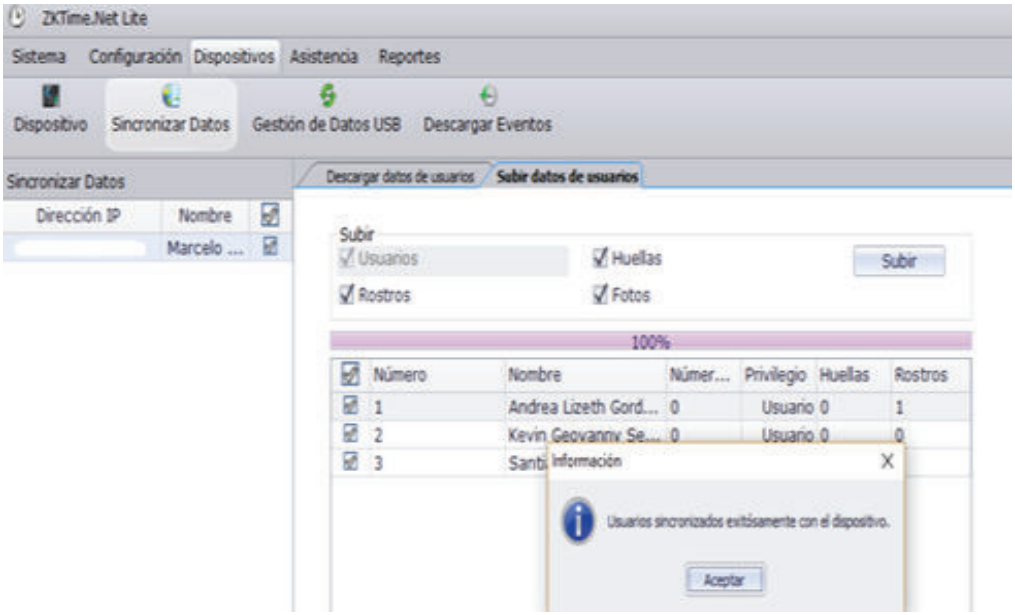


Figura 36 Sincronización con el dispositivo biométrico

3.10.7 Implementación en el router D-LINK

Para la conexión a internet se utiliza un equipo *router* marca D-LINK el cual se conecta directamente al *switch* principal, ubicado en el rack de la sala Marcelo Dávila.

Figura 37 *Router* DD-WRT

3.10.8 Configuración del *router* D-LINK

Se ingresa a la configuración del equipo *router* D-LINK con la dirección IP por defecto 192.168.1.1 desde un navegador web.

Se realiza la configuración de acuerdo al direccionamiento IP utilizado para la red y de igual forma se habilita el puerto del *switch.*

Figura 38 Configuración LAN del *switch*

Se deshabilita el servidor DHCP ya que el equipo solo funciona como un *switch*

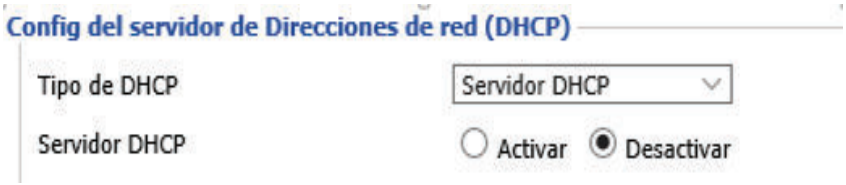


Figura 39 Configuración de IP estática del *switch*

3.10.9 Instalación del disco duro

El sistema requiere almacenar gran cantidad de información diaria correspondiente a la video grabación de las cámaras IP, para este propósito se instaló un disco duro de características adecuadas que soporte la escritura y sobre escritura de información continua con 1,0 TB de capacidad de almacenamiento.

Figura 40 Disco duro 1,0 TB

Para garantizar el correcto funcionamiento de todos los programas que operan en la máquina, se realiza una partición con 10 GB de capacidad destinada al software y 920 GB destinados al almacenamiento de la información.

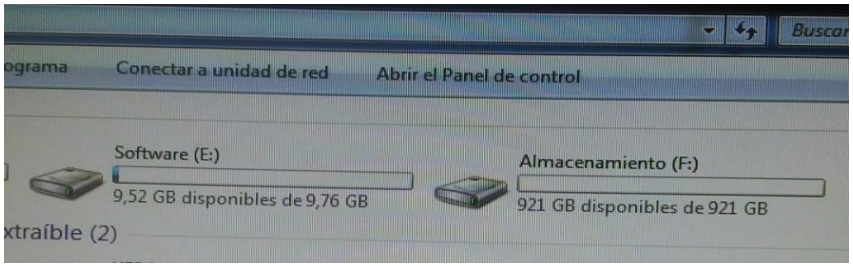


Figura 41 Partición de disco duro

3.10.10 Configuración del sistema de video vigilancia

El sistema de video vigilancia es monitoreado desde una estación de trabajo (servidor) mediante software IVMS [3] completamente unificado que permite visualizar todas las cámaras IP instaladas en la sala Marcelo Dávila, así mismo almacenará la información en este servidor, el software tiene privilegios de administrador y de usuario.

IVMS es un sistema de gestión inteligente de video desarrollado y utilizado para la administración y monitoreo a través de cámaras IP. Contiene varios subsistemas que serán utilizados según el entorno y las aplicaciones dedicadas. En este proyecto se utilizó:

- IVMS-4200 PC-NVR (servidor de almacenamiento virtual)
- IVMS-4500 (aplicación para dispositivos móviles)

3.11 Monitoreo local

Monitoreo local vía web browser

Para el monitoreo local vía web, se puede acceder a cualquiera de las dos cámaras desde un computador conectado a la red LAN local, para lo cual se requiere tipiar en el URL de navegador web (internet Explorer) la dirección IP correspondiente:

- IP Privada cámara 01: 192.168.0.253/ 24
- IP Privada cámara 02: 192.168.0.252/ 24

[3] IVMS (Intelligent Video Management System)

Para el acceso se requiere el usuario y contraseña de administrador

- Usuario: usuario
- Contraseña: *******

Hay que instalar un plugin en el primer acceso, se realiza la acción y se actualiza el navegador web.

Figura 42 Descarga de plugin para acceso local

Después de escribir el usuario y contraseña de administrador en la interfaz principal de acceso ya se tiene conexión vía web desde un computador conectado a la red localmente.

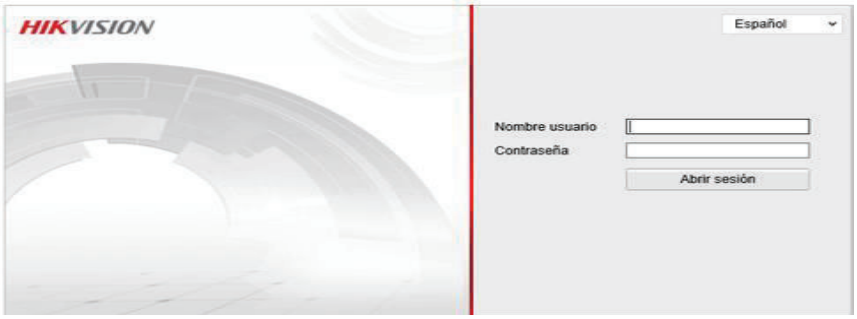


Figura 43 Interfaz de acceso local a las cámaras IP

Monitoreo local vía software IVMS-4200 PCNVR

El software se encuentra en la página de hikvision.com, este software es principalmente el servidor virtual de almacenamiento de la información y monitoreo de video de las cámaras IP.

- Requerimientos mínimos del computador:
  Sistema operativo: Microsoft Windows 7 / Windows 2008 (32/64-bit), Windows 2003 / Windows XP (32-bit) CPU: Intel Pentium IV 3.0 GHz o superior Memoria: 1G o por encima Pantalla: 1024 * 768 o superior.

En la primera ejecución de IVMS-4200 PCNVR, el software solicitará un usuario y contraseña de administrador.

- Nombre de Usuario: usuario
- Contraseña: *******

Una vez fijados el usuario y contraseña se inicializa el programa.

Figura 44 Inicialización IVMS-4200 PCNVR

En la opción Main View se añaden las cámaras para visualizar en la pantalla y se puede observar que la disposición física permite unificar el monitoreo las dos cámaras existentes.

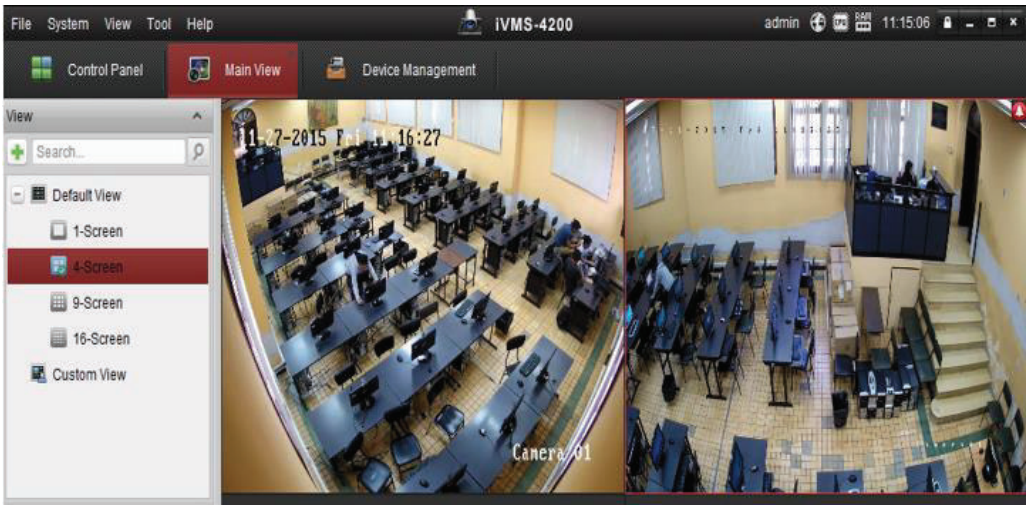


Figura 45 Monitoreo IVMS-4200 PCNVR

- **CREACIÓN DE USUARIOS IVMS-4200 PCNVR**

Se crea un usuario sin privilegios de administrador con el objetivo de que no se pueda cambiar la configuración propia de los dispositivos instalados.

- Usuario: usuario
- Contraseña: *******

Para poder acceder con privilegios de administrador el usuario y contraseña es el creado en un inicio:

- Usuario: usuario
- Contraseña: *******

Para el usuario sin privilegios de administrador se crea un perfil de tipo operador y se le asigna permisos limitados para acceder a las funciones que podrá modificar o administrar.

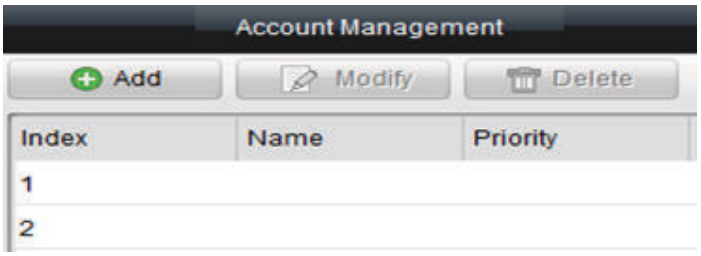


Figura 46 Creación de usuarios en IVMS-4200 PC-NVR

- **HORARIOS DE GRABACIÓN**

Para optimizar el almacenamiento de información en el disco duro se establecen horarios fijos de grabación y también horarios de grabación por detección de movimiento, la figura 46 muestra esta configuración.

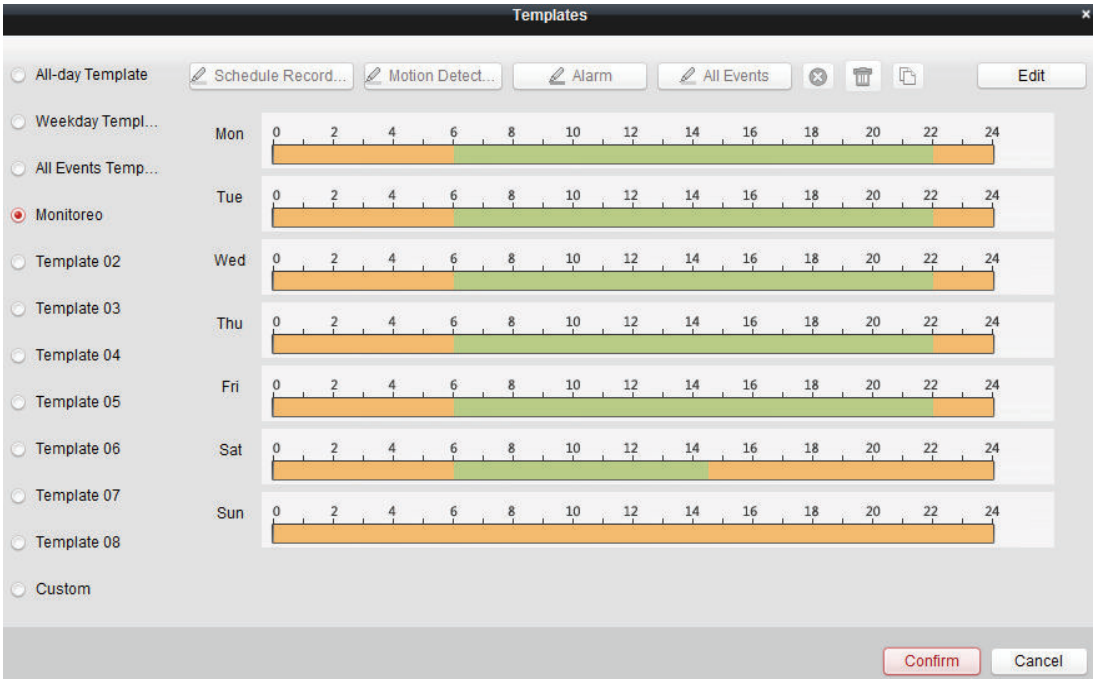


Figura 47 Horario de grabación

Los horarios configurados son los que muestra la Tabla 9. Estos están dispuestos de acuerdo a las jornadas laborables de la sala Marcelo Dávila. Es decir, grabación continua de lunes de viernes de 06h00 a 22h00 y de 22h00 a 06h00 grabación por detección de movimiento. El día sábado las actividades se graban desde las 06H00 hasta las 14h30 y el domingo las 24h00 se configura grabación por detección de movimiento.

Tabla 9 Horarios de grabación del sistema

CONFIGURACIÓN DE GRABACIÓN							
Horario	Lunes	Martes	Miércoles	Jueves	Viernes	Sábado	Domingo
00:00 06:00	Detección movimiento	Detección movimiento	Detección movimiento	Detección movimiento	Detección movimiento	Detección movimiento	
06:00 22:00	Continuo	Continuo	Continuo	Continuo	Continuo		
22:00 24:00	Detección movimiento	Detección movimiento	Detección movimiento	Detección movimiento	Detección movimiento		
06:00 14:30						Continuo	
14;30 24:00						Detección movimiento	
00:00 24:00							Detección movimiento

3.12 Monitoreo remoto

Monitoreo remoto vía web browser

Para el monitoreo remoto se puede acceder a la cámara principal la cual utiliza una dirección IP pública proporcionada por la DGIP de la EPN. La dirección IP pública para el monitoreo remoto la conoce el administrador:

IP PÚBLICA: 209.165.X.X

Para el acceso también se requiere el usuario y contraseña de administrador:

- Usuario: usuario
- Contraseña: *******

Para poder visualizar el video en la página web en la primera ocasión se solicita instalar un plugin, se descarga e instala.

