

# **ESCUELA POLITÉCNICA NACIONAL**

## **ESCUELA DE FORMACIÓN DE TECNÓLOGOS**

### **IMPLEMENTACIÓN DE UNA RED DE VIDEO PORTEROS IP EN LA ZONA B DE LAS OFICINAS DE PROFESORES DE LA ESFOT**

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

**DAVID EDUARDO DÍAZ POMA**  
**david.diaz04@epn.edu.ec**

**JORGE DAVID SARANGO LOZADA**  
**jorge.sarango@epn.edu.ec**

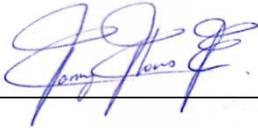
**DIRECTOR: ING. FANNY PAULINA FLORES ESTÉVEZ, MSC.**  
**fanny.flores@epn.edu.ec**

**CODIRECTOR: ING. FABIO MATÍAS GONZÁLEZ GONZÁLEZ, MSC.**  
**fabio.gonzalez@epn.edu.ec**

**QUITO, Mayo 2020**

## CERTIFICACIÓN

Certificamos que el presente trabajo fue desarrollado en su totalidad por DAVID EDUARDO DÍAZ POMA y JORGE DAVID SARANGO LOZADA, bajo nuestra supervisión.



---

Ing. Fanny Flores, MSc.

**DIRECTORA DEL PROYECTO**

---

Ing. Fabio González, MSc.

**CODIRECTOR DEL PROYECTO**

## DECLARACIÓN

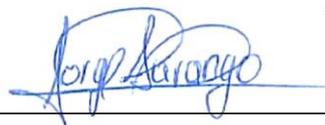
Nosotros, David Eduardo Díaz Poma y Jorge David Sarango Lozada, declaramos bajo juramento que el trabajo aquí descrito es de nuestra autoría; que no ha sido previamente presentado para ningún grado o calificación profesional; y, que hemos consultado las referencias bibliográficas que se incluyen en este documento.

Sin perjuicio de los derechos reconocidos en el primer párrafo del artículo 114 del Código Orgánico de la Economía Social de los Conocimientos, Creatividad e Innovación -COESC-, somos titulares de la obra en mención y otorgamos una licencia gratuita, intransferible y no exclusiva de uso con fines académicos a la Escuela Politécnica Nacional. Entregaremos toda la información técnica pertinente. En el caso de que hubiese una explotación comercial de la obra por parte de la EPN, se negociará los porcentajes de los beneficios conforme lo establece la normativa vigente.



---

David Eduardo Díaz Poma  
CI: 1721349981



---

Jorge David Sarango Lozada  
CI: 1722315312

## DEDICATORIA

Este trabajo se lo dedico a mis padres, las personas a quienes más admiro y quiero, me han apoyado incondicionalmente y con sus enseñanzas han hecho de mi la persona que soy hoy en día. A ustedes debo todos mis logros; gracias por su esfuerzo, ejemplo y paciencia. Su apoyo y su amor han sido el motor principal para poder finalizar un sueño más.

A mis hermanos y al resto de mi familia, que han aportado con un granito de arena con su amistad, ejemplo, consejos y en especial con su apoyo incondicional.

Jorge David Sarango

El presente trabajo va dedicado a mi familia, a mis hermanos Romel, Anahí y especialmente a mi madre quien ha sido un gran ejemplo a seguir, brindando su apoyo incondicional en los momentos más difíciles, ofreciendo todo su amor y sus enseñanzas para forjar la persona que soy hoy en día.

A mi abuela Yolanda quien siempre estuvo para mí cuando más la necesitaba sin importar las circunstancias.

David Díaz

## AGRADECIMIENTO

A mis padres Jorge y Lucía, quienes han llenado todos mis días de amor y alegría, por todo el esfuerzo que han dedicado para que pueda perseguir mis sueños y cumplir una de mis más anheladas metas.

A mis hermanos, Gaby y Andrew por su cariño y apoyo incondicional. A toda mi familia por parte de padre y madre, por su motivación y consejos, que siempre me daban ese pequeño empujón para seguir luchando por este sueño.

A todos los amigos que he tenido durante este periodo, amigos de prepo, que a pesar de los años han estado siempre apoyándome, amigos que conocí en el trayecto de la carrera, que más que amigos son mi segunda familia. No pretendo dar nombres, pues cada uno de ellos sabe quiénes son, amigos que llevaré siempre en el corazón ya que han estado en los momentos de alegría y más aún en los de tristeza. Gracias por su gran amistad y por todas las experiencias compartidas. Espero siempre poder contar con ustedes.

A todos los profesores que me han aportado con su conocimiento a lo largo de toda esta travesía, en especial a la Ing. Fanny Flores quien ha sido una enorme guía durante gran parte de mi periodo académico en la EPN. Ha demostrado ser una gran persona, ganándose mi admiración. Gracias por sus palabras, consejos y grandes enseñanzas.

Jorge David

A la Escuela de Formación de Tecnólogos, por haberme permitido formarme como un profesional dentro de sus aulas, gracias a todas las personas que formaron parte de ese proceso de enseñanza y aprendizaje.

A todos mis maestros que me brindaron su sabiduría y conocimiento necesario para forjarme como una mejor persona, gracias por su paciencia, consejos y todo su esfuerzo dentro y fuera de las aulas, para ayudarme a llegar a donde me encuentro en estos momentos.

A mi madre y mi abuela quienes siempre estuvieron para mí sin importar la circunstancia, brindándome todo apoyo y cariño para que logre salir adelante.

David Díaz

# CONTENIDO

CERTIFICACIÓN .....	I
DECLARACIÓN .....	II
DEDICATORIA .....	III
AGRADECIMIENTO .....	IV
CONTENIDO .....	V
ÍNDICE DE FIGURAS .....	VII
ÍNDICE DE TABLAS .....	IX
ÍNDICE DE ECUACIONES .....	X
RESUMEN .....	XI
ABSTRACT .....	XII
<b>1. INTRODUCCIÓN .....</b>	<b>1</b>
<b>1.1. Marco Teórico .....</b>	<b>2</b>
<i>Hardware</i> .....	2
Estándar 802.3af PoE .....	6
Modelo TCP/IP .....	7
Sistema de Cableado Estructurado.....	8
Conexión mediante un servidor P2P .....	11
Protocolo VoIP.....	12
Codificación QR.....	13
Mifare.....	15
<i>Software</i> .....	16
<b>2. METODOLOGÍA.....</b>	<b>18</b>
<b>2.1 Método Exploratorio .....</b>	<b>18</b>
<b>2.2 Método Analítico .....</b>	<b>18</b>
<b>2.3 Método Aplicado y Experimental.....</b>	<b>19</b>
<b>3. RESULTADOS Y DISCUSIÓN .....</b>	<b>20</b>
<b>3.1 Análisis de la infraestructura de la zona B de oficinas de docentes. ....</b>	<b>20</b>
<i>Hardware</i> de red .....	20
<i>Hardware</i> de intercomunicación.....	20
Alimentación eléctrica .....	20

<b>3.2</b>	<b>Requerimientos para la red de video porteros IP</b> .....	21
<b>3.3</b>	<b>Diseño del cableado estructurado</b> .....	<b>21</b>
<b>3.4</b>	<b>Diseño de la red de video porteros IP</b> .....	22
<b>3.5</b>	<b>Implementación del cableado estructurado</b> .....	22
	Adquisición del <i>hardware</i> de red.....	22
	Adquisición del <i>hardware</i> de intercomunicación.....	23
	Instalación del cableado estructurado` .....	25
<b>3.6</b>	<b>Implementación de la red de video porteros IP</b> .....	28
	Instalación de monitores de video portero IP .....	28
	Instalación del sistema IP para multiapartamentos .....	30
	Activación y configuración de equipos .....	32
<b>3.7</b>	<b>Pruebas de funcionamiento</b> .....	37
<b>3.8</b>	<b>Costos</b> .....	41
<b>4.</b>	<b>CONCLUSIONES Y RECOMENDACIONES</b> .....	42
<b>4.1</b>	<b>Conclusiones</b> .....	42
<b>4.2</b>	<b>Recomendaciones</b> .....	44
<b>5.</b>	<b>REFERENCIAS BIBLIOGRÁFICAS</b> .....	45
	<b>ANEXOS</b> .....	48

## ÍNDICE DE FIGURAS

<b>Figura 1.1.</b> Sistema IP Hikvision DS-KD3002-VM .....	2
<b>Figura 1.2.</b> Monitor IP Hikvision DS-KH-6310-WL .....	3
<b>Figura 1.3.</b> Distribuidor de audio y video Hikvision DS-KAD612 .....	4
<b>Figura 1.4.</b> Protector de voltaje 120V/10A Multimatic .....	5
<b>Figura 1.5.</b> Conexión en un Sistema PoE.....	7
<b>Figura 1.6.</b> Cable de Par Trenzado de 4 pares.....	9
<b>Figura 1.7.</b> Cable Par Trenzado UTP .....	10
<b>Figura 1.8.</b> Estándar T-568B .....	11
<b>Figura 1.9.</b> Esquema de conexión de un servidor P2P .....	12
<b>Figura 1.10.</b> Ejemplo Micro Código QR .....	14
<b>Figura 1.11.</b> Ejemplo Código iQR.....	14
<b>Figura 1.12.</b> Administración de equipos en el <i>software</i> iVMS-4200 3.1.1 .....	17
<b>Figura 2.1.</b> Implementación Videoportero IP Hikvision .....	18
<b>Figura 3.1.</b> Instalación de una caja de paso .....	25
<b>Figura 3.2.</b> Ponchado del cableado estructurado .....	25
<b>Figura 3.3.</b> Testeo del ponchado del cableado .....	26
<b>Figura 3.4.</b> Etiquetado del cableado estructurado .....	26
<b>Figura 3.5.</b> Montaje de canaletas .....	27
<b>Figura 3.6.</b> <i>Rack</i> del área de oficinas 2 .....	27
<b>Figura 3.7.</b> Cajas de soporte para pared .....	28
<b>Figura 3.8.</b> Soporte de Equipo.....	29
<b>Figura 3.9.</b> Comprobación del funcionamiento del monitor .....	29
<b>Figura 3.10.</b> Soporte metálico .....	30
<b>Figura 3.11.</b> Alimentación de la placa.....	31
<b>Figura 3.12.</b> Protección metálica de la placa .....	31
<b>Figura 3.13.</b> Activación y configuración de equipos .....	32
<b>Figura 3.14.</b> Activación de equipos.....	32
<b>Figura 3.15.</b> Configuración de red en los equipos .....	33
<b>Figura 3.16.</b> Nombres de los dispositivos .....	33
<b>Figura 3.17.</b> Asignación de extensión.....	34
<b>Figura 3.18.</b> Directorio de contactos.....	35
<b>Figura 3.19.</b> Grupos de personas .....	35
<b>Figura 3.20.</b> Creación de usuarios para el control de acceso .....	36
<b>Figura 3.21.</b> Vinculación de tarjetas de acceso a usuarios .....	36

<b>Figura 3.22.</b> Grupos de acceso .....	36
<b>Figura 3.23.</b> Concesión de permisos a usuarios.....	37
<b>Figura 3.24.</b> Prueba de comunicación entre placa y monitor .....	38
<b>Figura 3.25.</b> Prueba de comunicación con <i>Hik Connect</i> .....	39

## ÍNDICE DE TABLAS

<b>Tabla 1.1.</b> Especificaciones del sistema IP Hikvision DS-KD3002-VM.....	2
<b>Tabla 1.2.</b> Especificaciones del monitor IP DS-KH-6310-WL.....	4
<b>Tabla 1.3.</b> Especificaciones del distribuidor de audio y video Hikvision DS-KAD612 .....	5
<b>Tabla 1.4.</b> Características técnicas del protector de voltaje Multimatic .....	6
<b>Tabla 3.1.</b> Requerimientos y funciones para la red de video porteros IP.....	21
<b>Tabla 3.2.</b> Elementos de <i>hardware</i> de red con sus respectivas funciones .....	23
<b>Tabla 3.3.</b> Comparativa de equipos analizados en el mercado .....	23
<b>Tabla 3.4.</b> Verificación de apertura desde los monitores.....	38
<b>Tabla 3.5.</b> Verificación de comunicación entre monitores .....	39
<b>Tabla 3.6.</b> Apertura desde la aplicación <i>Hik Connect</i> .....	40
<b>Tabla 3.7.</b> Apertura con tarjetas Mifare .....	40
<b>Tabla 3.8.</b> Costos Referenciales .....	41

## ÍNDICE DE ECUACIONES

<b>Ecuación 3.1.</b> Longitud promedio de cable UTP .....	22
---	----

## RESUMEN

El presente documento se basa en el diseño, implementación y pruebas de funcionamiento de la red de video porteros IP instalada en la zona B de las oficinas de docentes de la Escuela de Formación de Tecnólogos (ESFOT).

La primera sección detalla la problemática detectada con relación al sistema de acceso anterior existente en el área de docentes de la ESFOT. Se plantea una posible solución a través del uso de tecnología moderna. Adicionalmente, se detallan requerimientos de la red, características y la teoría que sustenta el contenido desarrollado en este trabajo.

La segunda sección presenta la metodología aplicada y los datos técnicos que se recopilaron mediante un análisis e investigación para posteriormente desarrollar el diseño e implementación de la red de video porteros IP.

La tercera sección detalla los resultados y discusión; en un inicio se presenta el análisis de requerimientos de la red, seguido del diseño e implementación. Finalmente, se realizan las pruebas necesarias y correcciones para garantizar el óptimo funcionamiento de la red implementada.

La cuarta y quinta sección presentan las conclusiones y recomendaciones generadas tras la implementación de la red, así como las fuentes bibliográficas que respaldan el marco teórico.

Por último, en la sexta sección se presentan los anexos necesarios para facilitar la administración de la red con documentación como: planos, diagramas de red, manuales de administración y de usuario, entre otros.

**PALABRAS CLAVE:** video portero IP, control de acceso, red LAN.

## **ABSTRACT**

*The current document focuses on the design, implementation and functional tests of the IP video doorphone network installed in zone B of teachers' offices of Training School of Technologists (ESFOT).*

*The first section details the problems detected in relation to the previous access control system in the ESFOT teachers area. A possible solution is proposed through the use of modern technology. In addition, network requirements, characteristics and the theory that supports the content developed in this work are detailed.*

*The second section presents the applied methodology and the technical data that was collected through analysis and research in order to carry out the design and implementation of the IP video doorphone network.*

*The third section details the results and discussion; initially presenting the network requirements analysis, followed by the design and implementation. Finally, the necessary tests and corrections are carried out to guarantee the optimal functioning of the implemented network.*

*The fourth and fifth sections include the conclusions and recommendations generated after the implementation of the network, as well as the bibliographic sources that support the theoretical framework.*

*Finally, the sixth section presents the necessary annexes to facilitate the administration of the network with documentation such as: plans, network diagrams, administration and user manuals, and others.*

**KEY WORDS:** *IP video doorphone, access control, LAN network*

# 1. INTRODUCCIÓN

La ESFOT cuenta con un área extensa de oficinas de Docentes, las mismas que se encuentran divididas en distintas áreas y a su vez son separadas por estructuras internas. Previo a la implementación del presente proyecto, los docentes únicamente podían acceder al área de oficinas mediante una llave asociada al sistema de apertura instalado. Lo que representaba un punto de inseguridad, debido a que esta llave podía ser usurpada o en el peor de los casos duplicada, ocasionando que cualquier persona pueda ingresar al área sin control de ningún tipo.

El equipo de citofonía que se encontraba previo a la implementación del presente proyecto en la parte externa de las oficinas, era antiguo y ya había cumplido su vida útil. Esto se lo podía evidenciar por su limitado funcionamiento, debido a que la calidad y legibilidad del audio no eran adecuadas; además presentaba ruido y distorsión durante la comunicación, lo que generaba problemas en la interacción entre estudiante y profesor.

Como una solución, se propone implementar un sistema de intercomunicación acorde a las nuevas tecnologías, junto con un control de acceso a las oficinas de los docentes de la ESFOT, con la finalidad de mejorar la calidad de comunicación entre usuarios; a la vez modernizar el sistema de acceso a las oficinas.

Se pretende instalar un sistema de video porteros IP mediante la creación de una red, con el afán de optimizar recursos y obtener más beneficios. Por ejemplo, el uso de una aplicación móvil que permita la comunicación con el docente sin necesidad de que se encuentre en su oficina. También, que el estudiante pueda dejar un recado para el docente en casos que lo ameriten; de la misma manera, emplear tecnología MIFARE para que el personal autorizado pueda ingresar al área de oficinas, sin necesidad de utilizar la llave.

Consecuentemente, es necesario realizar un estudio del área en donde se va a instalar los equipos, identificar los requerimientos del sistema, diseñar los planos y conexiones esenciales, determinar las especificaciones técnicas de los elementos y equipos necesarios. En base a ello, se genera un presupuesto de referencia.

## 1.1. Marco Teórico

- **Hardware**

- **Sistema IP para multiapartamentos Hikvision DS-KD3002-VM**

En la Figura 1.1 se muestra el sistema IP para multiapartamentos DS-KD3002-VM de la marca Hikvision, este equipo es recomendado para oficinas, departamentos y edificios residenciales. El equipo cuenta con comunicación TCP/IP, vista en vivo, control de acceso a través de tarjetas Mifare (soporta hasta 2500 tarjetas). Por otra parte, soporta hasta 254 equipos terminales. Además, es compatible con el *software* de administración y configuración iVMS4200 [1].



**Figura 1.1.** Sistema IP Hikvision DS-KD3002-VM [1]

Las especificaciones más relevantes del sistema se detallan en la Tabla 1.1.

**Tabla 1.1.** Especificaciones del sistema IP Hikvision DS-KD3002-VM [2]

CARACTERÍSTICA	DESCRIPCIÓN
Cámara	1.3 MP HD a color
Estándar de compresión de video	H.264
Resolución de video	1280 x 720
Cuadros de video por segundo	PAL: 25 fps, NTSC: 30 fps

Continúa →

Pantalla	3.5 pulgadas LCD a color
Estándar de compresión de audio	G.711 U
Tasa de compresión de audio	64 kbps
Comunicación	TCP/IP, RTSP
Fuente de alimentación	12(VDC), 1,5(A)
Temperatura de operación	-40(°C) a 60(°C)
Humedad de operación	10% a 90%
Nivel de protección IP	IP65
Dimensiones	357(mm) x 124(mm) x 55(mm)

- **Monitor de video portero IP Hikvision DS-KH-6310-WL**

Es un sistema simple y eficaz de comunicación local. Este equipo funciona con videoporteros y otros paneles que operan dentro de la gama de equipos IP Hikvision. Este módulo también es usado como panel de control de alarmas. Además, es compatible con el *software* de configuración iVMS4200 y puede trabajar con la aplicación *Hik Connect* para dispositivos móviles. En la Figura 1.2 se muestra el monitor IP Hikvision DS-KH-6310-WL [3].



**Figura 1.2.** Monitor IP Hikvision DS-KH-6310-WL [4]

Las características técnicas del monitor se detallan en la Tabla 1.2.

**Tabla 1.2.** Especificaciones del monitor IP DS-KH-6310-WL [4]

CARACTERÍSTICA	DESCRIPCIÓN
Pantalla	LCD a color de 7 pulgadas
Resolución	800 x 480
Estándar de compresión de audio	G.711 U
Tasa de compresión de audio	64 kbps
Comunicación	TCP/IP, RTSP
Entradas de Alarmas	2 CH de entrada para sensores de alarmas
Fuente de alimentación	12(VDC) ó 24(VDC) PoE
Humedad de operación	10% al 90%
Temperatura de operación	-10(°C) a 55(°C)
Dimensiones	217(mm) x 142(mm) x 26(mm)
Certificación	FCC, IC, CE, C-TICK, ROHS, REACH, WEEE

- **Distribuidor de audio y video Hikvision DS-KAD612**

El distribuidor de audio y video Hikvision mostrado en la Figura 1.3 es un equipo que permite la comunicación entre los sistemas IP para multiapartamentos y los monitores. Además, gracias a que cuenta con el estándar PoE (*Power over Ethernet*) propietario, puede alimentar un máximo de 12 dispositivos conectados a él; cabe recalcar que los equipos tienen que ser de la misma marca del distribuidor (Hikvision) [5].

En la Tabla 1.3 se presenta las características relevantes de este equipo.



**Figura 1.3.** Distribuidor de audio y video Hikvision DS-KAD612 [6]

**Tabla 1.3.** Especificaciones del distribuidor de audio y video Hikvision DS-KAD612 [6]

CARACTERÍSTICA	DESCRIPCIÓN
Número de interfaces	16 interfaces de 10/100 Mbps
Estándar	IEEE802.3, IEEE802.3u, IEEE802.3x,
Tipo de procesamiento	<i>Store and Forward</i>
Fuente de alimentación	220 (VAC)
Temperatura de operación	-15(°C) a 55(°C)
Humedad de operación	5% a 95%
Dimensiones	268.6(mm) x 118.4(mm) x 102.2(mm)
Certificaciones	FCC, IC, CE, C-TICK, ROHS, REACH, WEEE

- **Protector de Voltaje 120V/10A Multimatic**

El protector de voltaje Multimatic mostrado en la Figura 1.4 es un dispositivo electrónico que protege a los equipos contra elevaciones o caídas de tensión durante la operación habitual o cuando el suministro eléctrico es restablecido después de un apagón. Este equipo verifica constantemente el estado de la red eléctrica, para permitir el funcionamiento de equipos, dentro de los niveles de energía adecuados. Si la energía fluctúa fuera del rango correcto al que operan los equipos, el protector los aísla de la conexión y espera a que el voltaje vuelva a encontrarse dentro del rango apropiado y así volver a suministrar energía a los equipos conectados [7].



**Figura 1.4.** Protector de voltaje 120V/10A Multimatic [8]

Las características técnicas del protector de voltaje se describen en la Tabla 1.4.

**Tabla 1.4.** Características técnicas del protector de voltaje Multimatic [8]

CARACTERÍSTICA	DESCRIPCIÓN
Voltaje de entrada	100(VAC) a 130(VAC)
Voltaje de salida	100(VAC) a 130(VAC)
Frecuencia	60 Hz
Temperatura de operación	Máximo 55(°C)
Humedad de operación	Menor al 85% no condensada
Dimensiones	82(mm) x 50(mm) x 28(mm)
Certificación	RETIE
Indicadores LED	Exhiben el estado del protector

- **Estándar 802.3af PoE**

La energía sobre Ethernet (*Power over Ethernet, PoE*) es una tecnología que se usa para proveer la alimentación eléctrica a una infraestructura LAN. Permite el suministro de la corriente eléctrica necesaria para el funcionamiento de un dispositivo de red (*router, switch, punto de acceso, video portero o teléfono IP, etc*) por medio del mismo cable que se utiliza para la transmisión de datos [9].

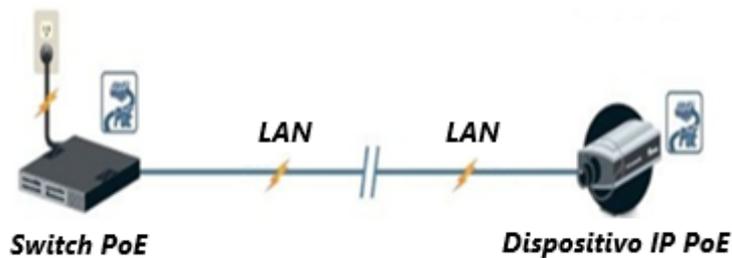
La tecnología PoE minimiza la necesidad de usar tomacorrientes en las zonas donde se localiza el dispositivo que se desea alimentar y permite una instalación más sencilla que con el cableado tradicional [9].

PoE se encuentra regulado por medio del estándar IEEE 802.3af, posee un diseño el cual permite que el rendimiento de la transmisión de datos y el alcance de la red no se vea afectado [9].

La corriente suministrada por medio del cable de datos es emitida de forma automática cuando se identifica un dispositivo compatible y se bloquea ante equipos que no sean compatibles. Esta característica permite la libertad y seguridad para diseñar una red mixta donde se mezcle equipos preexistentes con nuevos dispositivos que soporten PoE [9].

- **Ventajas de usar PoE**

- Reducción de gastos en material y en el tendido del cableado puesto que PoE utiliza el mismo cable tanto para la transmisión de datos como para la alimentación, como se observa en la Figura 1.5 [10].
- PoE facilita la ampliación o instalación de una red en una infraestructura donde resulte complicado incorporar nuevas instalaciones eléctricas [10].



**Figura 1.5.** Conexión en un Sistema PoE [9]

- **Modelo TCP/IP**

Denominado como Protocolo de Control de Transmisión y Protocolo de Internet, permite la transferencia de datos de una manera confiable, desde que los datos son enviados hasta llegar a su destino final entre equipos informáticos que se encuentran dentro de una red. Está conformado por 4 capas en forma jerárquica. Es usado en redes y corresponde al protocolo estándar de Internet [11].

- **Capas del modelo TCP/IP**

El modelo TCP/IP cuenta con 4 capas que son:

- **Capa de acceso de red:** es la primera capa del modelo, permite el acceso físico a la red utilizando un protocolo que permita enviar datagramas sobre la red [12].
- **Capa de Internet:** segunda capa en el modelo, en esta capa actúan varios protocolos como IP, ARP, ICMP, IGMP y RARP. Permiten que los datagramas lleguen a su destino utilizando una dirección IP [12].
- **Capa de Transporte:** tercera capa que permite intercomunicación entre terminales o entidades del mismo nivel, bajo esta capa trabajan dos protocolos que son: TCP,

permitiendo que los datos sean entregados sin error alguno y UDP el cual es un protocolo no confiable, utilizado para una entrega rápida de paquetes como puede ser voz y video [12].

- **Capa de Aplicación:** cuarta capa, consiste en programas de aplicación que se utilizan en una red como son TELNET, FTP, SMTP, DNS, HTTP entre otros [12].

- **Ventajas de TCP/IP**

- Apropiado para redes grandes o medianas ya sean domésticas o empresariales.
- Diseñado para una transmisión de datos segura, confiable y rápida.
- Utilizado a nivel mundial en el Internet y la mayoría de servidores *web* [12].

- **Desventajas de TCP/IP**

- No es conveniente para redes pequeñas debido a que resulta lenta, comparada con redes de mayor tráfico [12].
- Tiene un bajo rendimiento al utilizarse en servidores de archivos [12].

- **Sistema de Cableado Estructurado**

Un sistema de cableado estructurado se refiere a un sistema compuesto por cables, conectores, dispositivos y canalizaciones que conjuntamente forman la infraestructura de una red. Sus elementos son el cableado vertical, cableado horizontal, medios de transmisión y normativa [13].

