UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERÍA EN SISTEMAS, ELECTRÓNICA E INDUSTRIAL

CARRERA DE INGENIERÍA EN ELECTRÓNICA Y COMUNICACIONES

TEMA:

"SISTEMA DE ALARMA COMUNITARIA PARA EL MERCADO SAN JUAN DE LA CIUDAD SANTIAGO DE PÍLLARO"

Proyecto de Graduación. Modalidad: Proyecto de Investigación, presentado previo la obtención del título de Ingeniera en Electrónica y Comunicaciones

SUBLÍNEA DE INVESTIGACIÓN: Comunicaciones Inalámbricas

AUTOR: Karla Gabriela Chicaiza Guachi

TUTOR: Ing. Geovanni Danilo Brito Moncayo

AMBATO – ECUADOR

Enero 2020

APROBACIÓN DEL TUTOR

En mi calidad de tutor del Trabajo de Investigación sobre el tema: "SISTEMA DE ALARMA COMUNITARIA PARA EL MERCADO SAN JUAN DE LA CIUDAD SANTIAGO DE PÍLLARO", de la señorita KARLA GABRIELA CHICAIZA GUACHI, estudiante de la Carrera de Ingeniería en Electrónica y Comunicaciones de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial de la Universidad Técnica de Ambato, considero que el informe investigativo reúne los requisitos suficientes para que continúe con los trámites y consiguiente aprobación de conformidad con el numeral 7.2 de los Lineamientos Generales para la aplicación de Instructivos de las Modalidades de Titulación de las Facultades de la Universidad Técnica de Ambato.

Ambato enero, 2020

EL TUTOR

Ing. Geovanni Danilo Brito Moncayo, Mg

AUTORÍA

El presente Proyecto de Investigación titulado: "SISTEMA DE ALARMA COMUNITARIA PARA EL MERCADO SAN JUAN DE LA CIUDAD SANTIAGO DE PÍLLARO", es absolutamente original, auténtico y personal, en tal virtud, el contenido, efectos legales y académicos que se desprenden del mismo son de exclusiva responsabilidad del autor.

Ambato enero, 2020

AUTOR

Karla Gabriela Chicaiza Guachi

CI: 1805508023

APROBACIÓN DEL TRIBUNAL DE GRADO

La Comisión Calificadora del presente trabajo conformada por los señores docentes Ing. Santiago Altamirano e Ing. Andrea Sánchez, revisó y aprobó el Informe Final del Proyecto de Investigación Titulado "SISTEMA DE ALARMA COMUNITARIA PARA EL MERCADO SAN JUAN DE LA CIUDAD SANTIAGO DE PÍLLARO", presentado por la señorita Karla Gabriela Chicaiza Guachi, de acuerdo al numeral 9.1 de los Lineamientos Generales para la Aplicación de Instructivos de las Modalidades de Titulación de las Facultades de la Universidad Técnica de Ambato.

Ing. Mg. Elsa Pilar Urrutia Urrutia
PRESIDENTA DEL TRIBUNAL

Ing. Santiago Altamirano
DOCENTE CALIFICADOR

Ing. Andrea Sánchez.
DOCENTE CALIFICADOR

DERECHOS DE AUTOR

Autorizo a la Universidad Técnica de Ambato, para que haga uso de este Trabajo de Titulación como un documento disponible para la lectura, consulta y procesos de investigación.

Concedo los derechos de mi Trabajo de Titulación, con fines de difusión pública, además autorizo su reproducción dentro de las regulaciones de la Universidad.

Ambato enero, 2020

Karla Gabriela Chicaiza Guachi

CI: 1805508023

DEDICATORIA

A mi madre Glorita Guachi, por su sacrificio y dedicación constante día a día, por todo el apoyo incondicional que me ha brindado hasta la culminación de mi formación profesional, una persona muy importante, luchadora y que a pesar de sus limitaciones me ha ensañado siempre a ser una buena persona, a vencer todos los restos que se me presenten en la vida, una persona ejemplar y guía en mi vida.

A mis hermanos Diego y Lizbeth por su apoyo incondicional, por su cariño y por sus palabras alentadoras para llegar a ser profesional.

Karla Gabriela Chicaiza Guachi

AGRADECIMIENTO

Principalmente a Dios por haberme dado salud y vida hasta el día de hoy, a la Virgencita del Cisne por darme fuerzas para seguir a delante y llegar a culminar esta etapa profesional.

A mi madre por confiar en mí y brindarme todo su apoyo, por enseñarme a seguir adelante aun cuando el camino sea muy difícil y a todos mis familiares que de una u otra manera me apoyaron en lo largo de mi formación profesional.

Un agradecimiento especial a mi tutor Ing. Geovanni Brito, por sus conocimientos impartidos para lograr el desarrollo de este proyecto y por sus palabras de ánimo y fuerzas para seguir adelante.

Karla Gabriela Chicaiza Guachi

ÍNDICE

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

En el presente proyecto de investigación, se realizó el prototipo de un sistema de alarma comunitaria para el mercado “San Juan” de la ciudad Santiago de Píllaro, un centro que no cuenta con un sistema de seguridad y que a través de la tecnología, permite a la comunidad estar en alerta ante situaciones de vandalismo, brindándoles una forma de medidas de protección humana.

El diseño del prototipo se ejecutó en una tarjeta Raspberry Pi 3B+, la cual se desempeña como el centro de procesamiento de todo el sistema, en base a dos modos de funcionamiento, de acuerdo a los horarios de apertura del mercado. Se hizo uso de la mensajería instantánea Telegram y WhatsApp, para el envío de alertas y alarmas tanto auditivas como visuales hacia los diferentes terminales de usuarios y unidades policiales. Para la alarma auditiva se utilizó un puerto GPIO de la Raspberry Pi y una cámara IP para el monitoreo y activación de alarmas en función a la detección de movimiento; todo esto se desarrolló a través del lenguaje de programación Python, en donde se crearon objetos, clases y funciones para ejecutar tanto las alarmas como el sistema de video vigilancia para un control remoto, por medio de una página web. La interconexión entre los dispositivos fue mediante la comunicación inalámbrica wifi que proporcionó el router.

Otro servicio desarrollado fue la telefonía IP, en donde se usó Asterisk como centralita para la comunicación entre usuarios, todo ello en base a la configuración de extensiones e instalación del software softphone zoiper en los teléfonos móviles. Adicionalmente, se elaboró el diseño de la red wifi y del sistema de video vigilancia IP, utilizando equipos óptimos para el funcionamiento, en caso llegase a ser implementado.

Palabras Clave: Sistema de alarma, Telegram, WhatsApp, Video Vigilancia, Raspberry Pi, Python, OpenCV.

ABSTRACT

In the present research project, the prototype of a community alarm system for the "San Juan" market of the city of Santiago of Píllaro was carried out, a center that does not have a security system and that through technology, It allows the community to be on alert for vandalism situations, providing them with a form of human protection measures.

The prototype design was executed on a Raspberry Pi 3B + card, which is carried out as the processing center for the entire system, based on two modes of operation according to the opening hours of the market. Telegram and WhatsApp instant messaging was used to send both auditory and visual alerts and alarms to the different user terminals and police units. For the auditory alarm, a GPIO port of the Raspberry Pi and an IP camera were used for monitoring and activation of alarms based on motion detection; All this is executed based on the Python programming language, where objects, classes and functions are created to execute alarms such as the video surveillance system for a remote control, through a web page. The interconnection between the devices was powered by the wireless Wi-Fi communication provided by the router.

Another service developed is IP telephony, where Asterisk is used as a switchboard for communication between users, all based on the configuration of extensions and installation of the zoiper softphone software on mobile phones. In addition, the design of the Wi-Fi network and the IP video surveillance system was developed, using optical equipment for operation, in case you get implemented.

Key Words: Alarm system, Telegram, WhatsApp, Video Surveillance, Raspberry Pi, Python, OpenCV

CAPÍTULO I

MARCO TEÓRICO

1.1. ANTECEDENTES INVESTIGATIVOS

Para el desarrollo de esta investigación se ha utilizado fuentes bibliográficas y repositorios de diferentes universidades que existen fuera y dentro del país, relacionados al desarrollo de varios sistemas de alarmas comunitarias utilizando distintos tipos de tecnología como se detalla a continuación:

Zhaoxia W, Hanshi W, Lizhen L, Wei S y JingLi L, desarrollan en el año 2015 el "Diseño de un sistema de alarma comunitaria basado en MCU y GSM" , en donde usan un módulo PTC35i para el diseño de la red móvil GSM y enviar señales de voz y datos a través de comandos AT, mientras que para el diseño del hardware un microcontrolador AT89C52 el cual controla el sistema de alarma de monitoreo infrarrojo, muestran la alarma en una pantalla lcd y el control del módulo GSM, además optaron por usar un sensor infrarrojo pasivo para la detección de intrusos, convirtiendo la seguridad tradicional de la red y de las ventanas antirrobos en una red robusta e invisible. Con el desarrollo de este sistema logran que las personas emitan las alarmas auditivas y visuales a través de mensajes de texto cortos ya sean a los demás usuarios como al administrador [1].

En el año 2017 Freddy Aguilar Villalba, realiza el "Desarrollo de un Prototipo de Alarma Multimodal Comunitaria Utilizando el Protocolo Ipv6 y GPRS para Smart Cities con Monitoreo en Tiempo Real" que controla cada hogar y en general todo un bloque residencial, ha sido diseñada de acuerdo a las necesidades, como el control de acceso por clave, una central programable colocada en la garita del guardia, control y monitoreo remoto de cada hogar y una alarma de activación urgente, para ello usa un Arduino Mega como centralizador y gestor de recursos, una Shield SIM900 para el diseño de un sistema GSM permitiendo alertar la violación de acceso y una RaspBerry Pi3 para el monitoreo, cada residencia tiene su propio sistema de alarma. Con este

proyecto logran alertar a todo el bloque residencial en caso de existir eventos extraños enviando un mensaje al propietario del domicilio y al guardia de seguridad; además al usar el protocolo IPv6 permitió la interoperabilidad entre redes LowPan e Internet optimizando la utilización de estándares de internet sobre redes inalámbricas de baja potencia [2].

Evelyn Llagua Mosquera en el año 2017, desarrolla un "Sistema de Monitoreo de Alarmas mediante Mensajería SMS e Interface hacia un computador para la Recepción de Eventos de Emergencia" diseñado para la empresa de seguridad electrónica SIDEPRO con la finalidad de brindar un mejor servicio a sus clientes, cuenta con una central de alarma en donde usa un arduino mega 2560, un módulo GSM/GPRS, sensores de humo, magnético y movimiento, permitiendo detectar una situación de emergencia en las viviendas y la información receptada enviarla mediante mensajes de texto SMS a través de la red GSM a la central de monitoreo que al igual que la central de alarma consta de un arduino mega y un módulo GSM/GPRS SIM 900 para la recepción de información y mostrarla en una página web para una mejor visualización de datos, con ello eleva los niveles de seguridad en las viviendas debido al monitoreo a distancia y al aviso que brinda el sistema tanto a los propietarios de las viviendas como a las diversas entidades de seguridad [3].

En el año 2017, Sruthy, S y Sudhish, N, desarrollan un "Sistema de vigilancia para hogares basado en IoT y Raspberry", en donde usan conectividad wifi y crean nodos de sensores inalámbricos con un sistema de control para vigilancia. El sistema está compuesto de dos nodos sensores, el nodo sensor de movimiento infrarrojo pasivo y el nodo sensor de detección de incendios, un módulo NodeMCU ESP8266 que lo utilizan para procesar eventos que provienen de los sensores y enviarlos al controlador; una vez que reciben la notificación activan una cámara para capturar el evento y enviar alertas al usuario por correo electrónico, mensajes o llamadas telefónicas. Este sistema permitió a los usuarios vigilar sus hogares y recibir alertar mediante la observación de videos en vivo de su hogar a través de una página web [4].

Boris Gómez en el año 2018, realiza un "Estudio de Sistemas de Alarma Comunitaria. Caso de Estudio Conjunto Residencial Ruiseñor 2", Boris efectúa varios estudios para llegar a diseñar e implementar un sistema de alarma comunitaria para el conjunto

residencial, el cual consta de botones de pánico inalámbricos con cobertura de hasta 100 metros y línea de vista, una red GSM para emitir mensajes y llamadas hacia la central y sensores que permiten activar alarmas sonoras y visuales con la finalidad de poder alertar a los propietarios de las viviendas, esta es colocada a la entrada del conjunto residencial, en donde la alerta emitida por un usuario acciona las alarmas y a su vez notifica a los demás usuarios registrados e informa a la central de monitoreo esto en base a la red celular GSM ya sea claro, movistar o cnt, toda la configuración la realiza usando software libre de arduino. Con este sistema logra que los usuarios sean alertados mediante llamadas o mensajes en un tiempo menor a 2 minutos [5].

En el año 2018 Victor O, Etinosa N, Praise J, Morgan K, Uzairue S, realizan un "Sistema de alerta de seguridad para emergencia comunitaria" en donde dan solución a inseguridades que atraviesan lugares rurales y suburbanos de Nigeria , desarrollan una aplicación basada en JavaScript denominada "CEMAS", la cual consta de un botón de pánico que permiten a los habitantes activar las centrales de alarma por medio de mensajes SMS, estas centrales las ubican en el centro de la comunidad y en la estación de policía. Hacen uso de un arduino uno, un módulo GSM, una sirena, un servidor en la nube y una base de datos MySQL con sus respectivos softwares de configuración. Con el diseño de una interfaz gráfica móvil fácil de usar, los miembros de la comunidad pueden emitir alarmas hacia las entidades de seguridad y obtener ayuda en un menor tiempo de respuesta [6].

Actualmente, la inseguridad se da por varios factores, trayendo así la delincuencia en diferentes modalidades, como abortos, homicidios, robo a instituciones públicas, a personas, de accesorios, entre otros. Principalmente este tipo de delitos hoy en día es controlado por varios dispositivos como elementos de prevención o disuasión; dentro de estos se hallan los sistemas de video-vigilancia, que de cierta manera, su eficacia es señalada para determinados lugares, mostrando un déficit en el monitoreo de las imágenes captadas por las cámaras ya que la disponibilidad de pantallas y del personal que las opera es inferior a la cantidad de estos equipos de seguridad, restando así la efectividad del sistema [7].