Figura 48 Descarga de plugin para acceso remoto

Después de realizar el proceso indicado e instalado el Plugin, se actualiza el navegador web y se tiene acceso al monitoreo remoto vía web browser desde Internet.

El acceso se lo realiza utilizando el navegador web de preferencia Internet *Explorer*, se digita en la URL la dirección IP pública y se muestra la interfaz de la cámara principal en la que se ingresa el usuario y contraseña.

Figura 49 Acceso remoto a la cámara IP principal

Como se observa en la figura 50 se puede monitorear la sala Marcelo Dávila accediendo mediante la dirección IP pública desde Internet.

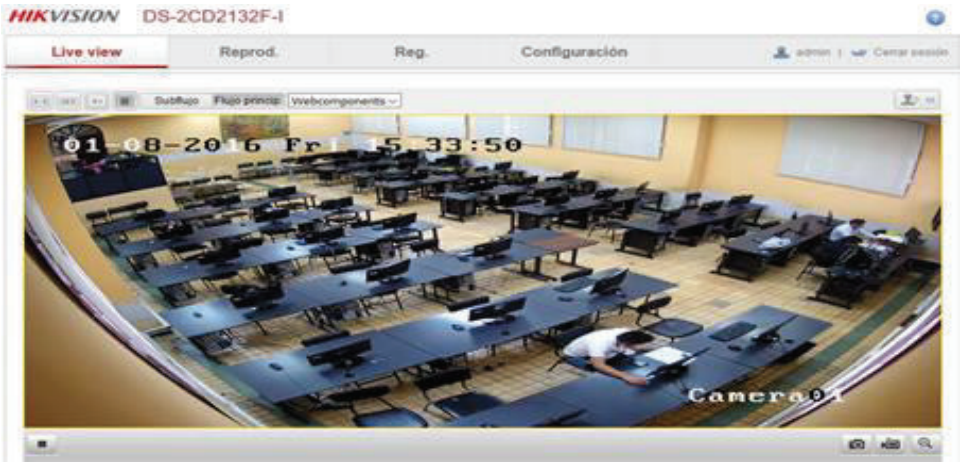


Figura 50 Monitoreo remoto desde Internet

Monitoreo remoto vía aplicación IVMS-4500

IVMS-4500 es un software libre de HIKVISION que sirve para conectar y monitorear los equipo a través de Smartphone con sistema operativo IOS o Android. La aplicación se puede descargar de App Store para IOS o del Play Store para Android. Después de descargar la aplicación se instala en el Smartphone y se inicia la aplicación.

Figura 51 Instalación de IVMS-4500

En la aplicación, en el menú de configuración > dispositivos. Se configura los parámetros de red como muestra la figura 52, los datos de salida a Internet son la IP pública, el puerto, el usuario y contraseña.

- IP Pública: 209.165.X.X
- Puerto: 9000
- Usuario: usuario
- Contraseña: *******

Se inicia la aplicación IVMS-4500 y se puede monitorear remotamente la sala Marcelo Dávila a través de la cámara principal la cual está configurada con una IP Pública.

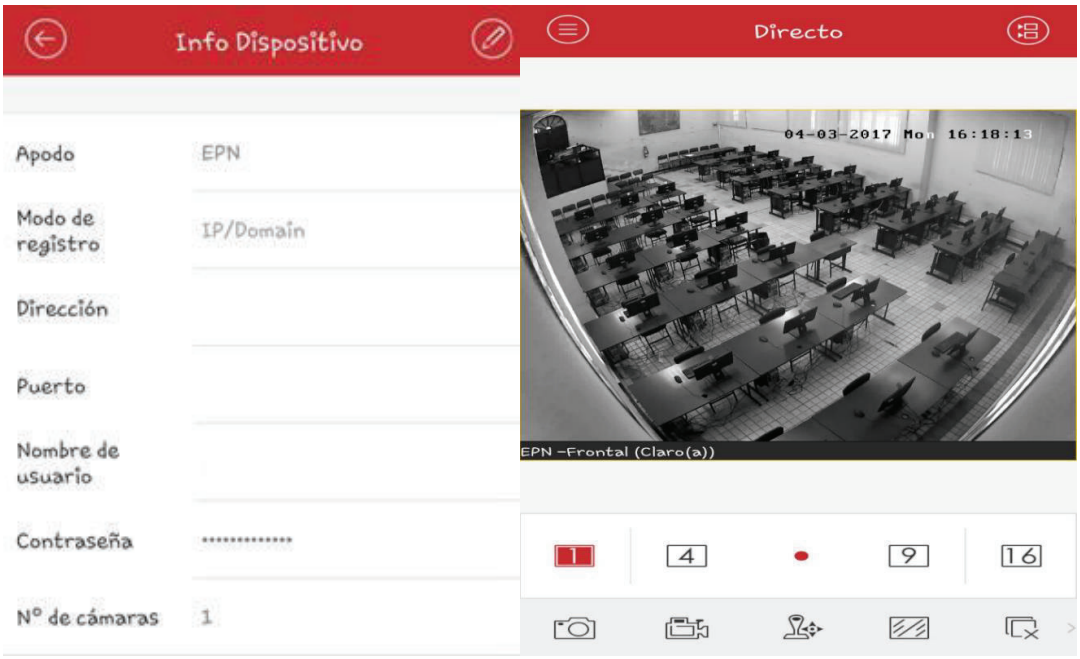


Figura 52 Configuración de IVMS-4500

Las principales funciones de la aplicación permiten:

-  Se puede hacer captura de imagen de la pantalla.
-  Se puede grabar un segmento de video.
-  Es una función habilitada para cámaras PTZ (no aplica).
-  Se puede configurar la calidad de video.
-  Se cancela la transmisión de video.

3.13 Funcionamiento del sistema

En esta sección se presentan los resultados obtenidos luego de la implementación y las mejoras obtenidas después de la experimentación. Posteriormente se verifica que cumpla los objetivos preliminares y el correcto funcionamiento del sistema.

Luego de la implementación del sistema se deja en funcionamiento para evaluar en una etapa de pruebas en la que se toma muestras de video y calidad de diferentes fechas, se puede verificar que el sistema trabaja sin problema en el proceso de almacenamiento en el disco duro. Para la evaluación se ingresa al sistema y se verifica el funcionamiento. En la figura 53 se muestra la correcta operación de los equipos luego de una etapa de funcionamiento.

Figura 53 Funcionamiento del sistema de monitoreo

En las figuras 54, 55 se muestra el funcionamiento de las cámaras frontal y lateral las cuales se encuentran trabajando correctamente según las pruebas con fecha 13/02/2017.

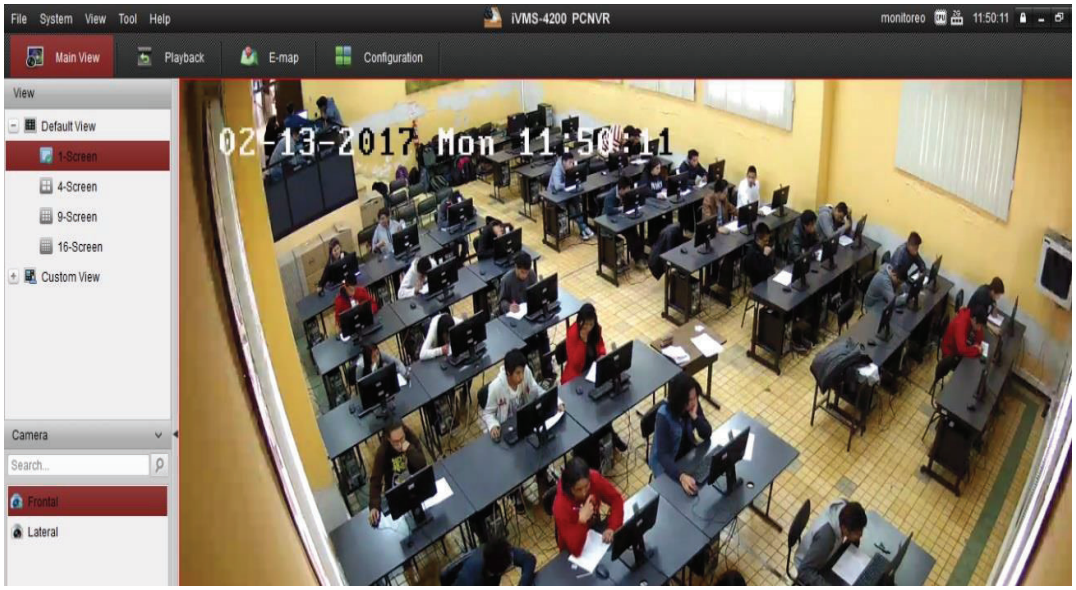


Figura 54 Funcionamiento de cámara frontal

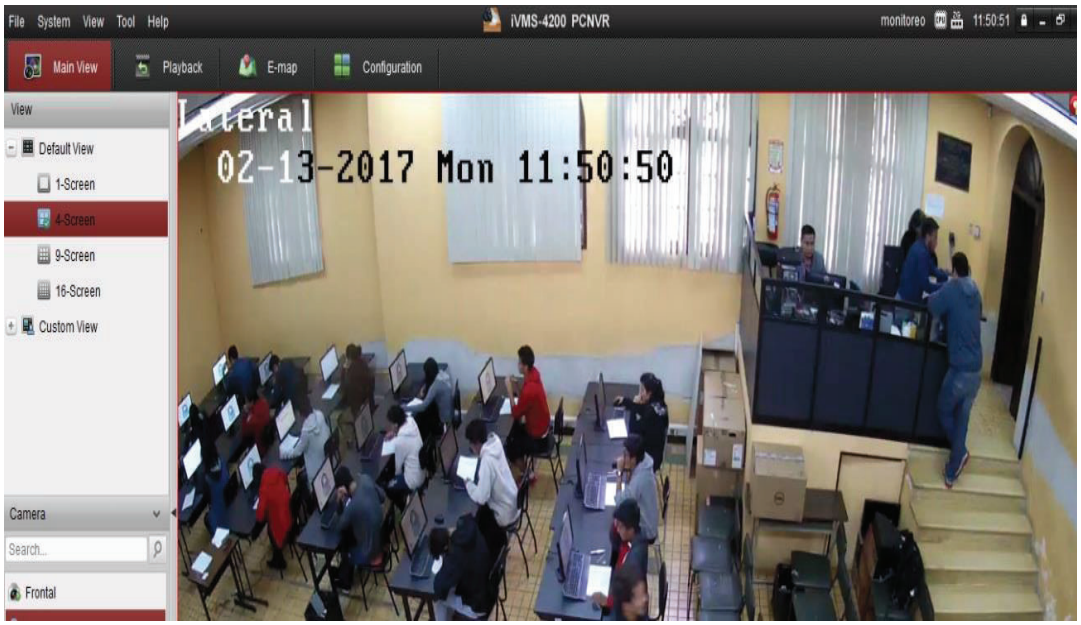


Figura 55 Funcionamiento de cámara lateral

3.14 Funcionamiento de visión nocturna

Mediante el acceso remoto se acede a la cámara principal para verificar su funcionamiento en total oscuridad. Para validar la visión nocturna, la figura 56 muestra una captura de imagen realizada a la 23:55 pm en la que se puede observar la imagen de la sala Marcelo Dávila en modo detección de movimiento.

Figura 56 Visualización nocturna

3.15 Evaluación del disco de almacenamiento

El disco duro de almacenamiento trabaja por sobre escritura, es decir sobre escribe la información cuando el disco duro está en su límite de capacidad. Concretamente borra la información más antigua y almacena la información actual.

En la figura 57 se puede ver que la capacidad del disco partición F (utilizada para almacenamiento) está en su límite por lo que está sobre escribiendo la información.

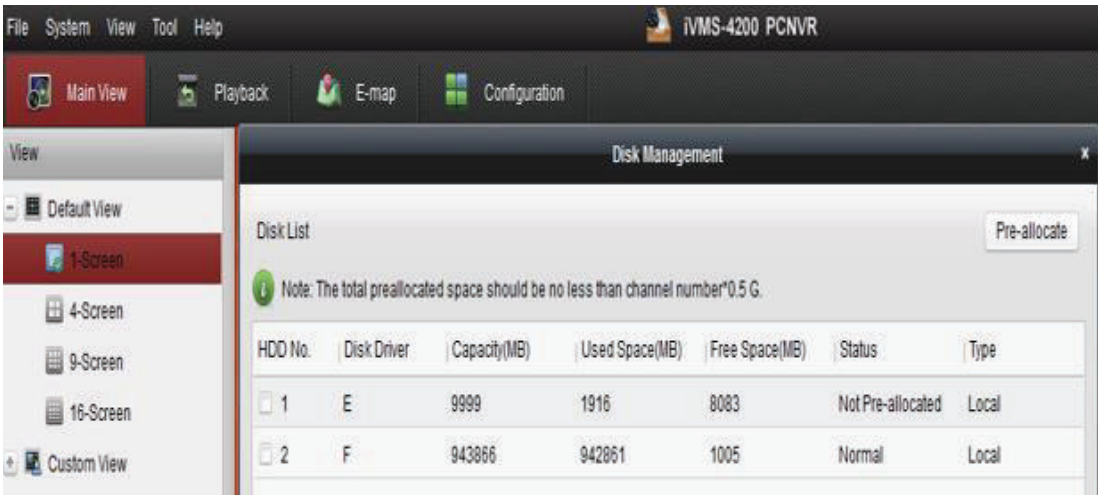


Figura 57 Evaluación del disco duro

Se procede a verificar la última fecha de grabación local en el disco para hacer una comparación con el cálculo de almacenamiento de información que se realizó teóricamente. Se observa que la última fecha de grabación que registra el disco es de Agosto del 2016. Figura 58