- **Cableado Horizontal**

Lleva la información desde el área de distribución hasta los usuarios, esta información es enviada por los medios de transmisión como cable de par trenzado de 4 pares bajo la normativa EIA/TIA 568. Es instalado a lo largo del techo o bajo el piso. Sus principales elementos son [13]:

- Conectores de telecomunicaciones.
- Cables horizontales.
- Interconexiones localizadas en el área de distribución.

- **Cableado Vertical**

Es conocido como *backbone*, crea interconexiones entre áreas de distribución o cuartos de equipos, interconecta cuartos de equipos que se encuentren en diferentes pisos de un edificio. Está conformado por conexiones cruzadas entre equipos principales, cordones de parcheo y terminaciones mecánicas [13].

- **Medios de transmisión y conectores**

Los equipos con un sistema IP por lo regular utilizan cable de par trenzado para la transmisión de datos, audio y video, para ello es necesario el uso de conectores RJ-45, dependiendo de la categoría del cable de par trenzado se obtienen diferentes velocidades de transmisión [14].

- **Cable de par trenzado**

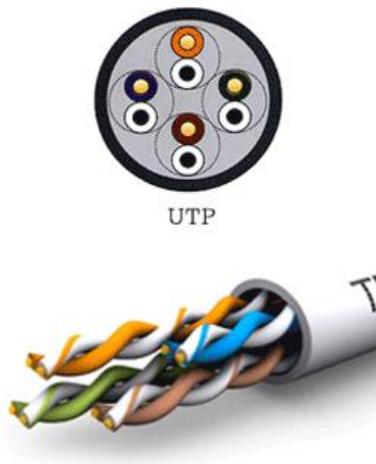
Este cable se encuentra formado por 8 hilos de alambre de cobre o aluminio, los cuales vienen recubiertos con su respectivo aislante. Para evitar interferencias y mantener las propiedades eléctricas del cable, estos vienen trenzados entre 4 pares, como se observa en la Figura 1.6 [14].



**Figura 1.6.** Cable de Par Trenzado de 4 pares [15]

- **Cable UTP (*Unshielded Twisted Pair*)**

Par trenzado no apantallado, es uno de los cables más utilizados, no tiene ningún tipo de protección extra, con una impedancia característica de 100 ohmios, como se observa en la Figura 1.7. El conector comúnmente utilizado para este tipo de cable es el RJ-45 [16].



**Figura 1.7.** Cable Par Trenzado UTP [16]

○ **Norma EIA/TIA 568**

Esta norma establece dos tipos de estándares T568-A y T568-B, Estándar de Edificios Comerciales para Cableado de Telecomunicaciones, donde se observa las diferentes configuraciones de cada uno de los pines de los conectores RJ-45 en el cable de par trenzado [16].

- **TIA/EIA-568-A**

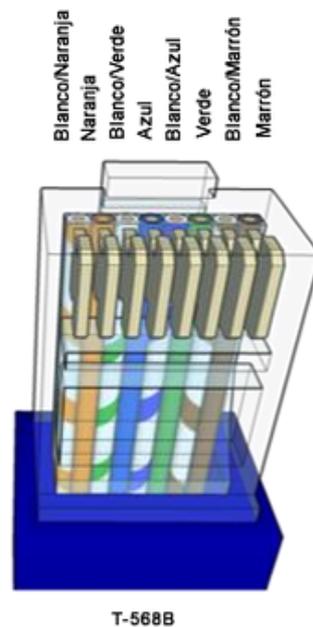
En este estándar se detalla los requisitos necesarios de cableado para telecomunicaciones como son: topología y límites de distancia, conectores utilizables y asignaciones de los pines. Este estándar es reemplazado por TIA/EIA-568-B [17].

- **TIA/EIA-568-B**

Estándar que describe los requisitos de componentes y de transmisión en los siguientes apartados [17]:

- TIA/EIA-568-B.1 especifica un sistema de cableado de telecomunicaciones genérico para edificios comerciales [17].
- TIA/EIA-568-B.2 especifica los componentes de cableado, de transmisión, los modelos de sistemas y los procedimientos de medición, para la verificación del cableado de par trenzado [17].
- TIA/EIA-568-B.3 especifica los componentes y requisitos de transmisión para un sistema de cableado de fibra óptica [17].

Para generalizar la disposición o configuración del orden de los cables que debe llevar un RJ45 en el ponchado, se utiliza el estándar T-568B, este se lo puede observar en la Figura 1.8 [18].



**Figura 1.8.** Estándar T-568B [18]

- **Conexión mediante un servidor P2P**

*Peer to peer* (P2P) es una conexión de red de datos entre dos equipos que se comportan como iguales entre sí. Esto quiere decir que cada uno de los equipos de la red P2P puede actuar al mismo tiempo como cliente y servidor entre todos los equipos, dependiendo de los requerimientos que estos tengan, normalmente cámaras IP o video porteros IP y el equipo terminal que se utiliza para conectarse a ellos. Para poder establecer una conexión IP, se requiere de los siguientes elementos [19]:

- Dirección IP, puertos de origen y destino (datos de los equipos que pretenden comunicarse).
- Protocolo (TCP, UDP o una combinación de ambos).

La mayoría de *firewall* o cortafuegos bloquean el ingreso del tráfico de Internet hacia la red local y permiten la salida de todo el tráfico que va desde la red local hacia Internet. Por esto, si el equipo de destino se encuentra en una red local con un *router* que da conexión a Internet a todos los equipos de la red, se debería redirigir un puerto del exterior hacia el puerto e IP local del equipo con el que se desee conectar. Con una conexión P2P esto no es necesario, puesto que, para poder acceder remotamente desde un ordenador, *smartphone* o *tablet* solo

se debe registrar los equipos en la nube del fabricante o proveedor introduciendo los datos de identificación de cada uno de los equipos [19].

Al activar la conexión P2P de los equipos, lo que se hace es registrar los dispositivos en un servidor que almacena las direcciones IP públicas de los equipos y los puertos UDP públicos que originan la conexión hacia este servidor. El servidor P2P realiza el envío de paquetes con frecuencia para que los equipos con los que se desea conectar mantengan la conexión UDP abierta. Entonces, si se desea conectar con un equipo mediante P2P, la aplicación de gestión que se utilice ya sea en un ordenador o en un equipo terminal móvil, pregunta al servidor P2P qué IP pública y qué puerto UDP utiliza el equipo requerido con número de serie. A lo que el servidor P2P responde a la aplicación de gestión con los datos necesarios y esta se conecta al equipo [19]. En la figura 1.9 se puede visualizar el esquema básico de conexión en un sistema P2P.



**Figura 1.9.** Esquema de conexión de un servidor P2P [20]

- **Protocolo VoIP**

El término VoIP significa Voz sobre Protocolo de Internet, por medio de VoIP se puede realizar llamadas de voz a través de la red en donde se utiliza un protocolo por medio del cual las ondas de sonido son convertidas en paquetes de datos. Posteriormente, estos paquetes son transmitidos por la red a otro dispositivo donde se realiza el proceso inverso para que se escuchen las ondas de audio emitidas inicialmente [21].

VoIP trabaja con una variedad de protocolos que difieren en sus características por la calidad de sus mecanismos de transmisión, su arquitectura, su disponibilidad y su grado de seguridad. Los protocolos más utilizados por VoIP son [22]:

- **SIP:** Es el protocolo de inicio de sesiones (*Session Initiation Protocol*). Este protocolo permite establecer sesiones multimedia entre usuario cliente y servidor para transmisión de voz o video. Se intercambian peticiones o respuestas entre agentes de usuario a través de un servidor *proxy*. La sintaxis que usa es parecida a la HTTP y la SMTP, que es lo que se usa en sitios *web* y servicios de correo electrónico.
- **IAX2:** Son las siglas de (*Inter-Asterisk eXchange Protocol*). Es un protocolo de código abierto que resulta más eficaz que SIP ya que los metadatos se transmiten *in-band*, lo que permite escuchar los datos por diferentes canales a la vez.
- **H.323:** Es uno de los protocolos de ITU-T (*International Telecommunication Union*). Originalmente fue creado para transportar aplicaciones multimedia en redes LAN, pero también es utilizado para voz IP. Es un protocolo que cuenta con una baja fiabilidad para videoconferencias y transmisión de voz IP.
- **MGCP:** (*Media Gateway Control Protocol*). Se caracteriza por utilizar un MGC (*Media Gateway Control*) como intermediario entre cliente y servidor. Su topología incluye tres componentes, lo que implica que la voz pasa por un controlador antes de transmitirse. Actualmente ha sido sustituido por el estándar H.248.

- **Codificación QR**

Sistema que almacena los datos codificados en forma de matriz, o código de barras bidimensional cuadrado, este puede ser impreso o digital. Son interpretados por dispositivos capaces de captar imágenes y decodificarlas [23].

La corporación japonesa Denso Wave en 1994 lo creó. El código QR es capaz de recopilar hasta 7.089 caracteres, normalmente es un cuadrado conformado con patrones oscuros y claros, además con cuadrados en tres de sus esquinas para una fácil identificación de la posición del código [23].

Su nombre viene dado por *Quick Response* o respuesta rápida, debido a que fue diseñado para obtener una alta velocidad en su decodificación. Además, es diseñado para codificar caracteres ASCII, información binaria. Una de las ventajas es que es omnidireccional el cual puede ser leído con una cámara, escáner o un *smartphone* [23].

- **Características y Aplicaciones**

- En un inicio, este tipo de código fue utilizado para el registro de repuestos de automóviles.
- Actualmente es utilizado por industrias para el manejo de información, identificación del personal, anclaje de dispositivos, acceso a información específica y detallada, etc [23].

- Permite una mayor comodidad al usuario evitando que este introduzca datos de forma manual en dispositivos móviles.
- Utilizado para brindar información al usuario como horarios o rutas de autobuses.
- Aplicado en servicios de mantenimiento o asistencia técnica.
- Autenticación de usuario.
- Herramienta publicitaria.

### ○ Tipos de Código QR

Debido a que el uso del Código QR se amplió a nivel mundial, se han creado varios tipos de Código QR como son:

- Micro código QR únicamente tiene un patrón para detectar su posición, fue diseñado por la necesidad de tener códigos más pequeños, puede ser impreso en lugares muy pequeños, se convirtió en un estándar JIS en 2004. En la Figura 1.10 se muestra un ejemplo de un micro código QR [24].



**Figura 1.10.** Ejemplo Micro Código QR [24]

- Código iQR, tiene forma de una matriz, es un código con gran capacidad comparado al ordinario código QR, debido a que puede almacenar más datos, este puede ser impreso de forma rectangular y esto permite una amplia gama de aplicaciones en diversas áreas, como se observa en la Figura 1.11 [25].



**Figura 1.11.** Ejemplo Código iQR [25].

- **Mifare**

Es una gama de tarjetas rápidas e inteligentes sin contacto, en la actualidad esta tecnología es una de las más utilizadas, bajo el estándar ISO 14443 [26].

- **ISO 14443**

Es un estándar internacional que está relacionado con tarjetas electrónicas de proximidad, que en su mayoría son utilizadas para control de acceso e identificación; este estándar está compuesto por diferentes partes como son [26]:

- Características físicas.
- Interfaz de señal y radiofrecuencia.
- Inicialización y anticolidión.
- Protocolos de transmisión.

En la parte del protocolo de transmisión, inicialización y anticolidión, se habla de 2 tipos de estándares como con el tipo A y B ubicado en la capa de enlace. Normalmente este tipo de tarjetas son utilizadas en sistemas de comunicaciones que trabajen con el estándar ISO 14443 [27].

- Permite una comunicación estándar y establece los protocolos de transmisión entre el lector y la tarjeta.
- Trabaja con una frecuencia de portadora de 13,56 MHz.
- Especifica un rango de lectura y escritura de 10 cm entre el lector y la tarjeta.
- Para evitar colisiones, trabaja a una velocidad predeterminada de 106 kbps.
- Establece protocolos de seguridad para la autenticación y tiene un microprocesador que brinda confiabilidad [27].

- **Mifare *Classic***

Existen dos tipos Mifare *Classic* 1K y 4K, fueron las primeras en el mercado presentadas por NXP *Semiconductors*, este tipo de tarjetas son las más utilizadas actualmente para controles de acceso o registro, debido a su confiabilidad y fidelidad [26].

Las versiones de estas varían dependiendo al tamaño o espacio de almacenamiento que brindan, pueden ser de 1kB o 4kB. Las funciones en ambas pueden llegar a ser las mismas, a diferencia que la tarjeta de 4kB tiene una mayor velocidad de procesamiento [26].

- **Mifare Classic 1K**

A nivel mundial, consta de 7 *bytes* como identificador único conocido como *Unique ID* (UID). La memoria se encuentra fraccionada en 16 sectores de 4 bloques; cada bloque consta de 16 *bytes*, en el bloque 0 se puede encontrar el UID y la información del fabricante [26].

- **Bloque 0,1,2:** Dentro de estos bloques se registra o se guarda información.
- **Bloque 3:** Aquí es almacenada la clave criptográfica; pueden ser de tipo A o B.

- **Software**

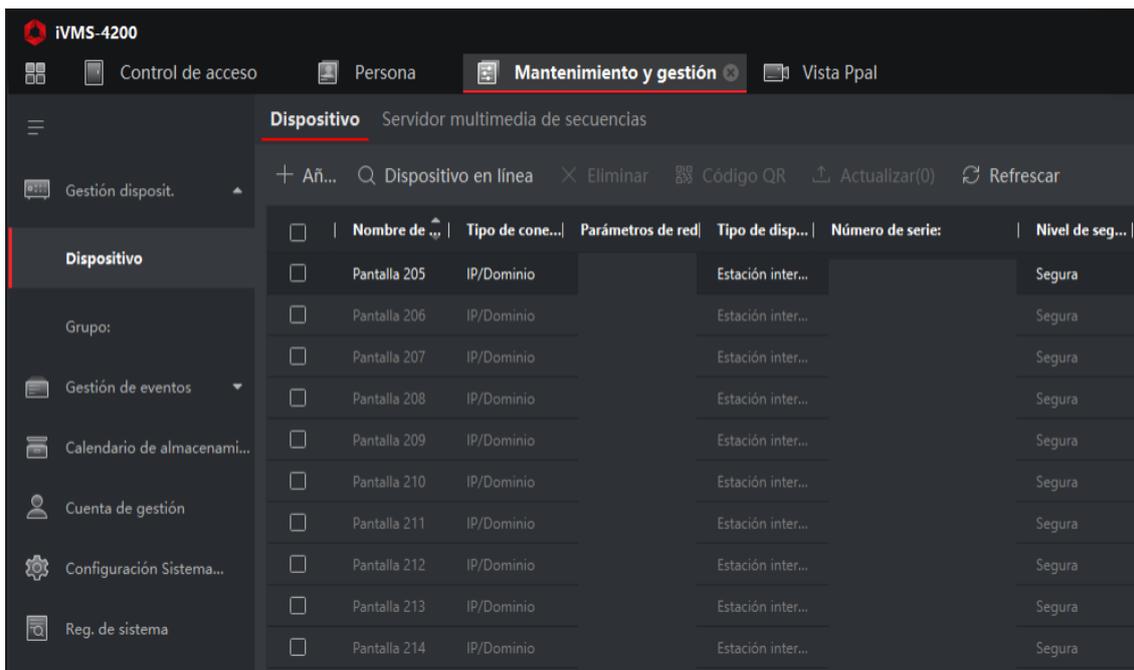
- **IVMS 4200**

Es un *software* que posee una estructura que ofrece una gestión centralizada a todos los dispositivos conectables de Hikvision, permite gestionar NVRs, DVRs, cámaras IP y decodificadores. Es un recurso ideal para ofertar soluciones de vigilancia a pequeña y mediana escala [28].

A través de distintos módulos de gestión y configuración, y una combinación razonable de estos, el *software* iVMS-4200 de Hikvision ofrece múltiples soluciones para casos de vigilancia a pequeña y mediana escala [28].

Esta plataforma es un sistema seguro y confiable ya que cuenta con protección de usuario y contraseña. Además, presenta funciones como monitoreo en tiempo real, grabación y búsqueda de video, copia de seguridad de archivos, visualización, audio de dos vías, configuración local y remota de equipos [28].

El *software* seleccionado es compatible con los sistemas operativos *Mac OS* y *Windows* ya sea de 32 o 64 bits. La figura 1.12 presenta la pantalla de la interfaz de iVMS-4200 3.1.1 *Client*.



**Figura 1.12.** Administración de equipos en el *software* iVMS-4200 3.1.1 [28]

### o **Hik Connect**

*Hik Connect* es un *software* por medio del cual se accede al uso del servicio P2P y DDNS para los equipos de Hikvision que se encarga de resolver el problema de la dirección IP privada y la escasez de DDNS y cuenta con un servidor distribuido globalmente. Este *software* permite el acceso a los distintos dispositivos de video por medio de un *smartphone* o una computadora. El *software* soporta dispositivos como DVR, NVR, IPC, PTZ y VMS, mientras que la tecnología que utiliza es *P2P Cloud*. La seguridad y privacidad están garantizadas y protegidas por HTTPS y SSL. Una vez instalada, la aplicación de *Hik Connect* permite [29]:

- Controlar dispositivos de forma remota.
- Administrar cuentas en la nube.
- Vincular los dispositivos con un *smartphone*.

La aplicación posee control de cámaras, notificaciones, video en vivo, opción de reproducción de grabación, audio bidireccional y permite administrar cuentas que están destinadas a usuarios finales [29].

## 2. METODOLOGÍA

Para el desarrollo de este proyecto se utilizó los métodos exploratorio, analítico, aplicado y experimental.

En la etapa inicial del proyecto se realizó la exploración de la zona de las oficinas de docentes de la ESFOT; posteriormente, por medio del método analítico se realizó investigaciones y con los conocimientos adquiridos se desarrolló el diseño de la red de video porteros IP. Una vez establecidos los diseños, se realizó la implementación del sistema utilizando el método aplicado. Finalmente, con el método experimental se realizó las pruebas del sistema para así poder identificar errores y realizar las respectivas correcciones hasta lograr el correcto funcionamiento del sistema. En la Figura 2.1 se presenta el diagrama de procesos de implementación de la red de video porteros IP.



**Figura 2.1.** Implementación Videoportero IP Hikvision

### 2.1 Método Exploratorio

Mediante el uso del método exploratorio se obtuvo información sobre la infraestructura física de la zona de docentes de la ESFOT, así como también se obtuvo datos sobre la estructura de red que maneja la Escuela Politécnica Nacional específicamente el área de la ESFOT y los equipos que se involucran en la misma.

### 2.2 Método Analítico

Una vez obtenida la información, aplicando la metodología analítica se determinó todos los elementos requeridos para solventar los problemas detectados en la zona B de docentes de

la ESFOT. Determinados los elementos del sistema, se procedió a seleccionar los equipos, realizando un análisis de las características físicas y técnicas de los distintos modelos encontrados en el mercado. Tomando en cuenta el presupuesto del proyecto, se escogió los equipos que mejor se acoplen a la red y además cumplan con los requerimientos del sistema.

Por medio de la metodología analítica se realizó el diseño de la red de video porteros IP, para lo cual se ha tomado en cuenta: el número de usuarios, modificaciones en las diferentes oficinas de la zona B, escalabilidad y el cableado estructurado necesario para la instalación de la red.

Todos los equipos conectados dentro de la red utilizan el protocolo TCP/IP para poder comunicarse; además, estos equipos pueden ser administrados y configurados por medio de un *software* amigable desde una PC que se encuentra conectada dentro de la misma red de los equipos instalados.

### **2.3 Método Aplicado y Experimental**

En base a la metodología aplicada, se realizó la instalación del cableado estructurado de acuerdo con la normativa investigada, esto permitió conectar todos los equipos a la red de la Escuela Politécnica Nacional. Una vez que se concluyó con la instalación del cableado estructurado, se procedió con el montaje de las estructuras de soporte para los equipos.

Con las estructuras montadas, se realizó la instalación de los monitores en cada una de las oficinas de la zona B. Posteriormente, se procedió a realizar las conexiones de alimentación para el portero de la parte exterior del área de oficinas 2 de docentes de la ESFOT, para lo cual se empleó un protector de voltaje para resguardar a los equipos de las variaciones de voltaje. Para finalizar la instalación de los equipos, se realizó el montaje de la placa exterior. Luego, se procedió con la conexión de todos los equipos al *switch* de administración y posteriormente a la red de la EPN, para lo cual se recurrió a reuniones con un representante de la Dirección de Gestión de la Información y Procesos (DGIP), quien otorgó el acceso y los permisos pertinentes para acceder a sus recursos.

Una vez finalizada la implementación de toda la red, mediante la metodología experimental, se ejecutó una evaluación de las configuraciones y del funcionamiento del sistema. De este modo, se realizó una serie de pruebas para verificar que exista una correcta comunicación entre todos los dispositivos de la red.

Con el sistema funcional, se procedió a la elaboración de manuales para la administración de los dispositivos y el uso de estos, mediante los manuales se proporcionó la información completa para un futuro escalamiento del proyecto.

### 3. RESULTADOS Y DISCUSIÓN

#### 3.1 Análisis de la infraestructura de la zona B de oficinas de docentes.

Dado que el proyecto desarrollado, constituye un proyecto macro a cargo de diez estudiantes de la carrera de Tecnología en Electrónica y Telecomunicaciones, se procedió a dividir las áreas de oficinas 2, 3 y 4 de la ESFOT en cuatro zonas: A, B, C y D. La zona B, que corresponde al presente proyecto, consta de 7 oficinas ubicadas en el área 2: 11, 12, 13, 14, 15, 16 y 17, como se observa en el **ANEXO A1**. Las oficinas se encuentran separadas por mamparas que definen los límites entre cada uno de los cubículos. Esta zona posee techo falso por encima de cada una de las oficinas.

- **Hardware de red**

Cada oficina cuenta con un punto de red simple, el cableado de cada punto se dirige hacia el techo por medio de canaletas. El cableado de cada una de las oficinas recorre el techo hasta llegar hacia el *rack* ubicado en la oficina número 17 del área 2 de oficinas de docentes de la ESFOT.

- **Hardware de intercomunicación**

Cada cubículo contaba con un citófono análogo, los cuales eran interconectados con el equipo exterior por medio de cables que se dirigían desde el equipo hacia el techo por medio de canaletas y posteriormente de manera horizontal hacia la placa principal.

- **Alimentación eléctrica**

La alimentación eléctrica tanto de la placa principal como de cada uno de los equipos de intercomunicación se la realizaba por medio de una fuente que se encontraba conectada a la red eléctrica de la ESFOT. Este cableado recorría la misma ruta que el cableado utilizado para la transmisión de voz análoga entre los equipos y la placa principal.

### 3.2 Requerimientos para la red de video porteros IP

Una vez recopilada la información de la zona B de oficinas de docentes de la ESFOT se determinaron todos los requerimientos para la implementación de la red de video porteros IP. En la Tabla 3.1 se describen de manera muy general los distintos requerimientos con su respectiva función.

**Tabla 3.1.** Requerimientos y funciones para la red de video porteros IP

REQUERIMIENTO	FUNCIÓN
Sistema de videoporteros IP con comunicación TCP/IP y <i>software</i> para configuración y administración	Administración de la comunicación con los monitores internos, control de acceso a la oficina, apertura de manera remota por medio de <i>software</i> .
Monitores con soporte PoE y comunicación TCP/IP	Intercomunicación entre los usuarios que lo hayan requerido, apertura de la puerta principal de la oficina.
Fuente de alimentación 12(V) 1(A)	Energiza el sistema IP para multiapartamentos.
<i>Switch</i> de 16 puertos (12 PoE)	Centraliza la información de cada uno de los equipos y los interconecta con el <i>switch</i> de la DGIP.
Protector de voltaje	Evita los picos de voltaje, resguardando a los equipos.
Red LAN ( <i>Local Area Network</i> )	Interconecta a todos los dispositivos anclados a la red.
Acceso a un <i>switch</i> de la DGIP	Acceso a la red de la EPN para obtener salida a Internet.

### 3.3 Diseño del cableado estructurado

Se realizó el diseño de la red en base a la red física y lógica de la Escuela Politécnica Nacional manejada en la ESFOT, por lo que para el proyecto se decidió considerar una topología física en estrella con comunicación TCP/IP y tecnología *Ethernet*. Además, el diseño se basó en el número de equipos involucrados en la red y en las distancias soportadas por el cable de red. En base al cálculo y el diseño, se definió que se requeriría un aproximado de 90 metros de cable UTP, 60 metros de manguera BX, 2 cajas de distribución, 8 cajas de paso y 16 conectores RJ45, debido a que son 8 los equipos terminales conectados en la red. La fórmula empleada en el cálculo de la longitud promedio de cable UTP, se presenta en la Ecuación 3.1 y el diseño del cableado estructurado, se presenta en el **ANEXO A2**.

$$\text{Distancia promedio (Dp)} = \frac{\text{Punto más lejano} + \text{Punto más cercano}}{2}$$

$$\text{Distancia promedio (Dp)} = \frac{13,20\text{m} + 2\text{m}}{2} = 7,6(\text{m})$$

$$\text{Cable UTP} = (\text{Dp} + 10\%\text{Dp} + 2.5\text{m holgura}) * \#\text{puntos de red}$$

$$\text{Cable UTP} = (7,6\text{m} + 0,76\text{m} + 2,5\text{m}) * 8 = 86,88(\text{m})$$

**Ecuación 3.1.** Longitud promedio de cable UTP

### 3.4 Diseño de la red de video porteros IP

Para el diseño de la red fue necesario realizar un análisis para identificar el número de oficinas y por ende el número de equipos que se involucrarían en la red, donde el equipo principal es el sistema IP para multiapartamentos DS-KD3002-VM de la marca Hikvision, el cual ha sido descrito en el marco teórico. Así mismo, en base al número de dispositivos involucrados en la red, se procedió a elegir el número de puertos del *switch* PoE.

El *switch* PoE sería el equipo encargado de administrar el tráfico de todos los dispositivos y el cual posteriormente se conectaría al *switch* administrable de la DGIP para así tener salida al Internet. Del diseño, se determinó que se requeriría un mínimo de 8 (7 para las oficinas y 1 del portero) para la zona B. Dicho diseño se presenta en el **ANEXO A3**.

### 3.5 Implementación del cableado estructurado

Una vez desarrollado el diseño, se procedió a realizar la implementación del cableado estructurado, considerando los siguientes puntos:

- **Adquisición del *hardware* de red**

Analizando los requerimientos de los diferentes equipos y respetando las normas de cableado estructurado, se procedió a seleccionar los elementos que se adapten de mejor manera a la infraestructura de la ESFOT priorizando el óptimo funcionamiento de la red y de los equipos. Dentro de este proceso se procedió a seleccionar los elementos descritos en la Tabla 3.2.