A nivel mundial la seguridad de los habitantes es una de las principales preocupaciones tanto para organizaciones como para los gobiernos, siendo un obstáculo social y

económico en todos los países, esto según el informe del Programa de Desarrollo de la ONU; varias de las naciones han visto la necesidad de optar diversas medidas y métodos que ayuden a garantizar la seguridad ciudadana, pero existen lugares que van creciendo exponencialmente a los que no llega el mismo tipo de ayuda o tienen un sistema de alerta ineficaz aumentando el tiempo de respuesta por parte de las autoridades y la gravedad de dichas emergencias [8].

La inseguridad en la última década es ubicada de acuerdo a varias encuestas realizadas en la región Latinoamérica, en el tope de las inquietudes nacionales, originada por el desempleo, la inflación o la corrupción. El aspecto más sobresaliente de este tipo de inseguridad es el delito contra la propiedad, predominando el robo de pequeña escala a un acto más violento como el robo a gran escala y asaltos, indicando que estos delitos implican niveles de organización para conducir la actividad vandálica, con circuitos de mercado negro [9].

La seguridad pública es muy importante en el país, pero a nivel nacional la ciudadanía no ha encontrado una respuesta positiva debido a que la región al poseer bajos ingresos económicos presenta bajos índices de nivel de seguridad y bienestar ciudadana, provocando pérdidas económicas y humanas. Actualmente, el país presenta una cifra de 125.528 delitos contra la propiedad en donde el robo a personas, de domicilios, de accesorios, a locales comerciales y a fábricas son los más notorios con una cifra de 67.061 delitos, según datos estadísticos presentados por el Ministerio del Interior en el año 2015 [10]; mientras que para el año 2016 existe una cifra de 29.741 robos a personas, 16.145 robos a domicilios y 6.138 robos a unidades económicas, siendo estas el número de denuncias de delitos de mayor incidencia a nivel nacional, esto según el Registro Administrativo de Denuncias Receptadas en el Sistema Integrado de Administración de Fiscalías (SIAF) [11].

Con 1.440 hechos delictivos cometidos en el año 2016 Tungurahua se convirtió en la novena provincia con el número más alto de delitos suscitados, esto según el Registro Administrativo de Denuncias Receptados en el Sistema Integrado de Administración de Fiscalías (SIAF) [11].

Santiago de Píllaro es otra de las ciudades que hoy en día es atacada por personas dedicadas a la delincuencia, una situación que pone en preocupación a sus habitantes, los acontecimientos más suscitados según datos de la Policía Nacional que se encuentra a cargo del cantón son: el robo a locales comerciales, a vehículos, de accesorios, a viviendas y de personas, con una cifra de 40 hechos delictivos cometidos en el año 2017, esto en base a datos proporcionados por diario La Hora [12], por lo que esta institución al no contar con sistemas de notificación pertinentes realizan patrullajes intensivos.

Uno de los lugares que no cuenta con un sistema de alarma para evitar y minimizar estos actos delictivos es el Mercado San Juan, un centro que cuenta con más de 100 locales comerciales, en donde los propietarios se ven afectados por varios acontecimientos que suscitan día a día en el lugar, específicamente generando pérdidas económicas y al no contar con un sistema de cámaras de seguridad no se tiene evidencias de anomalías presentadas generalmente en la noche y no poder dar aviso a la correspondiente UPC del sector.

1.2. OBJETIVOS

1.2.1. Objetivo General

Implementar un prototipo de sistema de alarma comunitaria para el Mercado San Juan de la ciudad Santiago de Píllaro.

1.2.2. Objetivos Específicos

- Analizar la situación actual del nivel de seguridad y de comunicaciones que existe en el Mercado San Juan.
- Estudiar las diferentes tecnologías para el desarrollo del sistema de alarma comunitaria integral.
- Realizar el diseño de la Red Inalámbrica en el Mercado San Juan para la implementación del proyecto.
- Diseñar el sistema de alarma comunitaria integral que permita el registro, monitoreo IP y servicio de VoIP para el Mercado San Juan de la ciudad Santiago de Píllaro.

1.3. FUNDAMENTACIÓN TEÓRICA

1.3.1. Seguridad Electrónica

Sistema que permite proteger personas, instalaciones o bienes materiales dentro de una empresa u hogar, a través de elementos tecnológicos interconectados entre sí, siendo gestionados desde una central de alarma, y activando diferentes elementos como sirenas, cámaras de video, luces, envío de mensajes a bomberos, policía, etc. En la figura 1, se presenta el esquema general de un sistema de seguridad electrónica [13].

Figura N° 1. Esquema General de un Sistema de Seguridad. [13]

1.3.2. Seguridad Electrónica Antirrobos

Sistema electrónico que brinda seguridad a un área, capaz de gestionar: intrusión, robos, control de accesos y presencia, cuyo objetivo es la prevención de hechos delictivos mediante la disuasión de intrusos y dar aviso a las respectivas autoridades [13]. En la figura 2 se presenta los elementos que constituye un sistema de este tipo:

Figura N° 2. Elementos de un Sistema de Seguridad. [13]

Elementos de sistema de seguridad electrónica antirrobos

Estos sistemas se encuentran conformados por los siguientes elementos:

- **Central de alarmas o Unidad de Proceso:** Recepta la señal proveniente de sensores, procesa de acuerdo a la programación establecida y esta información la envía hacia los actuadores para la ejecución de órdenes. Además proporciona

alimentación a todos los elementos conectados a esta central y da aviso oportuno hacia las unidades de ayuda y propietarios, que se encuentran en áreas externas mediante conexión remota. En esta central se toma en cuenta las placas base, microprocesadores, memorias, teclados de control, fuentes de alimentación y baterías de respaldo de energía.

- **Detectores automáticos o sensores:** Son las entradas al sistema, compuesto por dispositivos que funcionan con tensión continua de 9, 12, 24 o 48V.
- **Elementos de aviso:** Ejecutan acciones procedentes de la central de alarma, estos dispositivos son sirenas o luces.
- **Central de recepción de alarmas:** Perteneciente a una empresa de seguridad que permite gestionar las alarmas a distancia, estando disponible las 24 horas. Estas centrales trabajan con conexiones GSM, TCP/IP, GPRS, etc, para el control de varias instalaciones [13].

1.3.3. Sistema de Alarmas Comunitarias

Sistema de prevención ante conductas delictivas que afectan a miembros de una comunidad o sector y permiten la participación organizada de barrios o cuadras, facilitando la intervención de la Policía.

a) Tipos de Alarmas Comunitarias

Estas alarmas se distinguen por la forma de conexión a la central de monitoreo, a continuación se presentan los diferentes tipos:

- **Con conexión a la central:** Estos sistemas envían una señal de alarma a una instalación externa que ofrece los servicios de seguridad, para esta enviar los avisos pertinentes a la policía.
- **Sin conexión a la central:** Solo se emite la difusión de la alarma a toda la comunidad mediante alarmas sonoras y visuales, usando el servicio de mensajería que ofrece la telefonía móvil [14].

b) Especificaciones de un Sistema de Alarma Comunitaria

El uso de las alarmas tienen diferentes funciones de acuerdo a las aplicaciones y al objetivo a cumplir, entre ellas se tiene:

- **Accesibilidad:** Se toma en cuenta los mecanismos usados para accionar la alarma y acelerar el proceso de identificación. Esta depende si la activación es por medio del panel de control o por botones inalámbricos.
- **Disuasiva:** Impide o detiene acciones que ponen en riesgo la vida de los miembros de una comunidad, advirtiendo así que el lugar se encuentra protegido.
- **De difusión:** Se da en dos ámbitos, interna dando aviso a toda la comunidad de forma masiva y externa enviando avisos de hechos eventos anormales a la máxima autoridad como la Policía [14].

1.3.4. Redes Inalámbricas

Las redes inalámbricas hoy en la actualidad se han convertido en una tecnología predominante, que permiten a usuarios estar conectados a cualquier hora y en cualquier lugar del mundo para acceder a información u otro tipo de recursos, todo esto gracias a los enlaces inalámbricos que se han venido desarrollando.

Estas redes inalámbricas son redes que se comunican por medios no guiados a través de ondas electromagnéticas, efectuando la transmisión y recepción por medio de antenas [15].

Clasificación de las Redes Inalámbricas

Según la aplicación y el alcance de la señal las redes inalámbricas se pueden clasificar en redes de área personal, de área local, metropolitanas y de amplia área [16], en la figura 3, se presenta los 4 tipos de redes existentes.

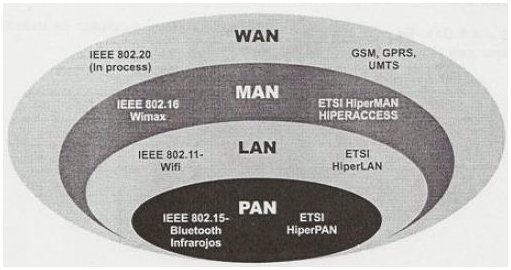


Figura N° 3. Clasificación de las Redes Inalámbricas. [16]

a) WPAN

Son redes basadas en el estándar 802.15 que permiten un rango de cobertura de 10 metros, caracterizadas por su bajo consumo de energía y la baja velocidad de

transmisión, encontrándose así, la tecnología Bluetooth, IrDA, ZigBee RFID, como las importantes [16], en la tabla 1, se observan las características de cada una de ellas.

Tabla 1. Tipos y Características de las Redes WAN.

Tecnología	Alcance	Velocidad	Banda de frecuencia	Aplicación
Bluetooth	20 metros	3Mbps	2.4GHz	Transmisión de voz y datos sin cables entre dispositivos móviles.
IrDA	1-2 metros	9.6Kbps-4Mbps	850-900nm Infrarrojos	Mandos a distancia y calculadoras programables.
ZigBee	75 metros	250Kbps	2.4Ghz	Redes de sensores, domótica
RFID	3 metros	106Kbps	2.4GHz, 13.56MHz	Control de inventarios

Elaborado por: Investigadora

b) WLAN

Diseñadas para comunicaciones a distancias de hasta 100 metros, basadas en el estándar 802.11, utilizadas específicamente en hogares, instituciones educativas, permiten escalabilidad y expansión, generando así más puntos de conexión en zonas de difícil acceso [16].

El estándar 802.11 a su vez comprende toda una familia. El primer estándar fue el 802.11b con una velocidad de transmisión de 11Mbps en la banda de frecuencia de 2.4GHz, posteriormente el 802.11g con mayor ancho de banda a una velocidad de transmisión de 54Mbps en la banda de los 2.4Ghz y soportando 802.11b, así se hasta la aprobación del estándar 802.11ac en las bandas de 2.4 y 5GHz; más adelante se detallará este estándar [16].

c) WMAN

Son redes basadas en el estándar 802.16 denominadas como WiMAX, tecnología con arquitectura punto a multipunto, proporcionando alta velocidad de transmisión de datos, WiMAX opera con una banda licenciada y una banda no licenciada de 2GHz a

11GHz y de 10GHz a 66GHz, alcanzando velocidades de transmisión de 70Mbps a distancias de 50Km para miles de usuarios [16].

Red Inalámbrica de Área Local WLAN

Son redes designadas a operar en la banda ISM (Bandas de radio Industriales, Científicas y Médicas), que permiten la comunicación inalámbrica entre usuarios que se encuentran en ambientes movibles. La IEEE 802.11 es la encargada de desarrollar varios estándares para las redes WLANs, incluyendo los estándares para wifi como: 802.11a en la banda de los 5GHz, 802.11b en la banda de los 2.4GHz, 802.11g compatible con los dos estándares anteriores y wifi de alta velocidad, 802.11n y 802.11ac de doble banda 2.4GHz y 5GHz [16].

Una red WLAN establece conexión entre el router y el usuario permitiendo el acceso a internet, a continuación se presentan varias consideraciones para el uso de una WLAN:

- **Seguridad:** Se usa técnicas de encriptación para la privacidad de la información.
- **Interferencia y confiabilidad:** La calidad de la señal se ve afectada por agentes externos o transmisiones simultáneas. En base a la tasa de bit de errores se puede medir la confiabilidad y para un mejoramiento se usa técnicas de detección y corrección de errores.
- **Movilidad:** Un usuario puede experimentar handoffs dentro de la red inalámbrica [16].

Elementos de una red WLAN

- **Access Point:** Son dispositivos encargados de interconectar los demás dispositivos inalámbricos entre sí con la red cableada existente a través de cable ethernet, comunicándose por medio de enlaces de radiofrecuencia hacia las estaciones móviles. El uso de varios AP’s pueden soportar handoff con un radio de cobertura de 20 a 500 metros y en base a la tecnología soportando entre 15 a 250 usuarios.
- **Adaptadores de red:** Conocidos como NIC, instalados en los dispositivos informáticos que requieren conexión a la red inalámbrica, los cuales disponen de

una antena pequeña conectándose a una ranura de la placa base o por medio de un dispositivo USB.

- **Repetidores:** Dispositivos que permiten extender el área de cobertura de la red inalámbrica, generando y amplificando la señal entre los dispositivos finales y los Access point.
- **Bridges inalámbricos:** Elementos que permiten la conexión entre dos redes inalámbricas o una red inalámbrica con una red cableada mediante software o hardware, utilizando diferentes protocolos o arquitecturas de red [17].

Topologías de Red WLAN

Las redes WLAN se pueden implementar con tres topologías más importantes:

- **Topología Punto a Punto (Redes Ad Hoc):** En esta topología los elementos esenciales son los dispositivos finales equipados con los adaptadores inalámbricos, el único requisito es el rango de cobertura de la señal para que los terminales se puedan conectar a la red.
- **Topología Infraestructura:** Esta topología usa el concepto de celda, la cual se entiende como el área efectiva de la señal radioeléctrica, en las redes inalámbricas las celdas son de tamaño reducido, para aumentar el número de celdas y el área de cobertura se usan los puntos de acceso, permitiendo doblar la distancia de cobertura de la red. Cada vez que se traslade a un nuevo Access point, se necesita establecer una nueva conexión usando el método de roaming.

  El roaming permite que los dispositivos móviles se puedan interconectar libremente a otro Access point mientras se esté movilizando, dentro de ello puede existir interferencia de la señal por solapamientos, para evitar este problema se divide el rango de frecuencias y se asignan rangos diferentes a cada área de cobertura contiguas.