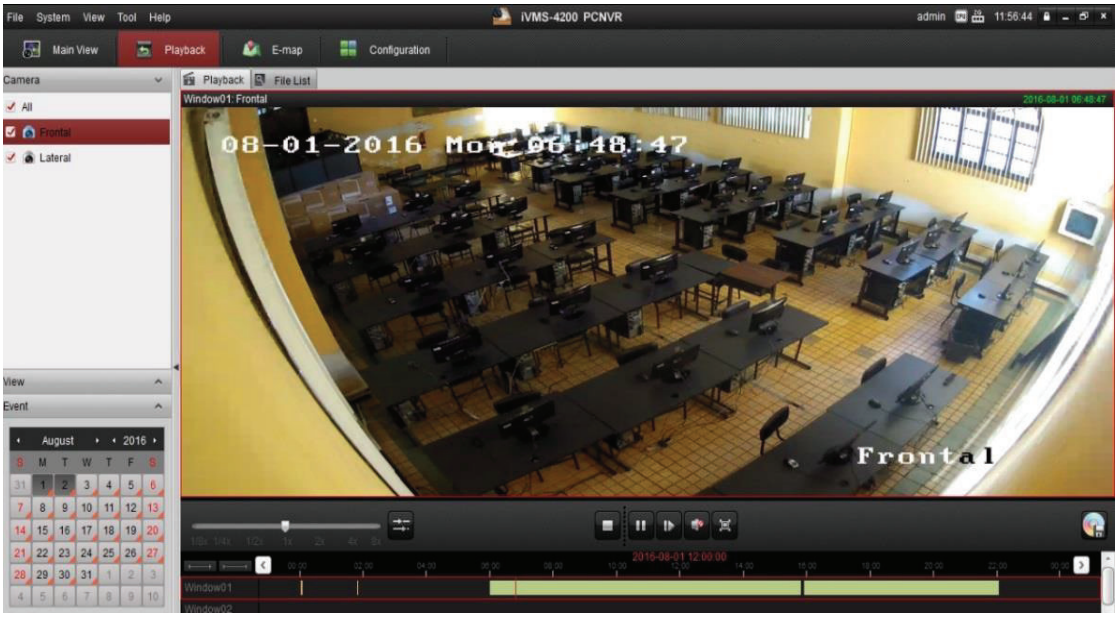


Figura 58 Registro de grabación de Agosto 2016

Se adjunta la captura de la imagen de registro de video grabación con su respectivo calendario. (la franja inferior naranja indica los registros de grabación). Figura 59

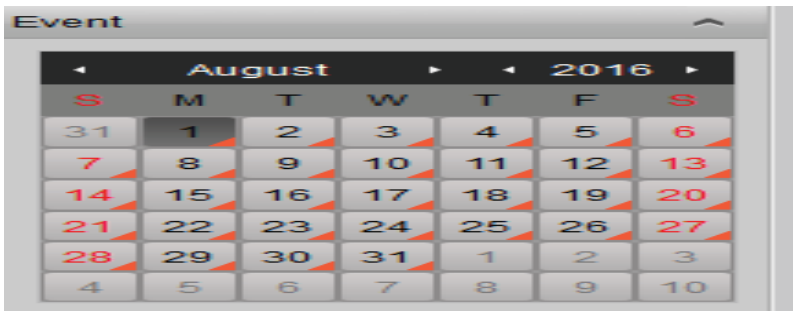


Figura 59 Calendario de registro de grabación 01/08/2017

Se puede ver en la figura 60 el registro de grabación tomado hasta la fecha de la obtención de esta muestra (13/02/2017).

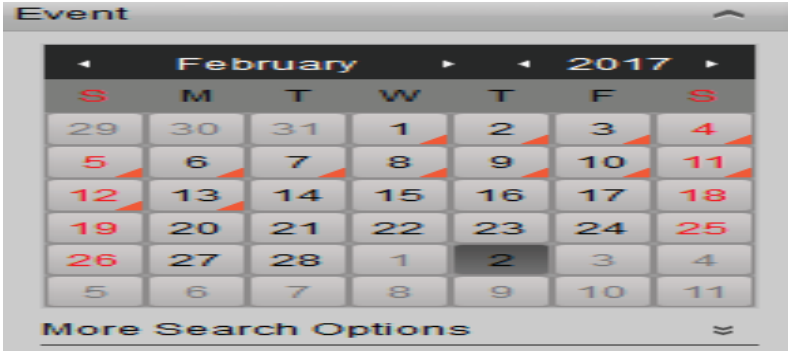


Figura 60 Calendario de registro de grabación 13/02/2017

Se hace la diferencia por fechas y se puede notar, que el sistema está almacenando la información por un tiempo aproximado de 6 meses 23 días, luego de este tiempo la información almacenada en el disco será borrada automáticamente (proceso de sobre escritura de disco).

3.16 Recuperación de información almacenada

Se verifica que el disco duro trabaja correctamente, el sistema es eficiente y como prueba se realiza una recuperación de información del disco duro, de una fecha aleatoria, es decir, un evento grabado dentro de las fechas de registro del calendario de grabación.

En la pestaña Playback se observa todos los eventos registrados por fechas, en el calendario se descarga el video correspondiente a la fecha 23/08/2016 como se muestra en la figura 61.

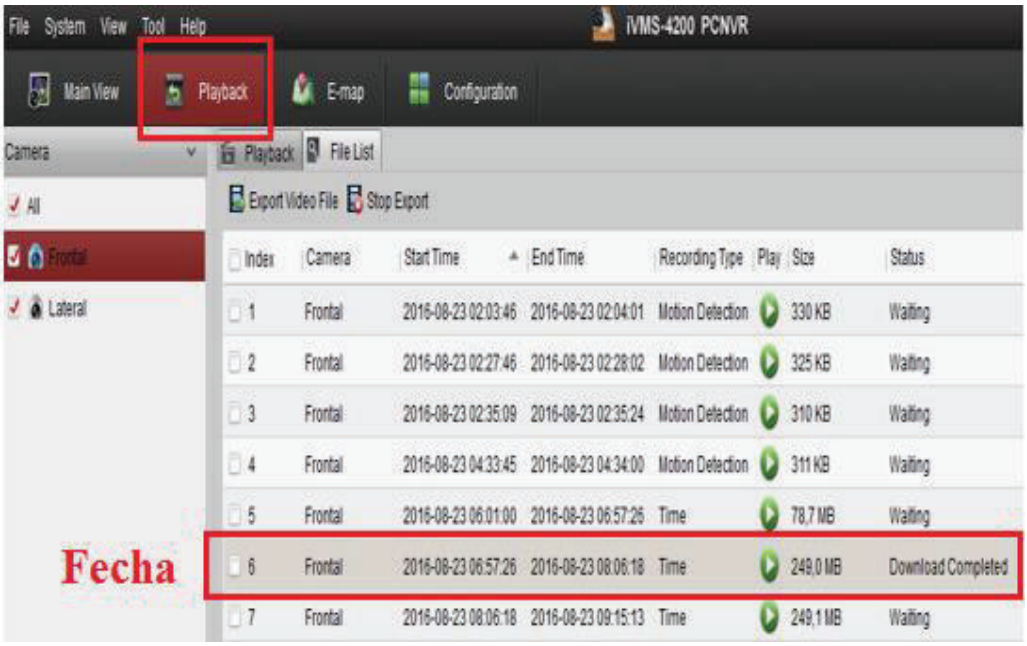


Figura 61 Recuperación de información

3.17 Ruta de descarga de video

En la configuración del sistema se direcciona la ruta para que la información descargada del programa se almacene según corresponda a las carpetas video, imágenes y configuración. Esta configuración se muestra en la figura 62.

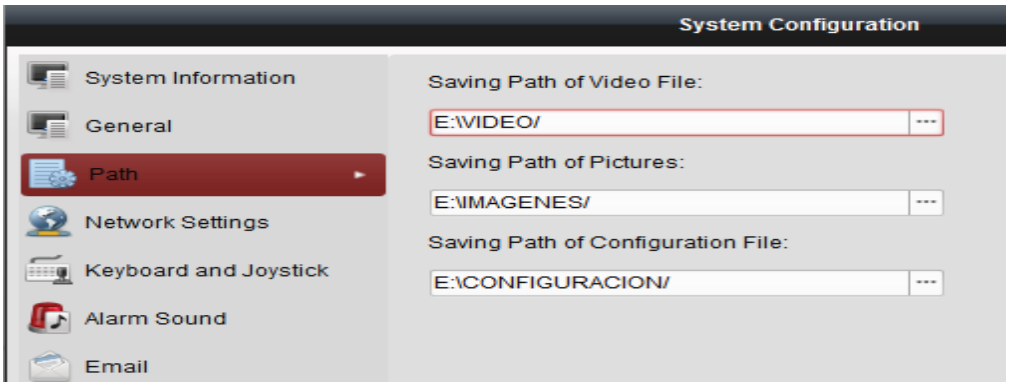


Figura 62 Configuración de rutas de descarga

Para verificar la descarga se busca en la ruta y carpeta especificada en la configuración, tal como muestra la figura 63, la descarga de la información de video está en la carpeta VIDEO.

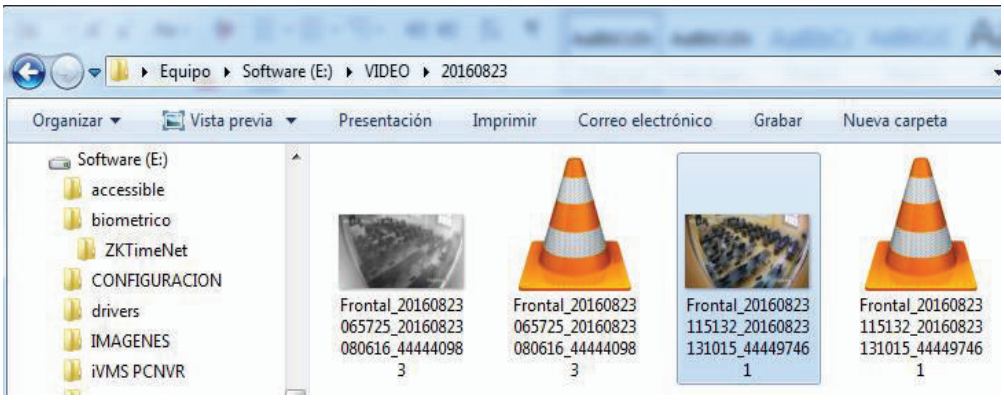


Figura 63 Descarga de video

También se realiza una captura de imagen y se verifica la ruta y carpeta configurada para el almacenamiento de imágenes, como se muestra en la figura 64 la imagen está almacenada en la carpeta IMÁGENES.

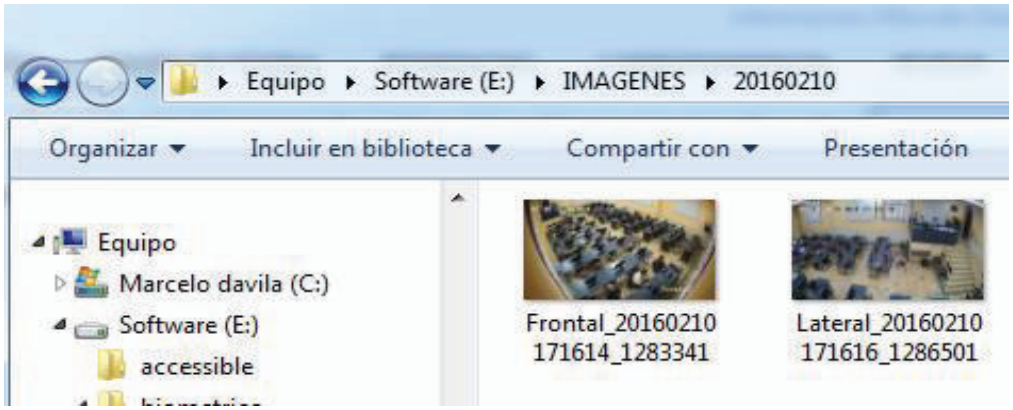


Figura 64 Descarga de imágenes

En el proceso de pruebas se verificó que, para revisar la información de video grabación, los códec con los que trabajan los equipos no son compatibles con el reproductor Windows multimedia, para solventar este inconveniente se debió actualizar los códec de Windows multimedia o trabajar con otro reproductor. Se optó por descargar y trabajar con el reproductor de software libre VLC versión 2.2.1 el cual trabaja correctamente.

Figura 65 Reproductor multimedia VLC

3.18 Funcionamiento del biométrico.

Para gestión del biométrico se autentica como administrador en el programa ZKTimeNet instalado en el servidor con el que se genera el reporte general.

- Usuario: admin
- Contraseña: *******

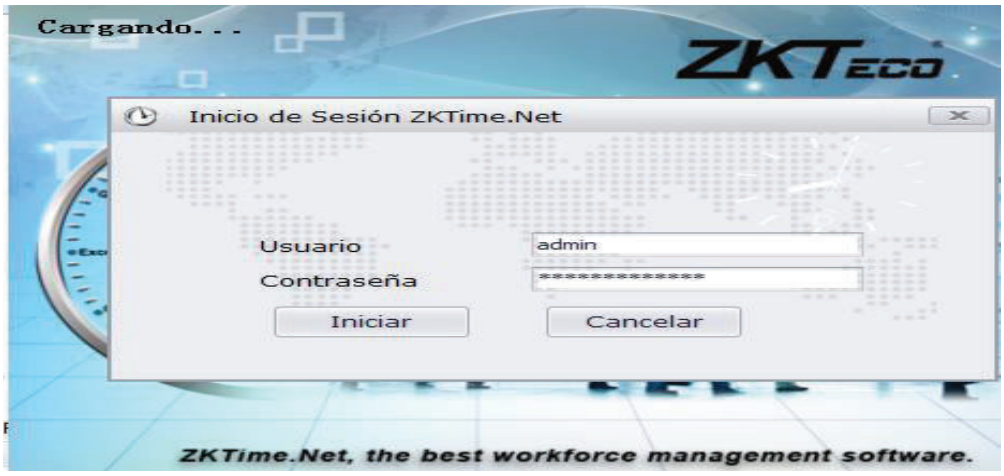


Figura 66 Inicio de sesión ZKTIMENET

Se verifica la conectividad con el equipo y se observa que trabaja correctamente.

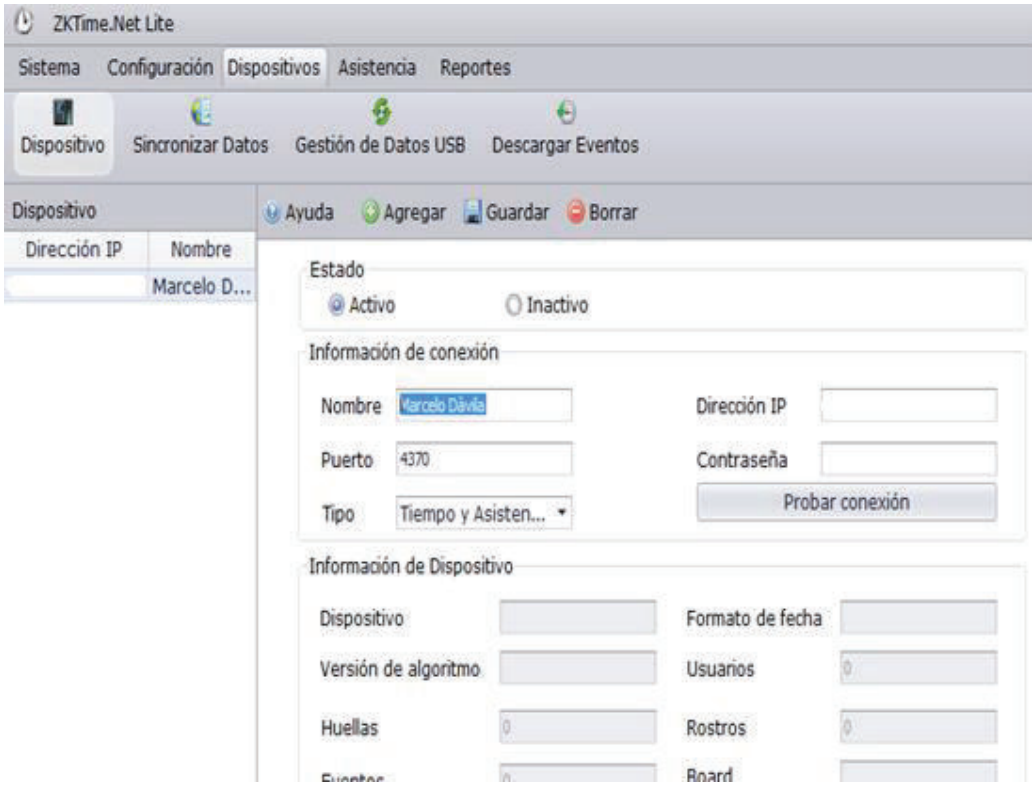


Figura 67 Funcionamiento del programa ZKTIMENET

El dispositivo trabaja correctamente, está configurado con los usuarios registrados en los horarios establecidos y detecta automáticamente los patrones faciales para la autenticación.