**Tabla 3.2.** Elementos de *hardware* de red con sus respectivas funciones

ELEMENTO	FUNCIÓN
Manguera BX de 1/2" y 1".	Alberga el cableado horizontal de UTP.
Cajas cuadradas de paso galvanizadas.	Distribuye el cable de red e interconecta las distintas mangueras.
Cable UTP categoría 5e (Recomendado por el fabricante)	Transporte de datos de red entre equipos().
Conectores RJ45 categoría 5e.	Permite la conexión entre la tarjeta de red de los equipos y el cable UTP.
Capuchones para RJ45.	Salvaguarda los conectores RJ45.
Switch de 16 puertos (12 PoE)	Administra el tráfico de datos entre los equipos y permite la conexión con el <i>switch</i> de la DGIP.
Canaletas	Contienen el cableado de red vertical.

- **Adquisición del *hardware* de intercomunicación**

En base al análisis de las características específicas de los equipos que se pueden adquirir dentro mercado ecuatoriano, se tomó en cuenta el costo, el rendimiento y las características que se acoplen de mejor manera a los requerimientos del sistema planteado. En base a lo anterior mencionado se eligió el equipo DS-KD3002-VM de la marca Hikvision; ya que este presenta características bastantes similares a versiones superiores y a la vez es mucho más accesible en comparación a otros modelos encontrados en el mercado. En la Tabla 3.3 se puede observar una comparativa entre las características, beneficios y costos de los equipos analizados dentro del mercado.

**Tabla 3.3.** Comparativa de equipos analizados en el mercado [30]

MODELOS	MARCA	CARACTERÍSTICAS	BENEFICIOS	COSTOS
DS-KD8102-V	Hikvision	<ul style="list-style-type: none"> <li>• Teclado táctil Capacitivo</li> <li>• Función de notificación de mensajes.</li> <li>• Ethernet TCP / IP autoadaptable de 10/100/1000 Mbps.</li> <li>• 418 mm x 145 mm x 61 mm</li> </ul>	<ul style="list-style-type: none"> <li>• Desbloqueo remoto a través de la aplicación.</li> <li>• Apertura desde cualquiera de los monitores.</li> <li>• Envío automático de las imágenes capturadas a FTP o al cliente</li> </ul>	\$452.72

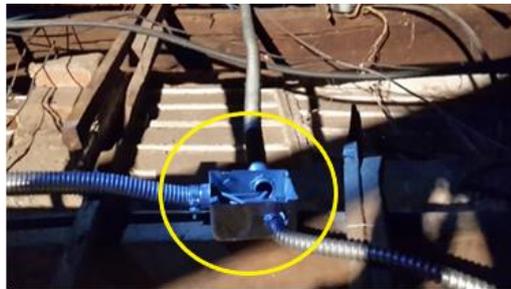
Continúa →

DS-KD8002-VM	Hikvision	<ul style="list-style-type: none"> <li>• Lector de proximidad Mifare 13.56 MHz</li> <li>• Pantalla LCD</li> <li>• Compresión de video H.264.</li> <li>• 418 mm x 145 mm x 61 mm</li> <li>• Protocolos TCP/IP, RTSP</li> </ul>	<ul style="list-style-type: none"> <li>• Notificación de mensajes.</li> <li>• Desbloqueo remoto a través del cliente o la aplicación.</li> <li>• Detección de remoción de la superficie de montaje.</li> </ul>	\$381.15
DS-KD3002-VM	Hikvision	<ul style="list-style-type: none"> <li>• Lector de proximidad Mifare 13.56 MHz</li> <li>• Soporta un máximo de 2500 tarjetas.</li> <li>• Teclado incorporado.</li> <li>• Compresión de video H.264.</li> <li>• 357 mm x 124 mm x 55 mm.</li> <li>• Controlar hasta 254 monitores.</li> </ul>	<ul style="list-style-type: none"> <li>• Desbloqueo remoto a través del cliente o la aplicación.</li> <li>• Detecta el estado magnético de la puerta.</li> <li>• Control de acceso desde cualquier equipo interior.</li> </ul>	\$ 346.18
DS-KV8402-IM	Hikvision	<ul style="list-style-type: none"> <li>• 4 x Botón del timbre.</li> <li>• Tarjetas de control de acceso – Mifare.</li> <li>• Compresión de video H.264.</li> <li>• Ethernet TCP / IP autoadaptable de 10/100 Mbps.</li> <li>• 182 mm x 100 mm x 33 mm.</li> </ul>	<ul style="list-style-type: none"> <li>• Notificación de mensajes.</li> <li>• Desbloqueo remoto a través del cliente o la aplicación.</li> <li>• Detecta el estado magnético de la puerta.</li> </ul>	\$172.26
VTO1210C-X	Dahua	<ul style="list-style-type: none"> <li>• Lector de Mifare 13.56 MHz.</li> <li>• Pantalla LCD.</li> <li>• Comunicación bidireccional.</li> <li>• Detección de remoción de la superficie de montaje.</li> <li>• 406mm x 143mm x 42 mm.</li> <li>• Soporta protocolo de red TCP/IP.</li> </ul>	<ul style="list-style-type: none"> <li>• Soporta hasta 1000 monitores.</li> <li>• Apertura desde cualquiera de los monitores.</li> <li>• Apertura con tarjeta.</li> <li>• Cuenta con detección de presencia.</li> </ul>	\$371.91
DHI-VTO9341D	Dahua	<ul style="list-style-type: none"> <li>• Teclado touch screen.</li> <li>• Material metálico.</li> <li>• Protección: IP 55, IK 07.</li> <li>• 475 x 174 x 174 mm</li> </ul>	<ul style="list-style-type: none"> <li>• Reconocimiento facial.</li> <li>• Huella dactilar.</li> <li>• Tarjeta Mifare.</li> </ul>	\$ 1081.20

- **Instalación del cableado estructurado`**

Una vez adquirido el *hardware*, se procedió con la instalación del cableado, para lo cual se realizó el siguiente proceso:

- a) En cada una de las oficinas se colocó una referencia para poder identificar la ruta del cableado correspondiente a los diferentes equipos.
- b) Sobre el techo falso se colocó una caja de paso metálica en la viga más cercana a cada una de las oficinas del área y se realizó el tendido de la manguera BX de 1/2" y 1" entre cada caja; el tamaño de la manguera BX dependió del número de cables UTP que pasan por esta. En la Figura 3.1 se visualiza una de las cajas de paso anclada a una viga y conectada a la manguera BX.



**Figura 3.1.** Instalación de una caja de paso

- c) Mediante alambre galvanizado, se realizaron guías para pasar el cable UTP desde los monitores hacia el *switch* por medio de la manguera BX, se decidió dejar una holgura de 2 m. por equipo.
- d) Se realizó el pochado en cada uno de los extremos de cada cable UTP, para este proceso se utilizó la norma EIA/TIA 568B, como se observa en la Figura 3.2.



**Figura 3.2.** Pochado del cableado estructurado

- e) Finalizado el ponchado de todos los cables, como se indica en la Figura 3.3, se realizó las respectivas pruebas de funcionamiento por medio de un *tester*. En algunos casos, se vio la necesidad de volver a pochar los cables ya que no pasaron la prueba; este proceso no presentó un mayor inconveniente gracias a que se había dejado holgura en el cableado.



**Figura 3.3.** Testeo del ponchado del cableado

- f) Con el correcto funcionamiento del cableado estructurado, se realizó el etiquetado en los extremos de cada uno de los cables para así identificar el dispositivo al cual corresponde el cable. En la Figura 3.4 se observa el etiquetado de uno de los extremos del cableado.



**Figura 3.4.** Etiquetado del cableado estructurado

- g) Una vez etiquetado el cableado, se procedió con la instalación de canaletas de 20 mm. x 20 mm. x 2000 mm. para el cableado horizontal en cada una de las oficinas, como se observa en la Figura 3.5.



**Figura 3.5.** Montaje de canaletas

- h) Se conectó los cables necesarios a los puertos del *switch* Hikvision y se realizó el correspondiente peinado del cable en el *rack* de la DGIP ubicado en el área 2 de las oficinas de docentes de la ESFOT, finalizando el proceso con la conexión del cable de red desde el *switch* Hikvision hacia el *switch* Cisco de la DGIP. En la Figura 3.6 se observa el *rack* del área de oficinas 2 con las conexiones entre *switches*.



**Figura 3.6.** *Rack* del área de oficinas 2

- i) A partir de la instalación del cableado estructurado, se desarrollaron los planos correspondientes a la zona B de las oficinas de profesores de la ESFOT. Ver **ANEXO A2**.

### **3.6 Implementación de la red de video porteros IP**

Con la finalización de la instalación del cableado estructurado, se procedió a implementar la red de video porteros IP.

- **Instalación de monitores de video portero IP**

Los monitores IP DS-KH-6310-WL se empotraron a la pared a una altura de 1,30 m. del piso. Para la instalación de los monitores se desarrolló el siguiente procedimiento:

- a) Se colocó las cajas de soporte para pared, las cuales permiten colocar el soporte metálico y albergar el conector RJ-45 de cada uno de los monitores; en la Figura 3.7 se puede visualizar una de las cajas de soporte. Para esta actividad, se realizó dos perforaciones en la pared con la ayuda de un taladro y se aseguró las cajas con la ayuda de tornillos.



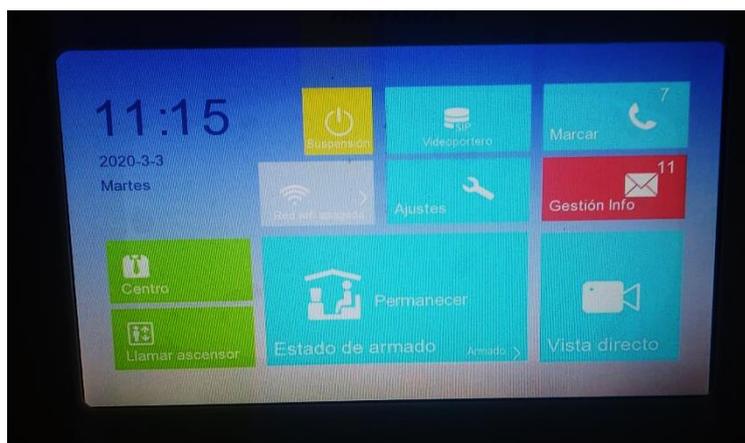
**Figura 3.7.** Cajas de soporte para pared

- b) Sobre las cajas plásticas, con un par de tornillos, se aseguró los soportes metálicos propios de cada monitor, como se visualiza en la Figura 3.8.



**Figura 3.8.** Soporte de Equipo

- c) Colocados los soportes metálicos, se procedió a bajar el cable UTP por medio de la canaleta instalada previamente y a conectar el cable a los monitores para posteriormente empotrar los equipos sobre el soporte metálico.
- d) Conectado el cable UTP al equipo, se verificó que el monitor se encienda. En la Figura 3.9 se puede observar el monitor energizado y funcional.



**Figura 3.9.** Comprobación del funcionamiento del monitor

- e) Por último, se cubrió la canaleta con su respectiva tapa.

- **Instalación del sistema IP para multiapartamentos**

El sistema IP para multiapartamentos Hikvision DS-KD3002-VM, fue instalado a una distancia recomendada de 1.45 m. desde la base hacia el suelo, siguiendo el siguiente proceso:

- a) Se procedió a hacer un hueco en la pared de 350 mm. de alto x 120 mm. de base x 55 mm. de profundidad, para empotrar una caja metálica que permitirá el soporte y la protección del equipo. En la Figura 3.10 se muestra el soporte empleado para esta actividad.



**Figura 3.10.** Soporte metálico

- b) Al empotrar la caja, fue necesario realizar perforaciones en la caja metálica y en la pared, respectivamente.
- c) Una vez empotrada la caja metálica, se procedió a bajar por una manguera el cable de alimentación a 12 V, el cable UTP y el cable de apertura de la chapa.
- d) Se identificó cada cable, tanto el de alimentación como el de apertura de la chapa y se procedió a colocar en las respectivas borneras; además, se realizó el ponchado en el cable UTP del equipo. En la Figura 3.11 se puede visualizar la colocación de borneras y la alimentación del equipo.



**Figura 3.11.** Alimentación de la placa

- e) Para reforzar la seguridad del equipo, fue necesaria la instalación de un marco de seguridad metálico, encargado de proteger la parte externa del equipo como se observa en la Figura 3.12.



**Figura 3.12.** Protección metálica de la placa

- f) Colocado el soporte interno, la seguridad externa e identificados cada uno de los cables, se procedió al montaje del equipo y sus conexiones necesarias para su funcionamiento y encendido.

- **Activación y configuración de equipos**

Dentro del *software* de administración se realizó las siguientes actividades, para más detalles revisar el **ANEXO A4**. En la Figura 3.13 se observa a uno de los integrantes del grupo, desarrollando la configuración de los equipos.



**Figura 3.13.** Activación y configuración de equipos

a) Activar los equipos

Para poder realizar cualquier tipo de configuración en los equipos de la red de video porteros, es necesario realizar la activación de estos. Para la activación, es necesario seleccionar el dispositivo sin activar y se procede a establecer una contraseña, la cual brindará una seguridad a los equipos ya que sin esta no es posible modificar las configuraciones del equipo. En la Figura 3.14 se observa el ingreso de la contraseña de activación para un equipo inactivo. En el campo (*status*) se puede verificar si el dispositivo se encuentra activado.

ID	Device Type	Status	IPv4 Address	Port	Enhanced SDK Service Port	Software Version	IPv4 Gateway
<input type="checkbox"/>	001	DS-KH6310-WL	Active		8000	N/A	VI.5.1build 1901...
<input checked="" type="checkbox"/>	002	DS-KH6310-WL	Inactive		8000	N/A	VI.5.1build 1901...
<input type="checkbox"/>	003	DS-KH6310-WL	Active		8000	N/A	VI.5.1build 1901...

**Figura 3.14.** Activación de equipos

Para culminar el proceso de activación, es necesario asignar la dirección IP y la máscara de la red; para efectuar estos cambios se utiliza la contraseña previamente establecida. En la Figura 3.15 se observa la asignación de una dirección IP y de máscara de red a un equipo.

**Figura 3.15.** Configuración de red en los equipos

**NOTA:** Por motivos de seguridad, no se muestran contraseñas ni las verdaderas direcciones IP y de la máscara de subred.

b) Agregar los equipos al *software* iVMS 4200

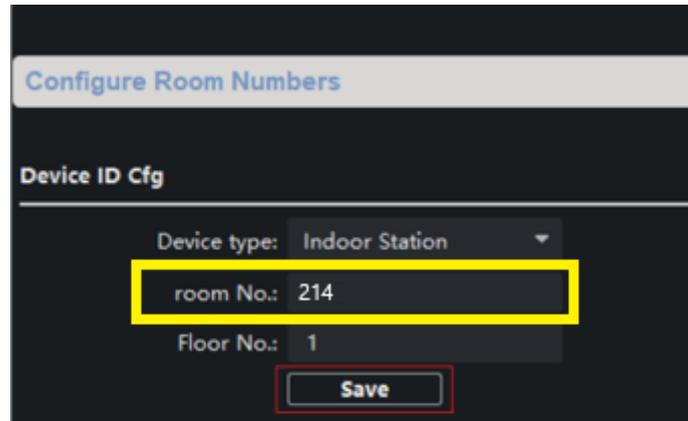
Para agregar los diferentes equipos fue necesario configurar la computadora que contenía el *software* de administración con una dirección IP dentro del mismo segmento de red que el resto de los equipos. Al momento de vincular los dispositivos, se agregó nombres para facilitar la identificación de cada uno de los equipos, como se observa en la Figura 3.16.

<input type="checkbox"/>	Nombre de archivo	Tipo de cone...
<input type="checkbox"/>	Portero 2	IP/Dominio
<input type="checkbox"/>	Pantalla 211	IP/Dominio
<input type="checkbox"/>	Pantalla 212	IP/Dominio
<input type="checkbox"/>	Pantalla 213	IP/Dominio
<input type="checkbox"/>	Pantalla 214	IP/Dominio
<input type="checkbox"/>	Pantalla 215	IP/Dominio
<input type="checkbox"/>	Pantalla 216	IP/Dominio
<input type="checkbox"/>	Pantalla 217	IP/Dominio

**Figura 3.16.** Nombres de los dispositivos

c) Configuración de los monitores

Se realizó la configuración de extensiones en cada uno de los monitores IP; para esta actividad, se decidió relacionar la extensión con el número del área de oficinas 2 y al número de cubículo. Por ejemplo, al monitor del cubículo 14 se le asignó la extensión 214. En la figura 3.17 se puede observar la asignación de la extensión 214 a uno de los monitores IP.



**Figura 3.17.** Asignación de extensión

Se verifica que la IP del monitor sea la correcta y posteriormente se vincula el monitor con el equipo principal, por medio de la dirección IP de este dispositivo. Este proceso permite la futura comunicación entre estos equipos.

d) Configuración del sistema IP para multiapartamentos

La placa exterior al ser el equipo principal, se debe encontrar en óptimo funcionamiento por lo que el primer paso a realizar es verificar que el dispositivo se encuentre configurado con la dirección IP correcta.

Luego de haber verificado las configuraciones de red del equipo, se procede a establecer el tiempo de un 1 segundo para el pulso de la apertura de la chapa eléctrica.

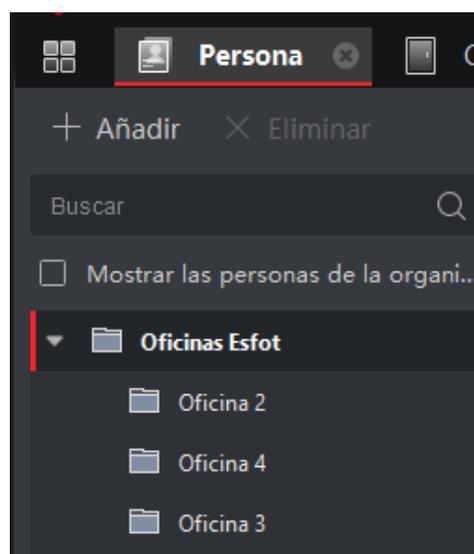
En base a un listado, se crea un directorio de profesores del área de oficinas 2 para después proceder a cargar esta información en el sistema. Este directorio cuenta con el nombre del docente y la extensión del monitor correspondiente a su oficina. El directorio tiene como finalidad facilitar la comunicación entre alumnos y docentes, ya que de esta manera no es necesario que los visitantes conozcan la extensión del monitor correspondiente a la persona que deseen visitar. En la Figura 3.18 se puede observar el documento con el directorio de contactos.

	A	B
1	<b>Room</b>	<b>Name</b>
2	205	Ing Carlos Romo
3	206	Ing Marina Veintimilla
4	207	
5	208	Ing Leandro Pazmiño
6	209	Ing Adrián Llumiquinga
7	210	Ing Cevallos/Ing Parraga
8	211	
9	212	
10	213	Ing Santiago Guerra
11	214	Ing Fanny Flores
12	215	Ing Fernando Becerra
13	216	Ing Mónica Vinuesa

**Figura 3.18.** Directorio de contactos

e) Configuración del control de acceso

Como se puede observar en la Figura 3.19, para el control de accesos se decidió crear grupos de personas de acuerdo con el número del área de oficinas 2, 3 ó 4. Este proceso pretende organizar a los usuarios por su ubicación dentro del área de oficinas y así facilitar la administración de los permisos de acceso a cada una de las áreas. En el caso de la zona B, el grupo de interés es el de Oficina 2.



**Figura 3.19.** Grupos de personas

Una vez creados los grupos, se procede a añadir los usuarios dentro del grupo (Oficina 2). En la Figura 3.20 se observa los datos del usuario Fanny Flores.

**Figura 3.20.** Creación de usuarios para el control de acceso

Al usuario creado, se vincula una tarjeta de acceso mediante el lector de tarjetas del sistema IP para multiapartamentos, para más detalles de este proceso observar el **ANEXO A4**. Cada tarjeta se registra con un código único de 10 dígitos, como se muestra en la Figura 3.21.

Santiago Guerra	10	3069261
Fanny Flores	11	246630
Fernando Becerra	12	306943
Mónica Vinuesa	13	2465955

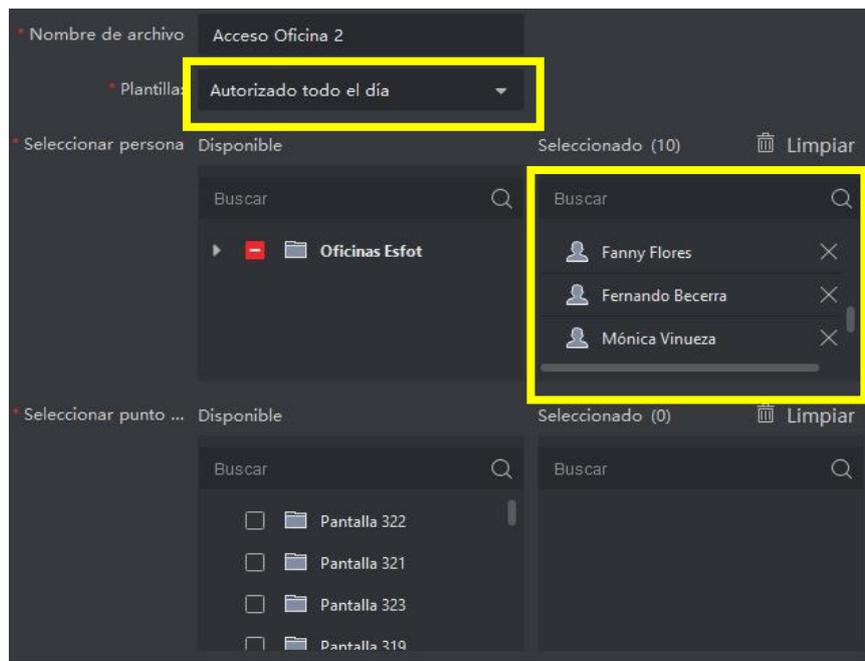
**Figura 3.21.** Vinculación de tarjetas de acceso a usuarios

En la Figura 3.22 se puede observar que, al igual que en los grupos de personas, se crea tres grupos de acceso (2, 3 y 4) para gestionar los permisos de acceso de cada usuario.

Nombre de arch...	Plantilla:	Empleado	Punto de co...	Estado	Operación
Acceso Oficina 3	Autorizado to...	Byron Loarte...	Puerta1_Port...	Todo aplicado.	[Icono]
Acceso Oficina 2	Autorizado to...	Marina Veintil...	Puerta1_Port...	Todo aplicado.	[Icono]
Acceso Oficina 4	Autorizado to...	Pedro Buitrón	Puerta1_Port...	Todo aplicado.	[Icono] Editar

**Figura 3.22.** Grupos de acceso

En el grupo (Acceso Oficina 2) se gestiona los usuarios a los que se les permite el acceso. Para evitar inconvenientes de acceso, se ha autorizado el ingreso a las oficinas todo el día los 365 días del año, esto debido a que varios docentes necesitan acudir a sus oficinas en fines de semana o feriados. En la Figura 3.23 se visualiza el listado de algunos usuarios que contienen los permisos de acceso al área de oficinas 2 de docentes de la ESFOT.



**Figura 3.23.** Concesión de permisos a usuarios

### 3.7 Pruebas de funcionamiento

Con la red de video porteros IP instalada, etiquetada y con las respectivas configuraciones, se procedió a hacer las pruebas necesarias para verificar el correcto funcionamiento de la red. Entre las pruebas más relevantes se destacan:

- a) Comunicación entre la placa externa y los monitores

Se marcaron las extensiones correspondientes a cada uno de los monitores y se estableció una comunicación para poder verificar la fluidez de la red. En la Figura 3.24 se puede apreciar a un usuario empleando el sistema.



**Figura 3.24.** Prueba de comunicación entre placa y monitor

b) Apertura de puertas desde los monitores

Después de establecer la comunicación, se procedió a realizar la apertura de la puerta desde las diferentes oficinas y así poder descartar problemas relacionados a este proceso. En la Tabla 3.3 se puede observar el monitoreo de la apertura de la puerta de los distintos monitores.

**Tabla 3.4.** Verificación de apertura desde los monitores

OFICINA	EXTENSIÓN	APERTURA
11	211	✓
12	212	✓
13	213	✓
14	214	✓
15	215	✓
16	216	✓
17	217	✓

c) Comunicación entre monitores

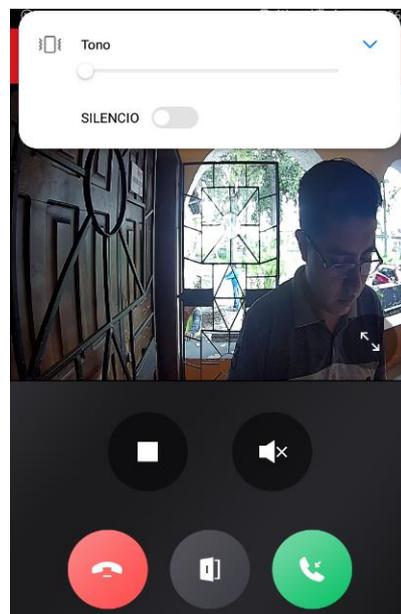
Se comprobó la conexión entre monitores, realizando llamadas entre diferentes dispositivos; esto para verificar que no se presenten problemas de comunicación cuando se ejecute este tipo de conexión. La Tabla 3.4 presenta los resultados del seguimiento de la comunicación entre monitores.

**Tabla 3.5.** Verificación de comunicación entre monitores

MONITOR	211	212	213	214	215	216	217
211	NA	✓	✓	✓	✓	✓	✓
212	✓	NA	✓	✓	✓	✓	✓
213	✓	✓	NA	✓	✓	✓	✓
214	✓	✓	✓	NA	✓	✓	✓
215	✓	✓	✓	✓	NA	✓	✓
216	✓	✓	✓	✓	✓	NA	✓
217	✓	✓	✓	✓	✓	✓	NA
Zona A	✓	✓	✓	✓	✓	✓	✓
Zona C	✓	✓	✓	✓	✓	✓	✓
Zona D	✓	✓	✓	✓	✓	✓	✓

d) Comunicación a través de la aplicación *Hik Connect*

Se realizó el marcado a las diferentes extensiones desde la placa exterior y se verificó que la llamada ingrese a la aplicación, en caso de que no exista respuesta desde el monitor ubicado en cada una de las oficinas. Además, se comprobó que la comunicación sea fluida entre usuarios. En la Figura 3.25 se puede observar la interacción por medio de la aplicación *Hik Connect*.



**Figura 3.25.** Prueba de comunicación con *Hik Connect*

e) Apertura remota desde *Hik Connect*

Luego de comprobar que la comunicación haya sido fluida, se procedió con la apertura de la puerta desde el aplicativo. Con este proceso se confirmó el correcto funcionamiento del aplicativo. En la Tabla 3.5 se presenta los resultados de las pruebas de apertura desde la aplicación.