  En esta topología cada trama de los puntos de acceso requieren de dos emisiones de radio, además al ser dispositivos fijos, las antenas suelen ser ubicadas en lugares de alta ganancia.
- **Topología Punto-Multipunto:** Topología usada al interconectar APs de diferentes edificios, cuyos dispositivos deben tener línea de vista directa soportando condiciones ambientales [18].

1.3.5. Tecnología Wi-Fi

Actualmente las telecomunicaciones han crecido exponencialmente en base a la evolución de las comunicaciones vía radio, a continuación se describirá la tecnología inalámbrica Wi-Fi.

La tecnología Wi-Fi denominada Wireless Fidelity creada por la agencia INTERBAND, se usa en redes de datos conectados mediante ondas de radio, la cual está basada en el estándar 802.11 que va desde a hasta el ac, permitiendo la comunicación inalámbrica entre los diferentes dispositivos dentro de un radio geográfico restringido, determinado por la estación base. Esta tecnología permite la transmisión de datos a altas velocidades y la conexión a internet de banda ancha, desde velocidades de 54 Mbps hasta 1Gbps [19].

Esta tecnología trabaja en bandas del espectro radioeléctrico de los 2.4GHz y 5GHz, bandas que son de uso libre.

a) Estándar IEEE 802.11

El estándar IEEE 802.11 se basa en una arquitectura celular, en donde el sistema se divide en celdas denominado BSS o conjunto de servicios básicos y que dentro de este es conocido como Access point. El grupo IEEE802.11 define estándares que se sitúan en los niveles bajos del modelo OSI, específicamente en el nivel de capa física y en el nivel de la capa de enlace. En la figura 4, se muestra la arquitectura funcional del estándar IEEE 802.11 [20].

Figura N° 4. Arquitectura funcional del estándar IEEE 802.11. [20]

El estándar 802.11 maneja una familia de estándares, a continuación en la tabla 2, se presenta las características más importantes de cada uno de los estándares que se encuentran en la capa física y de enlace de datos, considerados como la base para el desarrollo de redes WLAN.

Tabla 2. Características de la familia del estándar 802.11.

Estándar	Banda de frecuencia	Velocidad de Transmisión	Modulación	Características
802.11a	5GHz	54Mbps	OFDM	Cada banda posee 8 canales de radio, rango de cobertura 10m, ancho de banda 20MHz. Desventaja de no ser compatible con 802.11b y 802.11g.
802.11b	2.4GHz	11Mbps	DSSS, CCK	Canales de operación 1, 6 y 11, rango de cobertura 200m, ancho de banda 20MHz. Desventaja de ocasionar interferencias.
802.11g	2.4GHz	54Mbps	OFDM, DSSS, CCK	Canales de operación 1, 6 y 11, rango de cobertura hasta 50Km, ancho de banda 20MHz. Desventaja ante presencia de nodos reduce la velocidad de transmisión.
802.11n	2.4-5GHz	540Mbps	OFDM, MIMO	Ancho de banda de 20MHz o 40MHz, diseñada para el reemplazo completo de la tecnología inalámbrica actual (ethernet). Desventaja de ser sustituido por 802.11ac con velocidades de transmisión de hasta 1.3Gbps.
802.11ac	5GHz	1.3Gbps	OFDM, MIMO	Ancho de banda 20, 40, 80 y 160MHz. Distancia de cobertura de hasta 8Km con antenas parabólicas. Desventaja ser sustituido por 802.11ad

				con velocidades de transmisión superiores a 7Gbps.

Elaborado por: Investigadora

b) Arquitectura de estándar IEEE 802.11

El estándar IEEE 802.11, trabaja con dos capas, la capa física y la subcapa MAC de la capa de enlace, del mismo modelo de la familia 802 o modelo OSI. En la tabla 3, se muestra las capas de la arquitectura del estándar 802.11 [21].

Tabla 3. Capas de la arquitectura del estándar 802.11

	Subcapa LLC			
Capa de Enlace	Subcapa MAC: Acceso al medio (CSMA/CA) Acuses de recibo Fragmentación Confidencialidad (WEP)			
Capa Física	PLCP (Physical Layer Convergence Procedure)			
	PMD (Physical Media Dependent)			
	Infrarrojos	FHSS	DSSS	OFDM

Elaborado por: Investigadora

Capa Física

En esta capa se distinguen dos subcapas, la capa PMD que muestra las especificaciones de los sistemas de transmisión a nivel físico, la subcapa PLCP encargada de convertir los datos a un formato compatible con el medio físico.

Además en la capa física se define el tipo de modulación, la señalización y las características de la transmisión de datos. En este nivel se usa la tecnología de radiofrecuencia de espectro ensanchado, la cual consisten el enviar la información a través de todo el ancho de banda disponible, existen dos tipos de esta tecnología [21]:

- **Espectro Ensanchado por Secuencia Directa (DSSS):** Trabaja con frecuencias comprendidas entre 2.412 y 2.484GHz, la cuales son divididas en canales, y para cada canal es necesario un ancho de banda de 22MHz parque no exista solapamiento y se pueda transmitir la información sin interferencias, así existen 3 canales que no se solapan, los cuales pueden ser: 2, 7 y 12; 3, 8 y 13; 4, 9 y 14 o 1, 6 y 11. Usa la modulación DBPSK y DQPSK para alcanzar velocidades de

transmisión de 1 a 2Mbps, respectivamente. En la figura 5, se observa la distribución de canales que maneja esta técnica en la banda de los 2.4GHz [21].

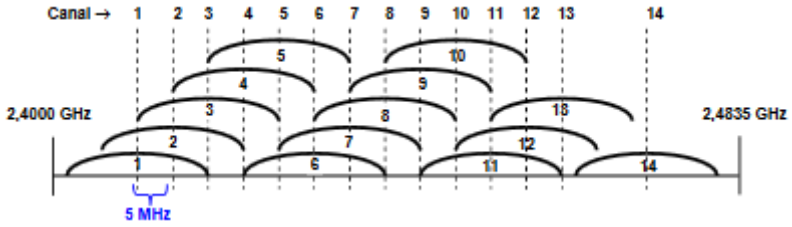


Figura N° 5. Distribución de canales en la banda de los 2.4GHz. [21]

- **Espectro Ensanchado por Salto en Frecuencia (FHSS):** Se transmite la información a determinada frecuencia en cierto intervalo de tiempo, el cual debe ser inferior a 400ms, pasado este tiempo se cambia a otra frecuencia de emisión y se continúa con la transmisión a otra frecuencia. También trabaja en la frecuencia de 2.4GHz, con 79 canales de 1Mhz de AB cada uno, se usa la modulación en frecuencia FSK (Frecuency Shift Keying), con velocidades de 1 Mbps a 2Mbps.
  Con las nuevas versiones del estándar 802.11a y 802.11g se estableció una técnica denominada OFDM, conocida como Multiplexación por División de Frecuencias Ortogonales [21].
- **Multiplexación por División de Frecuencias Ortogonales OFDM:** Técnica que envía un conjunto de portadoras de diferentes frecuencias y cada portadora es modulada en QAM o en PSK, las velocidades normalizadas que trabaja OFDM son 6, 9, 12, 18, 24, 36, 48 y 54Mbps, y cuya ventaja principal es alta resistencia a interferencia causadas por ondas reflejadas [21].

Capa de Enlace de Datos

Esta capa se subdivide en dos capas, la capa MAC y la capa LLC (Subcapa de Control de Enlace Lógico) que se encarga del control de errores y de flujo de información. El algoritmo base usado en este nivel es similar al que se usa en el estándar 802.3, llamado CSMA/CA (Carrier Sense Multiple Access witch Collision Avoldance), protocolo que evita colisiones sin detectarlos. La subcapa MAC está dividida a su vez en dos subcapas:

- **Subcapa de Control de Acceso al Medio (MAC):** Realiza la fragmentación de los paquetes y el control de acceso al medio por medio de CSMA/CA.
- **Administrador de subcapa MAC:** Administra los procesos de roaming dentro del conjunto de servicios extendidos y la energía [21].

c) Seguridad de IEEE 802.11

Dentro de una red inalámbrica, es necesario la seguridad de la información, para ello se aplica el estándar 802.11i, el cual establece mecanismos de autenticación, autorización y distribución de contraseñas para acceder a la red [22]. Se forma de tres elementos:

- El suplicante que se une a la red.
- El autenticador que autoriza el acceso a la red, generalmente un Access point.
- El servidor de autenticación que habilita el acceso a la red, mediante decisiones.

Para la seguridad en el estándar se tiene dos escenarios, el primero autoriza el acceso a la red, mediante una lista de clientes y claves que se pueden almacenar localmente en una base de datos como el servidor Radius, en la figura 6, se ilustra la autenticación usando el servidor Radius [22].

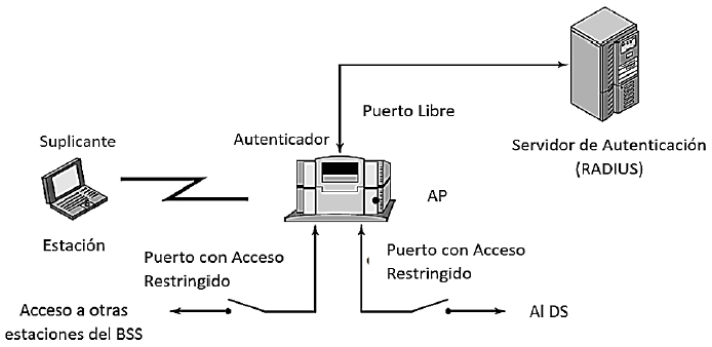


Figura N° 6. Autenticación usando Radius, Seguridad en IEEE 802.11. [22]

1.3.6. Internet de las Cosas IoT

Es una tecnología basada en la conexión de objetos cotidianos a Internet que intercambian, agregan y procesan información sobre su entorno físico con la finalidad de proporcionar servicios a usuarios finales. Además puede reconocer eventos reaccionando de forma autónoma y adecuada, en la figura 7, se presenta la estructura de un sistema IoT [23].

La información que es enviada a través de aplicaciones IoT, deben cumplir ciertas características:

- Bajo consumo energético.
- Confirmación de recepción de mensajería no necesaria.
- Uso eficiente del ancho de banda.

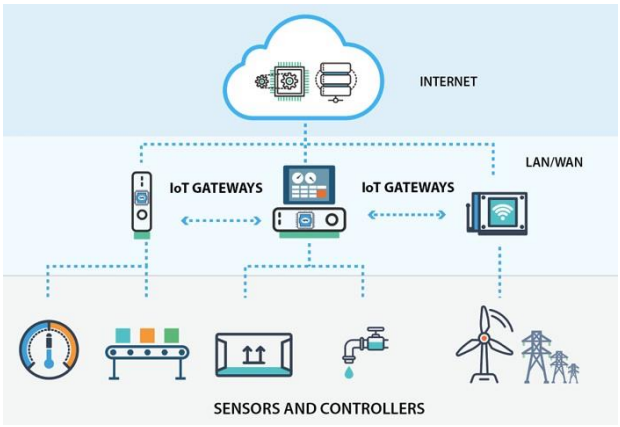


Figura N° 7. Estructura de un sistema IoT. [23]

a) Arquitectura IoT

La arquitectura de un sistema IoT se basa en la orientación de eventos, como se ilustra en la figura 8, es construida desde abajo hacia arriba y cada capa debe se identifica como una tecnología específica con diferentes componentes [23].

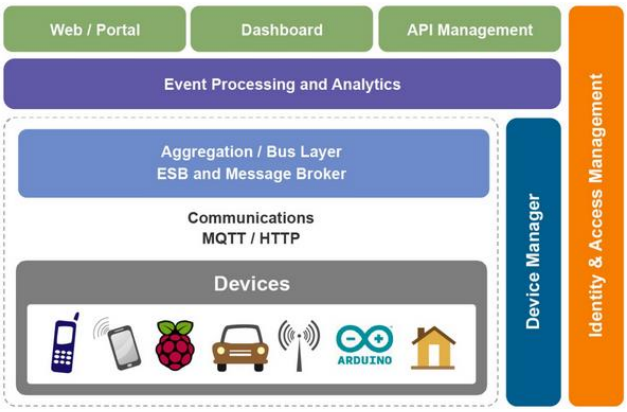


Figura N° 8. Arquitectura IoT. [23]

La primera capa está compuesta de portales web o aplicaciones propias del usuario, los datos emitidos a través de esta capa pasan a ser procesadas y analizada en la siguiente capa, para ser emitidas mediante comunicaciones HTTP, MQTT, hacia los

diferentes dispositivos como teléfonos celulares, Raspberry Pi, arduino, equipos wifi y sensores [23].

b) Protocolos de Comunicación de IoT

Existen varios protocolos de comunicación que se manejan en el Internet de la Cosas, a continuación se presenta en la figura 9, diferentes protocolos que son usados en cada capa de un sistema IoT en función de la tecnología de comunicación usada [23].

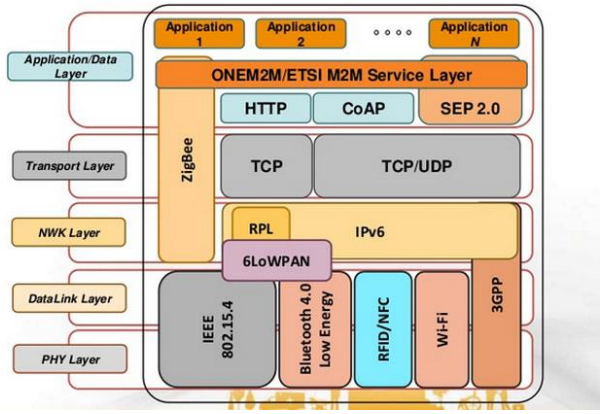


Figura N° 9. Protocolos de Comunicación de IoT. [23]

1.3.7. Mensajerías Instantáneas

Telegram

Telegram es un tipo de mensajería instantánea desarrollada por los hermanos Nikolái y Pável Dúrov, que permite enviar, texto, fotos, videos y archivos de cualquier tipo, los remitentes y receptores pueden ser usuarios grupos o canales [24]. Tiene varias opciones como, creación de grupos o canales, a continuación se presentan las características de estas formas de comunicación:

- *Grupo:* Varios usuarios se unen a un grupo, en donde todos los miembros pueden enviar y recibir mensajes, además los usuarios pueden ser invitados o otros miembros del grupo.
- *Canal:* Es una forma para enviar mensajes públicos a varios usuarios, generalmente se tiene un solo administrador o pocos, siendo los únicos en emitir información

a) Características de Telegram

- Envío de archivos de hasta 1.5GB
- Cifrado de información por MTProto
- Chats en grupos permite hasta 200000 usuarios
- El inicio de sesión es mediante un número telefónico

b) Seguridad de Telegram

Telegram tiene su propio protocolo de comunicación, denominado MTProto, permitiendo la transmisión de mansajes de forma segura entre los móviles. Principalmente cifra los mensajes con una clave y los descifra con la diferente clave.