Figura 68 Biométrico AZ-FACE-400

Pruebas de funcionamiento del biométrico

Para las respectivas pruebas de funcionamiento de biométrico, se procede a verificar los usuarios registrados actualmente, como se muestra en la Figura 69. Se encuentra el listado de los usuarios.

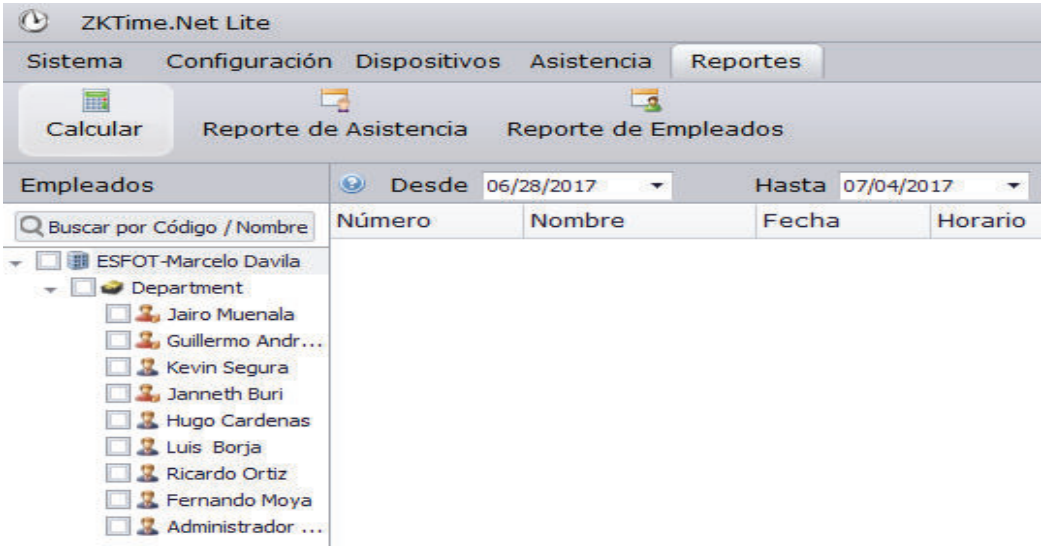
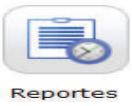


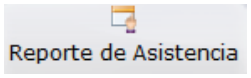
Figura 69 Usuarios registrados en el Biométrico

Se selecciona los usuarios de interés para verificar la asistencia, se elige una fecha inicio y fin de registro, en la figura 70 se observa el registro realizado a los usuarios desde 28/06/2017 hasta /04/07/2017.

Figura 70 Registro de asistencia de usuarios

Reportes de asistencia

Para obtener el reporte, hacer clic en 

o 

que se muestra la pantalla mostrada en la figura 71, se puede descargar 14 tipos de plantillas de acuerdo al requerimiento.

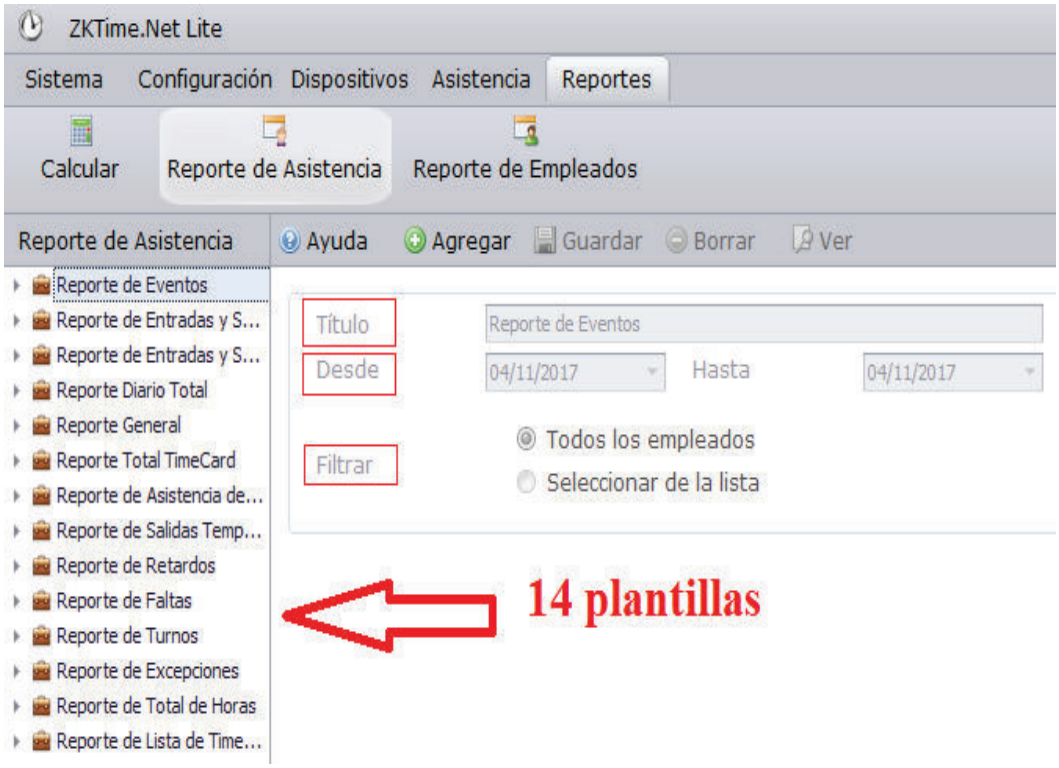


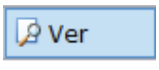
Figura 71 Plantillas de reportes de asistencia

Plantillas de Reportes

Existen 14 tipos de plantillas de reportes que son reporte de eventos, entradas y salidas vertical y horizontal, diario total, general, total, asistencia de personal, salidas tempranas, retardos, faltas, turnos, excepciones, total de horas y lista de timecard.

- Título: Establece el título del reporte. El título predeterminado es el título de la plantilla del reporte. Puede ser modificado según sea necesario.
- Desde/Hasta: Selecciona la fecha inicial y final del reporte.
- Filtrar: Selecciona el rango de empleados que se mostrará en el reporte

Después de elegir el tipo de plantilla, hacer clic en guardar de preferencia en formato PDF.

Se Puede hacer clic en 

para mostrar el reporte previo a descargar.

De acuerdo a este segmento de fechas, se obtiene el reporte o plantilla de entrada y salida de los usuarios registrados.

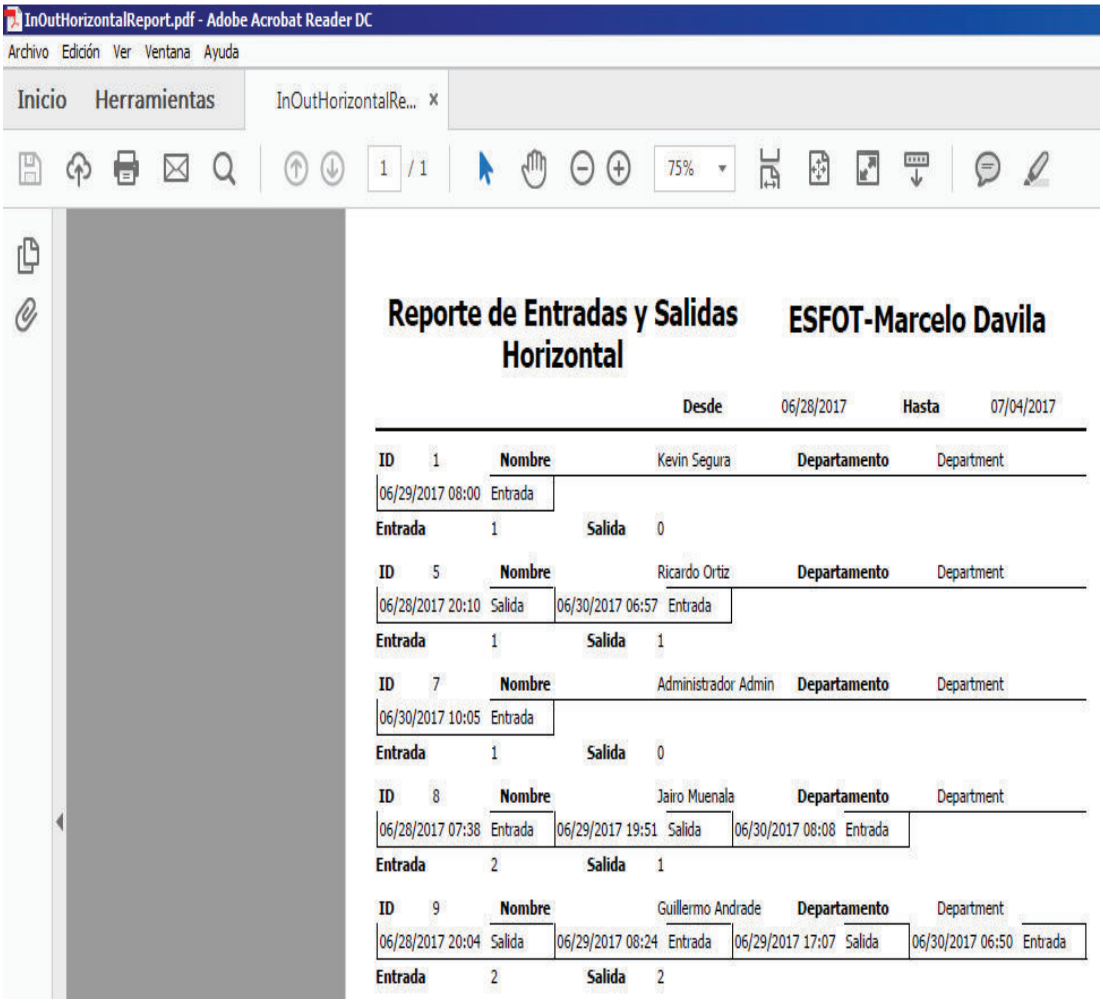


Figura 72 Reporte de entrada y salida

4 CONCLUSIONES Y RECOMENDACIONES

Conclusiones

- Después de realizar un análisis del sistema de seguridad a implementar se concluye instalar dos cámaras IP tipo domo para interiores y un biométrico de reconocimiento de patrón facial. La administración se realiza por software instalado en el servidor principal de la sala Marcelo Dávila de ESFOT.

- El software de monitoreo IVMS-4200 PCNVR es una herramienta de virtualización de servidor que permite centralizar los servicios de monitoreo y almacenamiento de información. Las cámaras IP funcionan independientemente de un ordenador o servidor, el software instalado lo que hace es unificar los servicios para poderlos administrar fácilmente.

- El sistema biométrico es de tecnología reciente que permite al usuario facilitar los medios requeridos para la autenticación y/o permiso de acceso utilizando así sus rasgos biométricos como llave o pin, de igual forma se convierte en una herramienta de seguridad inviolable al acceso, cumple en términos de biometría que los rasgos biométricos son características propias de cada individuo.

- Para la implementación se utilizó material que cumple con las características establecidas por la normativa de cableado estructurado, a fin de garantizar su correcto funcionamiento. En este caso para el presente proyecto, diseño para instalaciones en interiores.

Recomendaciones

- En el dimensionamiento y posterior diseño e implementación del proyecto en general se experimentó que siempre se va a encontrar operaciones o funciones que no estaban dentro del análisis específico, estos por lo general son de carácter técnico práctico, es decir el cálculo realizado no siempre coincide con las expectativas que se plantearon por lo cual se debe considerar tolerancias a fallas en sistemas de procesamiento de información (software), tolerancia a fallas en materiales o medios físicos (hardware).

Como recomendación, se debe considerar las tolerancias de acuerdo al alcance del proyecto con el objetivo de poder sustentar fallas fortuitas y así poder corroborar el dimensionamiento del proyecto.

- Como recomendación general para futuros proyectos similares a este presente trabajo se puede mencionar, considerar cámaras IP o cámaras análogas de acuerdo a las necesidades del sitio en el que se va a instalar los dispositivos, es decir si es un edificio inteligente conviene instalar cámaras IP ya que simplemente se conectan a la red cableada ya existente en el edificio inteligente a diferencia de las cámaras análogas en las que implicaría un gasto adicional en el cableado de la red específica para la transmisión de señales análogas hacia el *switch* o servidor central.

- Para la adquisición e instalación del disco duro dedicado al almacenamiento de información se recomienda adquirir uno de alta capacidad que soporte sobre escritura de disco cada determinado intervalo de tiempo, los discos duros convencionales no poseen estas características y pueden resultar defectuosos al operar en estas funciones y condiciones.

5 REFERENCIAS BIBLIOGRÁFICAS

[1] J. C. Santos, Seguridad Informática, Madrid: RA-MA Editoral, 2014.

[2] I. Escalona, Transductores y sensores en la automatización industrial, México: El Cid Editor, 2007.

[3] H. Vivani, «Cableado estructurado, cable directo y cable cruzado,» 2012. [En línea]. Available: https://hvivani.com.ar/2012/04/11/cableado-estructurado-cable-directo-cable-cruzado/.

[4] «Conceptos básicos en comunicaciones de video en red,» [En línea]. Available: https://www.tecnoseguro.com/tutoriales/video-ip/conceptos-basicos-en-comunicaciones-de-video-en-red.html.

[5] «Planet security USA,» 27 Octubre 2015. [En línea]. Available: https://www.planetsecurityusa.com/blog/ip-cameras-vs-tvi-cameras/.

[6] «Fundamentos básicos / vigilancia IP,» [En línea]. Available: http://global.level1.com/es/lcenter_iframe.php?lc3id=28.

[7] Tapiador Marino, Singuenza Juan, "Tecnologías biométricas aplicadas a la seguridad", Alfaomega, 2005.

[8] C. Bravo Medina. [En línea]. Available: https://www.slideshare.net/LeonardlenCorazndeGato/la-biometra-66041994.

[9] "Network fundamentals", [En línea]. Available: https://dmo.partnernet.xerox.com/Pages/default.aspx.

[10] G. A. Cortes, «Cálculo del ancho de banda,» [En línea]. Available: http://www.rnds.com.ar/articulos/065/108w.pdf.

[11] «Development of IP surveillance,» [En línea]. Available: http://www.wh-tech.com/products/about_camera/development_surveillance.htm.

[12] E. Portiansky, Análisis multidimencional de imágenes digitales, La Plata: D-editorial de la Universidad de La Plata, 2013.

[13] G. B. D. S. M. Callicó y S. D. L. Suárez, Técnicas de super-resolución para la mejora de secuencias de video comprimido, Fundación Universitaria de Las Palmas, 2009.