**Tabla 3.6.** Apertura desde la aplicación *Hik Connect*

MONITOR	APERTURA
211	✓
212	✓
213	✓
214	✓
215	✓
216	✓
217	✓

f) Apertura de la puerta con tarjetas Mifare para el control de acceso

Se efectuó pruebas de apertura de la puerta con todas las tarjetas programadas, constatando el funcionamiento de cada una de las tarjetas y que se ejecute la apertura de la puerta sin inconvenientes. En la Tabla 3.6 se observan los resultados del uso de tarjetas Mifare.

**Tabla 3.7.** Apertura con tarjetas Mifare

TARJETA	APERTURA
Ing. Carlos Romo	✓
Ing. Santiago Guerra	✓
Ing. Fanny Flores	✓
Ing. Fernando Becerra	✓
Ing. Mónica Vinuesa	✓

### 3.8 Costos

Previo a la implementación, una parte fundamental del proyecto fue el análisis de proformas.

Establecidos los equipos necesarios y materiales a utilizar, se procedió a obtener costos de varias empresas o proveedores de monitores IP, sistemas IP para multiapartamentos, cableado estructurado, cableado eléctrico y metalmecánica.

Se obtuvo varias cotizaciones de los elementos necesarios, se analizó y se procedió a escoger cada una de ellas, dependiendo de los requerimientos a cumplir.

Una vez seleccionados los equipos, elementos y materiales necesarios para la implementación del proyecto, se procedió a realizar un presupuesto como referencia, de la zona B en donde se iban a instalar los equipos. En la Tabla 3.7 se describen los costos de los equipos, elementos y materiales utilizados en la implementación de la red de video porteros IP en la zona B del área de docentes de la ESFOT.

**Tabla 3.8.** Costos Referenciales

DETALLES	Cantidad	Valor Unitario	Total
Sistema IP para multiapartamentos Hikvision DS-KD3002-VM	1	\$ 346.18	\$ 346.18
Monitor IP Hikvision DS-KH-6310-WL	7	\$ 104.70	\$ 732.90
Distribuidor de Audio Y Video Hikvision DS-KAD612	1	\$ 96.75	\$ 96.75
Protección externa metálica de Sistema IP para multiapartamentos.	1	\$ 25.00	\$ 25.00
Canaletas Dexson 20x12.	7	\$ 2.50	\$ 17,50
Bobina de Cable de par Trenzado UTP.	1	\$ 98.00	\$ 98.00
Protector de Voltaje 120V/10A Multimatic.	1	\$ 10.00	\$ 10.00
Cajetin metálico 12x12 cm.	8	\$ 1.20	\$ 9.60
Tapa Dexson metálica 12x12 cm.	8	\$ 0.45	\$ 3.60
Caja de paso Inelmsur 20x20x10 cm.	2	\$ 5.90	\$ 11.80
Cajas para empotrar Monitor IP Hikvision DS-KH-6310-WL.	7	\$ 2.94	\$ 20.58
Conectores RJ45 Cat. 5e	20	\$ 0.35	\$ 7.00
Organizador Cable Horizontal	1	\$ 15.00	\$ 15.00
Manguera BX ½" y 1", Conectores ½" y 1", Abrazaderas.		\$ 80.00	\$ 80.00
Extras		\$ 30.00	\$ 30.00
<b>Valor Total</b>			<b>\$ 1503.91</b>

## 4. CONCLUSIONES Y RECOMENDACIONES

### 4.1 Conclusiones

- Con un estudio previo, se determinó los requerimientos necesarios y el tipo tecnología que es conveniente utilizar dentro del proyecto, identificando las dimensiones del área de trabajo y el problema que es necesario solventar, brindando así una solución moderna, escalable y de una mayor calidad.
- Se utilizó el estándar 802.3af PoE, gracias a este estándar se logró la mayor eficiencia en recursos, tanto financieros como humanos, ya que facilita el proceso de instalación del cableado necesario para la red.
- Seguir la respectiva normativa para el cableado estructurado es de suma importancia puesto que al realizar instalaciones respetando las normativas y con un testeo de los hilos de cableado, se garantiza el óptimo transporte de datos a través de toda la red.
- Un sistema de cableado estructurado está compuesto por varios elementos que permiten el dimensionamiento correcto de una red, basado en normas EIA/TIA que define la forma de diseñar, construir y administrar. Por ejemplo, EIA/TIA 568-B, que hace referencia al ponchado de los conectores RJ45 en UTP categoría 5, 5e y 6, con un orden de colores especificado en la norma.
- En el diseño de instalación de la red se decidió utilizar, una topología tipo estrella que permite cuidar el óptimo funcionamiento de la red, ya que, si un equipo se desconecta de la red o deja de funcionar, los demás equipos funcionarán con total normalidad.
- Hoy en día, la mayoría de redes se encuentran trabajando bajo el protocolo TCP/IP, que utiliza direccionamiento IP, permitiendo que cada equipo que se encuentre conectado a la red, tenga una dirección IP y máscara de la subred. Una de las mayores ventajas que se tiene es la escalabilidad de la red, que permite un crecimiento continuo de la misma y su adaptación a nuevas tecnologías sin ningún inconveniente.

- MIFARE es una tecnología de tarjetas inteligentes sin contacto, que permite el rápido y eficaz acceso a un establecimiento ya sea administrativo, educativo u otros; esto es únicamente para personal que tenga registrada la tarjeta en el sistema permitiendo que este pueda ingresar, brindando así una mayor seguridad para el personal y sus recursos.
- El código QR es actualmente una estrategia óptima y fácil de comunicación o administración debido a que la sociedad actual trabaja con celulares inteligentes. Una de las características importantes es la cantidad de información codificada que este puede almacenar, ha sido de gran ayuda en el anclaje de dispositivos; como por ejemplo cámaras, impresoras, monitores, permitiendo al usuario la administración de los mismos.
- Con la ayuda de la DGIP, se realizó pruebas y monitoreo de puertos TCP y UDP necesarios para establecer una conexión desde la red de video porteros IP con los servidores de Hikvision. Durante este proceso, se constató que para conexiones P2P de este tipo, es necesario habilitar ciertos rangos de puertos; estos rangos pueden variar de acuerdo con los requerimientos de la red de video porteros y de la ubicación del servidor de Hikvision con el que se conecte la red.
- Debido a las sobrecargas y fluctuaciones de voltaje que la red eléctrica presenta, es muy necesario el uso de protecciones eléctricas, para preservar la vida de los dispositivos de la red y garantizar su correcto funcionamiento.
- El desarrollo de la documentación del sistema como planos de cableado, manual de administración y manual de usuario son de suma importancia puesto que en un futuro facilitarán trabajos de mantenimiento, así como configuraciones y ampliaciones de la red.
- Con la investigación de las posibles soluciones IP del mercado, se determinó que la tecnología actual aporta nuevas herramientas para la mejora de varios aspectos; por ejemplo, la seguridad con el control de acceso a las oficinas, así también como la comunicación con un docente en tiempo real, a pesar de que no se encuentre en su oficina.

## 4.2 Recomendaciones

- Para realizar cualquier tipo de cambio o configuración en la red, se recomienda revisar los distintos manuales, los cuales presentan la información detallada para realizar las configuraciones necesarias sin presentar inconvenientes.
- Se recomienda realizar un respaldo de todas las configuraciones del *software* antes de realizar cualquier tipo de cambio o configuración, con el fin de poder restaurar las configuraciones en caso de requerirlo.
- Es recomendable mantener un constante monitoreo de la red, para prevenir posibles fallas o errores y corregirlas a tiempo, garantizando así el óptimo funcionamiento de la red y de los dispositivos conectados.
- Se recomienda mejorar o cambiar el sistema de puesta a tierra que existe en las instalaciones, ya que cuando hay fallas o fluctuaciones en la red eléctrica, se podría causar daños en equipos eléctricos y electrónicos.
- Se recomienda la revisión y supervisión del cableado eléctrico y de datos existente en los techos de las instalaciones, puesto que, se observó que existen varios desperfectos y esto puede provocar daños en equipos e infraestructura.
- Se recomienda considerar este proyecto para uso o aplicaciones de proyectos futuros, ya que ofrece una gran escalabilidad y adaptación a nuevas tecnologías.
- Se recomienda unificar en un solo *software* de administración todos los equipos de la marca Hikvision instalados en la ESFOT, este proceso ayudará a tener una mejor administración de la información y de los equipos, logrando un mayor control de seguridad.
- Considerar la implementación de alarmas y de otros dispositivos, con el fin de aprovechar todas las funcionalidades de los equipos instalados, para así lograr un sistema compacto y de gran tecnología.

## 5. REFERENCIAS BIBLIOGRÁFICAS

- [1] SYSCOM, «SYSCOM,» [En línea]. Available: <https://www.syscom.mx/producto/DS-KD3002-VM-HIKVISION-157051.html>. [Último acceso: 18 Marzo 2020].
- [2] Hikvision, «HIKVISION,» [En línea]. Available: [https://www.hikvision.com/uploadfile/image/10618\\_CUserswuqianyiDesktopUD06952BSpecofDSKD3002VMDoorStationV1.4.2320170817.pdf](https://www.hikvision.com/uploadfile/image/10618_CUserswuqianyiDesktopUD06952BSpecofDSKD3002VMDoorStationV1.4.2320170817.pdf). [Último acceso: 18 Marzo 2020].
- [3] DELTAeu, «DELTA,» [En línea]. Available: [https://shopdelta.eu/strongpanel-interno-strongip-ds-kh6310-wl-hikvision\\_l6\\_p13049.html](https://shopdelta.eu/strongpanel-interno-strongip-ds-kh6310-wl-hikvision_l6_p13049.html). [Último acceso: 18 Marzo 2020].
- [4] Hikvision Digital Technology, «HIKVISION,» [En línea]. Available: [https://www.hikvision.com/mtsc/uploads/product/accessory/UD06971B\\_Spec\\_of\\_DS-KH6310-WL\\_Indoor\\_Station\\_V1.5.1\\_20190612\(1\).pdf](https://www.hikvision.com/mtsc/uploads/product/accessory/UD06971B_Spec_of_DS-KH6310-WL_Indoor_Station_V1.5.1_20190612(1).pdf). [Último acceso: 18 Marzo 2020].
- [5] SYSCOM, «SYSCOM,» [En línea]. Available: <https://www.syscom.mx/producto/DSKAD606N-HIKVISION-96521.html>. [Último acceso: 18 Marzo 2020].
- [6] Hikvision Digital Technology Co., Ltd., «HIKVISION,» [En línea]. Available: <https://www.hikvision.com/es-la/Products/Video-Intercom/Accessories/Distributor/DS-KAD612>. [Último acceso: 18 Marzo 2020].
- [7] «Mi PC,» [En línea]. Available: [https://www.mipcparquecentral.com/item-multimatic\\_protector\\_automatico\\_de\\_voltaje-207987](https://www.mipcparquecentral.com/item-multimatic_protector_automatico_de_voltaje-207987). [Último acceso: 21 Marzo 2020].
- [8] «POWEST,» [En línea]. Available: <http://powest.com/landing/wp-content/uploads/2019/12/POWEST-REFRIMATIC.pdf>. [Último acceso: 21 Marzo 2020].
- [9] TECNO Seguro, «Tecnoseguro,» [En línea]. Available: <https://www.tecnoseguro.com/faqs/electronica/que-es-poe>. [Último acceso: 19 Marzo 2020].
- [10] NETGEAR, «NETGEAR,» 6 Noviembre 2019. [En línea]. Available: <https://kb.netgear.com/es/209/Qu&eacute;-es-PoE-alimentaci&oacute;n-a-trav&eacute;s-de-Ethernet>. [Último acceso: 19 Marzo 2020].
- [11] IONOS España S.L.U., «www.ionos.es,» [En línea]. Available: <https://www.ionos.es/digitalguide/servidores/know-how/tcpip/>. [Último acceso: 30 Marzo 2020].
- [12] Á. Robledano, «openwebinars.net,» 18 Junio 2019. [En línea]. Available: <https://openwebinars.net/blog/que-es-tcpip/>. [Último acceso: 30 Marzo 2020].



- [25] DENSO WAVE INCORPORATED, «QRcode,» [En línea]. Available: <https://www.qrcode.com/en/codes/iqr.html>. [Último acceso: 20 Marzo 2020].
- [26] O. G. LÓPEZ, «upcommons.upc.edu,» [En línea]. Available: <https://upcommons.upc.edu/bitstream/handle/2117/105644/Treball%20Fi%20de%20Grau%20-%20Oriol%20Gegundez%20Lopez.pdf?sequence=1&isAllowed=y>. [Último acceso: 20 Marzo 2020].
- [27] C. C. Javier Bateman. [En línea]. Available: <file:///C:/Users/David-PC/Desktop/DEBERES%20momen/Dialnet-DisenodeUnProtocoloRFIDPropietarioParaUnaAplicacio-3165144.pdf>. [Último acceso: 20 Marzo 2020].
- [28] «Tecno Seguro,» [En línea]. Available: <https://www.tecnoseguro.com/productos/vidovigilancia/ivms-4200-hikvision-software-gestion-video>. [Último acceso: 23 Marzo 2020].
- [29] «CENTRONIC,» 17 Mayo 2018. [En línea]. Available: <http://blog.centronic.com.py/hik-connect-como-funciona/>. [Último acceso: 23 Marzo 2020].
- [30] Hikvision, «www.hikvision.com,» 2019. [En línea]. Available: <https://www.hikvision.com/content/dam/hikvision/es-la/brochures-esp/Gu%C3%ADa-AR%C3%A1pida--Control-de-Acceso,-Video-Portero-y-Alarmas.pdf>. [Último acceso: 7 enero 2020].

# **ANEXOS**

**ANEXO A1: DISTRIBUCIÓN DE OFICINAS POR ZONAS**

**ANEXO A2: PLANOS DE CABLEADO ESTRUCTURADO DE LA ZONA B**

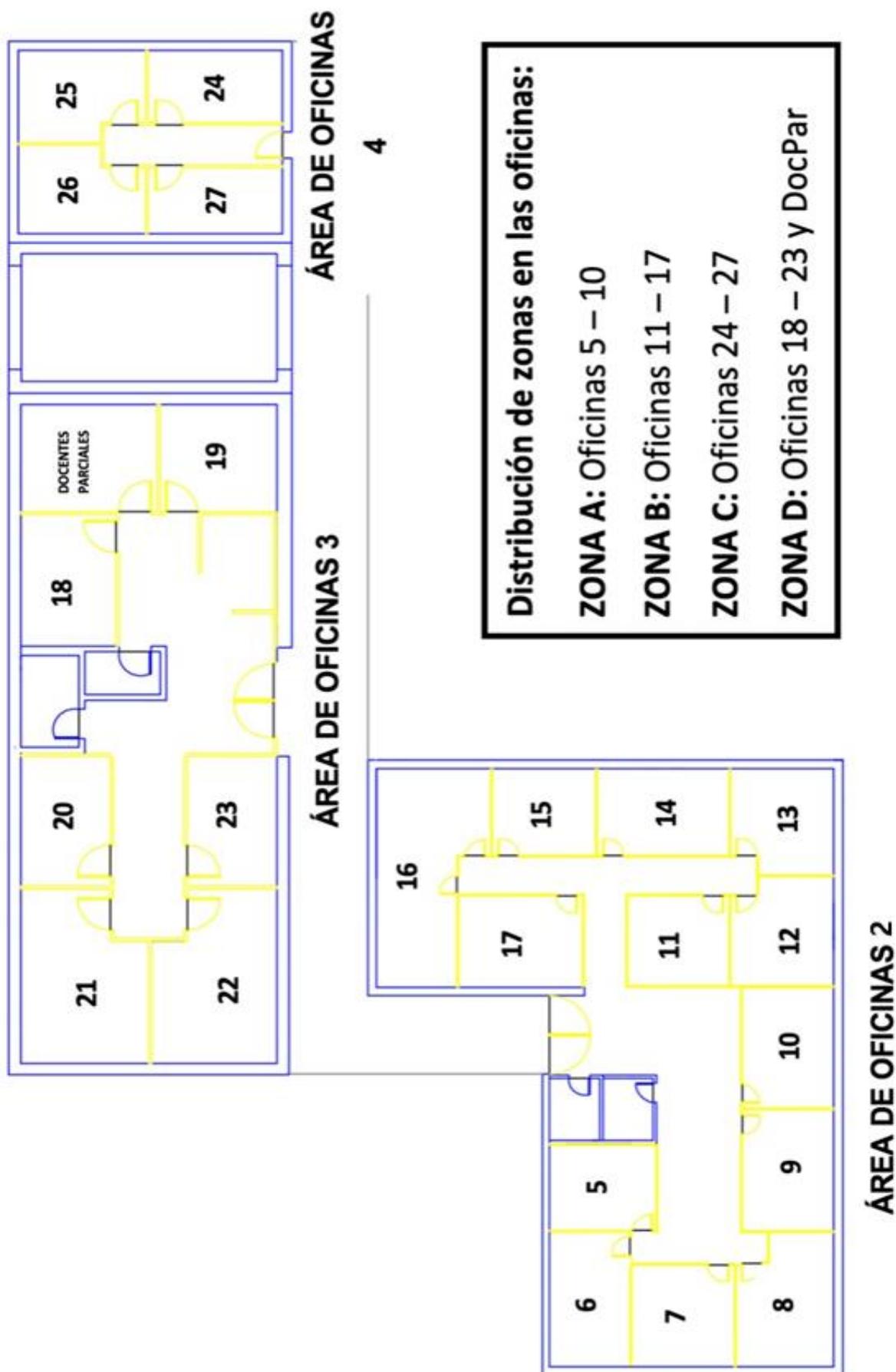
**ANEXO A3: DIAGRAMA DE RED**

**ANEXO A4: MANUAL DE ADMINISTRACIÓN**

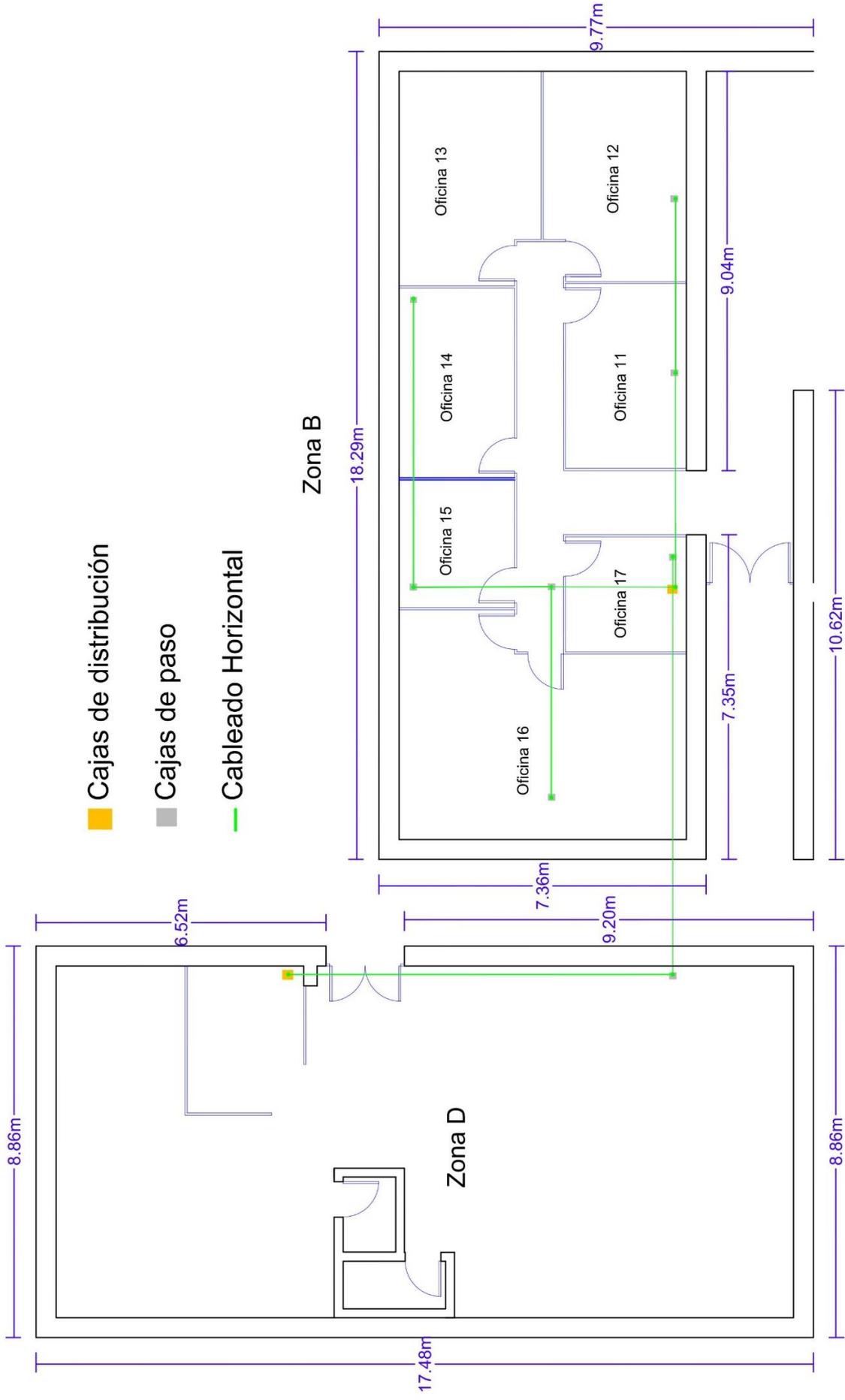
**ANEXO A5: MANUAL DE USUARIO**

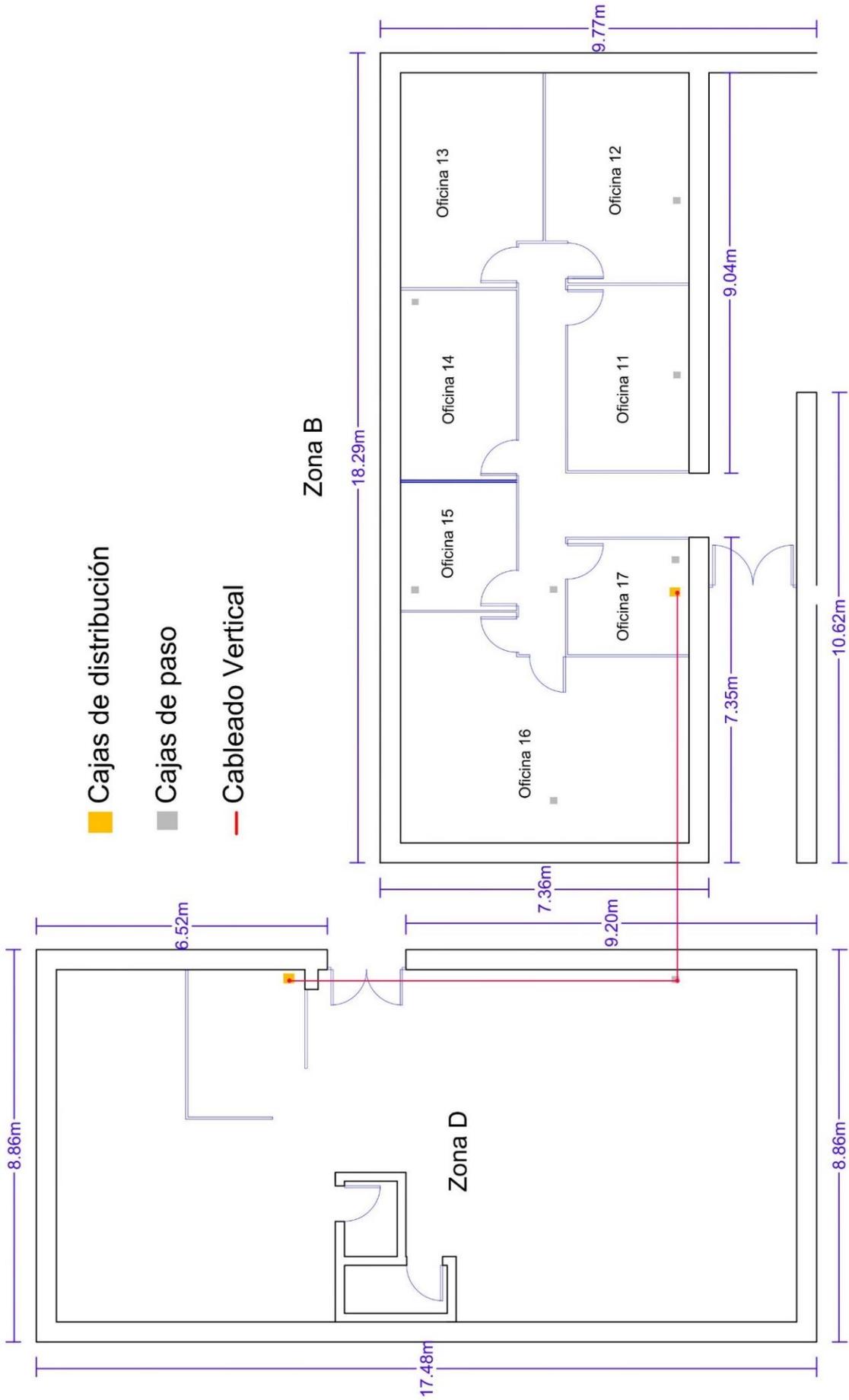
**ANEXO A6: CABLE DE PAR TRENZADO**

## **ANEXO A1: DISTRIBUCIÓN DE OFICINAS POR ZONAS**

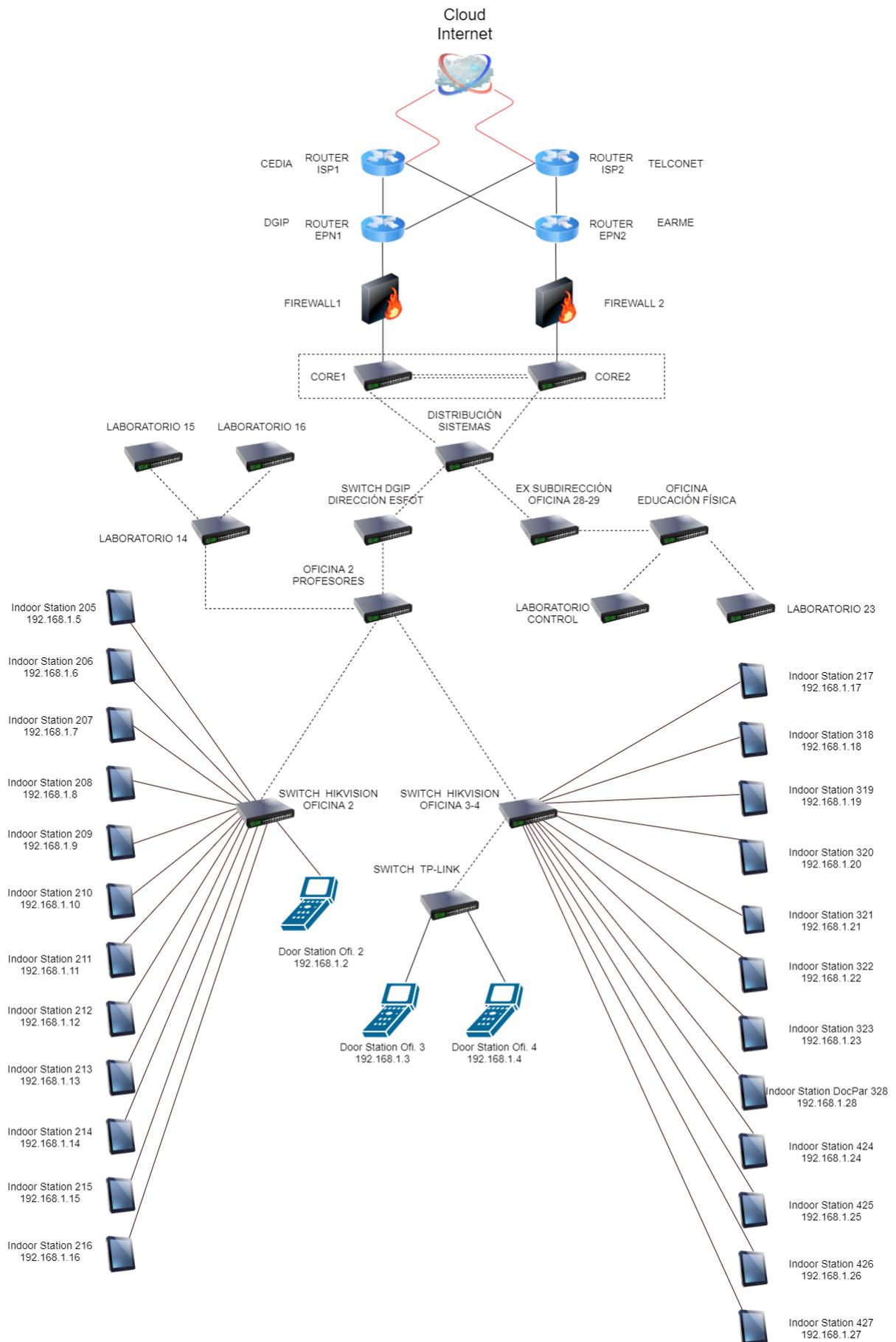


**ANEXO A2: PLANOS DE CABLEADO ESTRUCTURADO DE LA  
ZONA B**





## **ANEXO A3: DIAGRAMA DE RED**



## **ANEXO A4: MANUAL DE ADMINISTRACIÓN**

# CONFIGURACIONES DE LOS EQUIPOS MEDIANTE EL SOFTWARE iVMS 4200 3.1.1

## 1. CONFIGURACIONES BÁSICAS EN LA PANTALLA Y EL PORTERO

### 1.1. Sincronización de hora

Para configurar la hora en los equipos mediante el *software iVMS 4200.3.1.1 Client*, se debe seguir los siguientes pasos:

1. Ingresar al menú de mantenimiento y gestión.
2. Seleccione la opción **“Gestión dispositivos”**.

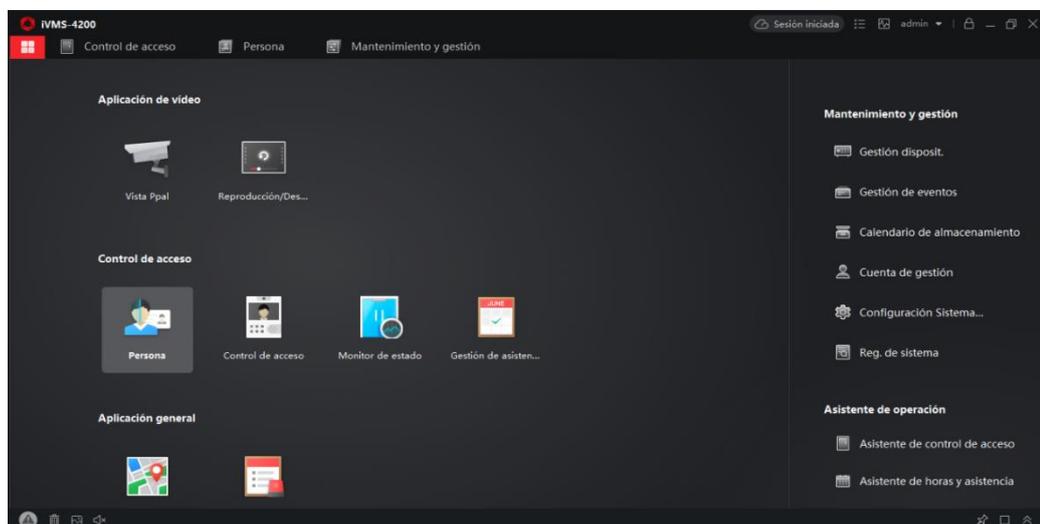
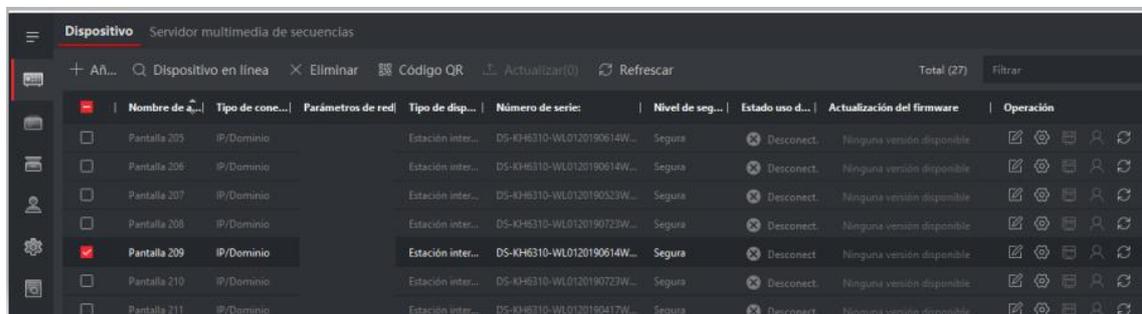


Figura A4.1 Menú principal del *software iVMS-4200* opción Gestión dispositivos

3. Seleccione el dispositivo (Pantalla o Portero) a modificar.
4. En la sección de Operación de clic en .



	Nombre de d...	Tipo de cone...	Parámetros de red	Tipo de disp...	Número de serie	Nivel de seg...	Estado uso d...	Actualización del firmware	Operación
<input type="checkbox"/>	Pantalla 205	IP/Dominio		Estación inter...	DS-KH6310-WL0120190614W...	Segura	Desconnect.	Ninguna versión disponible	   
<input type="checkbox"/>	Pantalla 206	IP/Dominio		Estación inter...	DS-KH6310-WL0120190614W...	Segura	Desconnect.	Ninguna versión disponible	   
<input type="checkbox"/>	Pantalla 207	IP/Dominio		Estación inter...	DS-KH6310-WL0120190623W...	Segura	Desconnect.	Ninguna versión disponible	   
<input type="checkbox"/>	Pantalla 208	IP/Dominio		Estación inter...	DS-KH6310-WL0120190723W...	Segura	Desconnect.	Ninguna versión disponible	   
<input checked="" type="checkbox"/>	Pantalla 209	IP/Dominio		Estación inter...	DS-KH6310-WL0120190614W...	Segura	Desconnect.	Ninguna versión disponible	   
<input type="checkbox"/>	Pantalla 210	IP/Dominio		Estación inter...	DS-KH6310-WL0120190723W...	Segura	Desconnect.	Ninguna versión disponible	   
<input type="checkbox"/>	Pantalla 211	IP/Dominio		Estación inter...	DS-KH6310-WL0120190417W...	Segura	Desconnect.	Ninguna versión disponible	   

Figura A4.2 Dispositivo a ser configurado

5. Abrir la pestaña **“System”**, dar clic en la opción **“Time”**.

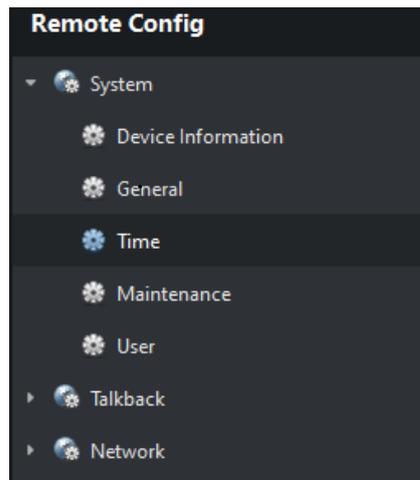


Figura A4.3 Menú System

6. Desplegar la pestaña **“Select Time Zone ▼”**, escoja la zona horaria correspondiente a su zona.

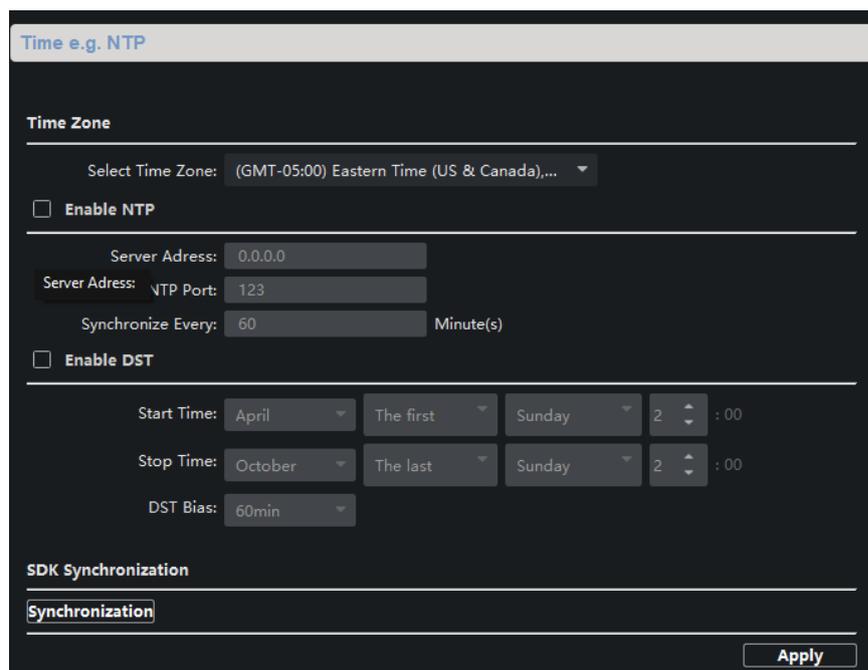


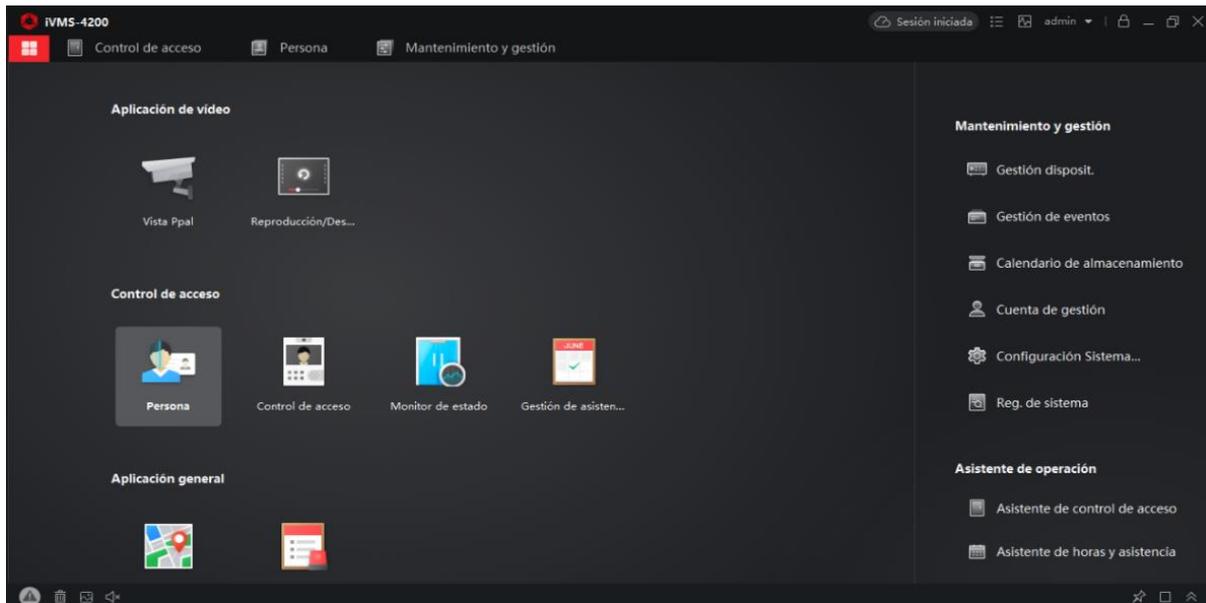
Figura A4.4 Panel de Configuración del Tiempo

7. De clic en **“Synchronization”**.
8. Finalmente, para guardar la configuración de clic en **“Apply”**.

## 1.2. Cambio de idioma

Para configurar el idioma en los equipos mediante el *software* **iVMS 4200.3.1.1 Client** siga los siguientes pasos:

1. Ingresar al menú de mantenimiento y gestión.
2. Seleccione la opción “**Gestión dispositivos**”.



**Figura A4.5** Menú principal del *software* iVMS-4200 opción Gestión dispositivos

3. Seleccione el dispositivo (Pantalla o Portero) a modificar.
4. En la sección de “**Operación**”, de clic en .

	Nombre de dispositivo	Tipo de conexión	Parámetros de red	Tipo de dispositivo	Número de serie	Nivel de seguridad	Estado uso dispositivo	Actualización del firmware	Operación
<input type="checkbox"/>	Pantalla 205	IP/Dominio		Estación inter...	D5-KH6310-WL0120190614W...	Segura	Desconect.	Ninguna versión disponible	
<input type="checkbox"/>	Pantalla 206	IP/Dominio		Estación inter...	D5-KH6310-WL0120190614W...	Segura	Desconect.	Ninguna versión disponible	
<input type="checkbox"/>	Pantalla 207	IP/Dominio		Estación inter...	D5-KH6310-WL0120190323W...	Segura	Desconect.	Ninguna versión disponible	
<input type="checkbox"/>	Pantalla 208	IP/Dominio		Estación inter...	D5-KH6310-WL0120190723W...	Segura	Desconect.	Ninguna versión disponible	
<input checked="" type="checkbox"/>	Pantalla 209	IP/Dominio		Estación inter...	D5-KH6310-WL0120190614W...	Segura	Desconect.	Ninguna versión disponible	
<input type="checkbox"/>	Pantalla 210	IP/Dominio		Estación inter...	D5-KH6310-WL0120190723W...	Segura	Desconect.	Ninguna versión disponible	
<input type="checkbox"/>	Pantalla 211	IP/Dominio		Estación inter...	D5-KH6310-WL0120190417W...	Segura	Desconect.	Ninguna versión disponible	

**Figura A4.6** Dispositivo a ser configurado

5. Abrir la pestaña **“System”**, dar clic en la opción **“Maintenance”**.

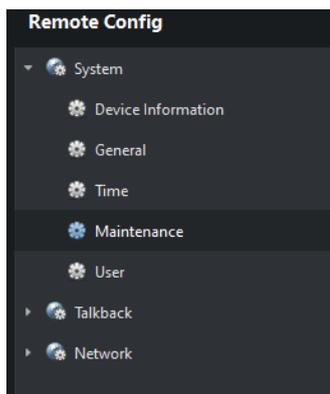


Figura A4.7 Menú System

6. Desplegar la pestaña **“Language”** ▼, escoja el idioma de preferencia.

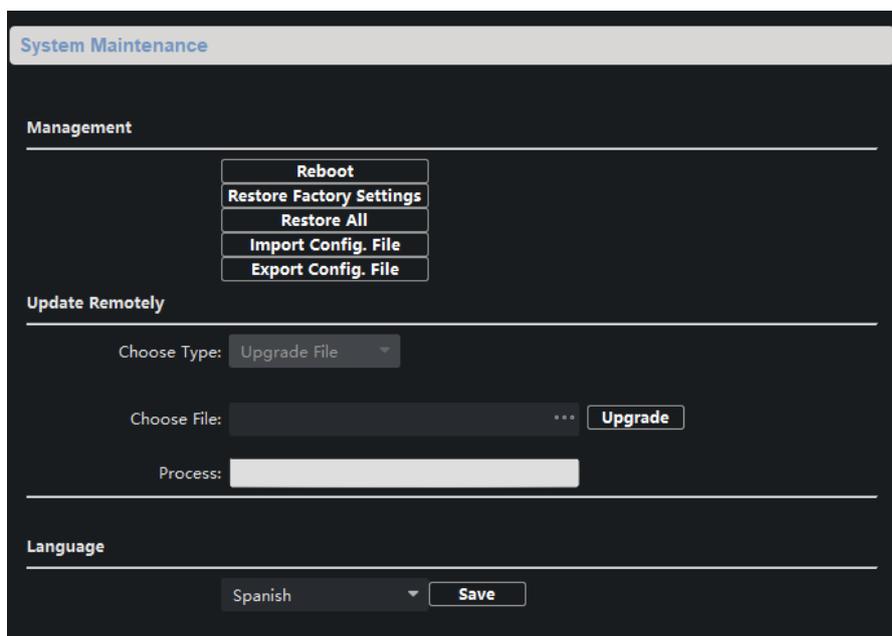


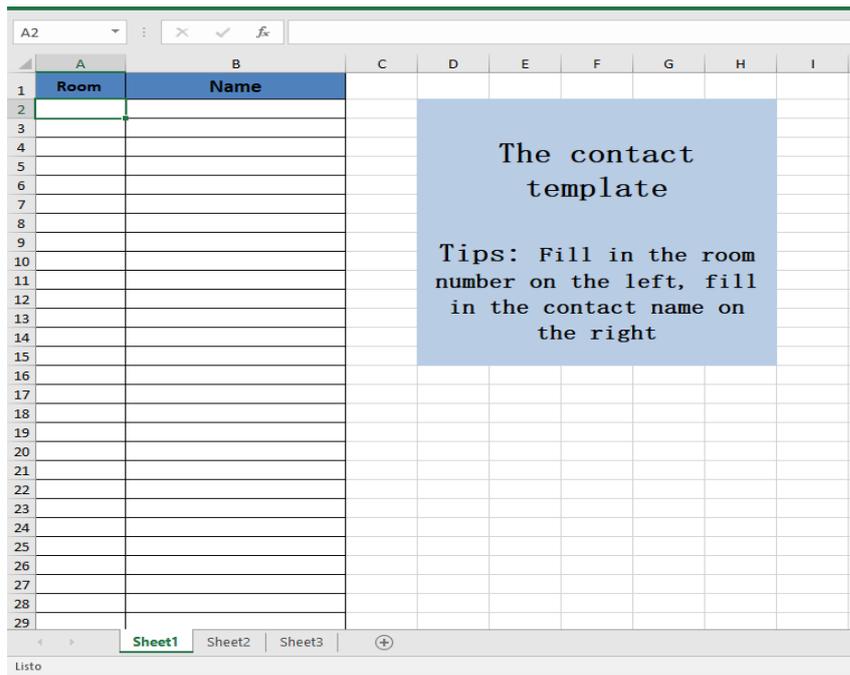
Figura A4.8 Panel de Configuración Idioma

7. Finalmente, para guardar la configuración de clic en **Save**.

## 2. CONFIGURACIONES ESPECÍFICAS EN LOS CITÓFONOS

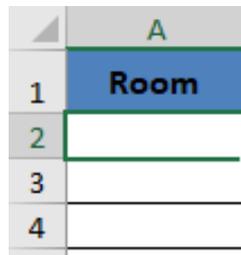
### 2.1. Modificación del directorio

1. Localizar el archivo de Excel que contiene las configuraciones, el cual tiene el nombre de **“Copia de Contracts Information Ofi X (2,3,4)”**.
2. Ingresar al archivo correspondiente al directorio de la oficina que se desee modificar.



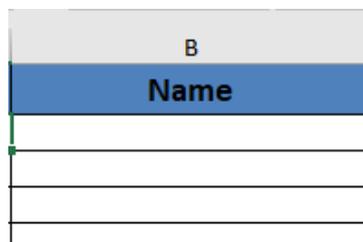
**Figura A4.9** Formato del directorio de contactos del portero

3. Editar el campo **"Room"** con la extensión que corresponda al monitor de cada oficina.



**Figura A4.10** Campo "Room"

4. Modificar el campo **"Name"** con el nombre de la nueva persona a la cual se le ha asignado la oficina.



**Figura A4.11** Campo "Name"

## 2.2. Cargar el archivo de directorio modificado

1. Ingresar al menú de mantenimiento y gestión.
2. Seleccionar la opción **Gestión dispositivos**.

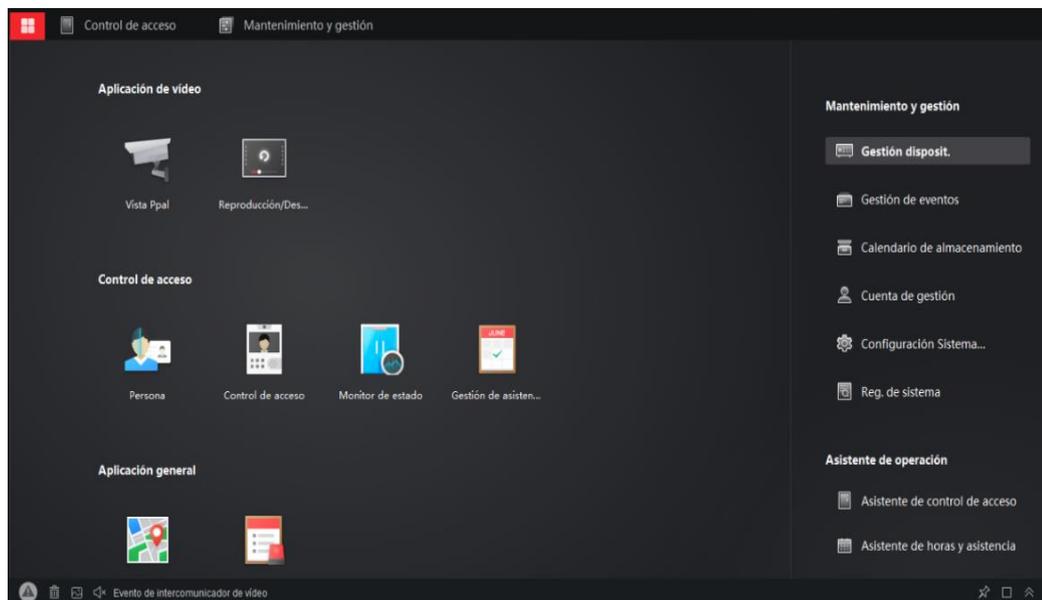
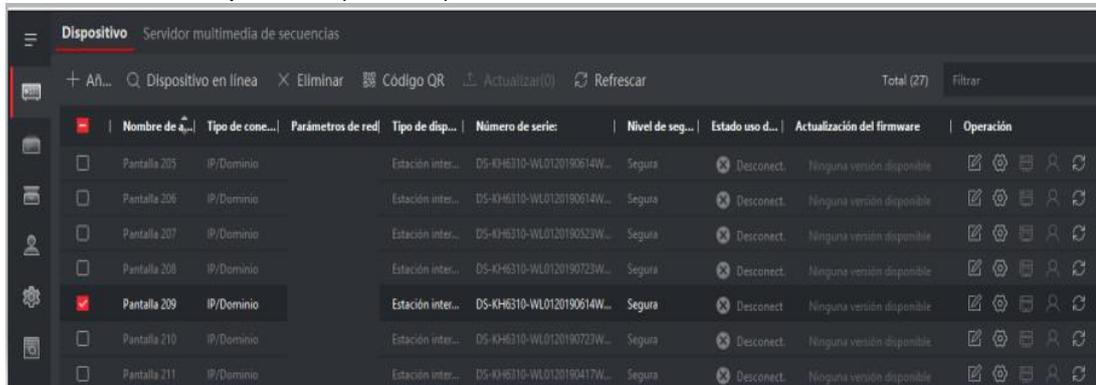


Figura A4.12 Menú principal del programa iVMS-4200 opción Gestión dispositivo

3. Seleccionar el dispositivo (Portero) a modificar.



	Nombre de dispositivo	Tipo de conexión	Parámetros de red	Tipo de dispositivo	Número de serie	Nivel de seguridad	Estado uso dispositivo	Actualización del firmware	Operación	
<input type="checkbox"/>	Pantalla 205	IP/Dominio		Estación inter...	DS-KH6310-WL0120190614W...	Segura	Desconnect	Ninguna versión disponible		
<input type="checkbox"/>	Pantalla 206	IP/Dominio		Estación inter...	DS-KH6310-WL0120190614W...	Segura	Desconnect	Ninguna versión disponible		
<input type="checkbox"/>	Pantalla 207	IP/Dominio		Estación inter...	DS-KH6310-WL0120190323W...	Segura	Desconnect	Ninguna versión disponible		
<input type="checkbox"/>	Pantalla 208	IP/Dominio		Estación inter...	DS-KH6310-WL0120190723W...	Segura	Desconnect	Ninguna versión disponible		
<input checked="" type="checkbox"/>	Pantalla 209	IP/Dominio		Estación inter...	DS-KH6310-WL0120190614W...	Segura	Desconnect	Ninguna versión disponible		
<input type="checkbox"/>	Pantalla 210	IP/Dominio		Estación inter...	DS-KH6310-WL0120190723W...	Segura	Desconnect	Ninguna versión disponible		
<input type="checkbox"/>	Pantalla 211	IP/Dominio		Estación inter...	DS-KH6310-WL0120190417W...	Segura	Desconnect	Ninguna versión disponible		

Figura A4.13 Dispositivo a ser configurado

4. En la sección de **Operación**, de clic en .
5. Abrir la pestaña **Talkback**, dar clic en la opción **Room NO. Manage**.