La mensajería para el cifrado usa el algoritmo AES modo IGE, con claves de 256 bits, al usar este cifrado la información puede ser vulnerable, pero telegram añade dos características importantes: la primera, se cifra el mensaje y se añade un salt, una cadena aleatoria definida por el servidor telegram, la hora actual y un número que indica el orden del mensaje, y la segunda es la clave ya que no usa la misma clave para el cifrado y descifrado de los mensajes [24].

c) Protocolo de encriptación MTProto

Para verificar que la información emitida no haya sufrido alteraciones, telegram usa una MAC (Código de Autenticación de Mensaje). Al momento de emitir un mensaje telegram adquiere una MAC en base al algoritmo SHA-1, con ello obteniendo una clave que identifica al mensaje, y esta es combinada con la clave que comparte el cliente y el servidor, con ello obtiene una nueva clave para el cifrado del mensaje. A continuación en la figura 10, se observa el esquema final del cifrado usado por telegram [24].

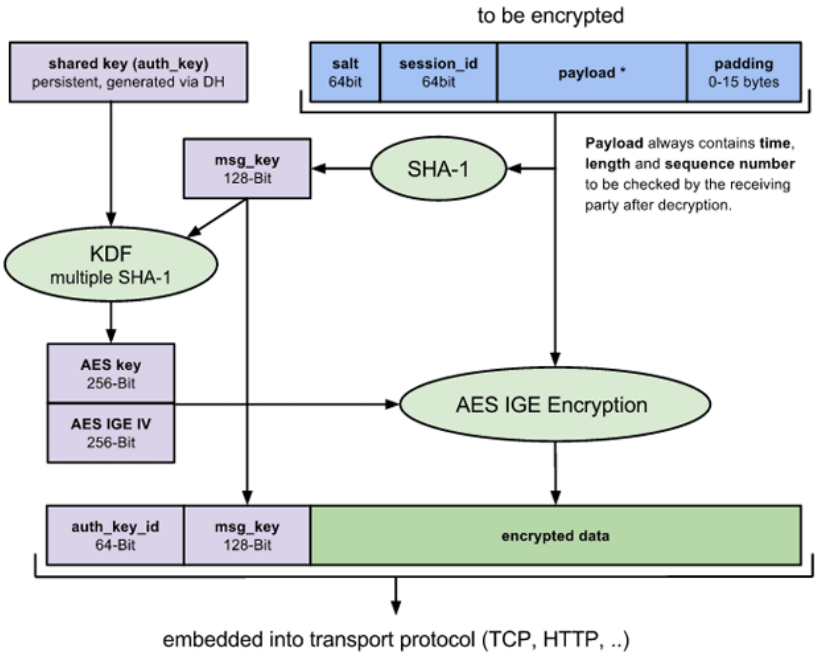


Figura N° 10. Esquema de Cifrado usado por Telegram [24].

d) Creación de ChatBots

Este servicio fue desarrollado para realizar servicios más grandes, los cuales tienen la funcionalidad de obedecer órdenes mediante comandos de texto, permitiendo administrar grupos y canales.

Para el desarrollo de aplicaciones usando esta mensajería es necesario tener un kit para interpretar tanto la API de MTProto y el Token, con ello validando el funcionamiento [24].

WhatsApp

"WhatsApp" es una aplicación de mensajería (XMPP) instantánea gratuita y en formato multiplataforma para instalación en el móvil, permitiendo enviar y recibir mensajes sin pagar por SMS, el mismo que funciona a través de Wi-Fi o a través del plan de datos del teléfono móvil contratado [25].

Existen diferentes posibilidades que ofrece WhatsApp entre las principales se tiene:

- Enviar y recibir fotografías.
- Enviar y recibir notas de audio.
- Enviar y recibir videos.
- Compartir nuestra ubicación.

A continuación se presenta las características técnicas de la mensajería instantánea WhatsApp:

- WhatsApp usa una versión personalizada de protocolo abierto Extensible Messaging and Presence Protocol. Una vez instalada la aplicación se crea una cuenta de usuario a través del número de teléfono.
- La versión de Android utiliza un hash MD5 (Algoritmo de Resumen del Mensaje 5) del IMEI invertido como contraseña, mientras que la versión de iOS usa un hash MD5 de la dirección MAC del teléfono duplicada.
- Los mensajes de imagen, audio o video se envían subiendo el contenido a un servidor HTTP y enviando un link al mismo, junto a un thumbnail codificado en Base 64 [25].

1.3.8. Sistema de Video Vigilancia IP

Un sistema de video vigilancia es un sistema que satisface necesidades a clientes de forma eficiente y eficaz, al gestionar cámaras que sean instaladas en un lugar determinado, de forma remota o local [26].

Un sistema de Video Vigilancia o CCTV conocido como Circuito Cerrado de Televisión, permite la supervisión, el control y el registro de actividades dentro de un área determinada, que a diferencia de los sistemas análogos, este sistema usa la tecnología IP que permite la visualización y la grabación del video a través del acceso a la red, ya sea a una red LAN o WAN como internet. Adicionalmente la alimentación de dispositivos de grabación se realiza mediante la red IP, es decir usando la tecnología PoE (Power Over Ethernet), que se basa en el estándar 802.3af. En la figura 11, se muestra un esquema básico de un sistema de video vigilancia IP [26].

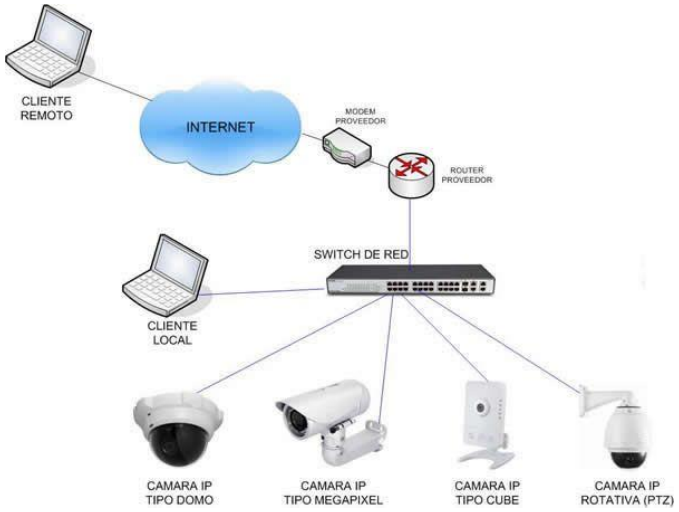


Figura N° 11. Estructura de un Sistema de Video Vigilancia IP. [26]

Elementos de un Sistema de Video Vigilancia IP

Un sistema de Video vigilancia IP consta de los siguientes elementos:

a) Cámara de Red

Dispositivo principal dentro de un sistema de video vigilancia IP que capta y transmite una señal de video y audio, a través de la red a otros dispositivos de red, que por medio de una dirección IP dedicada, un servidor web y protocolos de transmisión de video, en donde los usuarios pueden almacenar, visualizar y gestionar el video de forma local y remota, usando navegadores diferentes navegadores web [27]. Las características que presentan estos dispositivos son:

- **Tipo de sensor:** Un sensor de imagen es el encargado de transformar la luz en señales eléctricas, dentro las cámaras IP existen dos tipos de sensores, el sensor CCD con mayor sensibilidad a la luz, más caros y más complejos de añadir a una cámara, el sensor CMOS más económicos, y de menor tamaño, cuya desventaja es su menor sensibilidad a la luz y son usados tanto en web-cams, como en cámaras IP, en la figura 12, se observa el tipo de sensor CCD, CMOS [27].

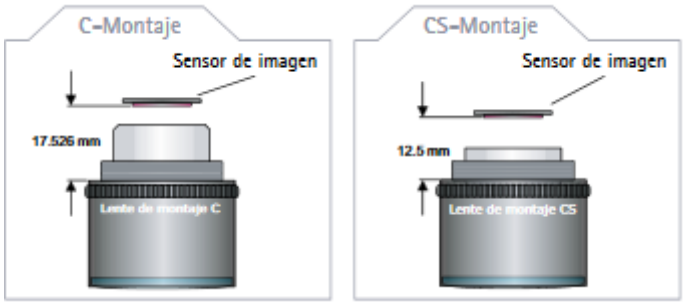


Figura N° 12. Tipo de sensor CCD y CMOS. [27]

- **Lente y tipo de Objetivo:** Para visualizar una escena u objeto a cierta distancia, es necesario elegir el lente en función de la distancia focal, teniendo así lentes fijos cuando se haya definido el lente que es necesario usar, y los lentes varifocales cuando el campo de visión es inseguro y el usuario debe definirlo, estos son muy útiles por su modo de ajustamiento manual de la distancia focal, a continuación en la figura 13, se presenta el tipo de lente con su ángulo y distancia de visualización.

Lens	4mm	6mm	8mm	12mm	16mm
Angle	69.9°	50°	38.5°	26.2°	19.8°
Distance	0-6M	5-10M	10-20M	20-35M	35-50M

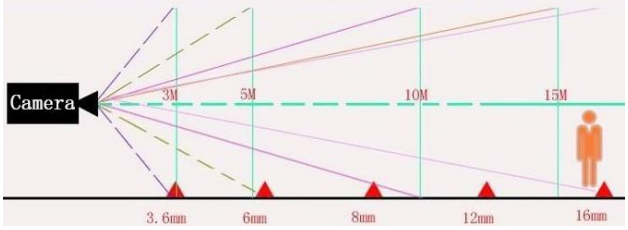


Figura N° 13. Tipo de Lente con ángulo y distancia de visualización. [27]

- **Resolución:** Medida de la calidad de la reproducción de una imagen, en los sistemas digitales la imagen se trabaja con pixeles, y mientras mayor pixeles tenga el CCD, mejor será la resolución de la cámara.
- **Sensibilidad:** Es la cantidad mínima de iluminación de una escena para adquirir una señal de video, que se mide en lux. Una cámara a blanco y negro tiene por lo general una sensibilidad de 0.01Lux y las de color una sensibilidad que va desde 0.1 a 1Lux [27].

b) Estándares de Compresión de Video

La compresión de video es un parámetro muy importante a tomar en cuenta en la selección de cámaras IP [28], ya que permiten reducir el ancho de banda del streaming de video, a continuación se describen los más actuales:

- **H.264:** Denominado como Codificación Avanzada de Video (AVC), formato de compresión que ocupa menor espacio de almacenamiento y ancho de banda, que consiste en reducir y eliminar datos redundantes que existan en el video, es decir las imágenes se dividen en boques y si alguno de los bloques sufre un desplazamiento en comparación con la siguiente imagen, solo se transmite ese bloque [28]. En la figura 14, se muestra la compensación de movimiento por bloques.

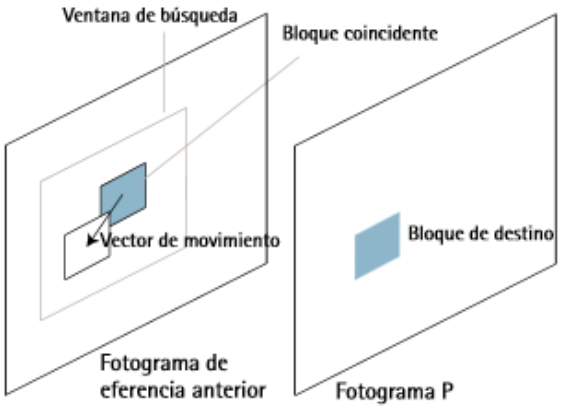


Figura N° 14. Compensación de movimiento por bloques [28].

- **MPEG 2:** Formato que se basa en una compresión temporal, que elimina la redundancia por predicción de movimiento, que trabaja con imágenes más grande y de alta calidad, usando una tasa de bits elevada y una menor relación de compresión [28]. La compresión se realiza en base a una comparación entre una escena anterior y siguiente, en la figura 15, se ilustra el formato MPG2 por predicción de movimiento.

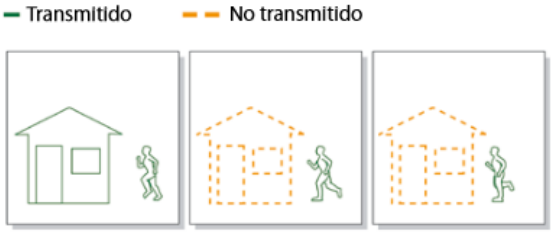


Figura N° 15. Formato MPG2 por predicción de movimiento [28].

- **JPEG Motion:** Compresión más usada en sistemas de video IP, usado por casi todas las cámaras IP, en donde la cámara al usar JPEG, muestra el video en base a una serie de imágenes individuales sucesivas. La tasa de imágenes por segundo es ajustable y con una velocidad de imagen de 16fps se recibe en pantalla completa una imagen animada (full motion video).

c) Tipos de Cámaras

Existen tres grandes tipos de cámaras usadas en sistema de video IP, a continuación se detallan sus características:

- **Cámara Fija:** Son cámaras que presentan un cuerpo y un objetivo, con mayor rango de visualización, y su facilidad de instalación en áreas externas.
- **Cámara Domo:** Son cámaras muy usadas por su diseño discreto que resisten a acciones vandálicas, incluyen sensores infrarrojos, con un radio de visualización inferior a 20 metros.
- **Cámara PTZ:** Cámaras desplazables en los ejes vertical y horizontal, y con acción de zoom, además posee visión panorámica la cual puede ser manipulada de forma manual o automática. Generalmente usadas en áreas internas. En la figura 16, se presentan cámaras que se pueden encontrar en un sistema de video vigilancia IP [29].