[14] A. Tanenbaum y D. Wetherall, "Redes de computadoras", Quinta ed., Prentice-Hall, 2012.

[15] A. M. Portera y I. M. Portera, Vigilancia y control de las comunicaciones electrónicas en el lugar de trabajo, Madrid, 2009.

[16] "CCTV análogo vs IP", [En línea]. Available: http://probo69.blogspot.com/2010/02/cctv-analogo-vs-ip.html.

[17] R. Castaño y López, Jesús, "Redes Locales", MacMillan Iberia S.A, 2013.

[18] M. Nuria Oliva, P. Castro y G. Orueta, "Sistemas de cableado estructurado", Alfa Omega, 2006.

[19] «"Biometría",» [En línea]. Available: http://www.biometria.gov.ar/metodos-biometricos/facial.aspx.

[20] Fundamentos básicos de vigilancia IP, [En línea]. Available: http://global.level1.com/es/lcenter_iframe.php?lc3id=28.

[21] «Switching and Routing CCNA,» [En línea]. Available: https://www.netacad.com/group/landing/.

6 ANEXOS

ANEXO I ESPECIFICACIONES TÉCNICAS DE LAS CÁMARAS IP

ANEXO II ESPECIFICACIONES TÉCNICAS DEL BIOMÉTRICO

ANEXO III ESPECIFICACIONES TÉCNICAS DEL ROUTER D-LINK

ANEXO IV MANUAL DE USO DEL SOFTWARE DE HIKVISION IVMS-4200 PCNVR

ANEXO V MANUAL DE USO DEL SOFTWARE DEL BIOMÉTRICO ZKTIMENET

ANEXO VI MANUAL DE MANTENIMIENTO DEL SISTEMA

ANEXOS

Anexo I

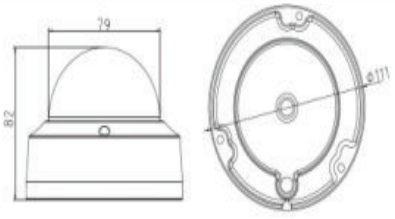
ESPECIFICACIONES TÉCNICAS DE LAS CÁMARAS IP

DS-2CD2132-I 3MP IR Fixed Focal Dome Camera

Key features

- 3 megapixel (2048 x 1536) resolution
- Full HD1080p real-time video
- 3D DNR & DWDR & BLC
- IR LEDs: up to 30m
- IP66
- PoE
- Vandal-proof

Dimensions



	DS-2CD2132-I
Camera	
Image sensor	1/3" progressive scan CMOS
Min. illumination	0.19 lux@F2.0, AGC on 0 lux with IR
Shutter time	1/30s ~ 1/100,000s
Lens	4mm @F2.0, angle of view: 75.8° (2.8mm, 6mm, 12mm optional)
Lens mount	M12
Angle adjustment	Pan: 0° ~ 355°, tilt: 0° ~ 65°
Digital noise reduction	3D DNR
Wide dynamic range	Digital WDR
Day & night	True
Compression standard	
Video compression	H.264 / MJPEG
H.264 codec profile	Main profile
Bit rate	32 Kbps ~ 16 Mbps
Dual stream	Yes
Image	
Max. image resolution	2048 × 1536
Frame rate	60Hz: 15fps (2048 x 1536), 30fps (1920 × 1080),30fps (1280 x 720)
Image settings	Saturation, brightness, contrast adjustable through client software or web browser
BLC	Yes, zone configurable
Network	
Network storage	NAS
Alarm trigger	Motion detection, tampering alarm
Protocols	TCP/IP, HTTP, DHCP, DNS, DDNS, RTP, RTSP, PPPoE, SMTP, NTP, SNMP, HTTPS, FTP, 802.1x, Qos
System compatibility	ONVIF, PSIA, CGI
General functionalities	User authentication, watermark
Interface	
Communication interface	1 RJ45 10M / 100M ethernet port
General	
Operating conditions	-30°C ~ 60°C (-22°F ~ 140°F) humidity 95% or less (non-condensing)
Power supply	12 VDC ± 10%, PoE (802.3af)
Power consumption	Max. 5W (7W with ICR on)
Impact protection	IEC60068-275Eh, 50J; EN50102, up to IK10
Ingress protection	IP66 / IK10
IR range	approx 10 to 30 meters
Dimensions	Φ 111 × 82 mm
Weight	500g (1.1 lbs)

Available models

DS-2CD2132-I

Anexo II

ESPECIFICACIONES TÉCNICAS DEL BIOMÉTRICO

www.autoidcorp.com

AUTO-ID INTL
Business Identification Solutions

AZ FACE 400

ESPECIFICACIONES TÉCNICAS

Capacidad

Caras	800 1:N (estándar) 3.000 1:1 (opcional)
Tarjetas	hasta 10.000
Proximidad	EM. Opcional Mifare
Registros	Hasta 100.000 sin descargar

Hardware

Algoritmo facial	ZK 7.0
Sensor	ZK Óptico
Teclado	En display
Display	TFT táctil Color 3"

Comunicaciones

Ethernet	SI
USB	NO
Puerto USB para Pendrive	SI

Accesos

Relé	SI: puerta o sirena
Wiegand	NO
Antipassback	NO
Zonas y grupos	SI

Otros

Tamaño	104.7x160x36 mm
Peso	0,3 kg
Temperatura	0° C- 45° C
Humedad	20%-80%
Alimentación	12V

CARACTERÍSTICAS GENERALES

Distintos modos de verificación: reconocimiento facial, huella y password.

Tarjeta opcional.

El modo de fichaje es configurable por empleado.

Incorpora puerto USB para descarga de fichajes.

Funcionamiento autónomo o con PC: no necesita estar conectado a PC para fichar.

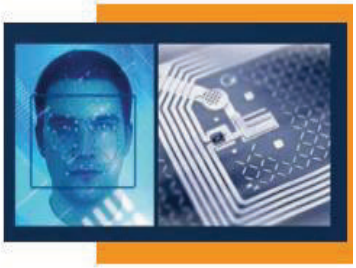
Permite la visualización en el terminal del nombre (Alias).

Admite la introducción incidencias que pueden ser listadas en el display.

Para el control de presencia y accesos, el terminal VF380 puede completarse con las aplicaciones ZKTime Lite-EU, ZKTime Pro-EU y ZKTime Enterprise.

SDK: Entorno de desarrollo para que el propio cliente desarrolle sus aplicaciones.

Permite integrarse fácilmente en cualquier aplicación gracias al programa Extractor que extrae la información contenida en el terminal en formato de texto plano.



Anexo III

ESPECIFICACIONES TÉCNICAS DEL ROUTER D-LINK

D-Link®

CREATE A HIGH-PERFORMANCE WIRELESS NETWORK

WHAT THIS PRODUCT DOES

Share your broadband Internet connection with multiple computers in your house by simply connecting the Wireless N 150 Home Router to your cable or DSL modem. Once connected, you can create your own personal wireless home network to connect to the Internet, or share documents, music, and photos.

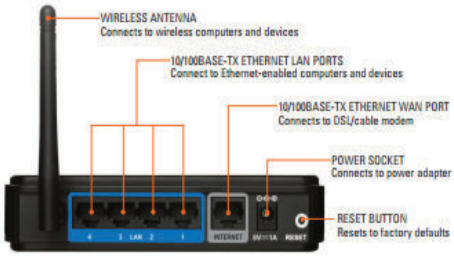
EASY INSTALLATION

Set up your new D-Link networking hardware in minutes using our new Setup Wizard. The wizard will guide you through an easy to follow process to install your new hardware and connect to your network.

ADVANCED WIRELESS FUNCTIONS

The D-Link Wireless N 150 Home Router includes everything you need to get a wireless network up and running:

- 802.11g/b wireless, compatible with 802.11n devices
- Advanced scheduling and website filtering
- WEP, WPA (TKIP) and WPA2 (AES) support
- UPnP™ support
- WPS™



TECHNICAL SPECIFICATIONS

SYSTEM REQUIREMENTS

- Cable or DSL modem with Ethernet port
- Computer with:
  - Windows XP SP2/Vista/7, Mac OS X (v10.4/v10.3), or Linux-based operating system
  - An installed Ethernet adapter
  - Internet Explorer 6 or Firefox 3.0 or higher

STANDARDS

- IEEE 802.11g/b, compatible with 802.11n devices
- IEEE 802.3
- IEEE 802.3u

WIRELESS FREQUENCY RANGE

- 2.4 GHz to 2.4835 GHz

ANTENNA

- Detachable dipole antenna (reverse SMA plug)

SECURITY

- WEP 64/128-bit data encryption
- Wi-Fi Protected Access (WPA/WPA2)

ADVANCED FIREWALL FEATURES

- Network Address Translation (NAT)
- Stateful Packet Inspection (SPI)
- MAC Address Filtering
- URL Filtering

DEVICE MANAGEMENT AND MONITORING

- Internet Explorer 6 or later, or Firefox 3.0 or later
- D-Link Network Monitor Yahoo! Widget
- D-Link Internet Usage Meter Yahoo! Widget

POWER INPUT

- 5 V DC/1 A through external power adapter

DIAGNOSTIC LEDs

- Power
- Internet
- WLAN
- LAN

DIMENSIONS (L x W x H)

- 113.2 x 147.5 x 31.5 mm (4.4 x 5.8 x 1.2 inches)

WEIGHT

- 246 grams (0.5 lb)

OPERATING TEMPERATURE

- 0 to 40 °C (32 to 104 °F)

STORAGE TEMPERATURE

- -20 to 65 °C (-4 to 149 °F)

OPERATING HUMIDITY

- 10% to 95% non-condensing

STORAGE HUMIDITY

- 10% to 95% non-condensing

CERTIFICATIONS

- FCC
- CE
- C-Tick
- Wi-Fi Certified
- Compatible with Windows 7

[1] Actual data throughput will vary. Network conditions and environmental factors, including volume of network traffic, building materials and construction, and network overhead lower actual data throughput rate and adversely affect the range.

Product specifications, size and shape are subject to change without notice, and actual product appearance may differ from that depicted on the packaging.

Compatible with Windows 7

802.11g WiFi CERTIFIED with some n features

FC CE ACN 052 202 838

D-Link Corporation
No. 289 Xinhu 3rd Road, Neihu, Taipei 114, Taiwan
Specifications are subject to change without notice.

Release 01 (March 2011)

WIRELESS N 150

WIRELESS N 150 HOME ROUTER
DIR-600

Anexo IV

MANUAL DE USO DEL SOFTWARE DE HIKVISION IVMS-4200 PCNVR

Registro de administrador / Súper Usuario

La primera vez que IVMS-4200 se inicia, es necesario registrar un usuario administrador / Súper usuario para iniciar sesión en el sistema.

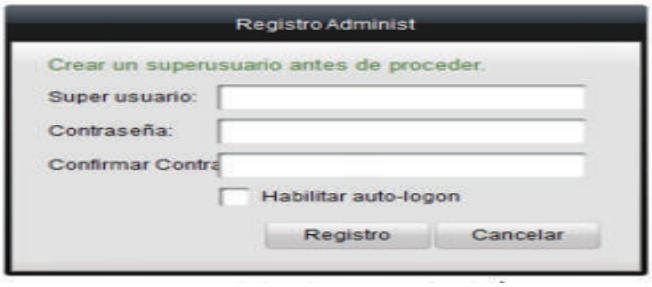
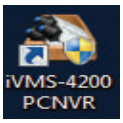


Figura 1 Registro de administrador / Súper usuario

Se ingresa el nombre de usuario, contraseña y confirmación de contraseña y se hace clic en el botón “Registro”. Iniciará sesión con el nombre de usuario creado.

Nota: Enter, espacio, TAB son teclas inválidas como nombre de usuario y contraseña, la contraseña no pude estar en blanco y no puede ser inferior a 6 caracteres.

Inicio Rápido

Haciendo clic en el acceso directo del escritorio 

iniciará el software IVMS-4200 PCNVR solicitando nombre de usuario y contraseña.

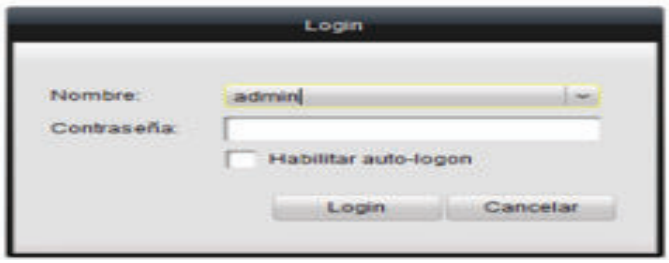


Figura 2 Inicio de sesión

1. Introducir el nombre de usuario y la contraseña. De forma predeterminada, el nombre de usuario y la contraseña son admin y 12345.

2. Opcionalmente, marcar la casilla de verificación activar inicio automático para iniciar sesión automáticamente en el software.

3. Hacer clic en Iniciar sesión.

Panel de control

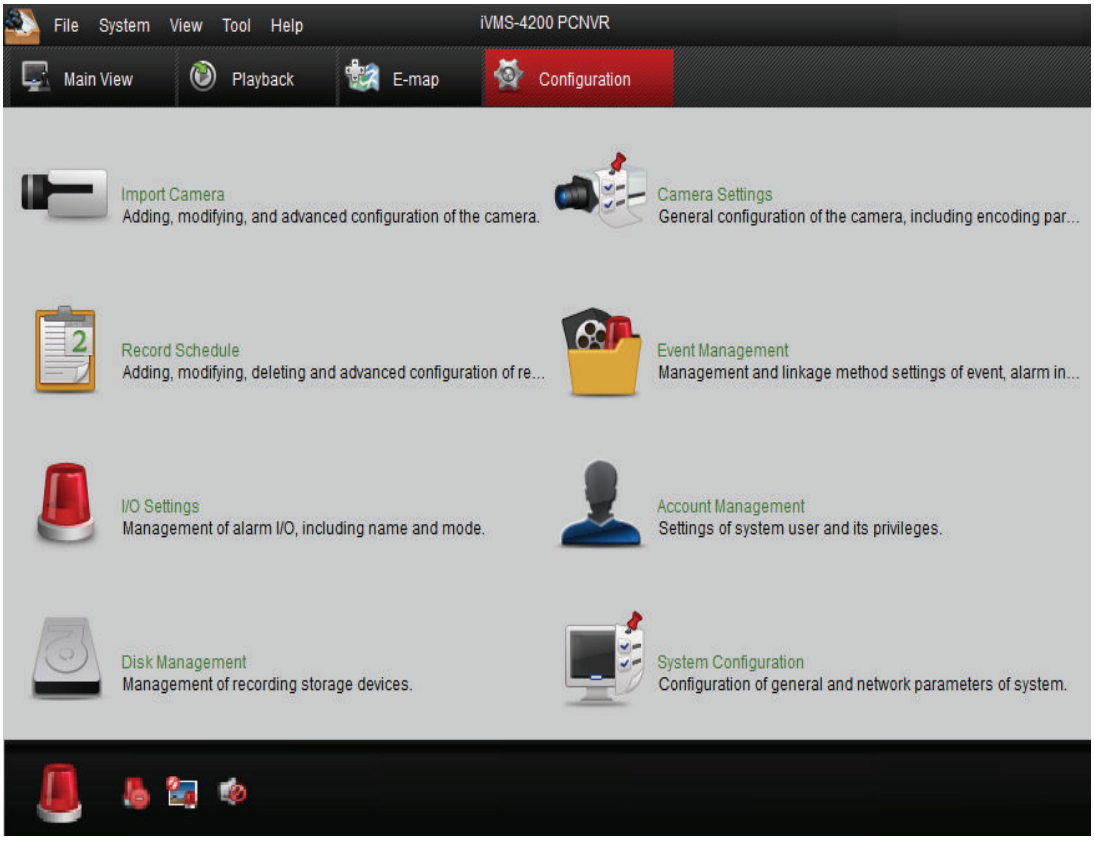


Figura 3 Panel de control

Barra de menú

File	Open Captured picture	Buscar y ver las imágenes capturadas almacenadas en la PC local
	Open Video File	Ver los archivos de vídeo de copia de seguridad almacenados en el PC local.
	Open Log File	Ver los archivos de registro de copia de seguridad almacenados en el PC local.
	Exit	Salga del software iVMS-4200 PCNVR.
	AutoRun	Ejecute el PCNVR o el sistema operativo automáticamente.
System	Lock	Bloquear las operaciones de la pantalla. Inicie sesión en el cliente de nuevo para desbloquear.
	Switch User	Cambiar el usuario de inicio de sesión
	Import Configuration File	Importar el archivo de configuración del software desde su computadora
	Export Configuration File	Exportar el archivo de configuración del software a su computadora.
	Restore Default Settings	Restaurar la configuración predeterminada del sistema