Figura A4.14 Campo *Room NO. Manage*

6. Dar clic en la opción ***"Import File"***.

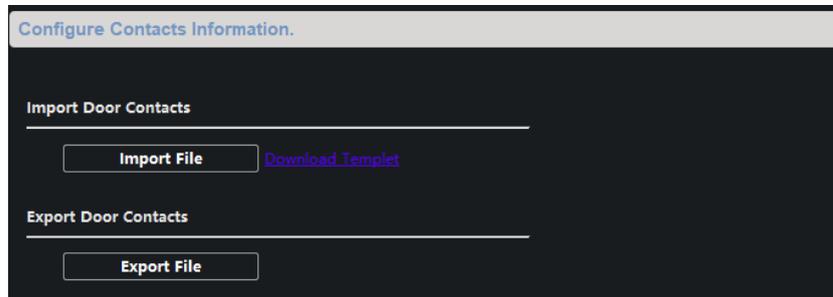


Figura A4.15 Importación del documento de la lista de contactos

7. Seleccionar el archivo previamente editado en la parte de **"Modificación del Directorio"**.

### 2.3. Añadir un usuario y asignación de tarjeta de acceso al mismo.

1. Ingresar a la opción **Persona** que se encuentra en el menú **Control de Acceso**.

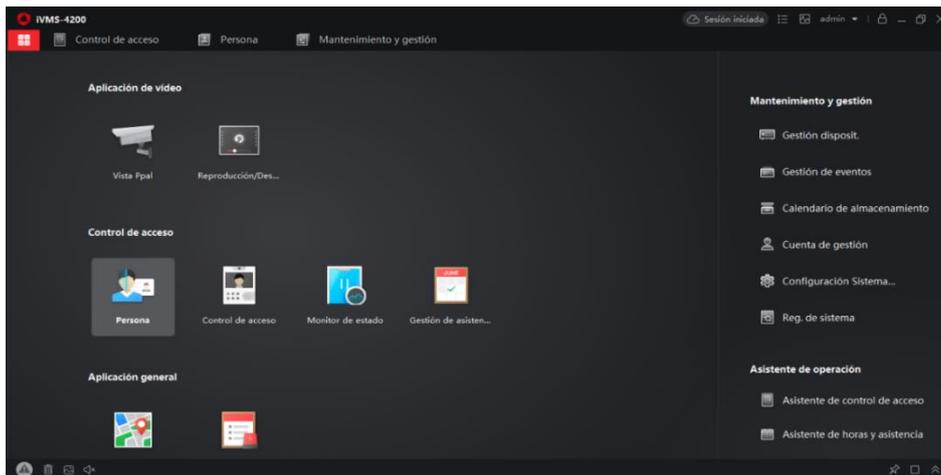


Figura A4.16 Menú principal del software iVMS-4200 opción Persona

2. Seleccionar el grupo al cual se desee añadir el nuevo usuario.

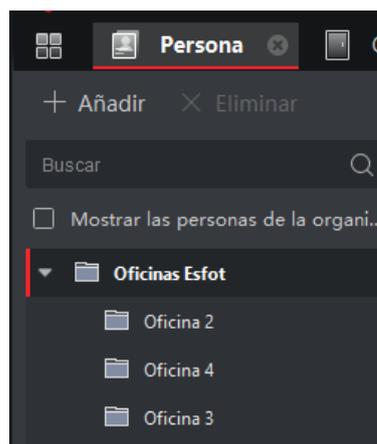


Figura A4.17 Selección del grupo

3. Dar clic en la opción “+ Añadir”.

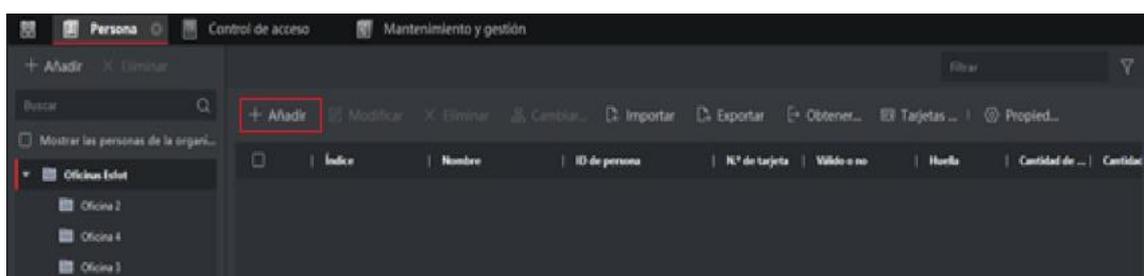
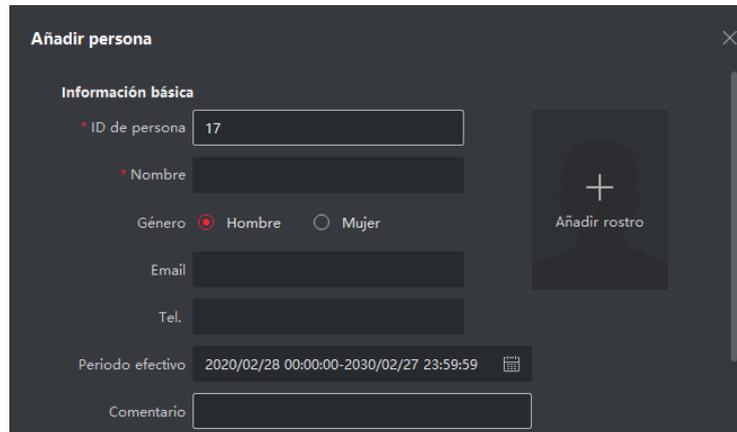


Figura A4.18 Adición de un miembro al grupo

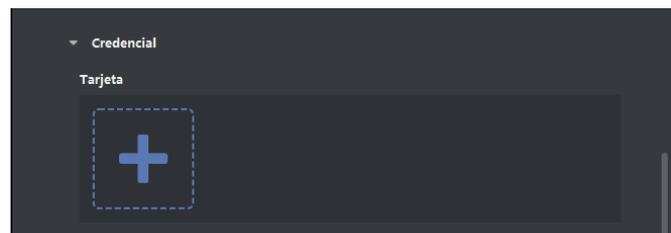
4. Llenar los campos de información con los datos del usuario, donde lo más relevante es el nombre y el género de la persona.



The screenshot shows a dark-themed form titled "Añadir persona". Under the "Información básica" section, there are several input fields: "ID de persona" with the value "17", "Nombre" (empty), "Género" with radio buttons for "Hombre" (selected) and "Mujer", "Email", "Tel.", "Periodo efectivo" with a date range "2020/02/28 00:00:00-2030/02/27 23:59:59" and a calendar icon, and "Comentario". To the right of the form is a "Añadir rostro" button with a plus sign icon.

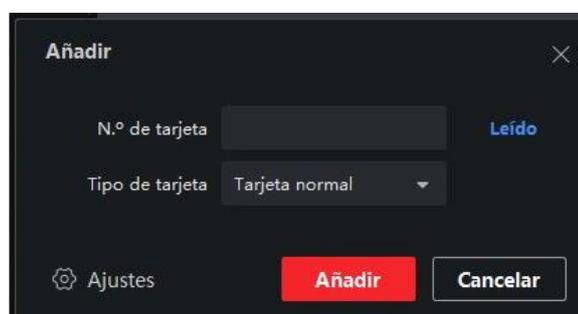
**Figura A4.19** Campo de datos del nuevo usuario

5. Para vincular una tarjeta al usuario en el menú credencial, se elige la opción tarjeta donde se desplegará un menú.



**Figura A4.20** Adición de tarjeta a un usuario

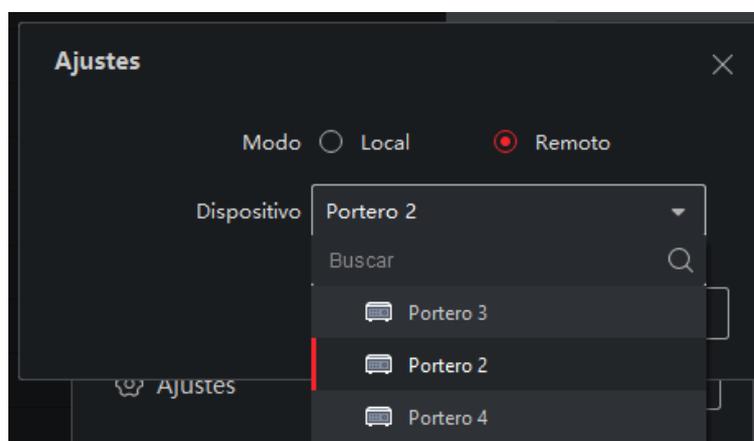
6. Una vez dentro del menú, se selecciona la opción **Tarjeta normal** en el campo **Tipo de tarjeta** y posteriormente se dirige hacia **Ajustes**.



The screenshot shows a dark-themed dialog box titled "Añadir". It contains two input fields: "N.º de tarjeta" (empty) and "Tipo de tarjeta" (set to "Tarjeta normal" in a dropdown menu). A "Leído" status is shown next to the first field. At the bottom, there are three buttons: "Ajustes" (with a gear icon), "Añadir" (in a red box), and "Cancelar".

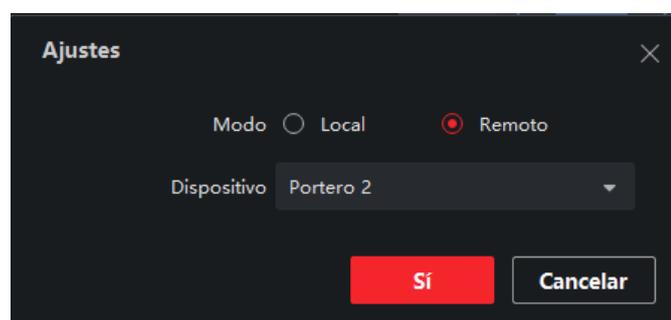
**Figura A4.21** Selección del tipo de tarjeta

- Una vez dentro de Ajustes, se selecciona en **Modo** (Remoto) y en la opción de **Dispositivo** se escoge el portero correspondiente a la oficina donde será agregado el nuevo usuario.



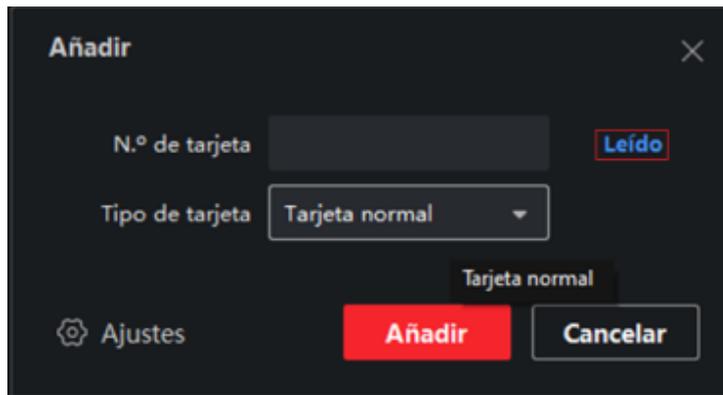
**Figura A4.22** Selección del portero

- Para guardar los ajustes se da clic en el botón de color rojo con el texto **SI**.



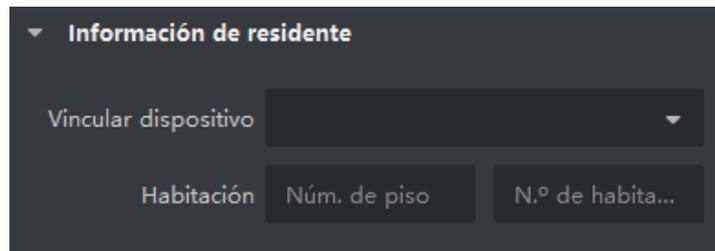
**Figura A4. 23** Confirmación de las configuraciones

- Posteriormente de haber realizado los ajustes y guardados los mismos, se procede a la lectura de la tarjeta para lo cual se da clic en la opción **Leído** y se colocará la tarjeta sobre el lector de tarjetas del portero previamente seleccionado. Si la lectura ha sido exitosa, se autocompletará el campo **N.º de tarjeta** con los datos correspondientes a la nueva tarjeta y para concluir se procederá a dar clic en añadir. En caso de que la lectura haya sido errónea, se debe repetir el proceso de lectura hasta que la tarjeta se ingrese de una manera exitosa.



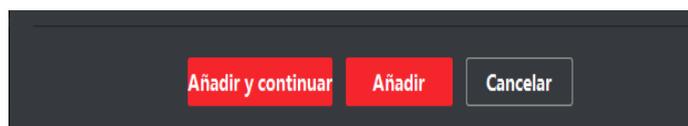
**Figura A4.24** Lectura de la nueva tarjeta

10. En la opción **Información de residente** se puede vincular una pantalla al nuevo usuario, la cual debe ser la correspondiente a la oficina asignada al nuevo usuario.



**Figura A4.25** Vinculación de un dispositivo al usuario

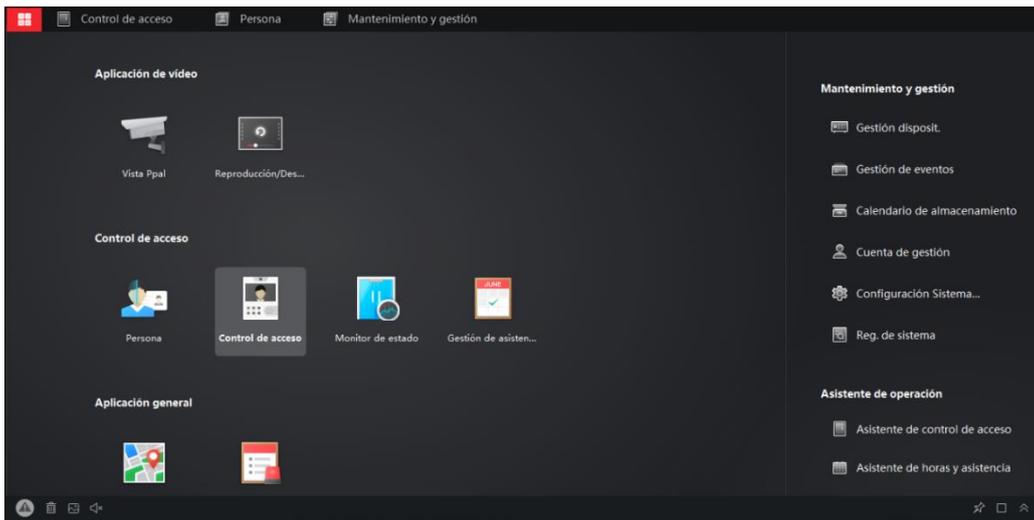
11. Para finalizar, se da clic en el botón de color rojo con el texto **Añadir** ubicado en la parte inferior del menú.



**Figura A4.26** Finalización del proceso

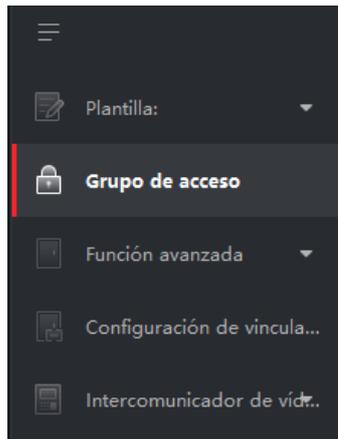
## 2.4. Añadir un usuario a un grupo de oficina

1. Ingresar a la opción **Control de acceso** que se encuentra en el menú **Control de Acceso**.



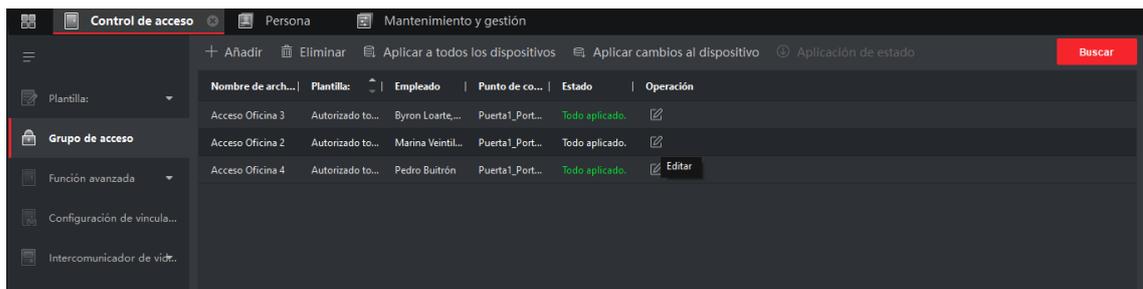
**Figura A4.27** Menú principal del programa iVMS-4200 opción Control de acceso

2. Seleccionar la opción **Grupo de acceso** en la parte izquierda de la pantalla.



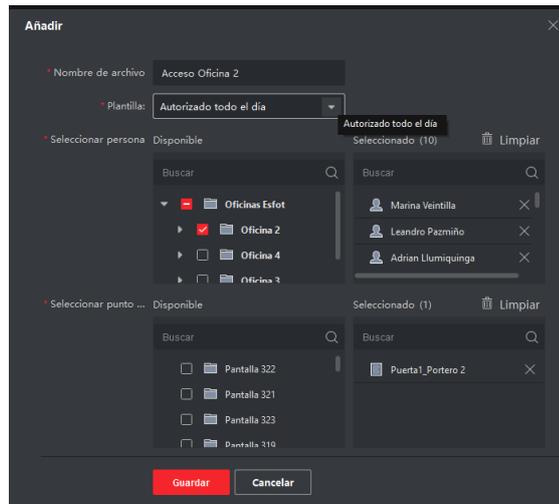
**Figura A4.28** Opción grupo de acceso

3. Escoger el grupo de la oficina donde se desea añadir al nuevo usuario y dar clic en **editar**.



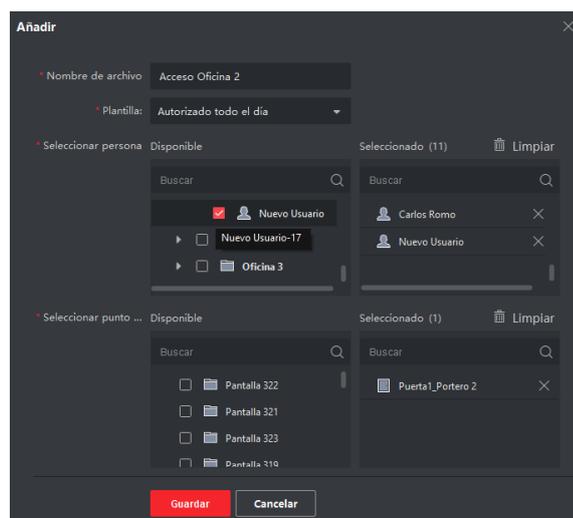
**Figura A4.29** Edición del grupo al que será añadido el nuevo usuario

- Para permitir el acceso del nuevo usuario indefinidamente, despliegue la flecha en la parte de **Pantalla** y seleccione **Autorizado todo el día**.



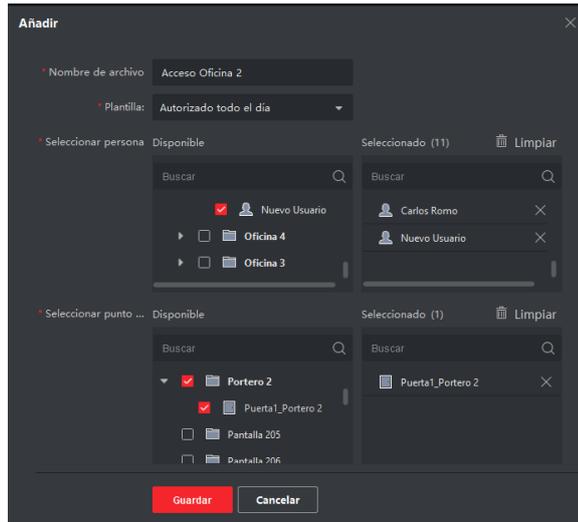
**Figura A4.30** Autorización del nuevo usuario

- En la sección **Seleccionar persona Disponible** marcar el grupo al cual ha sido asignado el nuevo usuario en el momento de su creación y seleccionar al mismo.



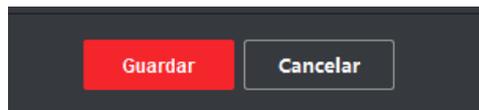
**Figura A4.31** Adición de usuario al grupo

- En la sección **Seleccionar puerto-Disponible** se procede a asignar una puerta al usuario, marcando el portero que le corresponde de acuerdo con la oficina que ha sido asignada y se selecciona la puerta asociada al portero escogido.



**Figura A4.32** Selección del portero y puerta

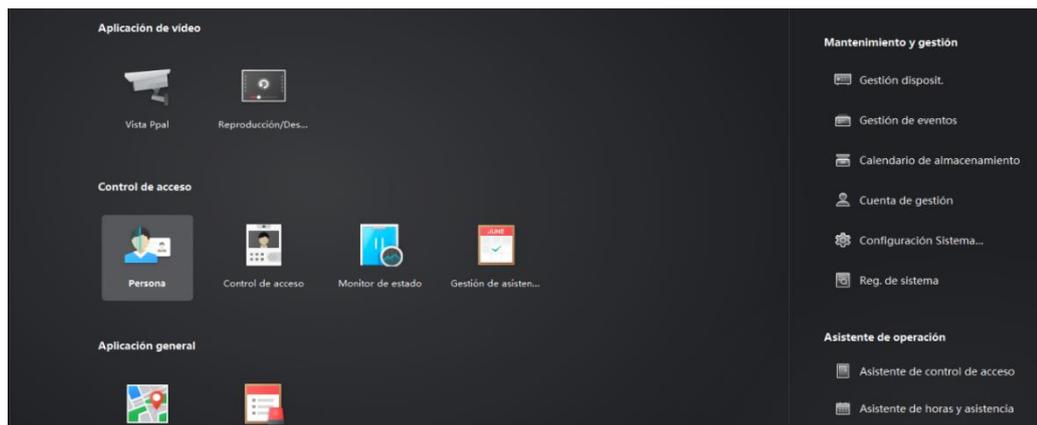
7. Guardar los cambios dando clic en el botón rojo **Guardar** de la parte inferior de la ventana.



**Figura A4.33** Botón guardar

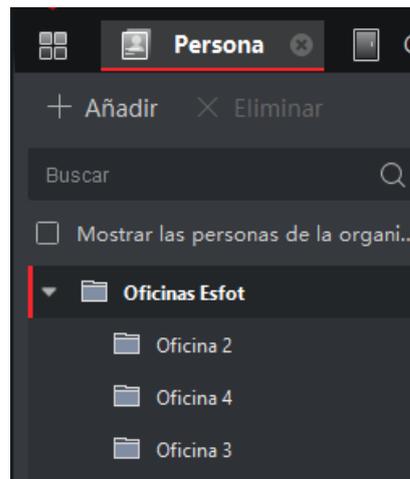
## 2.5. Eliminar un usuario de un grupo

1. Ingresar a la opción **Persona** que se encuentra en el menú **Control de Acceso**.



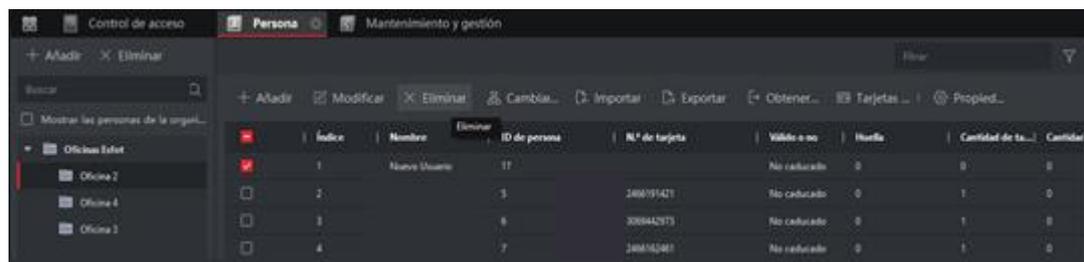
**Figura A4.34** Menú principal del programa iVMS-4200 opción Personas

2. Seleccionar el grupo al cual pertenece el usuario a eliminar.



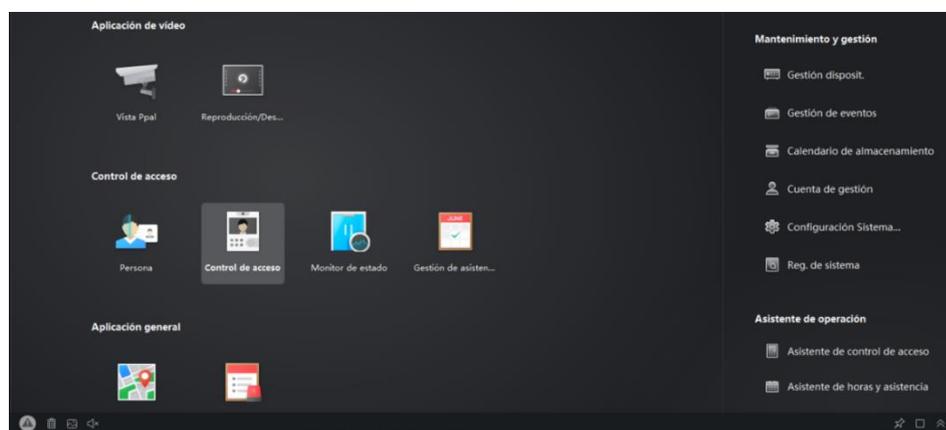
**Figura A4.35** Grupos creados para las oficinas 2, 3 y 4 de la ESFOT

3. Posteriormente, se mostrará todos los usuarios pertenecientes al grupo seleccionado y se marcará el usuario que se desee eliminar. Inmediatamente se da clic en la opción **Eliminar** que se ubica en la parte superior del listado de miembros del grupo.



**Figura A4.36** Usuarios pertenecientes al grupo Oficina 2

4. Luego, se debe regresar al menú principal e ingresar a la opción **Control de acceso** que se encuentra en el menú **Control de Acceso**.



**Figura A4.37** Menú principal del programa iVMS-4200 opción Control de acceso

5. Seleccionar la opción **Grupo de acceso** en la parte izquierda de la pantalla.

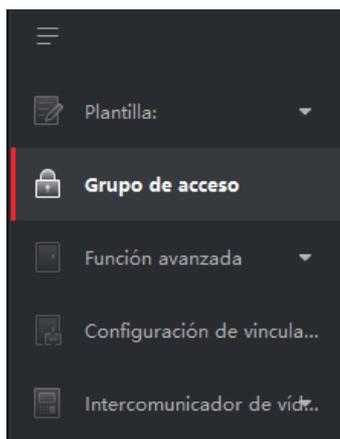


Figura A4.38 Opción Grupo de acceso

6. Escoger el grupo de la oficina donde se ubica el usuario a eliminar y dar clic en **editar**.

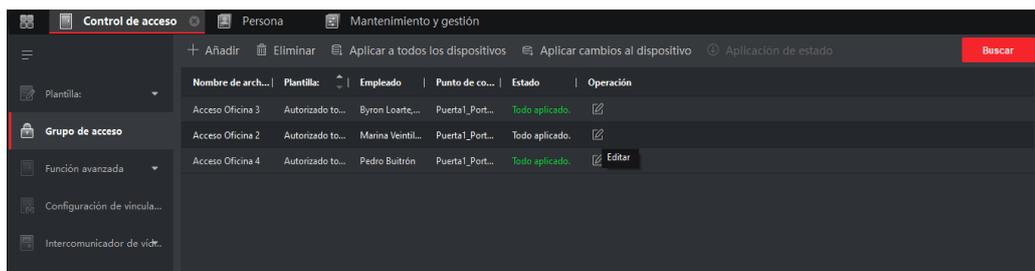


Figura A4.39 Opción de Editar en la parte de Operación

7. En la sección **Seleccionar persona Disponible** marcar el usuario a eliminar, el cual se encuentra localizado dentro del grupo al cual ha sido vinculado y en la parte derecha dar clic en la “X” correspondiente al usuario que se va a eliminar.