Figura N° 16. Tipos de cámaras IP [29].

d) Medio de Transmisión de Imagen

Medios guiados o no guiados para la transmisión de señal de video, el cual puede estar compuesto por amplificadores y distribuidores [29], en la tabla 4, se muestran las características de los tipos de los medios de transmisión usados en un sistema de video vigilancia IP.

Tabla 4. Características de Medios de Transmisión usados en video vigilancia IP.

Transmisión		**Características**
Medios	**Tipos**	
Cableados	Par trenzado UTP	Se usa cuando las distancias entre los dispositivos del sistema superan los 200m, además no requiere de amplificadores, debido a que toda interferencia al llegar a los conductores se cancela debido a que admiten señales en modo diferencial, por lo que no se requiere de amplificadores.
	Fibra Óptica	Medio inmune a las interferencias, no muy usado en sistemas de video vigilancia por su alto costo de implementación.
Inalámbricos	Señal de radiofrecuencia	La transmisión de imágenes a distancias entre 100 y 8000m, con línea de visión directa y en frecuencias de microondas, para el envío de video de alta calidad se requiere de un ancho de banda de 6Mz o 7Mhz.
	Señal infrarrojo	Solo es utilizada para mandos a distancias pequeñas.

Elaborado por: Investigadora

e) Equipo de Grabación

Dentro de un sistema de video vigilancia es necesario analizar grabaciones anteriores de imágenes, la calidad y la disponibilidad, para estas funcionalidades es necesario un equipo de grabación digital, con ello seleccionando equipos NVR, que receptan imágenes digitales, transmiten el video a través de la red y almacenan las grabaciones en un disco duro, además un NVR no posee un monitor y teclado para la gestión, por lo que se realiza de forma remota a través de una PC [29]. En la figura 17, se muestra el esquema de conexión de un grabador en conjunto a las cámaras hacia la red IP.

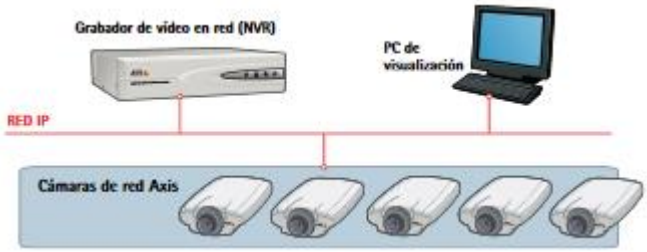


Figura N° 17. Esquema de conexión de un grabador y cámaras hacia red IP [29].

f) Monitores

Las imágenes que son captadas por las cámaras y transmitidas hacia el equipo de grabación, necesitan ser visualizadas y reproducidas en un dispositivo que presenten estas características, para que el personal pueda controlar y monitoreo el video de forma local o remota. Para ello se usan monitores que puedan traducir las señales eléctricas de video procedentes del NVR en imágenes [29].

g) Tecnología de Red IP Ethernet

En la actualidad el protocolo de internet IP es el más usado, para comunicaciones por internet, el tipo de Ethernet más común en sistemas de video vigilancia IP es el Gigabit Ethernet 1000Mbps [29]. Estándar más recomendado para redes troncales entre servidores y conmutadores de red, y a su vez se subdivide en:

- *1000BASE-T:* Velocidades de hasta 1Gbps mediante cable UTP categoría 5e ó 6.
- *1000BASE-SX:* Velocidades de hasta 1Gbps mediante fibra multimodo hasta 550m.
- *1000BASE-LX:* Velocidades de hasta 1Gbps mediante fibra multimodo y optimizado para distancias mayores a 10Km con fibra mono modo [29].

1.3.9. Servicio de Voz sobre IP

Es una tecnología que permite enviar la señal de voz a través de internet empleando el protocolo IP, siendo la aplicación principal la telefonía IP, la cual permite establecer llamadas telefónica a través de una PC, gateways y teléfonos. Por medio de VoIP se tiene una comunicación unificada, es decir la integración de varios servicios como video, mensajería, correo a través de internet [30].

a) Arquitectura de VoIP

Uno de los grandes beneficios de la tecnología IP, es la flexibilidad, que permiten a la redes ser reconstruidas a través de una arquitectura centralizada o distribuida. En la figura 18, se presenta la arquitectura general de VoIP [30].

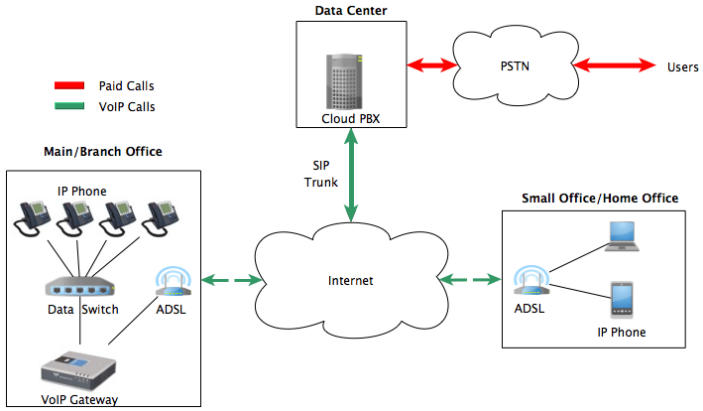


Figura N° 18. Arquitectura general de VoIP [30].

b) Protocolos de Señalización

Los Protocolos VoIP son de gran importancia ya que permiten la comunicación entre los equipos y códecs con la red; es decir son un conjunto de reglas que establecen las llamadas entrantes, salientes y los estados de la línea con los terminales IP. A continuación se detallan los protocolos que maneja FreePBX [30].

SIP: Protocolo a nivel de aplicación, para el establecimiento y gestión de sesiones con varios participantes, el cual define el proceso de llamadas, videoconferencias y otras aplicaciones multimedia a través de internet. Para el transporte de datos se usa el protocolo RTP/RTCP. Emplea el método de mensajes para inicializar sesiones que son enviadas por medio de TCP o UDP [30], su arquitectura fundamental es la siguiente:

- Cliente – Servidor
- Establecimiento de mensajes de petición y respuesta
- Integración de correos y URLs
- Agentes de usuarios
- Servidores proxys

IAX: Es un protocolo manejado por Asterisk que se encuentra incluido en FreePBX, destinado a la comunicación entre servidores Asterisk o a la comunicación entre clientes y servidores que soportan el protocolo, presenta las siguientes características:

- Para la transmisión de control y multimedia, se reduce el ancho de banda.
- La señalización y el tráfico de voz son transmitidos exclusivamente por el puerto UDP
- Configuración simple de los terminales IAX [30].

En la tabla 5, se presenta las características más importantes de los dos protocolos más usados por Asterisk y en telefonía IP.

Tabla 5. Características de protocolos SIP y IAX de Asterisk

Protocolo	**SIP**	**IAX**
Característica	Realiza gestión de comunicación.	Propio de Asterisk, por ello establecen comunicaciones solo entre estos servidores.
Ancho de Banda	Usa gran ancho de banda debido al formato de mensaje.	Menor ancho de banda por el formato de mensaje que usa.
Transmisión de audio/video	UDP, TCP	UDP
Formato de mensaje	Texto	Binario
Puertos de señalización	Un puerto para datos y otro para señalización.	Un solo puerto para los datos y la señalización.
Puerto	5060	4569

Elaborado por: Investigadora

c) Códec de Voz

Son dispositivos que permiten transformar la señal analógica de voz en digital y viceversa, este proceso de conversión se basa en la utilización de varios algoritmos de compresión y descompresión, en donde la mayoría usa variantes de la modulación PCM (Modulación por Codificación de Pulsos) y que gracias a los avances tecnológicos estos códec de voz hoy en la actualidad permiten la reducción del consumo del ancho de banda y mediante diferentes técnicas de compresión de audio se logra tener una buena transmisión de voz sobre las redes IP [31]. A continuación en la tabla 6, se presentan diferentes códecs más usados:

Tabla 6. Códecs de voz usados en Telefonía IP.

Códec	Descripción	Ancho de Banda	Modulación	Observación
G.711	Códec de audio de adquisición gratuita y usa modulación PCM. Latencia de 30ms	64Kbps	8KHz	Consumo de gran ancho de banda por no usar compresión.
G.723.1	Códec para videoconferencia en telefonía IP.	5.6/6.3 Kbps	8KHz	Capacidad de procesamiento alta por compresión y descompresión simultáneamente.
G.726	Códec de voz de forma de onda que usa ADPCM. De buena calidad y baja capacidad de procesamiento	16/24/32/40 Kbps	8KHz	No requiere de licencia.
G.729	Códec hibrido (compresión de audio y video). Usa estructura conjugada con código de salida algebraica de predicción lineal (CS-ACELP). Latencia de 20ms	8Kbps	8KHz	Usa menos ancho de banda y requiere de licencia para funcionamiento.

Elaborado por: Investigadora

d) Central IP

Una central IP o PBX (Private Branch Exchange), es un equipo que gestiona llamadas telefónicas internas y comparte líneas de acceso a una red pública entre diferentes usuarios, para que efectúen y recepten llamadas desde y hacia el exterior, usando el protocolo IP [32]. En la figura 19 se presenta la estructura y elementos que componen una central IP.

Figura N° 19. Estructura y elementos que componen una central IP [32].

e) Dispositivos finales IP

Existen dos elementos fundamentales en la telefonía IP, siendo la central y teléfonos IP, cada uno con diferentes funcionalidades y características.

- *Teléfono IP:* Dispositivo que se conecta directamente a internet a través de un puerto RJ45, o por medio de una extensión inalámbrica, al cual se le asigna una IP fija o mediante una la configuración DHCP y con alimentación PoE.
- *Sofphones:* Son softwares con funcionalidades de teléfonos IP, que son instalados en ordenadores o en teléfonos móviles para que funcione. Son softwares que permiten establecer llamadas telefónicas IP entre dispositivos que tengan la misma aplicación instalada.

f) FreePBX

FreePBX es una interfaz gráfica de usuario de código abierto con licencia GPL, que administra y controla asterisk, la cual puede ser instalada de forma manual o como parte de FreePBX preconfigurada que viene incluido en el sistema operativo, mantiene bases de datos de usuarios y extensiones, entre otras funciones como:

- Operadora automática o IVR
- Dialplan de llamadas efectuadas y recibidas.
- Gestión de llamadas recibidas con fecha y horario
- Monitorización de llamadas
- Grabación de llamadas
- Sistema de mensajería vocal
- Sistema de colas y agentes [33].

1) Archivos de Configuración en FreePBX

FreePBX está basado en Asterisk, es por ello que los archivos que permite configurarlos se encuentran el /etc/asterisk y son los siguientes:

- **asterisk.conf:** Fichero donde se configura todos los parámetros generales de asterisk, como sonidos, módulos, voicemail, etc
- **sip.conf:** Fichero donde se configuran los clientes SIP para establecer conexión con la centralita.
- **extensions.conf:** Fichero donde se configura el plan de marcado, en conjunto con el manejo y procesamiento de llamadas que llegan a la centralita.
- **voicemail.conf:** Fichero donde se configura el buzón de voz para cada cliente SIP [34].

CAPÍTULO II

METODOLOGÍA

2.1. MATERIALES

Para el desarrollo del proyecto de investigación fue necesario la selección de varios equipos y dispositivos, en correspondencia al hardware del prototipo, por otro lado está el software que se requirió para la configuración de todo el sistema y del hardware seleccionado, a continuación se presenta los materiales seleccionados:

Hardware

- Raspberry pi 3B+
- Cámara IP
- Sirena
- Router
- Disco Duro

Software

- Raspbian
- Visual Studio Code
- Python
- FreePBX-Asterisk

2.1.1. Dispositivo de recepción y procesamiento de datos (Hardware Libre)

Uno de los aspectos considerados, es la selección de los dispositivos de procesamiento que se encuentran en la central de alarma, los cuales permiten controlar eventos que ocurren dentro de un lugar específico, a estos equipos se les pueden dar enfoques diferentes; en esta situación se lo manipula para que emita una alarma, enviando mensajes a la UPC más cercana, con la finalidad de proteger el ambiente.

Para la implementación de este sistema de alarma comunitaria, existe una cantidad de herramientas tecnológicas disponibles en el mercado del país y en el exterior, que

cubren ciertos requerimientos para el desarrollo del proyecto, en la tabla 7 se analizan tres dispositivos más comerciales que existe en el mercado ecuatoriano y que permiten el desarrollo del mismo.

Tabla 7. Tabla Comparativa de Hardware Libre para el desarrollo del proyecto

CARACTERÍSTICAS	**PLATAFORMAS**		
	Arduino Uno	**Raspberry Pi 3B+**	**BeagleBoard Black**
Microcontrolador	ATMega 328	ARMv8 de 64 bits	AM335x
Memoria RAM	2 KB	1GB	512 MB
Voltaje de operación	5 V	5V	5V
Velocidad	16 MHz	1,4GHz	1GHz
Componentes	Necesita de adaptación de módulos para conexión a internet y bluetooth.	Wi-Fi + Bluetooth: 2.4GHz y 5GHz IEEE 802.11.b/g/n/ac, Bluetooth 4.2	Tarjeta de red Fast Ethernet 10/100Mbps Gráfica SGX530
Puertos	• 14 In/Out digitales • 6 In análogas	• GPIO de 40 pines • HDMI • 4 puertos USB 2.0 • CSI (cámara raspberry) • DSI pantalla táctil • Power-over-Ethernet (PoE) • Puerto para Micro SD	• 69 GPIO • 7 entradas análogas • Puerto para LCD • 4 puertos seriales • USB 2.0
Video	No	Si HDMI	microHDMI
Audio	No	Si HDMI	microHDMI
Tamaño	2,95” x 2,1”	3,37” x 2,125”	3,4” x 2,1”
Sistema Operativo	No tiene	Linux, raspbian	Android, Linux, Windows, Cloud9, CE
Entorno	Arduino IDE	Linux, IDEL, Eclipse, Embedded, Scratchbox, Java, Python,	Python, Scartch, Linux, Eclipse, Android ADK
Costo	$ 15,00	$ 95,00	$ 271,00

Elaborado por: Investigadora

La tarjeta más óptima para el desarrollo del proyecto fue la Raspberry Pi 3B+, debido a su costo, a la accesibilidad en el mercado, a sus funcionalidades para el desarrollo de

varias aplicaciones vinculadas a internet y a su entorno de programación. Las características técnicas se muestran en el Anexo A.