View	1024*768	Muestra la ventana con un tamaño de 1024 * 768 píxeles.
	1280*1024	Muestra la ventana a un tamaño de 1280 * 1024 píxeles.
	1440*900	Muestra la ventana con un tamaño de 1440 * 900 píxeles.
	1680*1050	Muestra la ventana con un tamaño de 1680 * 1050 píxeles.
	Full Screen	Mostrar la ventana en pantalla completa.
	Main View	Abre la página main view.
	Playback	Abre la página reproducción.
	E-map	Abre la página E-map.
	Configuration	Abre la página configuración.
	Auxiliary Screen Preview	Abre la ventana de previsualización de la pantalla auxiliar.
Tool	Import Camera	Abre la página Import camera (Importar cámara).
	Camera Settings	Abre la página configuración de la cámara.
	Record Schedule	Abre la página Programación de registros.
	Event Management	Abre la página gestión de eventos.
	I/O Settings	Abre la página configuración de E / S.
	Account Management	Abre la página gestión de cuentas.
	Disk Management	Abre la página administración de discos.
	System Configuration	Abre la página configuración del sistema.
	Log Search	Abre la página de búsqueda de registros.
	Broadcast	Selecciona la cámara para iniciar la transmisión.
	I/O Control	Activa / desactiva la salida de alarma.
	Soft Keyboard	Activa la función de teclado suave.
Help	Open Wizard	Abre la guía para la configuración del software.
	User Manual (F1)	Haga clic para abrir el Manual del usuario: También puede abrir el usuario Manual pulsando F1 en el teclado.
	About	Ver la información básica del software
	Language	Seleccione el idioma para el software y el software. Reinicie automáticamente para activar la configuración.

El IVMS-4200 PCNVR se compone de los siguientes módulos de función:

 **Main View**	El módulo Vista Principal proporciona una vista en vivo de las cámaras de vídeo y soporta algunas operaciones básicas, como captura de imágenes, grabación, control PTZ, etc.
 **Playback**	El módulo de reproducción proporciona la búsqueda, reproducción, exportación de archivos de registro.
 **E-map**	El módulo E-map proporciona la visualización y gestión de E-maps, entradas de alarma, regiones calientes y puntos calientes.
 **Configuration**	El módulo de configuración está compuesto de 8 sub-módulos de función: importar cámara, configuración de la cámara, programación de grabación, etc.

El módulo de configuración está compuesto de los siguientes sub-módulos de 8 funciones:

 **Import Camera**	Añade, modifica y elimina la cámara de red y el codificador de vídeo. Proporciona configuración remota para el dispositivo añadido.
 **Camera Settings**	Configura la imagen, los parámetros de codificación, en la pantalla (OSD), parámetros de control PTZ, etc.
 **Record Schedule**	Configura los parámetros de registro y configurar la plantilla de planificación para ser utilizado en la grabación.
 **Event Management**	Configurara grabaciones y alarmas mediante la definición de disparadores y enlaces de comportamiento.
 **I/O Settings**	Activa / desactiva la salida de alarma.
 **Account Management**	Agrega, modifica y elimina las cuentas de usuario y asigna diferentes permisos para los usuarios.
 **Disk Management**	Pre-asigna los discos duros para el almacenamiento de archivos de registro.
 **System Configuration**	Configura los parámetros generales, las rutas de salvación de archivos, los sonidos de alarma y otros ajustes del sistema.

Administración de cuentas

Se pueden agregar varias cuentas de usuario al software y se le permite asignar permisos para diferentes usuarios si es necesario.

Haga clic en el icono del panel configuración  , o haga clic en Herramienta > gestión de cuentas para abrir la página gestión de cuentas.

Nota:

- La cuenta de usuario admin es el súper administrador del software.
- La cuenta de usuario monitoreo es el operador.
- Para cambiar de usuario vaya a system > switch user, e ingrese el usuario deseado.

Vista en vivo

Para la tarea de vigilancia, puede ver el video en directo de las cámaras de red y vídeo añadido en la página Main View.

Es necesario agregar una cámara para ver en directo.
Haga clic en la pestaña Vista principal, O haga clic en View>Main View para abrir la página de vista principal.

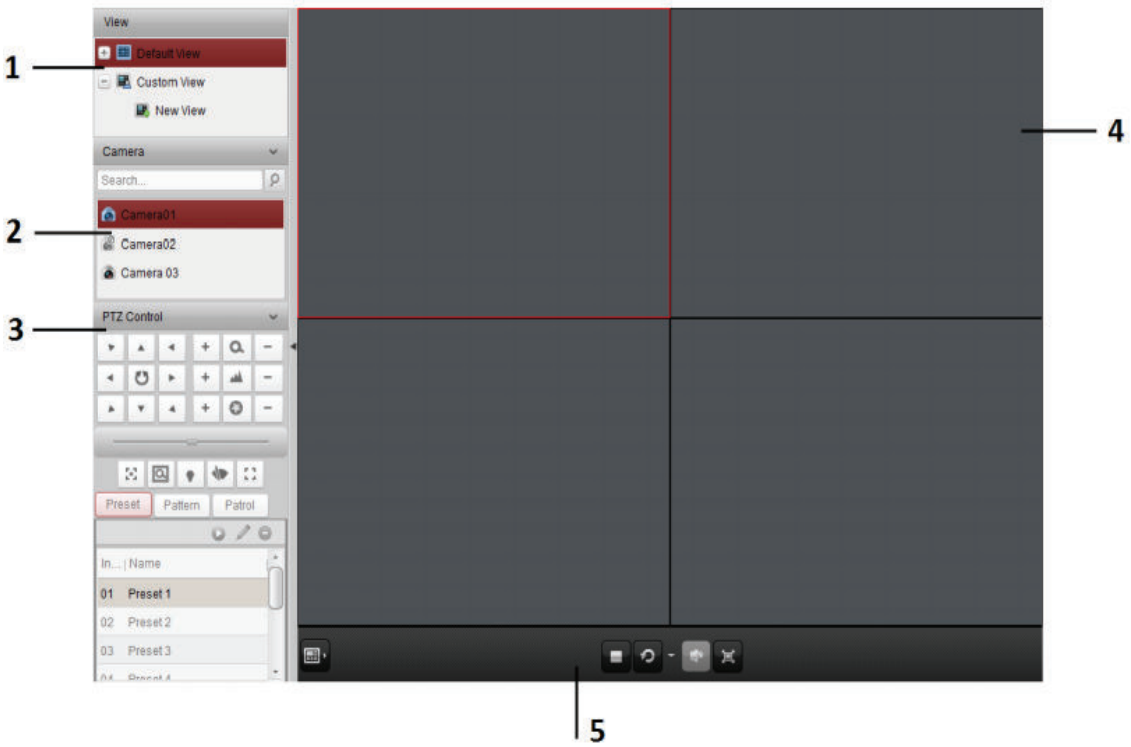


Figura 4 Vista principal

Página de vista principal:

1.- Ver lista: vista predeterminada y vista personalizada.
2.- Lista de cámaras.
3.- Panel de control PTZ.
4.- Ventana de visualización de Live View.
5.- Barra de herramientas de Live View.

Anexo V

MANUAL DE USO DEL SOFTWARE DEL BIOMÉTRICO ZKTIMENET

Registro de software

Después de instalar el programa ZKTIMENET se agrega un acceso directo 

. Al dar clic en el icono se procede al registro del software.

Cuando se inicia la sesión por primera ocasión se debe registrar un usuario y contraseña de administrador.

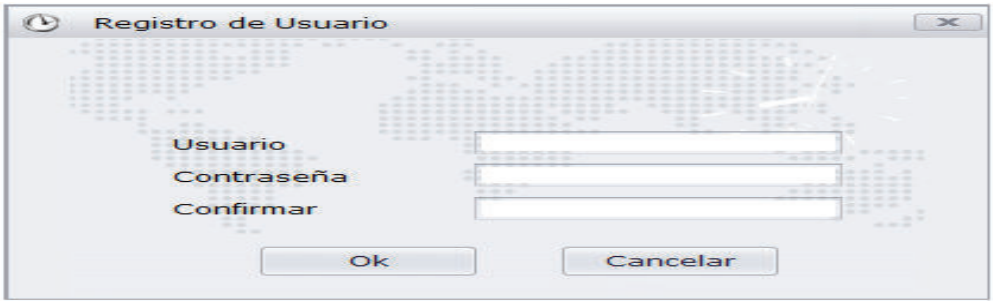


Figura 1 Registro de usuario

- Se registra el usuario como administrador y también la contraseña

Interfaz principal del sistema

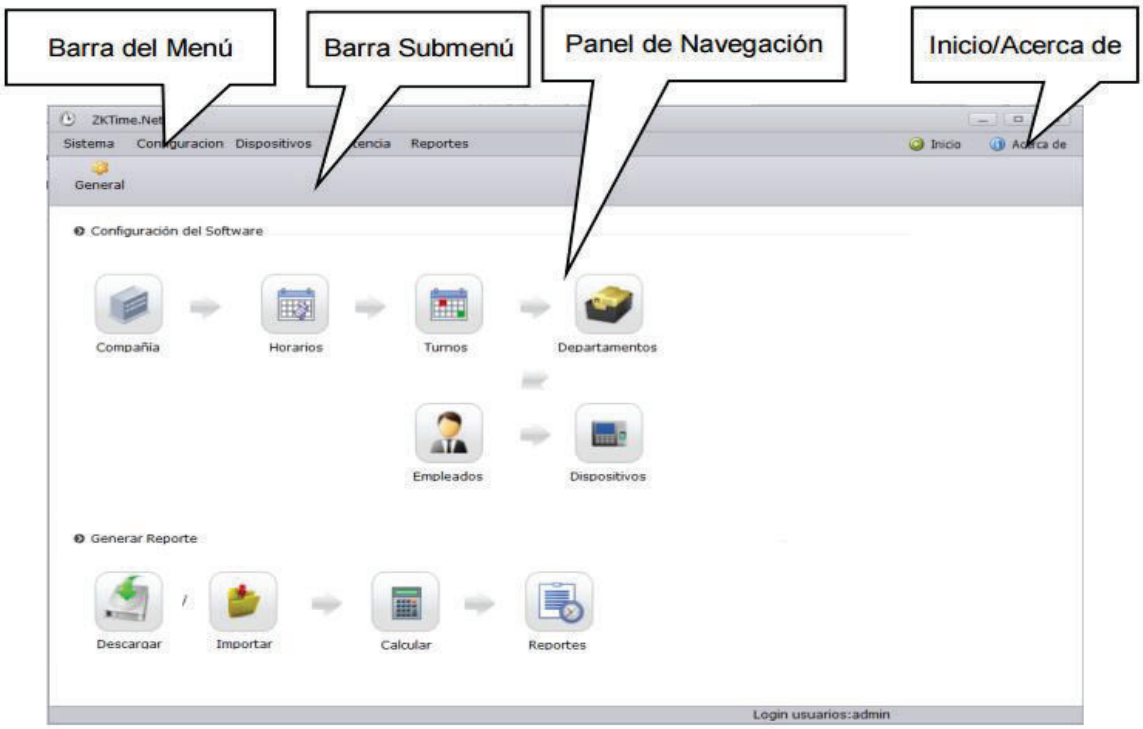


Figura 2 Interfaz de ZKTIMENET

Contenidos de la interfaz

Barra de Menús	Muestra las funciones del sistema que le ayudan a administrar la asistencia del personal de la empresa.
Barra de Submenú	Simplifica las funciones y ayuda a ejecutar las operaciones más eficientemente.
Área de Operación	Permite ver y realizar funciones de control y descarga de registros.
Accesos Directos	Acceso rápido al área de operación, registro del sistema y revisión la versión del sistema.

Elementos del menú

Sistema	Configuración del sistema.
Configuración	Gestiona la información común del control de asistencia como el tipo de pago, gestión de horarios, asignación de turnos, estructura de la empresa, arquitectura del departamento y empleados.
Dispositivo	Gestiona el dispositivo biométrico, la información de los empleados y registros en el dispositivo, así como la Importación y exportación de datos de asistencia mediante una memoria USB.
Asistencia	Asigna excepciones, permite buscar, importar, exportar registros.
Reportes	Permite procesar reportes, administrar los reportes basados en la información del empleado y los registros de asistencia. Permite exportar reportes por empleado o por tiempo.

Iconos de acceso directo

Inicio	Permite realizar las operaciones para ayudar a completar la administración de asistencia rápidamente.
Acerca de	Esta opción mostrará la versión del sistema.

Nota: Esta información está basada en el manual de usuario del software ZKTIMENET el cual se incluye en el mismo, para acceder realice lo siguiente:

Dar clic en el botón de configuración > luego dar clic en el botón ayuda.

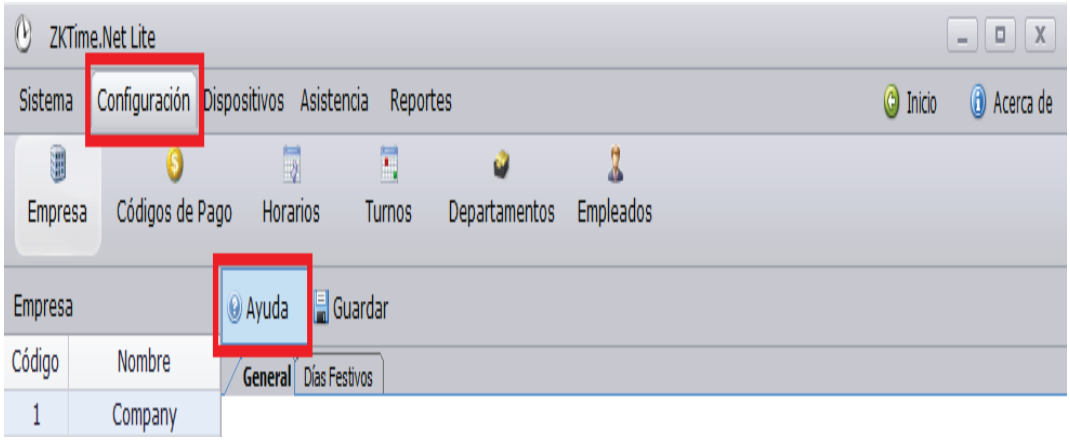


Figura 3 Acceso al manual HTML

Se despliega una página en HTML con un índice del manual de usuario y las instrucciones correspondientes.