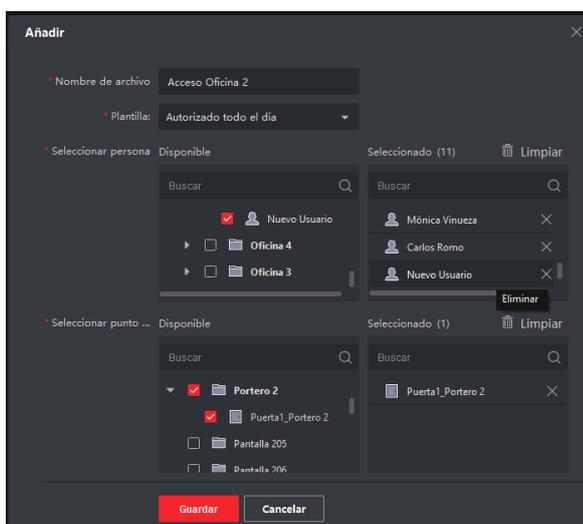
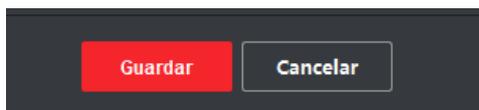


Figura A4.40 Configuración de acceso de usuarios de la Oficina 2

8. Guardar los cambios dando clic en el botón rojo **Guardar** de la parte inferior de la ventana.



**Figura A4.41** Botón Guardar

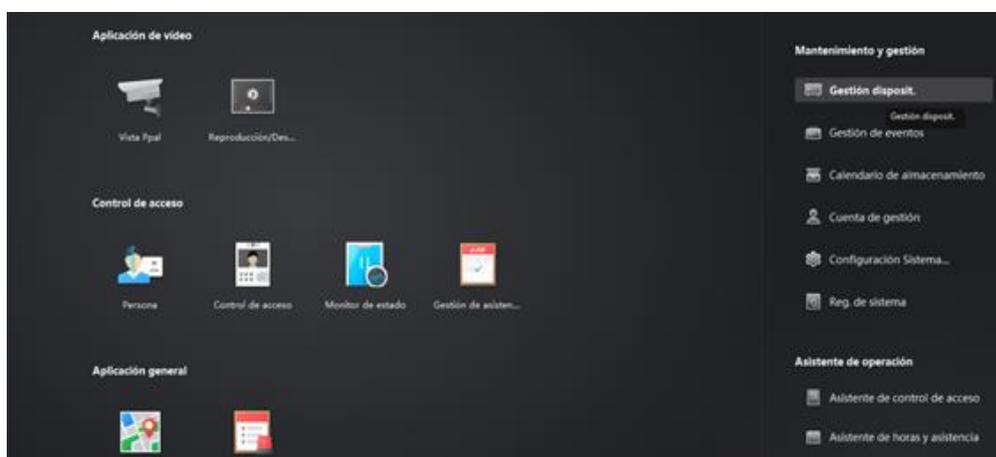
### 3. NOTA IMPORTANTE

En el caso de que exista un fallo con la conexión entre la pantalla y el interfono, se deberá seguir el siguiente procedimiento para solucionar el mismo.



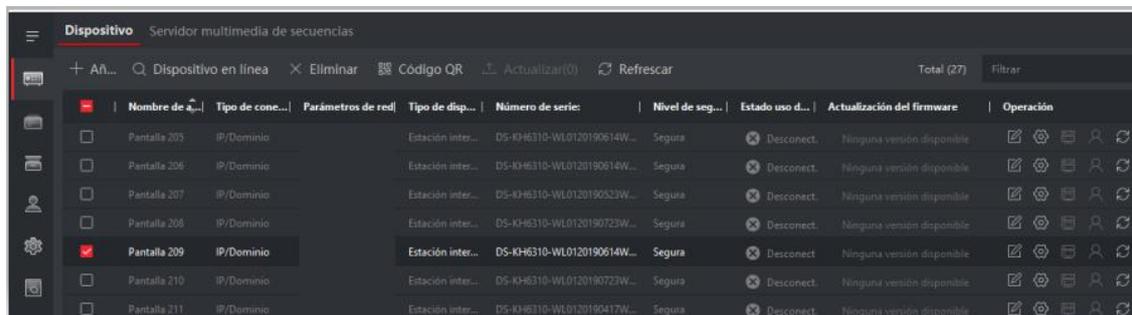
**Figura A4.42** Problema de conexión con el Interfono

1. Ingresar al menú de mantenimiento y gestión.
2. Seleccione la opción **Gestión dispositivos**.



**Figura A4.43** Menú principal del programa iVMS-4200 opción Gestión de dispositivos

3. Seleccione la pantalla a modificar.
4. En la sección de Operación de clic en .



	Nombre de dispositivo	Tipo de conexión	Parámetros de red	Tipo de dispositivo	Número de serie	Nivel de seguridad	Estado uso de	Actualización del firmware	Operación
<input type="checkbox"/>	Pantalla 205	IP/Dominio		Estación inter...	DS-KH6310-WL0120190614W...	Segura	Desconect.	Ninguna versión disponible	
<input type="checkbox"/>	Pantalla 206	IP/Dominio		Estación inter...	DS-KH6310-WL0120190614W...	Segura	Desconect.	Ninguna versión disponible	
<input type="checkbox"/>	Pantalla 207	IP/Dominio		Estación inter...	DS-KH6310-WL0120190323W...	Segura	Desconect.	Ninguna versión disponible	
<input type="checkbox"/>	Pantalla 208	IP/Dominio		Estación inter...	DS-KH6310-WL0120190723W...	Segura	Desconect.	Ninguna versión disponible	
<input checked="" type="checkbox"/>	Pantalla 209	IP/Dominio		Estación inter...	DS-KH6310-WL0120190614W...	Segura	Desconect.	Ninguna versión disponible	
<input type="checkbox"/>	Pantalla 210	IP/Dominio		Estación inter...	DS-KH6310-WL0120190723W...	Segura	Desconect.	Ninguna versión disponible	
<input type="checkbox"/>	Pantalla 211	IP/Dominio		Estación inter...	DS-KH6310-WL0120190417W...	Segura	Desconect.	Ninguna versión disponible	

Figura A4.44 Pantalla a ser configurada

5. Dirigirse a la zona **Talkback** y escoger la opción **Room Number**.

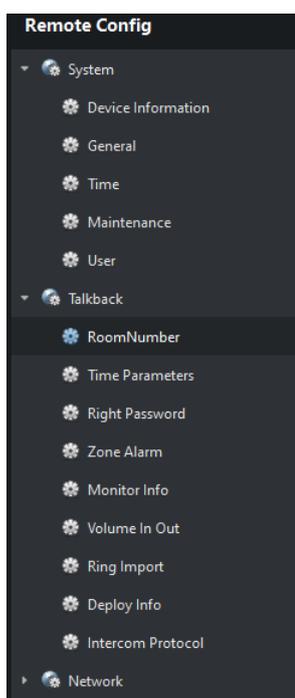


Figura A4.45 Opción *Room Number*

6. Comprobar que en la sección **Device type** se encuentre seleccionada la opción **Indor Station** y en la sección **room No** se encuentre correctamente escrita la extensión correspondiente al monitor de cada una de las oficinas.

Configure Room Numbers

Device ID Cfg

Device type: Indoor Station

room No.: 322

Floor No.: 1

Save

**Figura A4.46** Configuración *Device Type*

7. Por último, se procede a guardar cualquier cambio realizado dando clic en el botón **Save** ubicado en la parte inferior del cuadro.

Configure Room Numbers

Device ID Cfg

Device type: Indoor Station

room No.: 322

Floor No.: 1

Save

**Figura A4.47** Se guarda las configuraciones

**NOTA:** Cada extensión corresponde al área de oficina (2,3,4) y el número de cubículo dentro de cada una de estas.

**Ejemplo:** Área de Oficina 2

Cubículo 14

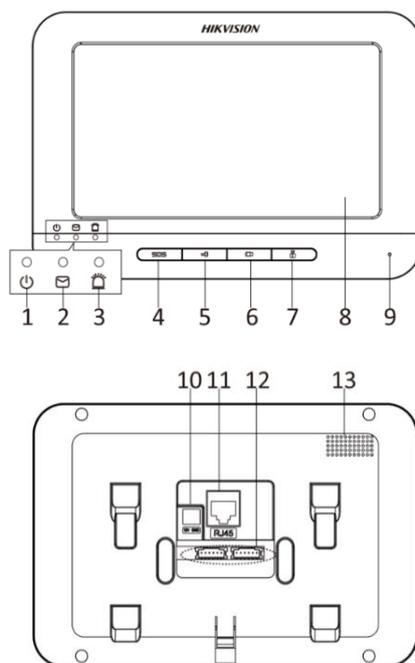
Extensión = 214

## **ANEXO A5: MANUAL DE USUARIO**

# 1. MONITOR

## 1.1. Descripción de los elementos del monitor.

Está compuesto por los elementos que se detallan en la figura A5.1 y se describen en la tabla A5.1 a continuación.



**Figura A5.1** Elementos monitor

**Tabla A5. 1** Descripción de elementos.

ÍNDICE	DESCRIPCIÓN
1	Indicador de fuente de alimentación
2	Indicador de información
3	Indicador de alarma
4	Llave SOS
5	Tecla de desbloqueo
6	Tecla de visualización en vivo
7	Clave del Centro de Gestión
8	Pantalla LCD
9	Micrófono
10	Interfaz de fuente de alimentación
11	Interfaz de red
12	Terminales
13	Altavoz

Los docentes tienen acceso a las funciones del monitor ubicado en sus oficinas, de las cuales se detallan las opciones de llamada, registro de llamadas y bloque de llamadas.

La figura A5.2 muestra la interfaz principal del equipo.



Figura A5.2 Interfaz principal

## 1.2. Llamada entre monitores

1. Presione la pestaña  para ingresar a la interfaz de llamada de los docentes, se desplegará la siguiente pantalla como lo muestra la figura A5.3.

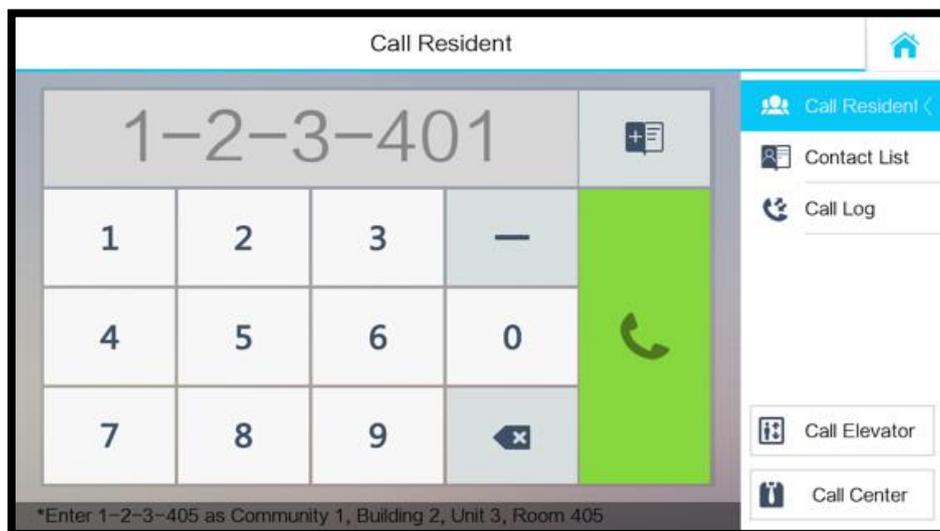


Figura A5.3 Interfaz de llamada

2. Introduzca el número de extensión a marcar.

- Presione  para iniciar una llamada.
- Presione  para terminar una llamada.

### 1.3. Llamada al centro de administración

Se puede llamar al centro de administración de dos maneras:

- Presione la pestaña  en la interfaz principal del equipo mostrada en la figura A5.2.
- a) Presione la pestaña  en la interfaz de llamada mostrada en la figura A5.4.

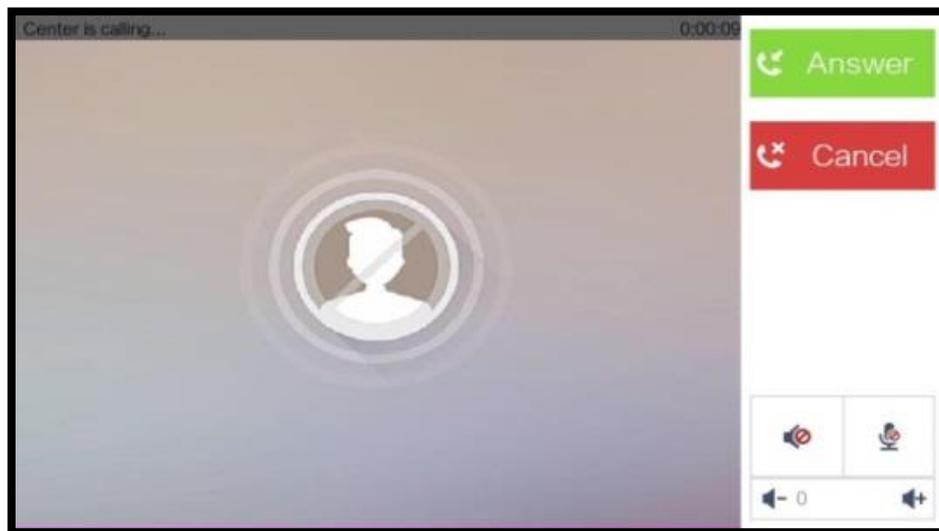


Figura A5.4 Llamada centro

### 1.4. Aceptar solicitud de llamada

1. Presione la pestaña  para aceptar la solicitud de llamada audiovisual.
2. Presione la pestaña  para terminar una llamada audiovisual.



**Figura A5.5** Llamada placa

3. Se puede desbloquear la puerta de dos formas:
  - a) Presione la pestaña  para desbloquear la puerta.
  - b) Presione el botón  para desbloquear la puerta.

**Tabla A5. 2** Funcionalidad de íconos.

	Captura la imagen de visualización en vivo de quien ha llamado a la puerta.
	Habilita/Deshabilita el altavoz.
	Habilita/Deshabilita el micrófono.
	Disminuye/Aumenta el volumen.

### 1.5. Administración del registro de llamadas

1. En la interfaz de llamadas de la figura A5.6 presione la pestaña  para ingresar al registro de llamadas.
2. Presione la pestaña **Llamadas Perdidas o Todas las Llamadas** para ver los registros.
3. Presione el ícono de imagen en la interfaz de registro para abrir la captura hecha por la placa externa, como se muestra en la figura A5.7.

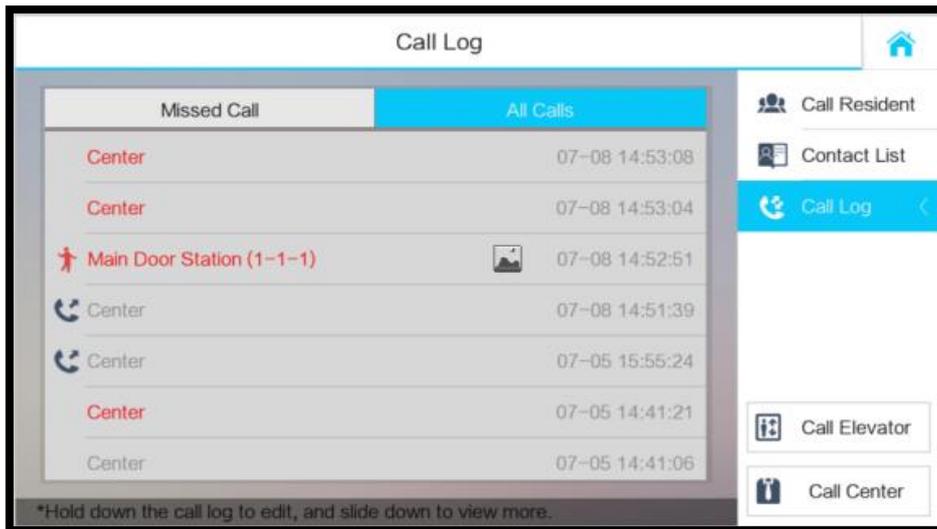


Figura A5.6 Interfaz de registro

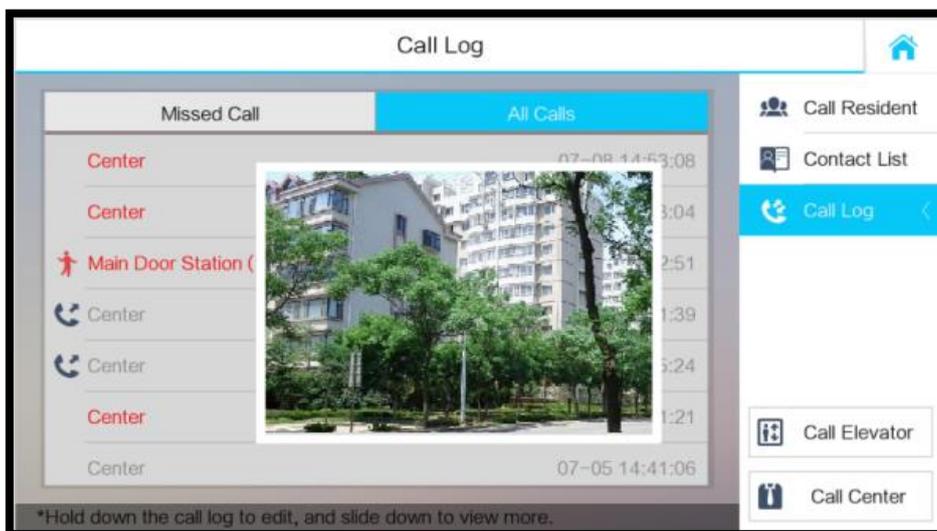


Figura A5.7 Captura placa exterior

## 1.6. Bloqueo de llamadas



1. Presione la pestaña de la figura A5.2  para ingresar a la interfaz DND (no molestar).
2. Se puede configurar dos tipos de modo sin molestias:
  - a) **Todo el día**

Cambie  a  para deshabilitar la entrada de llamadas al monitor, durante todo el día.

### b) Horario

Cambie  a  para deshabilitar la entrada de llamadas al monitor, en función del horario establecido por el docente.

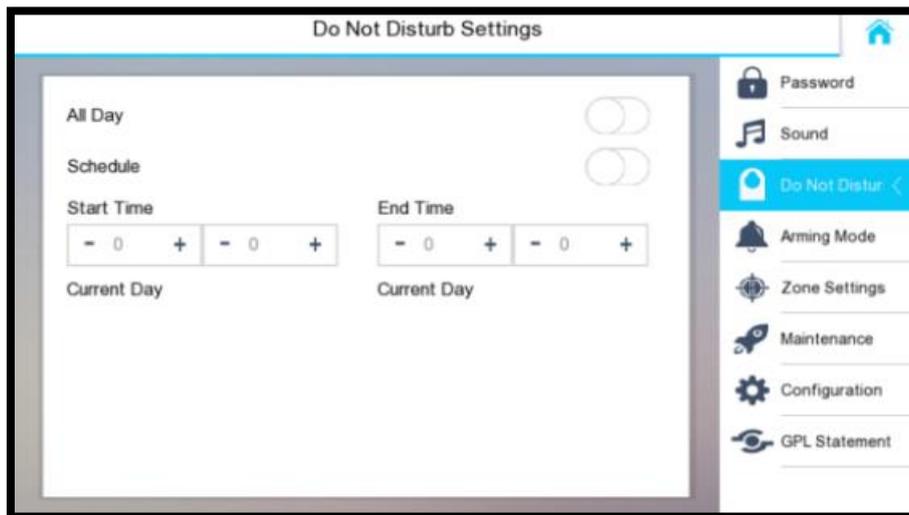


Figura A5.8 Interfaz DND

## 1.7. Agregar contactos

1. Presione la pestaña de la figura A5.9  en la interfaz de usuario para ingresar a la interfaz de la lista de contactos.

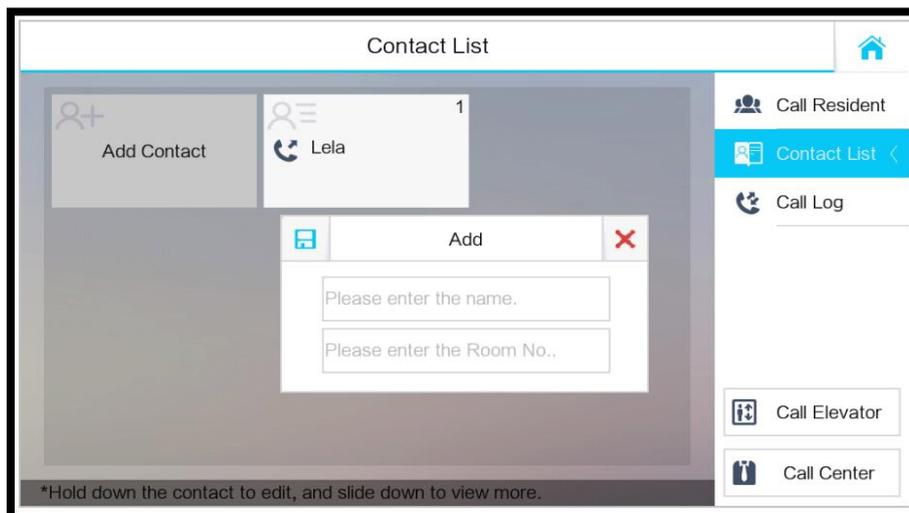


Figura A5.9 Lista de contactos

2. Presione la pestaña Agregar contacto para abrir el cuadro de diálogo de agregar contacto.

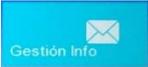
3. Ingrese el nombre y el número de habitación del contacto.

4. Presione la pestaña  para guardar la configuración.

Mantenga presionado un contacto agregado para abrir el menú de manejo de contactos.

 Call	Inicia la llamada con el contacto seleccionado.
 Edit	Modifica la información del contacto.
 Delete	Elimina el contacto seleccionado.
 Clear	Elimina todos los contactos agregados.

### 1.8. Registro de alarmas, mensajes e imágenes

1. Presione la pestaña de la figura A5.2  para ingresar a la interfaz de gestión de la información. Si existen mensajes nuevos la pestaña aparecerá en rojo



2. Se puede visualizar tres tipos de mensajes como se muestra en la Figura A5.10:

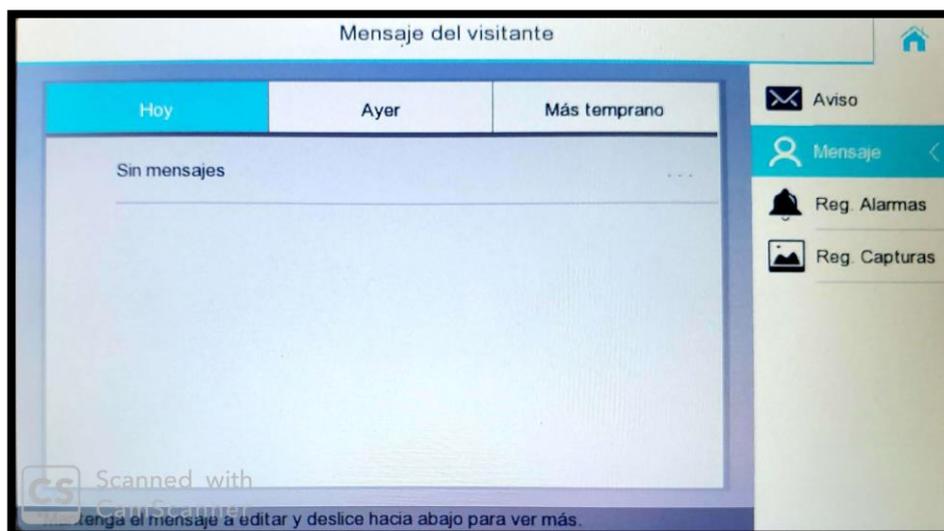


Figura A5.10 Interfaz Gestión de la información

### a) Registro de alarmas

Seleccione la pestaña  Reg. Alarma: < del interfaz de gestión de la información para su visualización como se muestra en la Figura A5.11.

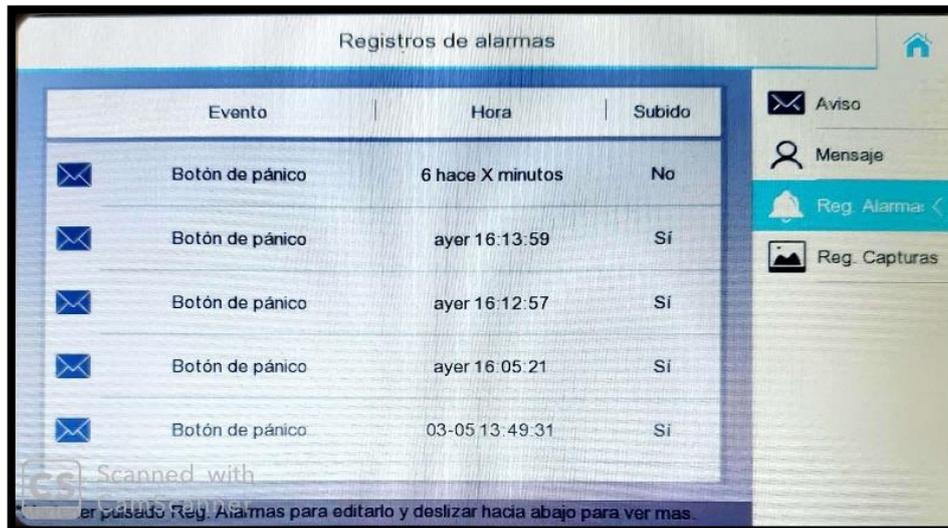


Figura A5.11 Registro de alarmas

### b) Mensajes de audio

Seleccione la pestaña  Mensaje < del interfaz de gestión de la información, para tener acceso a los mensajes de audio como se muestra en la Figura A5.12. Presione sobre el audio que desee escuchar.