2.1.2. Sirena

En una central de alarma, siempre es conveniente colocar una sirena que permita informar casos de emergencia, tanto al exterior como al interior del lugar, según la norma UNE 23007-14 indica que el nivel sonoro mínimo del dispositivo auditivo, debe ser 5dB por encima de cualquier otro ruido con más de 30 segundos de indicación; y no debe superar los 120dB al ser colocada a más de 1 metro de la fuente [35].

En base a lo descrito anteriormente, se usó la sirena con las siguientes características: 12V y 110dB, como se muestra en la figura 20.

Figura N° 20. Sirena de 12V, 110dB.
Fuente: Investigadora

2.1.3. Cámara IP

La cámara IP es otro dispositivo a usar dentro del sistema de alarma, en donde permanece activa en el horario de apertura del mercado y en el horario de cierre funcionando con detección de movimiento.

El dispositivo a seleccionar debe soportar ciertos parámetros como, presentar bajo consumo de ancho de banda, destinado para ambientes en donde existe movimiento constante, manejo del rango de visión y resolución, a continuación en la tabla 8, se presentan características de cámaras que pueden ser usadas:

Tabla 8. Características de cámaras IP, Hikvision, Onvif, Dahua

MARCA	HIKVISION	ONVIF	DAHUA
MODELO	DS-2CD2020F-I	P2P	DH-IPC-HFW1000S-W
RESOLUCIÓN	2Megapixel	1Megapixel	1Megapixel
LENTE	4mm	3.6mm	3.6mm
FRAME RATE (FPS)	30	15	25
COMPRESIÓN DE VIDEO	H.264/ MJPEG	H.264/ MJPEG	H.264/ MJPEG
RANGO IF	30 metros	20 metros	20 metros
ESTÁNDAR	ONVIF	ONVIF	ONVIF
POTENCIA CONSUMIDA	5.8W	5W	5.8W
APLICACIÓN	Sistemas de video vigilancia en hogares y edificios, interiores/exteriores, cajeros de bancos, conexión por cable y wifi	Sistemas de video vigilancia en hogares y edificios, interiores/exteriores, conexión wifi, Plug and Play	Sistemas de video vigilancia en hogares y edificios, conexión por cable.
ALIMENTACIÓN	12V 1A	5v 1.6A	12V 1A
COSTO	$60.00	$45.00	$60.00

Elaborado por: Investigadora

En base al análisis realizado, se seleccionó el dispositivo que más se ajustó a los requerimientos, siendo la cámara IP ONVIF P2P. En la figura 21, se ilustra la cámara a usar y presenta las siguientes características:

- Conexión Wi-Fi
- Resolución de 1Megapixel
- Frame Rate de 15fps
- Distancia RF de 20 metros
- Compresión de video HG.264/MJPEG
- Consumo de potencia de 5W

Figura N° 21. Cámara IP Onvif.

Fuente: Investigadora

2.1.4. Router Inalámbrico

El router inalámbrico se empleó para la conexión de los equipos que requieren acceder a una red para el funcionamiento del sistema, en este proyecto se usó un router TP-LINK modelo WR840N, que posee dos antenas omnidireccionales de 5dBi, permitiendo incrementar la transmisión y recepción de la señal inalámbrica, que presenta 4 puertos Ethernet, con ofrecimiento de conexión wifi y por cable.

Velocidad de 300Mbps a 2.4GHz para tareas que usan un gran ancho de banda, utiliza tecnología MIMO 2x2, que incrementa la eficiencia para la presentación de varias aplicaciones, como en el caso del proyecto la transmisión de video streaming y servicio de VoIP. TP-LINK TL-WR840N es un equipo de alta velocidad compatible con el estándar IEEE 802.11b/g/n, basado en la tecnología 802.11n [36]. En la figura 22 se presenta el equipo utilizado.

Figura N° 22. Router inalámbrico TP-LINK modelo WR840N.

Fuente: Investigadora.

2.1.5. Disco Duro

Dispositivo usado para el almacenamiento permanente de información, que no necesita de una fuente de alimentación externa, en este proyecto guarda los videos grabados cuando sucede un evento vandálico, seleccionando así un disco duro de la marca HITACHI modelo 0S00381, capacidad de almacenamiento de 320GB, velocidad de transmisión de 480Mbps y con un conector USB 2.0 [37]. En la figura 23, se observa el disco duro usado.

Figura N° 23. Disco de Almacenamiento Hitachi.

Fuente: Investigadora.

2.1.6. Sistema Operativo para Raspberry Pi

Existe una gran variedad de softwares que pueden ser instalados en la Raspberry Pi, cada uno de ellos destinados a varias aplicaciones. A continuación, en la tabla 9, se presenta una comparativa entre los diferentes sistemas operativos, tomando en cuenta que el dispositivo se va a usar como servidor.

Tabla 9. Sistemas Operativos usados en Raspberry Pi.

Sistemas Operativos			
Características	**Raspbian**	**Arch Linux**	**Ubuntu Mate**
Logotipo		archlinux	ubuntu MATE
Compatibilidad wifi	Si	No	Si
Tamaño de tarjeta microSD	16GB o más	6GB o más	6GB o más
Licencia	GPL	GPL	GPL
Entorno de escritorio	LXDE	No instalado	Mate

Elaborado por: Investigadora

En base al análisis realizado sobre los tres tipos de sistemas operativos que soporta la Raspberry Pi, se optó por instalar raspbian, debido a que es un sistema operativo de la distribución Linux, diseñado propiamente para la tarjeta, que al ser compilada para la plataforma se agilita procesos, software escogido desde la página oficial: " raspberry-asterisk.org".

2.1.7. Software para servicio de VoIP

Los softwares para gestionar la alarma en base a una llamada telefónica por medio de la red local hacia el guardia de seguridad y ofrecer el servicio de VoIP a los usuarios del mercado, se presentan en la tabla 10, los dos más usados potencialmente para estas aplicaciones mediante una comparativa técnica.

Tabla 10. Softwares para servicio de VoIP.

Software para Servicio de VoIP		
Características	**Asterisk**	**FeePBX**
Logotipo		
Función	Software como centralita, buzón de voz, IVR, conferencias, transferencias, ACD, registro de llamadas.	Interfaz de usuarios por configuración web, buzón de voz, IVR, colas de llamadas, panel de operador, software completo que controla Asterisk, capacidad de trabajar en la nube.
Escalabilidad	Capacidad desde 10 usuarios hasta 10000 repartidos en varias sedes.	Capacidad desde 10 usuarios hasta 30000 repartidos en varias sedes.
Protocolos de soporte	SIP, IAX, H.323	SIP, IAX, DAHDI
Sistema Operativo	Ejecuta sobre plataforma Linux	Ejecuta sobre plataforma Linux
Códec	G.711, G.723.1, G.726, G.729, GSM	G.722, G.723, G.726, G.729, GSM, iLBC
Libre Uso	Si	Si
OpenSource	Si	Si
Administración	Por consola	Por Interfaz gráfica
Soporte para ARM	Si	Si

Elaborado por: Investigadora

En base al análisis realizado, se seleccionó el software FreePBX, debido a que controla Asterisk, su administración por medio de consola e interfaz gráfica consiguiendo facilidad de configuración.

2.1.8. Lenguaje de Programación PYTHON

Tabla 11. Lenguajes de programación, PHP, PYTHON, RUBY.

Lenguajes de programación para servidor			
Características	**PHP**	**PYTHON**	**RUBY**
Logotipo			
Características	Diseñado para el desarrollo de páginas web dinámicas, ejecución en el servidor, lenguaje de alto nivel.	Diseñado para el desarrollo de varios programas, incluyendo sitios web, no necesita de compilación, manejo de códigos interpretados.	Fácil manejo de sintaxis.
Software Libre	Si	Si	Si
Paradigma	Multiparadigma, orientado a objetos, estructuración de programas en componentes.	Orientado a objetos.	Orientado a objetos.
Ventajas	• Sintaxis simple. • Facilidad de programación. • No requiere definición de variable. • Puede combinarse con HTML	• Lenguaje de propósito general. • Comparación de variables en ejecución.	• Diferencia en escritura. • Carga librerías si el S.O permite. • Desarrollo de programas de bajo costo.

Elaborado por: Investigadora

De estos tres lenguajes de programación se escogió Python debido a que es un lenguaje destinado más al desarrollo de páginas web, mientras que al usar PHP el código fuente no es ocultado ocasionando problemas de seguridad, por otro lado Ruby no es muy difundido y sin documentación suficiente.

Python es un lenguaje de programación de software libre, versátil orientado a objetos, de tipado fuerte y que al poseer una librería estándar, permite realizar varias cosas que involucran, bases de datos, páginas web, generación de documentos, correo electrónico, XML, HTML, entre otros.

2.1.9. Visual Studio Code

Es un programa editor de código fuente, basado en software libre, que admite varias funciones al trabajar con el código, diseñado para tres sistemas operativos Windows, Mac y Linux, el cual respeta varias reglas como, el uso de mayúsculas y minúsculas, espacios en blanco, cierres de bloques de código, entre otras reglas [38].

Ventajas:

- Es usado como lenguaje de programación
- Software liviano y rápido, lo que permite cargar e iniciar un programa rápidamente.
- Posee soporte nativo para una gran cantidad de lenguajes, principalmente desarrolladores web, como HTML, CSS, java script, entre otros [38].

Figura N° 24. Logotipo de software Visual Studio Code [38].

2.2. DESARROLLO DE LA PROPUESTA

2.2.1. Análisis de Necesidades

Como se ilustra en la figura 25, el cantón Santiago de Píllaro está limitado al norte con el cantón Salcedo, al sur con el cantón Patate y Pelileo, al este con el cantón Ambato y al oeste con la provincia del Napo, dentro de esta ciudad se encuentra el mercado San Juan, en donde se ejecutará el proyecto.

Figura N° 25. Mapa del Cantón Santiago de Píllaro.

Fuente: Administradora Mercado.

El mercado San Juan situado en el cantón Santiago de Píllaro, fue diseñado y construido en el año 2011 para la comercialización de productos. Se encuentra ubicado en la zona céntrica del cantón, colindada por: Al norte la calle Rocafuerte, al sur la calle Urbina, al este la calle Flores y al oeste la calle Montalvo, a una latitud de -1.172829 y una longitud de -78.5436624, como se observa en las figuras 26 y 27.

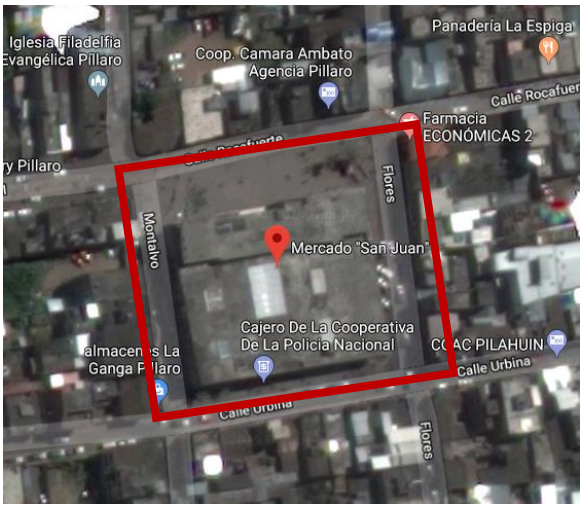


Figura N° 26. Mapa Satelital del Mercado San Juan en el cantón Santiago de Píllaro.

Fuente: Administradora mercado

Figura N° 27. Estructura física del Mercado San Juan.

Fuente: Administradora mercado

Al ser un centro de comercio que cuenta con más de 100 locales destinados para la comercialización de productos como para oficinas que trabajan en conjunto con la municipalidad del cantón, se vió la necesidad de diseñar un sistema de alarma comunitaria que permitió tanto a expendedores como a personas que trabajan en el mercado, estar en alerta y tener mayor seguridad al ocurrir eventos extraños; además se proporcionó el servicio de voz sobre IP para las diferentes instalaciones administrativas que se encuentran dentro del lugar y un sistema de video-seguridad que permitió grabar imágenes de los eventos suscitados, con ello obteniendo un efecto disuasorio contra el vandalismo que puede acontecer dentro del mercado.

Distribución de Plantas del Mercado

El centro de comercio cuenta con las siguientes plantas:

- *Nivel subterráneo:* Área de 2.651,28 m2 en donde se encuentran los parqueaderos, el área de reciclaje, área de limpieza, la cámara de transformación, cuarto de bombeo, recaudación y bodega, nivel con bajo índice de personas que acudan al lugar. Como se muestra en la figura 28.

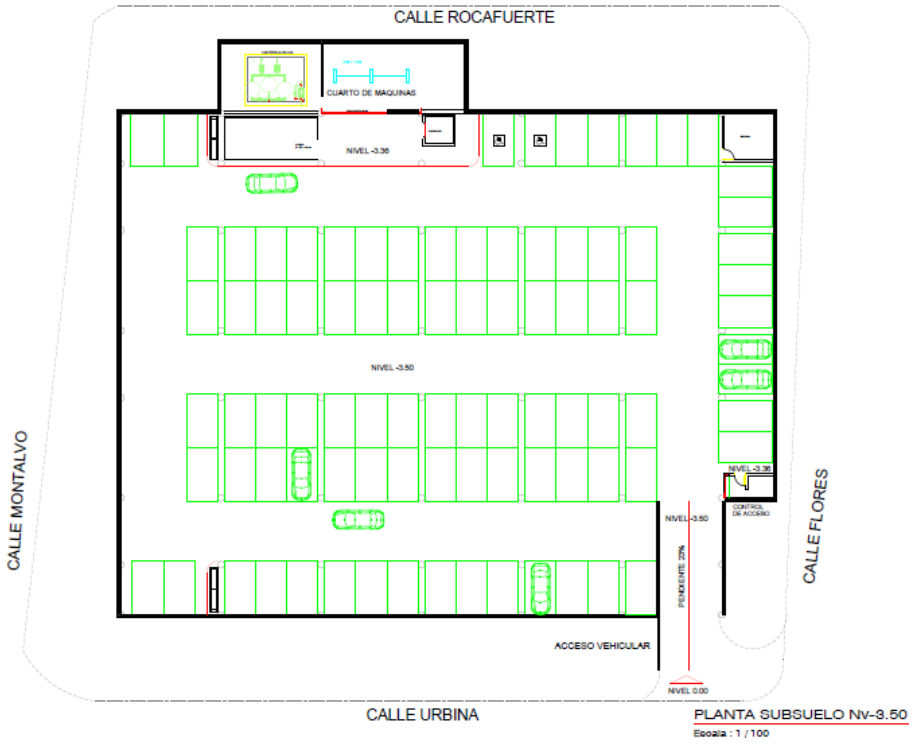


Figura N° 28. Plano físico del Nivel Subterráneo del mercado.