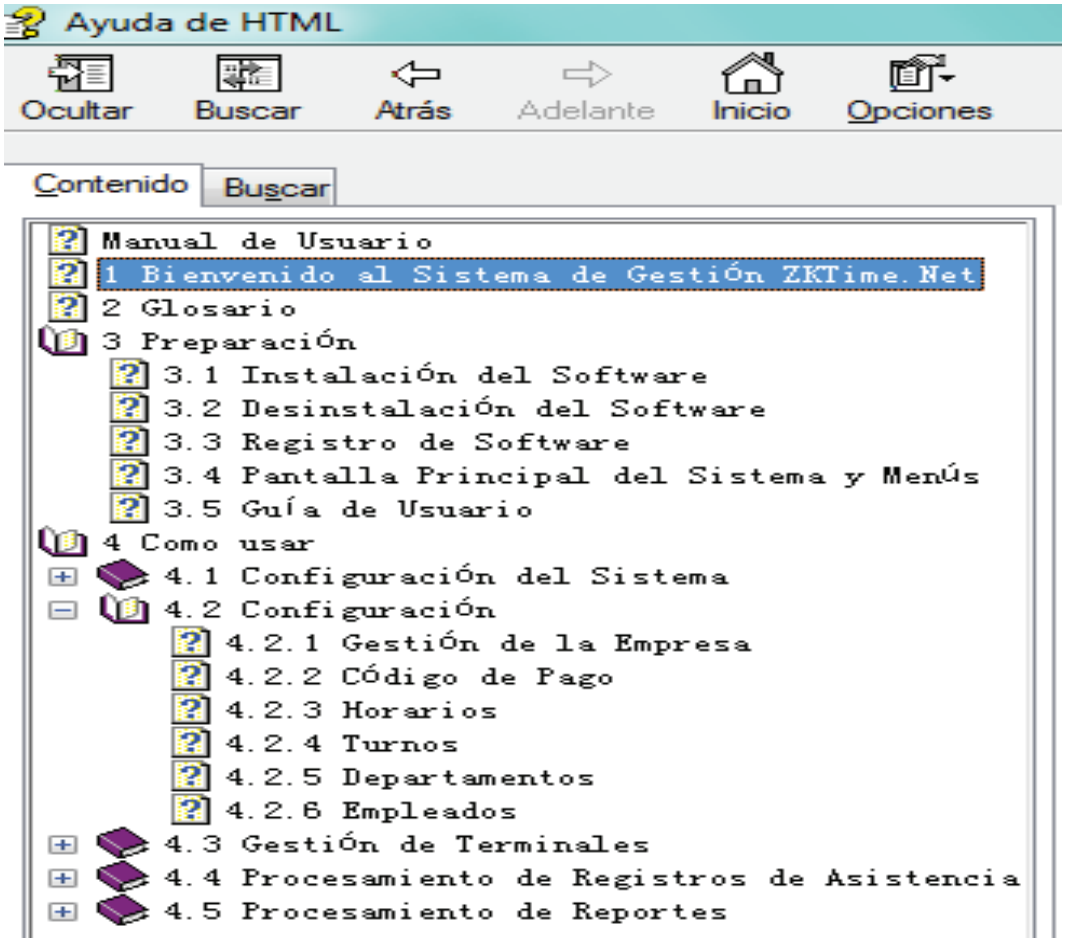


Figura 4 Ayuda de HTML

Guía de usuario.

Paso 1: Ingrese al sistema.

Paso 2: Configure la estructura de la empresa en la opción empresa incluyendo la información básica, modo de operación y los días festivos.

Paso 3: Defina los siguientes parámetros en horarios: hora de entrada/salida, contar retardo/contar salida temprano, descanso, y reglas de redondeo.

Paso 4: Programe y asigne turnos en la opción turnos.

Paso 5: Establezca la estructura organizacional de los departamentos basado en la estructura de la empresa en departamentos, incluyendo información básica del departamento, modo de operación y horario.

Paso 6: Realice las siguientes operaciones en la opción empleados: ingrese información del personal, registro de huellas, contraseña o tarjeta, mantenimiento de la información del personal, y establece el modo de operación, horario, y vacaciones para un turno individual y mensajes privados de empleados.

Paso 7: Agregue las terminales de asistencia, configure la información básica del dispositivo, y sincronice la información en dispositivos.

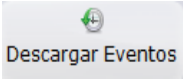
Paso 8: Calcule el resultado de la asistencia basada en el código de pago, horarios, salidas, registros y excepciones en calcular.

Paso 9: Administre los reportes de asistencia del personal en Reportes

Descargar registro de asistencia

Puede descargar los registros de asistencia desde el dispositivo al sistema.

Dar clic en 

dar clic en 

se muestra la pantalla de descarga de eventos.

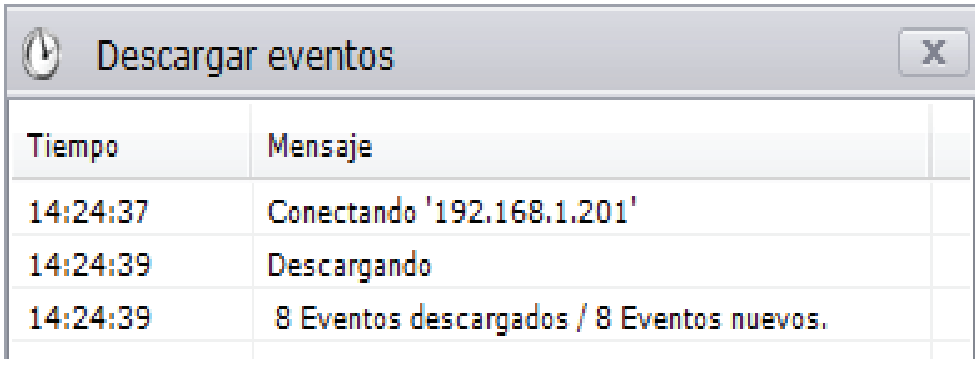
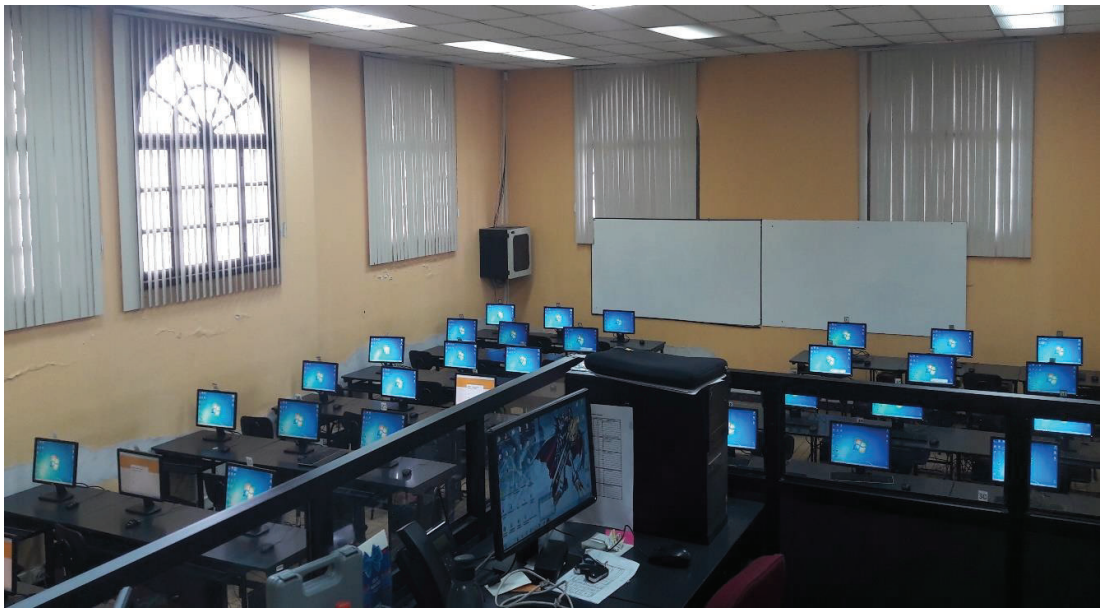


Figura 5 Descarga de eventos

Anexo VI

MANUAL DE MANTENIMIENTO DEL SISTEMA

IMPLEMENTACIÓN DE UN SISTEMA DE SEGURIDAD MEDIANTE CÁMARAS IP Y BIOMETRÍA PARA LA SALA MARCELO DÁVILA DE LA ESFOT



Sala Marcelo Dávila de la ESFOT-EPN

INTRODUCCIÓN

El sistema de seguridad está implementado en la sala Marcelo Dávila de la Escuela de Formación de Tecnólogos de la Escuela Politécnica Nacional, que está constituido por dos cámaras IP de marca HIKVISION y un biométrico de marca AZ-FACE-400. Permite el monitoreo local y remoto de la sala Marcelo Dávila a través de internet y a su vez permite el registro de usuarios administradores mediante el biométrico.

La información de almacenamiento de video y de registro se ubica en un disco de 1TB instalado en el servidor principal de la sala Marcelo Dávila.

OBJETIVO DEL MANUAL

- Mostrar los datos técnicos y de funcionamiento del sistema en general para facilitar la modificación, actualización o mantenimiento de los equipos que comprenden el sistema.
- Facilitar la información técnica para que en el proceso de mantenimiento se pueda leer, interpretar y volver a reconfigurar el sistema con el fin de solventar problemas de índole técnico.