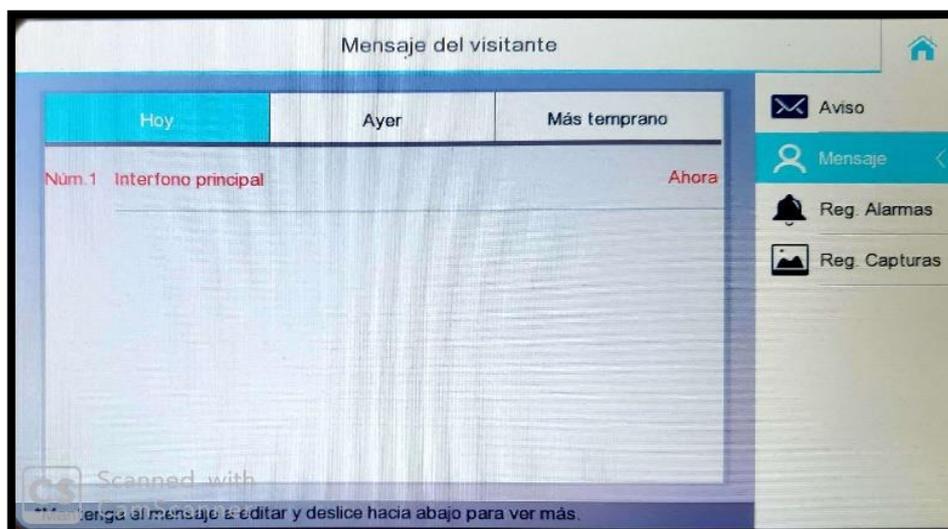


Figura A5.12 Mensaje del visitante

### c) Mensajes visuales

Seleccione la pestaña  Reg. Capturas < del interfaz de gestión de la información para observar las capturas de imagen hechas por el videoportero, como se muestra en la Figura A5.13. Presione sobre la imagen para tener una mejor visualización.

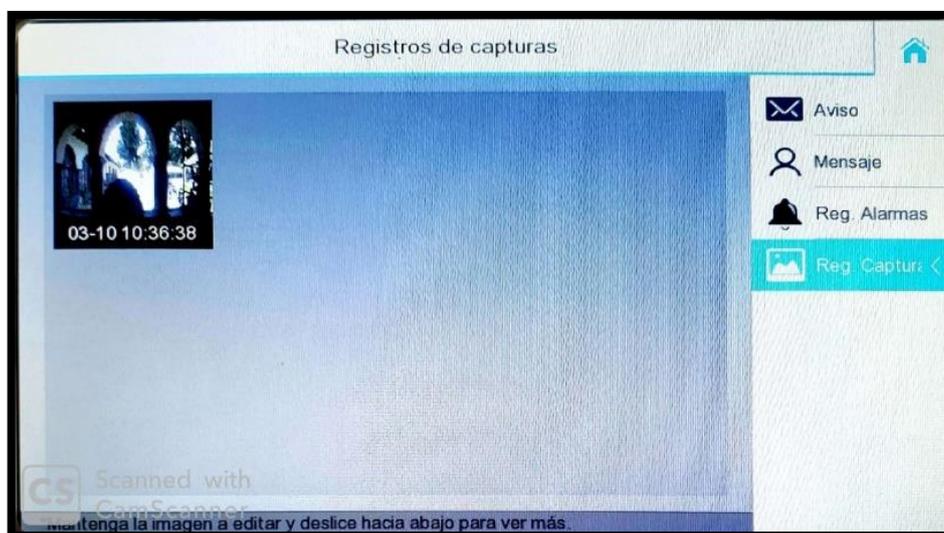
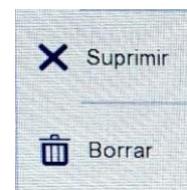


Figura A5.13 Registro de capturas

3. Para borrar el registro de alarmas, mensajes e imágenes mantenga presionado 5 segundos sobre el elemento a eliminar. Donde se tiene dos opciones: Suprimir (Elimina solo el elemento seleccionado) y Borrar (Elimina todos los elementos del registro).



## 2. HIK CONNECT

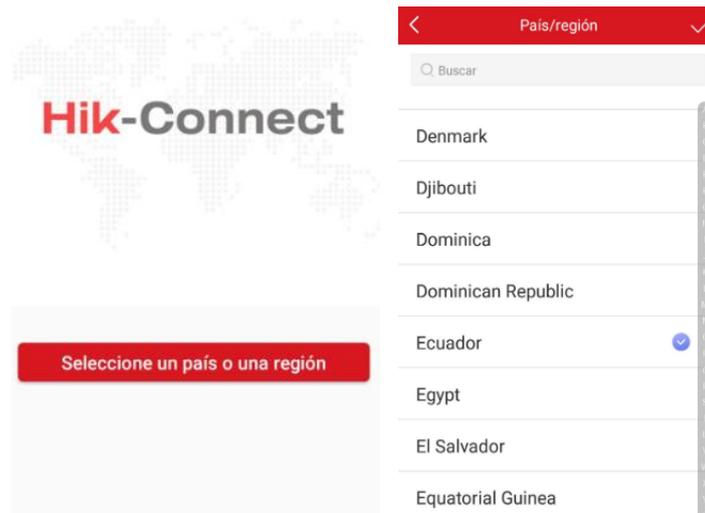
### 2.1. Instalación

1. Ingrese en *Google Play* o *App Store*.
2. En la barra de búsqueda digite "*Hik-Connect*".
3. Descárguelo e instálelo en su teléfono celular.

4. Al finalizar la instalación, toque para ejecutar  .

### 2.2. Registro e inicio de sesión de usuario

1. Toque  y a continuación, toque sobre **Seleccione un país o región**, seleccionar el país o la región y guardar los ajustes. Como se muestra en la figura A5.14.

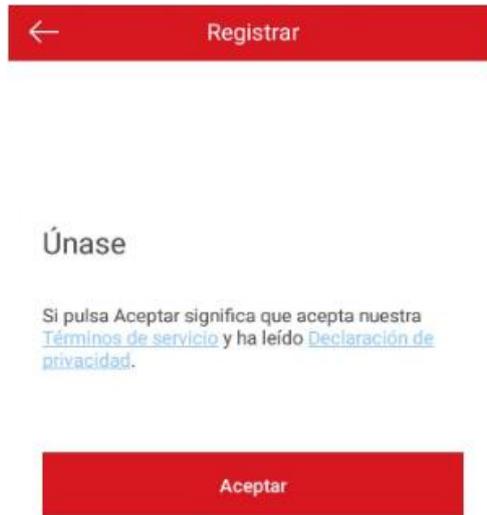


**Figura A5.14** Selección país o región

2. Una vez seleccionada la región o país, se procede a la creación de una cuenta o inicio de sesión, se presiona en iniciar sesión y se acepta los términos y condiciones, como se muestra en las figuras A5.15 y A5.16.

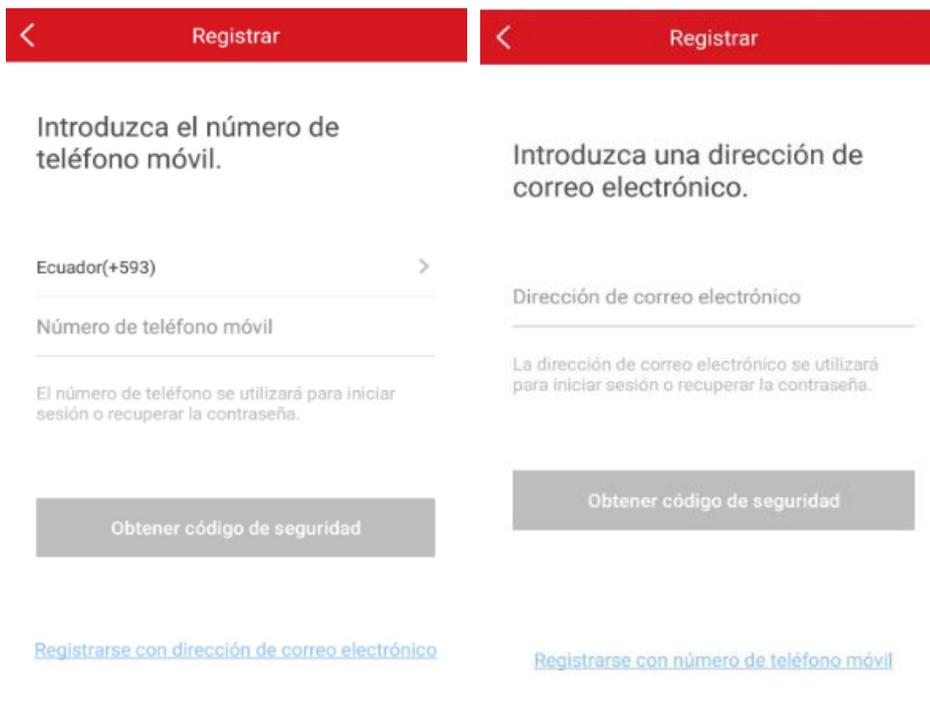


**Figura A5.15** Inicio de sesión



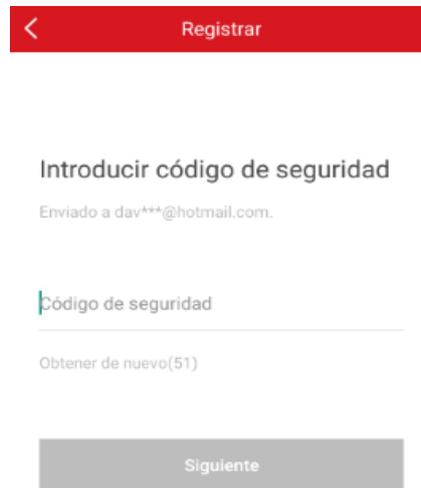
**Figura A5.16** Términos y condiciones

3. Para crear una cuenta, existe la posibilidad de registrarse con el número celular o correo electrónico, como se muestra en la figura A5.17.



**Figura A5.17** Registro de la cuenta

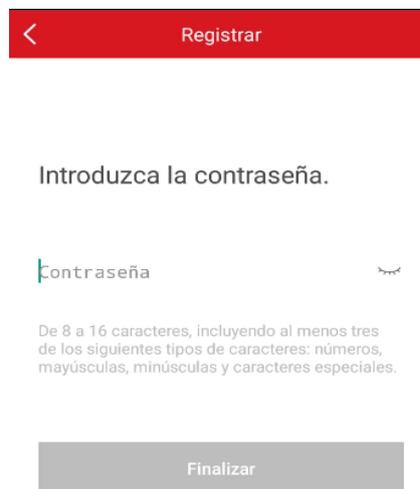
- Al seleccionar una de las dos opciones de registro, es necesario registrar el código de seguridad que es enviado al número telefónico o al correo electrónico como se muestra en la figura A5.18.



The screenshot shows a mobile application interface. At the top, there is a red navigation bar with a white left-pointing arrow and the text "Registrar". Below this, the main heading is "Introducir código de seguridad". Underneath the heading, it says "Enviado a dav\*\*\*@hotmail.com.". There is a text input field with the placeholder text "Código de seguridad". Below the input field, there is a link that says "Obtener de nuevo(51)". At the bottom of the screen, there is a grey button with the text "Siguiete".

**Figura A5.18** Registro del código de seguridad

- Para finalizar, una vez ingresado el código de seguridad generado por la aplicación, se ingresa una contraseña con la que el usuario va a poder acceder a la aplicación. Como se observa en la figura A5.19.

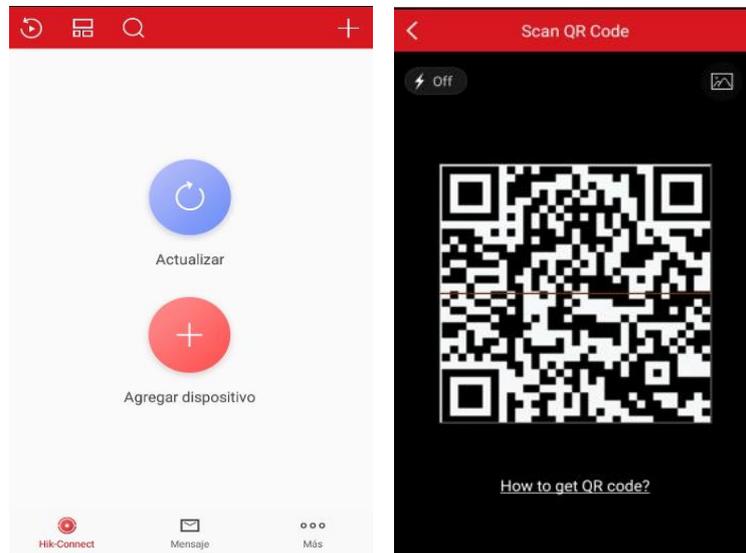


The screenshot shows a mobile application interface. At the top, there is a red navigation bar with a white left-pointing arrow and the text "Registrar". Below this, the main heading is "Introduzca la contraseña.". There is a text input field with the placeholder text "Contraseña" and a small eye icon to its right. Below the input field, there is a text block that says "De 8 a 16 caracteres, incluyendo al menos tres de los siguientes tipos de caracteres: números, mayúsculas, minúsculas y caracteres especiales.". At the bottom of the screen, there is a grey button with the text "Finalizar".

**Figura A5.19** Contraseña de usuario

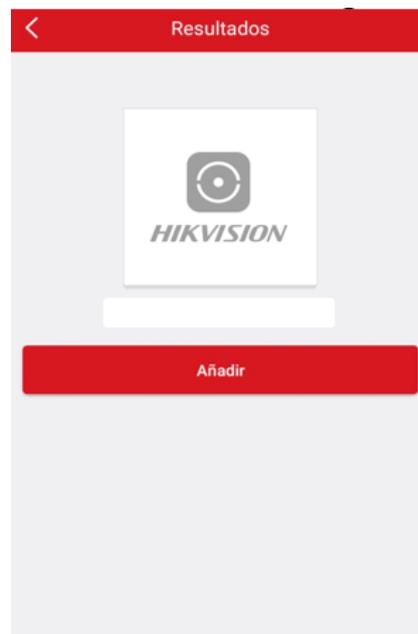
### 2.3. Añadir dispositivos

1. Seleccionar la opción de agregar dispositivos y se procederá a escanear el código QR del dispositivo que se desea agregar, como se muestra en la figura A5.20.



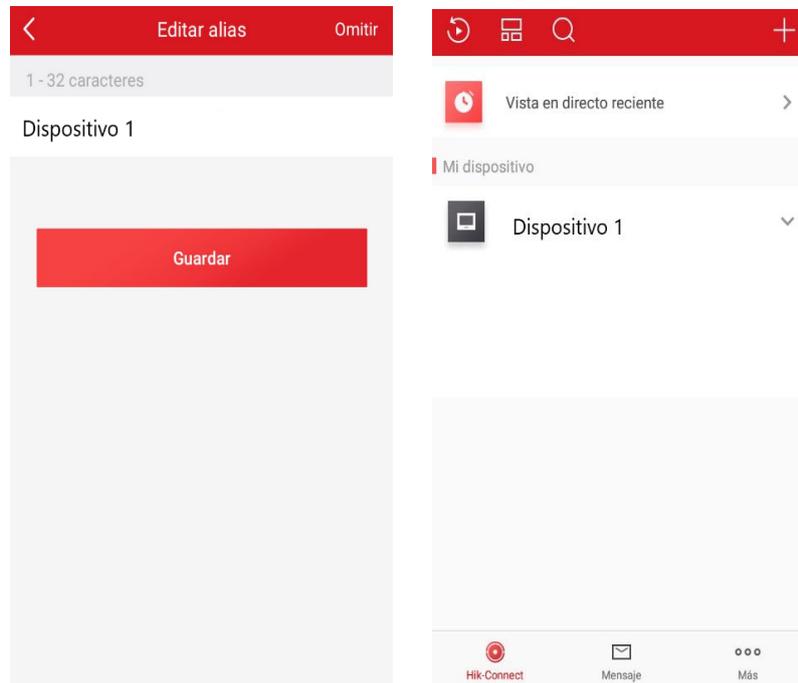
**Figura A5.20** Agregar Dispositivos

2. Una vez escaneado el código QR, se procederá a añadir el dispositivo como se observa en la figura A5.21.



**Figura A5.21** Añadir el dispositivo

3. Para finalizar, se procederá a insertar un nombre al dispositivo y se coloca en guardar como muestra la figura A5.22.



**Figura A5.22** Asignación de nombre al dispositivo

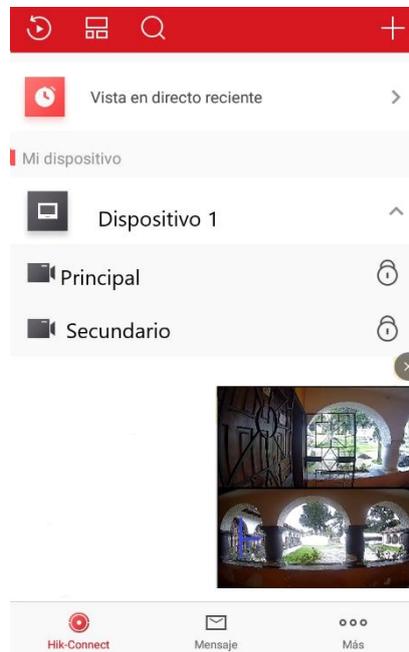
## 2.4. Control de vista en directo

1. Seleccionar  del dispositivo agregado, donde se desplegará dos opciones como se muestra en la figura A5.23. Al presionar el ícono permitirá  la apertura de la puerta.



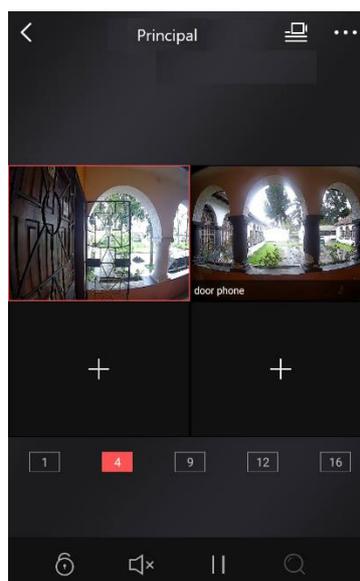
**Figura A5.23** Opciones de visualización del dispositivo

- Al seleccionar la opción principal, se mostrará la cámara de la estación maestra externa y el secundario mostrará la cámara correspondiente al portero donde se encuentra anclado el dispositivo. Como se muestra en la figura A5.24.



**Figura A5.24** Visualización de las diferentes cámaras

- Al seleccionar una de las dos visualizaciones se desplegará una ventana de visualización como se indica en la figura A5.25.



**Figura A5.25** Ventana de visualización en vivo

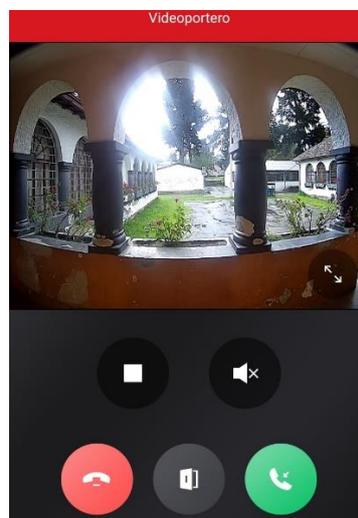
4. En la ventana de visualización, se encontrará en la parte inferior de la ventana una barra de herramientas, la cual contiene algunos de los íconos que se explican en la figura A5.26.

Icono	Descripciones
	Iniciar / parar la ventana de la vista en directo seleccionada.
	Iniciar / parar todos los videos en directo.
	Activar / desactivar el audio.
	Tocar para seleccionar el modo de división de ventanas. Es posible seleccionar 1 ventana, 4 ventanas, 9 ventanas, 12 ventanas o 16 ventanas.
	Habilitar la función de zoom digital.
	Iniciar/detener audio bidireccional.
	Capturar imágenes.
	Grabar.
	Abrir la puerta. <b>Nota:</b> Solo para los dispositivos videointercomunicadores y de control de acceso.
	Activará la cámara vinculada a la función de salida de alarma. <b>Nota:</b> El dispositivo debe ser compatible con la función.

**Figura A5.26** Íconos de la ventana de visualización

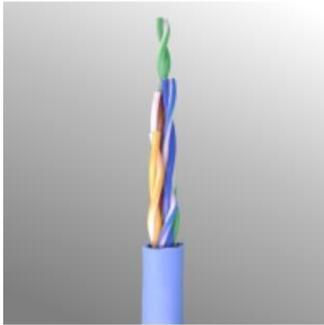
## 2.5. Control de una llamada

Al ingresar una llamada al dispositivo móvil, se mostrará una ventana como la que se presente en la figura A5.27. El ícono de color verde ubicado en la parte inferior permite contestar la llamada, el ícono de color rojo permite colgar o rechazar la llamada y el ícono con la imagen de una puerta permite la apertura de la puerta correspondiente a la oficina.



**Figura A5.27** Control de una llamada

## **ANEXO A6: CABLE DE PAR TRENZADO**



## MULTILAN CAT. 5E U/UTP 24AWGx4P - CMX

**Tipo del Producto** Cables LAN

**Familia del Producto** MultiLan

**Construcción**

RoHS Compliant
Categoría 5e
U/UTP (no blindado)
PVC - CMX

### Características Generales

**Descriptivo**

**Ambiente de Instalación** Interno

**Ambiente de Operación** No agresivo

**Compatibilidad** Toda la línea FCS

**Aplicaciones**

1. Cumple los requisitos físicos y eléctricos de los estándares TIA-568-C.2 y ISO/IEC 11801
2. El cable está de acuerdo con las directivas RoHS (Restriction of Hazardous Substances)
3. Puede ser utilizado con los siguientes padrones actuales de red citados abajo
  - a. Red locales tipo ETHERNET, padrón IEEE 802.3 tipo 10Base T (UTP);
  - b. Red locales tipo TOKEN-RING, padrón IEEE 802.5, 4Mbps y 16Mbps;
  - c. Redes locales 100 BaseTX y 100 BaseT4;
  - d. Redes locales de alta velocidad, padrones emergentes, transmisión de datos hasta 1000 Mbps GIGABIT ETHERNET;
  - e. Red locales ATM 25 y 155Mbps (ATM);
  - f. Compatible con conector RJ-45 macho Cat.5e

**Normas Aplicables** TIA-568-C.2 y sus complementos, ANSI/TIA/EIA-569, ISO/IEC DIS 11801, UL 444

**Certificaciones**

UL Verified	E257905
ETL 4 conexiones	3075278-003
ISO9001/ISO14001	A1969/A10659
Anatel	0036-08-0256

### Características constructivas

**Conductor** Cobre desnudo con diámetro nominal de 24AWG.

**Aislamiento** Poliolefina con diámetro nominal 0.9mm.



Ese informativo es de autoría y propiedad exclusiva de Furukawa Industrial S.A. Es vedada su reproducción en el todo o en parte sin mencionar su autoría, así como la alteración de su contenido o contexto. Todas las especificaciones están sujetas a cambios sin previo aviso. Las imágenes son meramente ilustrativas.

**Resistencia del Aislamiento** 10000 MΩ.km

**Cantidad de Pares** 4 pares 24 AWG

**Par** Los conductores aislados son trenzados dos a dos y forman un par con colores como se muestra en la tabla abajo. Los pasos de torsión deben ser adecuados para atender los niveles de diafonía previstos.

Código de Colores	Par	Conductor "A"	Conductor "B"
	1	Azul	Blanco / Raya Azul
	2	Naranja	Blanco / Raya Naranja
	3	Verde	Blanco / Raya Verde
	4	Marrón	Blanco / Raya Marrón

**Núcleo** Los cuatro pares son reunidos con paso adecuado, formando el núcleo del cable.

**Blindaje** Sin blindaje (U/UTP).

**Cubierta** Constituido por PVC retardante a llama.

**Diámetro Nominal** 4,8 mm

**Color** Azul Claro, Gris, Blanco, Negro.

**Peso del Cable** 26 kg/km

#### Características Físicas

**Grado de Flamabilidad** CMX: IEC 60332-1 según ABNT NBR 14705.

**Temperatura de Instalación** 0°C hasta 50°C

**Temperatura de Almacenamiento** -20°C hasta 70°C

**Temperatura de Operación** -20°C hasta 60°C

#### Características Eléctricas

**Desequilibrio Resistivo Máximo** 5%

**Resistencia Eléctrica CC Máxima del Conductor a 20°C** 93,8 Ω/km

**Capacitancia Mutua 1kHz - Máxima** 56 pF/m

**Desequilibrio Capacitivo Par x Tierra 1KHz - Máximo** 3,3 pF/m

**Impedancia Característica** 100±15% Ω

**Retraso de Propagación Máximo** 545ns/100m @ 10MHz

**Diferencia entre el Retraso de Propagación - Máximo** 45ns/100m

**Prueba de Tensión Eléctrica entre los Conductores** 2500 VDC/3s

**Velocidad de Propagación Nominal** 68%

**Desempeño de Transmisión**

Freq. (MHz)	IL (dB/100m)	NEXT (dB)	PSNEXT (dB)	ACR (dB)
	TIA/EIA Máx.	TIA/EIA MÍN.	TIA/EIA MÍN.	TIA/EIA MÍN.
1	2,0	65,3	62,3	63,3
4	4,1	56,3	53,3	52,2
8	5,8	51,8	48,8	46,0
10	6,5	50,3	47,3	43,8
16	8,2	47,3	44,3	39,0
20	9,3	45,8	42,8	36,5
25	10,4	44,3	41,3	33,9
31,25	11,7	42,9	39,9	31,2
62,5	17,0	38,4	35,4	21,4
100	22,0	35,3	32,3	13,3

Freq. (MHz)	PSACR (dB)	ACRF (dB)	PSACRF(dB)	RL (dB)
	TIA/EIA MIN.	TIA/EIA MIN.	TIA/EIA MIN.	TIA/EIA MIN.
1	60,3	63,8	60,8	20,0
4	49,2	51,7	48,7	23,1
8	43,0	45,7	42,7	24,5
10	40,8	43,8	40,8	25,0
16	36,0	39,7	36,7	25,0
20	33,5	37,7	34,7	25,0
25	30,9	35,8	32,8	24,3
31,25	28,8	33,9	30,9	23,6
62,5	18,4	27,8	24,8	21,5
100	13,3	23,8	20,8	20,1

Las medidas son realizadas a 20°C, en muestras de cable de 100m, sacadas de la bobina, estirados en una superficie no conductiva, conforme descrito en las normas ANSI/TIA-568-C.2.

**ESPECIFICACIÓN TÉCNICA**  
**1366 - V 22 (20/04/2016)**

<b>Grabación</b>	FURUKAWA MULTILAN U/UTP 24AWGx4P IEC 332-1 --- NBR 14703 --- ROHS COMPLIANT --- CMX --- E257905 VERIFIED BY UND. LAB. INC. IN ACCORDANCE WITH CATEGORY 5E TIA-568-C.2 ONLY ANATEL XXXX-XX-XXXX --- YAAMMDDHHmm {1}m  Rastreabilidad: Sobre la cubierta externa es grabado: Y- Proceso de fabricación AAMMDDHHmm :AA-Año, MM-Mes, DD - Día, HH - Hora, mm - minuto
<b>Embalaje</b>	
<b>Tipo de Embalaje</b>	Caja de cartón FASTBOX o bobina de madera.
<b>Cantidad por Carrete</b>	
<b>Dimensiones</b>	350x350x220mm (LAP)