Fuente: Administradora de mercado

- Primer Nivel: Área de 2.439,82 m2, constituido por locales comerciales externos, puestos permanentes y áreas comunes; nivel de mayor número de visitas de compradores y proveedores de productos. Como se ilustra en la figura 29.

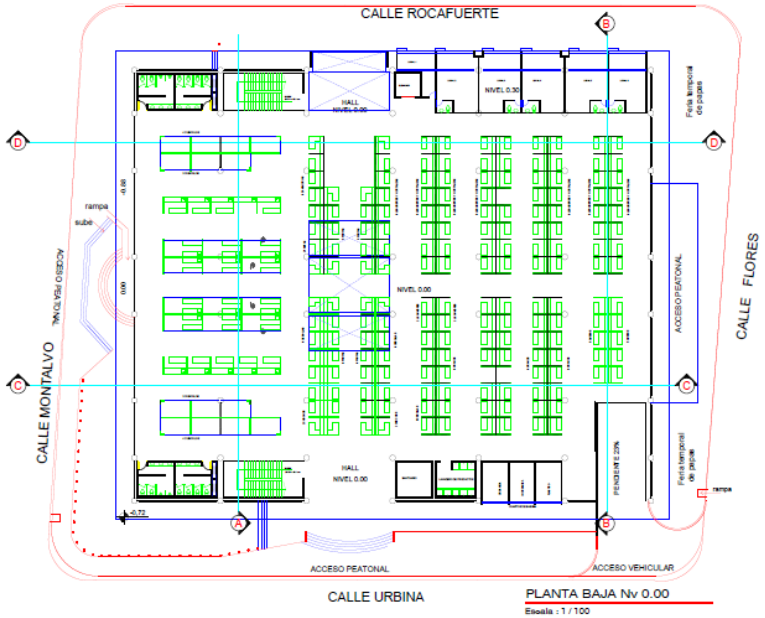


Figura N° 29. Plano físico del Primer Nivel del mercado.

Fuente: Administradora de mercado

- *Segundo Nivel:* Área de 2.625,43 m2, se encuentra el registro de la propiedad, almacenes de ropa y bisutería, abarrotes, ferreterías, artesanías y el patio de comidas; al igual que el primer nivel es un lugar de mayor número de visitas de compradores y proveedores de productos, plano presentado en la figura 30.

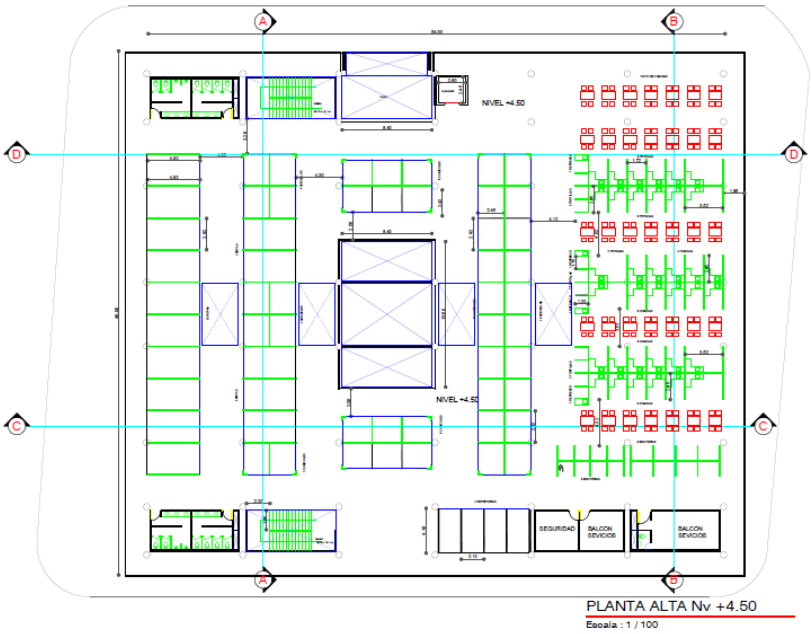


Figura N° 30. Plano físico del Segundo Nivel del mercado.

Fuente: Administradora de mercado

- *Tercer Nivel:* Tiene un área de 543,84 m2, se encuentra la administración, consultorio médico, guardería, salón de uso múltiple, patio de comidas rápidas y áreas comunes, plano ilustrado en la figura 31.

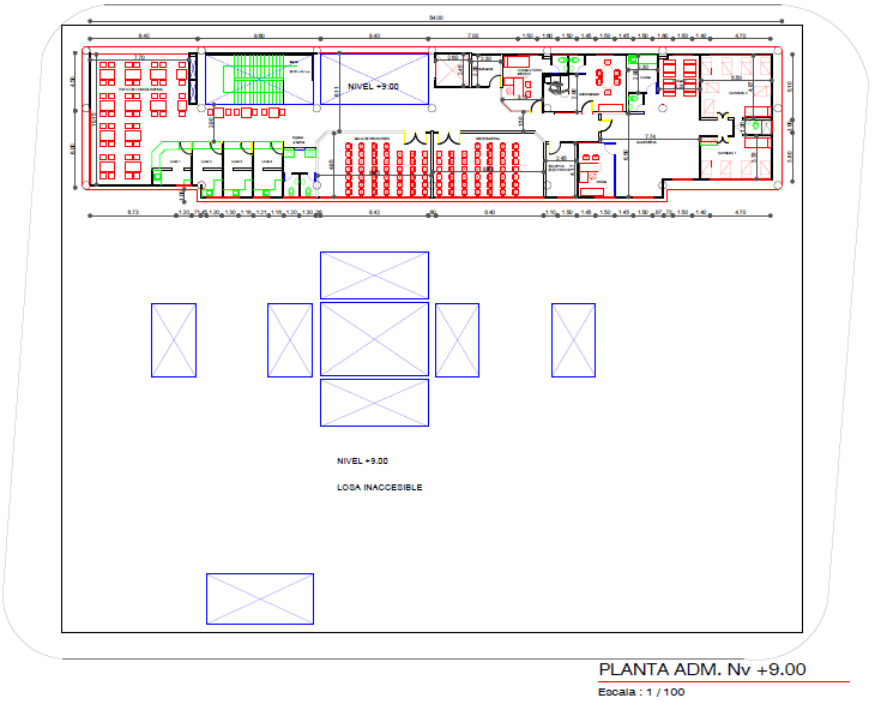


Figura N° 31. Plano físico del Tercer Nivel del mercado.

Fuente: Administradora de mercado

2.2.2. Situación Actual del Nivel de Seguridad

El mercado San Juan es un mercado de 8.260,37 m^2, que cuenta con cuatro plantas como: nivel subterráneo, primer nivel, segundo nivel y tercer nivel. Está construido de una estructura de hormigón armado, al igual que las paredes del subsuelo, con columnas de sección redonda, todo bajo normas antisísmicas, las mamposterías construidas de ladrillo y con recubrimiento de enlucido.

Respecto a las instalaciones, existen de: agua potable respaldadas de un equipo de bombeo e instalaciones de agua contra incendios, en cuanto a las instalaciones eléctricas están previstas de generadores, transformadores y equipos que garantizan la suficiente cantidad y calidad de energía.

Respecto al equipamiento, el más importante es el elevador electromecánico de 1500 kg de capacidad, permitiendo transportar una capacidad máxima de 20 personas, además del funcionamiento como elevador de productos, al ser de tipo industrial.

Respecto a la seguridad que existe actualmente dentro y fuera del mercado San Juan, en base a datos proporcionados por la Unidad de Policía Comunitaria, se citan los siguientes:

- En ocurrencia de eventos extraños dentro y fuera del mercado, los moradores pertenecientes al centro de comercio, llaman a las autoridades que velan por su seguridad como es al ECU 911, o se dirigen personalmente hacia la UPC más cercana, para que lleven a cabo las respectivas investigaciones o detenciones de personas que provocan el vandalismo, poniendo en peligro la vida de personas que estén presentes en ese momento, debido al tiempo de respuesta de las autoridades y por no contar con un sistema disuasorio, provocando el escape de dichas personas. Estos dos como uno de los métodos de seguridad y auxilio a eventos extraños que hacen uso la comunidad pillareña, en la figura 32, se presenta el modelo de gestión del sistema integrado ECU 911.

Figura N° 32. Modelo de Gestión del Sistema Integrado ECU 911.

Fuente: Policía Nacional

- Otro de los métodos de seguridad que existen para ciertos locales comerciales en el mercado es el botón de seguridad, un dispositivo que se instala en el teléfono celular del usuario, en donde el personal policial llena un formulario de solicitud para la implementación del sistema, con los datos y requisitos que previamente fueron establecidos para los usuarios interesados, una vez llenado el formulario, proceden a realizar la verificación de los mismos a través del número de cédula, para registrar el número telefónico dentro del programa. En el teléfono celular del beneficiario se agrega a "Tía Poli" en contactos, con un número de marcado rápido,

de preferencia el número “135”. El registro de los usuarios que requieren la ayuda, se realiza en el archivo de la UPC y la confirmación de activación del sistema es vía mensaje al teléfono celular del beneficiario. En el momento que la persona realiza una llamada al botón de seguridad, la aplicación instalada en la computadora de la UPC, genera una alarma audible y visible, indicando los datos de la víctima junto con la dirección exacta de su domicilio; mientras que a su vez el sistema remite un mensaje de texto, que llegan a los teléfonos celulares de los servidores policiales que se encuentran trabajando en ese subcircuito. Esta aplicación web denominada GISCNT sobre sistemas de seguridad es una herramienta brindada por la CNT, cuyo ingreso se realiza mediante un usuario y contraseña que son entregadas por parte de la empresa. En las figuras 33 y 34 se presenta la página web de ingreso GISCNT para el uso del botón de seguridad con su respectivo logotipo.

Figura N° 33. Ventana de Ingreso al sistema del Botón de Seguridad.

Fuente: Policía Nacional

Figura N° 34. Logotipo de Botón de Seguridad instalado en locales comerciales.

Fuente: Policía Nacional

- Al igual que el botón de seguridad, ciertos locales comerciales que existen en el exterior del mercado usan el sistema "Barrio Seguro", el cual es una estrategia que en conjunto con la Policía Comunitaria y la ciudadanía, interactúan ejecutando iniciativas y propuestas para ayudar a la seguridad del barrio, en donde los usuarios rentan un sistema de alarma y de video-seguridad a empresas de comunicaciones, cuyas alarmas son generadas por los beneficiarios y son enviadas directamente hacia la UPC, para tener respuesta de ayuda en caso de ser necesario, llevando así un convenio entre la UPC y miembros del barrio o comunidad, mientras que el sistema de video-seguridad es contratado por los usuarios hacia la empresa proveedora, pagando así cierta cantidad de dinero mensualmente por la vigilancia permanente de los locales, en la figura 35, se presenta el logotipo de implementación del sistema Barrio Seguro.

Figura N° 35. Logotipo de Barrio Seguro entre UPC y la Comunidad.

Fuente: Policía Nacional

Por otro lado, no existe un sistema de video-seguridad que cubra totalmente el mercado, el mismo que permita a las autoridades e incluso a los usuarios que estén presentes en el interior y exterior del lugar a tener evidencias de posibles situaciones extrañas, con los responsables de dichos eventos.

De lo anteriormente analizado sobre la situación actual del nivel de seguridad que existe dentro del mercado San Juan, al ser este un centro de comercio de servicio para toda la ciudad; así como para los cantones más cercanos y al encontrarse en un lugar estratégico, cerca del parque principal, de la municipalidad, de la iglesia, del coliseo de deportes y al ingreso llegando desde Ambato, los beneficiaros de este mercado, es toda la ciudad de Píllaro y las comunidades de su alrededor; es por ello que se vio la

necesidad de elaborar el diseño de un sistema de alarma comunitaria integral, que permitió estar en alerta a situaciones extrañas que puedan ocurrir en el centro de comercio, en la figura 36, se ilustra la estructura del mercado en el cuál se implementó el prototipo.

Figura N° 36. Estructura del Mercado San Juan.

Fuente: Administradora de mercado

2.2.3. Análisis de las Tecnologías de Comunicación Inalámbrica y el tipo de Mensajería Instantánea

En el ámbito del Internet de las cosas (IoT), se ve la necesidad de analizar tres tecnologías de comunicación inalámbrica, como son: Bluetooth, Zigbee y Wi-Fi, consideradas como las más óptimas e importantes para el desarrollo de varias aplicaciones en base a internet, en la tabla 12, se observa la comparativa de estas tecnologías, que permitieron la selección de una de ellas para nuestra aplicación como fue el sistema de alarma comunitaria.

Tabla 12. Tabla comparativa de las tecnologías de comunicación inalámbrica.

	Bluetooth	**Zigbee**	**Wi-Fi**
Estándar	802.15.1	802.15.4	802.11
Ancho de banda	1Mbps	20-250Kbps	54Mbps
Consumo de potencia	Tx: 40mA Stand By: 200µA	Tx: 35mA Stand By: 3µA	Tx: >400mA Stand By: 20mA
Memoria	Mayor a 100KB	32 a 60 KB	Mayor a 100KB
Bandas de frecuencia	2.4GHz	2.4GHz mundial 915MHz EE.UU	2.4 GHz, 5.8GHz
Tipos de datos	Digital y audio	Digital (texto)	Digital
Tipo de red	WPAN	Red inalámbrica de área personal con baja transferencia y	WLAN

		bajo consume (LR - LP WPAN)	
Arquitecturas	Estrella	Estrella, malla, árbol, poin to point.	Estrella
Alcance	1 -10 metros	1-75 metros	1-100 metros
Principal característica	Interoperabilidad, bajo costo y potencia	Alta escalabilidad y bajo coste	Alta velocidad y gran ancho de banda
Aplicación	Sustituto de cableado.	Monitorización y control remoto.	Transmisión de ficheros en área local, navegación por Internet

Fuente: Investigadora

De acuerdo, al análisis realizado, se escogió la tecnología wifi, ya que permite trabajar en redes de área local con un alcance máximo de 100 metros, un ancho de banda de 54 Mbps dependiendo del estándar a elegir, operación en las bandas de frecuencia de 2,4 y 5,8GHz, siendo esta la característica principal para el desarrollo del proyecto, y por su aplicación.