DIAGRAMA ESQUEMÁTICO

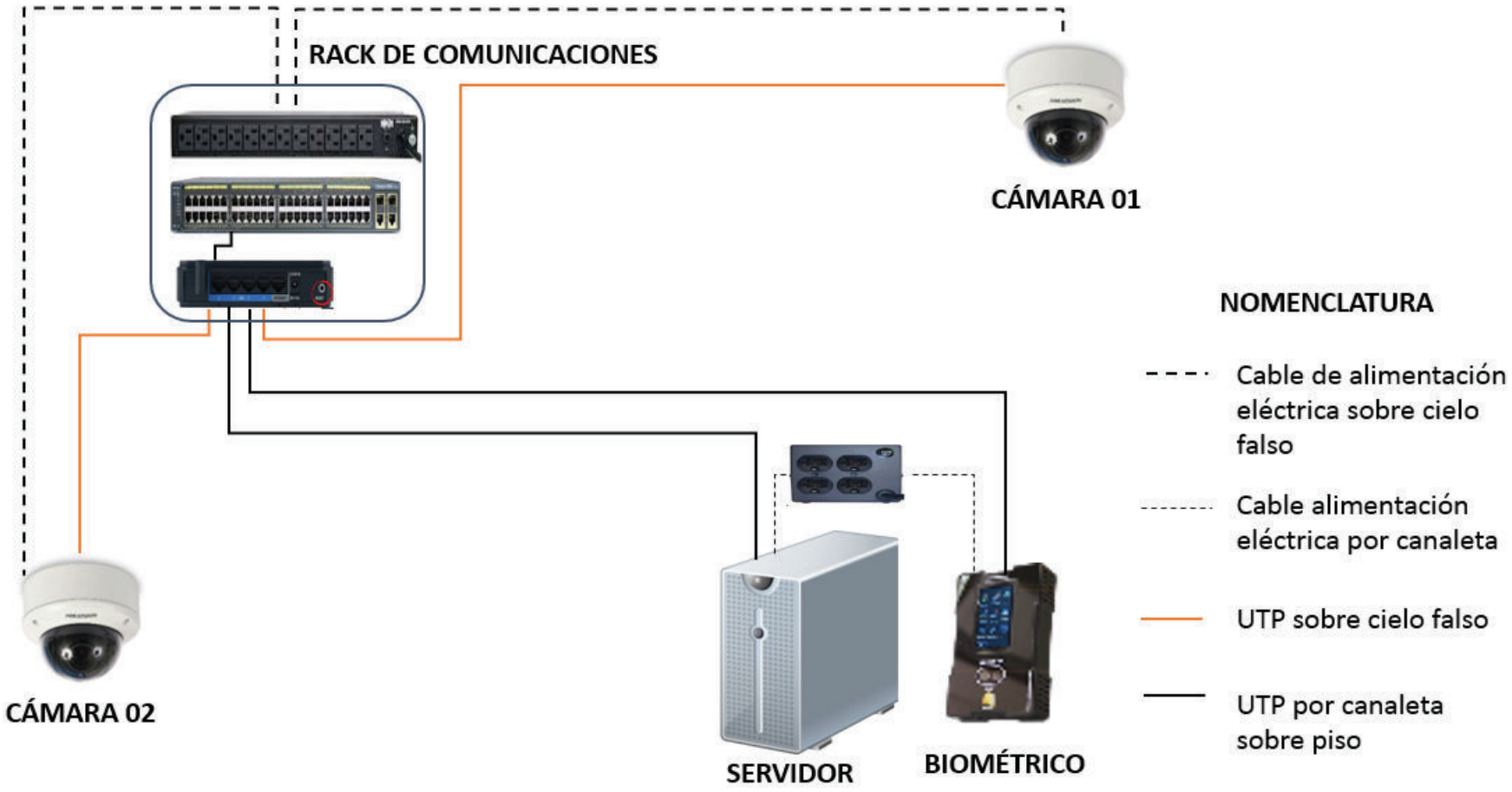


Figura 1 Diagrama esquemático

DIAGRAMA DE RED

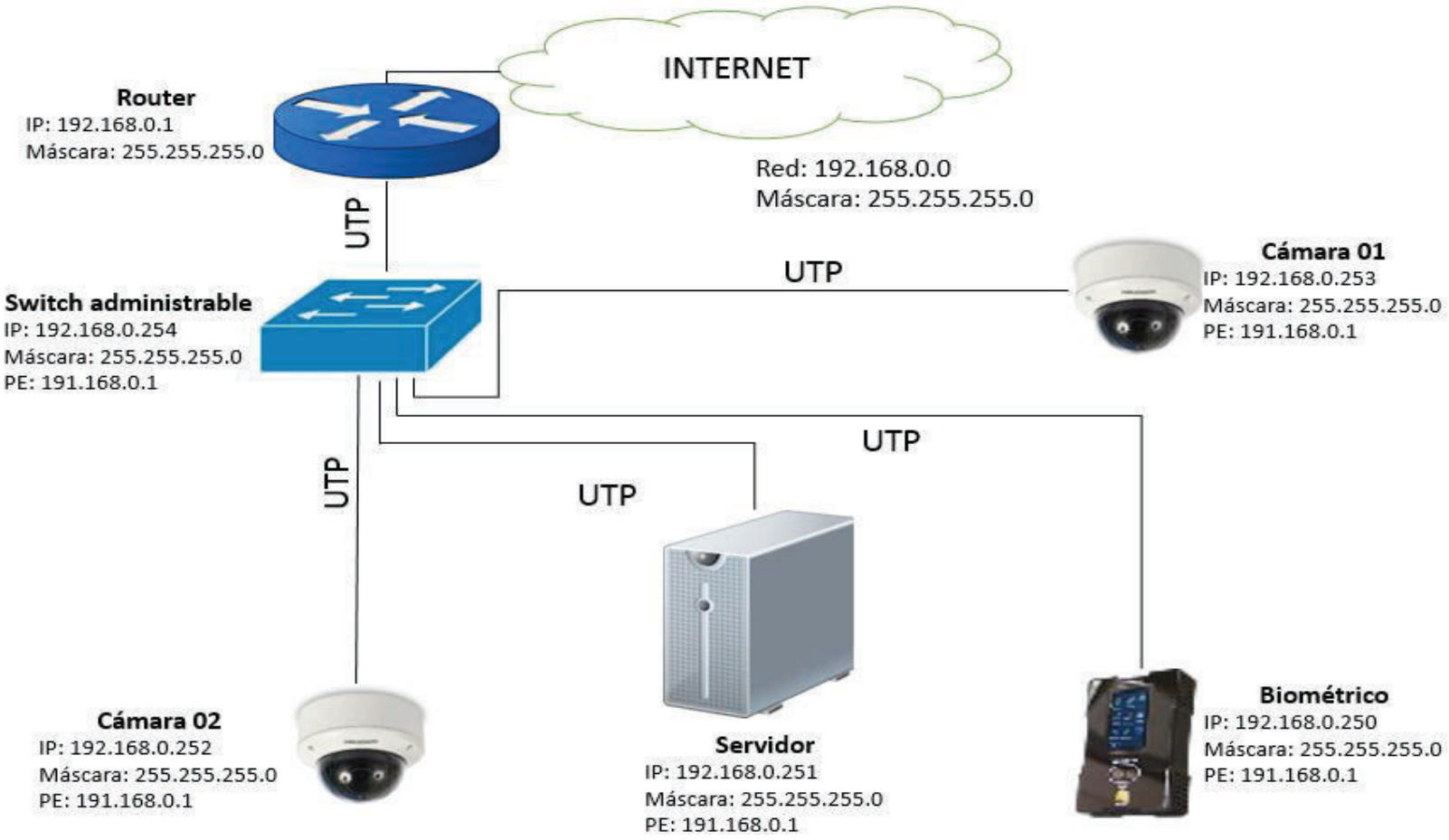


Figura 2 Diagrama de red

GUÍA DE MANTENIMIENTO

Las cubiertas de las cámaras deben ser limpiadas para evitar filtración de polvo y suciedad lo cual puede causar imágenes de video con defecto.

- Desconecte los cables de alimentación de las cámaras en el rack de comunicaciones y acceda a los equipos utilizando una escalera.
- Utilice una herramienta destornillador tipo T para abrir la carcasa o cubierta de las cámaras.
- Limpie la cubierta tipo cúpula de la cámara interna y externamente.
- Vuelva a colocar la cubierta y conecte los equipos, revise en el monitor su funcionamiento.

El equipo biométrico tiene un interfaz táctil evite limpiar la pantalla con paños húmedos o mojados.

- Limpie la pantalla táctil solamente con paños secos.
- Evite la exposición la luz o reflejo.
- Para el registro mire fijamente hacia el panel tal como lo indica el dispositivo (mediante audio).
- Si tiene problemas en la autenticación solicite al administrador se vuelva a registrar su patrón facial.

GUÍA DE SOLUCIÓN DE PROBLEMAS

Puede realizar estos procedimientos como guía de solución rápida a inconvenientes técnicos.

- Utilice el diagrama esquemático para ubicar el cableado físico.
- Verifique los cables de alimentación eléctrica en el rack de comunicaciones.
- Verifique los cables de alimentación eléctrica en el punto eléctrico ubicado cerca a los equipos.
- Utilice un multímetro y verifique que marque el voltaje apropiado en el adaptador de corriente de los equipos (12V, 1A).
- Utilice un tester y verifique que el cable UTP este correcto.

COMUNICACIÓN CON LAS CÁMARAS IP

Es probable que tenga que reiniciar las cámaras IP para restablecer la comunicación en caso de fallas del sistema.

REINICIO DE CÁMARAS

Abra un navegador web internet Explorer de preferencia y escriba la dirección IP de la cámara correspondiente (refiérase al diagrama de red)

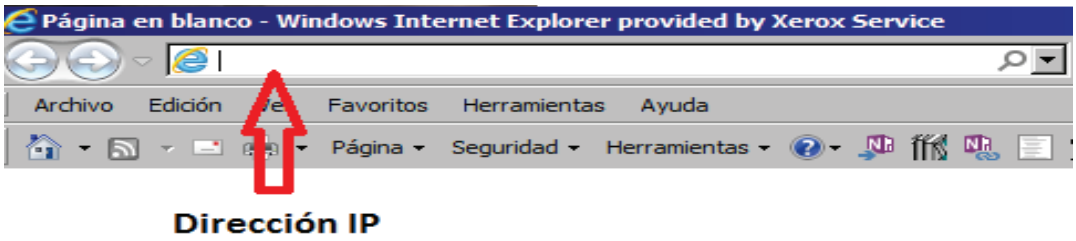


Figura 3 acceso vía web browser

Escriba el usuario, contraseña y presione iniciar sesión

Figura 4 acceso a las cámaras

Vaya a la pestaña configuración > configuración básica > sistema > mantenimiento.

- Reinicie el dispositivo

Figura 5 reinicio de cámara IP

IMPORTANTE: Antes de realizar este procedimiento revise “EXPORTAR FICHERO DE COFIGURACIÓN”.

RESTABLECER PARÁMETROS

Puede reestablecer los parámetros a modo predeterminado excepto la dirección IP.

Puede reestablecer todos los parámetros a modo predeterminado.

- Vaya a la pestaña configuración > configuración básica > sistema > mantenimiento.
- Seleccione restaurar o Por defecto.

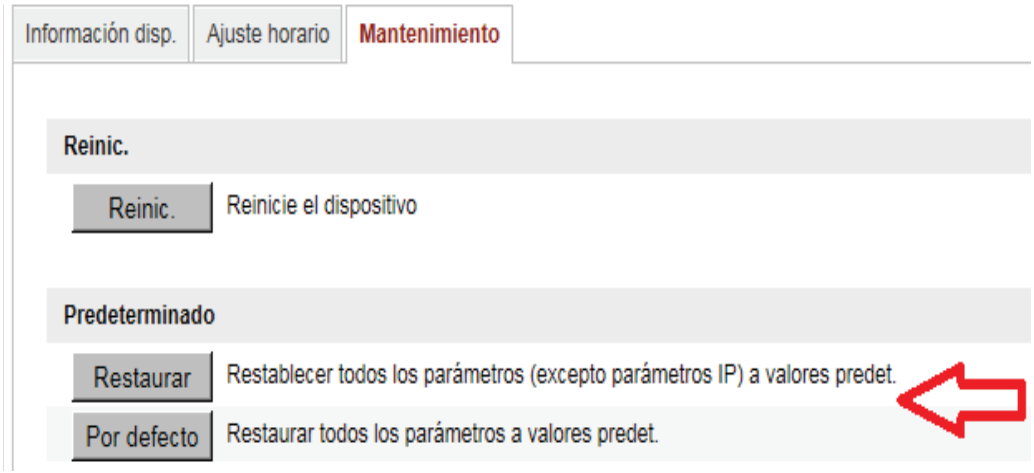


Figura 6 restablecer parámetros generales

FICHERO DE CONFIGURACIÓN

Esta función permite guardar un archivo de configuración el cual puede ser cargado luego de restablecer todos los valores de la cámara IP.

EXPORTAR FICHERO DE CONFIGURACIÓN

- Vaya a la pestaña configuración > configuración básica > sistema > mantenimiento.
- Ubique la pestaña exportar, coloque un nombre y guarde el archivo.

Figura 7 exportar fichero de configuración

IMPORTAR FICHERO DE CONFIGURACIÓN

- Vaya a la pestaña configuración > configuración básica > sistema > mantenimiento.
- Ubique la pestaña navegador y ubique el archivo antes guardado en su computador.

Figura 8 importar fichero de configuración

- Seleccione importar y aceptar reiniciar

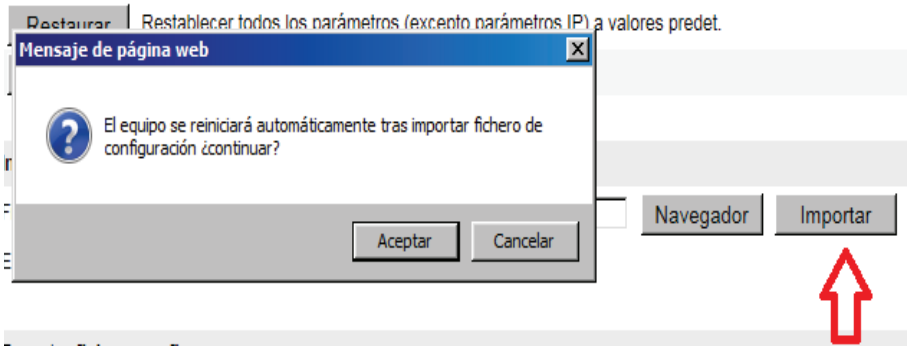


Figura 9 importar fichero y reinicio de equipo

- Si ha perdido el fichero de configuración y desconoce la configuración de las cámaras IP refiérase a 3.13 Configuración de cámaras.

INSTALACIÓN DE SOFTWARE IVMS-4200 PCNVR

Si por problemas técnicos tiene que instalar nuevamente el programa de monitoreo IVMS-4200 PCNVR.

- Descargue el programa de la plataforma de HIKVISION.
- Verifique que el disco duro reconozca como una unidad de almacenamiento nueva en el computador.
- Instale el programa nuevamente refiérase a 3.21 Monitoreo local > Monitoreo local vía software IVMS-4200 PCNVR para la creación de usuarios y contraseñas.
- Cree el usuario administrador.
- Una guía de instalación rápida (Wizard) le ayudará a configurar el sistema.

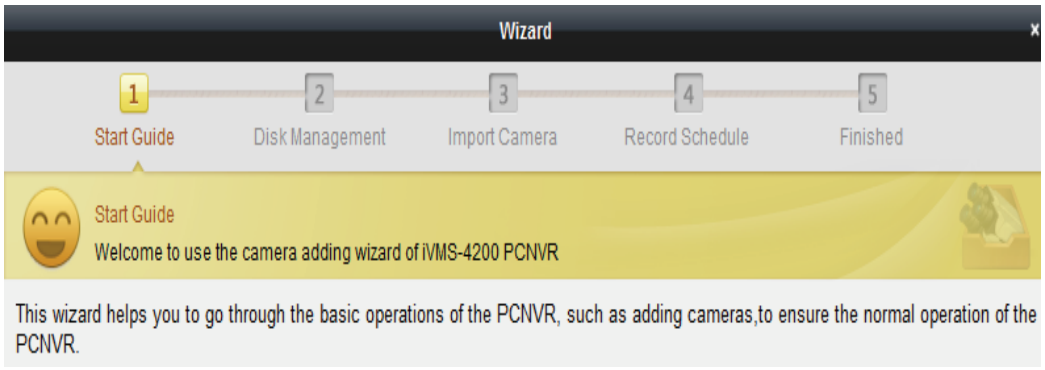


Figura 10 guía de instalación IVMS-4200

- En la administración de disco seleccione la partición asignada y presione “Pre-allocate”

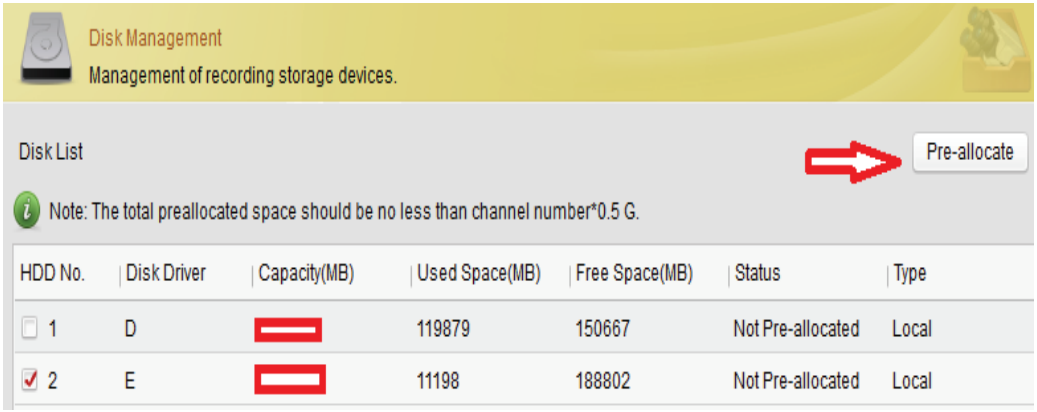


Figura 11 Asignación de unidad de disco duro

- Importar cámaras hacia el software, seleccione online detection, si no puede visualizar las cámaras, seleccione IP/Domain y escriba la dirección IP (refiérase al diagrama de red) escriba el password correspondiente para agregar las cámaras.

Figura 12 Importación de cámaras IP

- Configure el horario de grabación refiérase a la tabla 9 Horarios de grabación del sistema.
- La configuración ha finalizado. Refiérase a al anexo IV manual de uso del software IVMS 4200 PCNVR para conocer a detalle sus funciones.

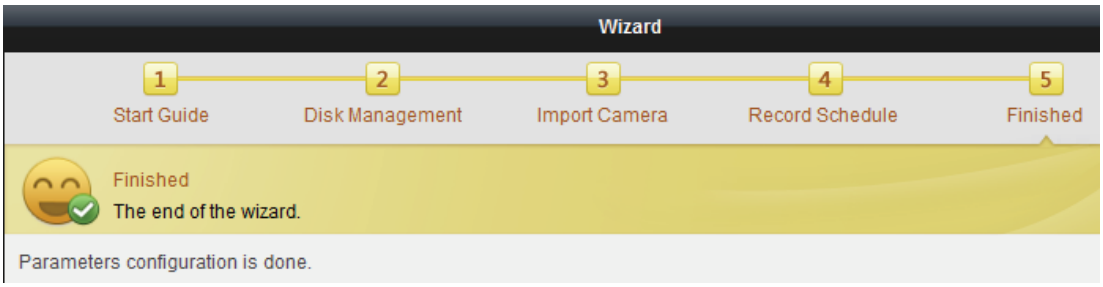


Figura 13 Instalación finalizada

BIOMÉTRICO

El dispositivo biométrico trabaja con el software ZKTIMENET el cual es instalado en el servidor principal. La gestión, registro y uso únicamente se la realiza con este software. Para realizar la configuración del software refiérase al anexo V manual de uso del software del biométrico ZKTIMENET.

Descargue el software del proveedor en http://www.idconsultants.us > descargas > asistencia > ZKTIMENET_LITE.