Al seleccionar ya el tipo de tecnología, se procedió al estudio de los diferentes tipos de mensajería instantánea existentes, que ayuden al desarrollo del proyecto, a continuación en la tabla 13, se presentan los aspectos más importantes de las mensajerías más usadas.

Tabla 13. Tipos de mensajería: WhatsApp, line, telegram y Messenger.

	WhatsApp	**Line**	**Telegram**	**Facebook Messenger**
Usuarios	800 millones	450 millones	50 millones	600 millones
Perfil particular/empresa	Particular	Particular y marcas	Particular	Particular
Listas	Hasta 256 usuarios	-	Hasta 100 usuarios	-
Capacidad de texto	500 caracteres	limitado	limitado	Limitado
Envío de archivos	Fotos, videos, voz, ubicación, contactos, documentos	Fotos, videos, voz, ubicación, contactos, snapmovie	Fotos, videos, voz, ubicación, contactos, documentos	Fotos, videos, voz, documentos y nuevas apps
Chat secreto	No	No	Si	No
Seguridad	No	Si	Si	Si

Versión escritorio	Todas excepto iOS	Windows Mac OS	Web, Mac OS y Linux	Web, Windows y Mac OS
Telefonía IP	Si	Si	No	Si
Videollamada	Si	Si	No	Si
Mensajes efímeros	No	No	Si	No
Destacado	Popularidad	Núm. de aplicaciones y perfil de empresa	Seguridad y tamaño de los archivos	Telefonía IP competencia de Skype
API	No	No	Si	Si

Elaborado por: Investigadora

De acuerdo al análisis realizado se optó por la mensajería instantánea Telegram, debido a la existencia de una API abierta para el desarrollo de varios programas; y la mensajería instantánea WhatsApp por su uso en la actualidad, por el número de usuarios suscriptores, por las acciones que permite realizar, como son: envío de fotos, ubicación, archivos, mensajes de texto, llamadas, video llamadas, etc; y por su interconectividad para el desarrollo de varias aplicaciones.

2.2.4. Requerimientos Técnicos del Sistema de Alarma

Para el desarrollo del proyecto se realizó un análisis técnico de los requerimientos necesarios que permitió tanto el desempeño óptimo del sistema como el ajuste a las necesidades de la comunidad. En función a ello se diseñó un prototipo de alarma comunitaria usando mensajería Telegram y el servidor cliente WhatsApp para el envío y recepción de eventos; además se elaboró un sistema de video vigilancia IP mediante detección de movimiento, en conjunto a un sistema de servicio VoIp para los usuarios del mercado. A continuación, se presentan las estructuras de los diferentes sistemas:

1. Estructura Para La Central De Alarma

El proyecto se desarrolló en dos etapas, la primera, corresponde a la central de alarma, en donde recepta los eventos emitidos por el usuario a través de mensajería instantánea Telegram, la segunda etapa corresponde, a los eventos emitidos por la central, hacia los actuadores (bocinas y activación de cámaras) y hacia la UPC más cercana del lugar. En la figura 37, se observa un diagrama de bloques del sistema en general para el mercado “San Juan”.

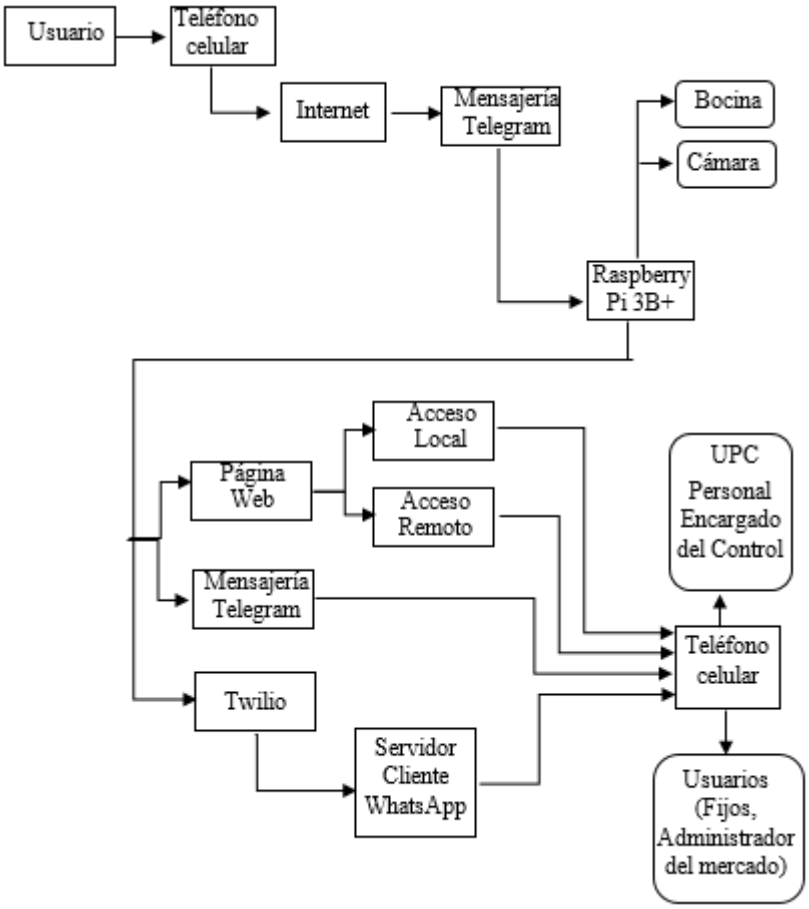


Figura N° 37. Diagrama de bloques del sistema de alarma comunitaria

Elaborado por: Investigadora

a) Primera Etapa: Central de Alarma

Esta etapa consiste en detectar la señal proveniente de los usuarios, como son los mensajes de alarma, emitidos a través de mensajería instantánea Telegram, a través de la red de área local (internet), la central procesa la información estableciendo conexión con la API de Telegram, para enviar los datos a la siguiente etapa. En la figura 38, se muestra el diagrama de bloques de la estructura básica para la central de alarma.

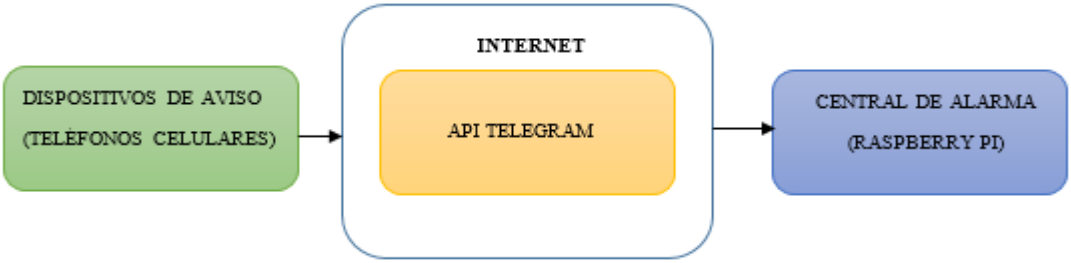


Figura N° 38. Diagrama de Bloques de Central de Alarma

Elaborado por: Investigadora

- **Dispositivos de Aviso**

Son un grupo de teléfonos celulares que permiten enviar mensajes de alerta o alarma de eventos extraños que ocurran dentro de un lugar y a su vez activar diferentes actuadores.

- **Api Telegram**

Telegram es una mensajería instantánea gratuita, que se puede usar en distintos dispositivos, presentando características de seguridad, velocidad y fácil manejo. En este punto se usa para activar Alertas y Alarmas, que son procesadas en la central.

b) Segunda Etapa: Central de Alarma y Monitoreo

En esta etapa, una vez procesado los datos, la central establece conexión, con el servidor Telegram y el servidor WhatsApp a través de la aplicación Twilio para enviar los mensajes de Alerta o Alarma hacia los usuarios fijos, la UPC y administradora del mercado, activando las diferentes alarmas tanto auditivas como visuales. Además se realiza una interfaz web, para mostrar e interpretar todos los eventos provenientes de la central, y a su vez activar desde este medio las diferentes alarmas de aviso contra emergencias, interfaz que puede ser usada por los usuarios anteriormente mencionados. En la figura 39, se observa su diagrama de bloques.

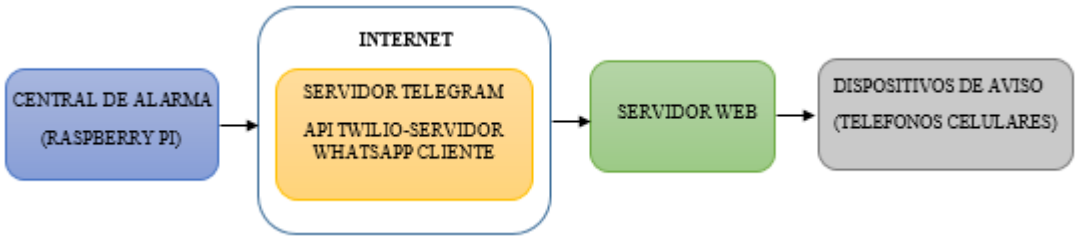


Figura N° 39. Diagrama de Bloques de central de Alarma y monitoreo.

Elaborado por: Investigadora

- **Central de Alarma**

La central de Alarma permite procesar todos los datos emitidos por los usuarios, a través de mensajería Telegram, y establecer conexión, tanto con la API de Telegram como la API Twilio para el servidor cliente WhatsApp, emitiendo así mensajes de activación de alarmas y alertas, usando la red local del mercado.

- **Servidor Web**

Es un programa responsable que procesa la aplicación creada por el usuario y establece comunicación bidireccional con el cliente, generando respuestas de solicitudes al usuario, a través de páginas web.

2. Estructura para el Sistema de Video Vigilancia IP

Como se presentó anteriormente en el análisis de la situación actual del mercado, este no cuenta con un sistema de video vigilancia, es por ello que se desarrolló un prototipo que permita simular dicho sistema, funcionando de acuerdo a los horarios de apertura del lugar, como se presenta a continuación:

- En el horario de 5am a 9pm: La cámara se centra, solo en monitorear el área donde se encuentre ubicada, sin almacenar ninguna grabación y por medio de la página web, tanto los usuarios fijos como la administradora del mercado, pueden visualizar lo que sucede, de forma local o remota.
- En el horario de 9:01pm a 4:59am: La cámara funciona en base a detección de movimiento, una vez detectado, el video es grabado y guardado en un disco de almacenamiento, emitiendo una llamada por medio del servidor asterisk al guardia de seguridad del mercado y activando la sirena.

En la figura 40, se ilustra la estructura principal del sistema de video vigilancia, usando tecnología IP, para el aprovechamiento de la red inalámbrica wifi que será diseñada más adelante.

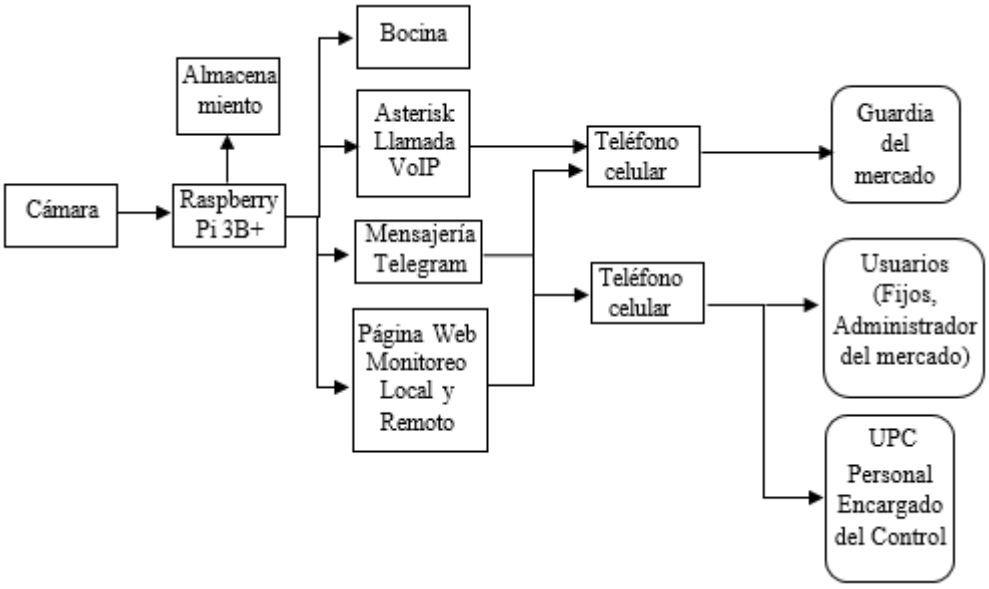


Figura N° 40. Diagrama de bloques del sistema de Video Vigilancia.

Elaborado por: Investigadora

3. Estructura para el Sistema de Servicio de VoIP

VoIP es otro servicio, que los usuarios del mercado requieren para comunicarse entre sí, a través de la red local y teléfonos celulares, en la figura 41, se presenta la estructura general del sistema.

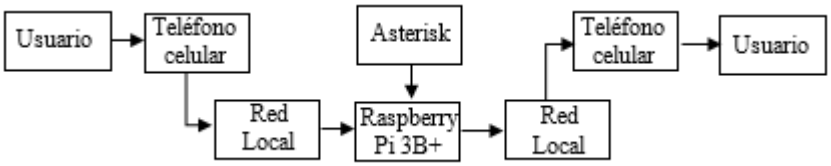


Figura N° 41. Estructura Para El Sistema De Servicio De VoIP

Elaborado por: Investigadora

2.2.5. Diseño General del Sistema de Alarma Comunitaria

1. Diagrama de bloques

A continuación, en la figura 42, se observa el funcionamiento general del sistema de alarma comunitaria, en conjunto al sistema de video vigilancia IP basado en detección ade movimiento y el sistema de servicio de VoIP, mediante un diagrama de bloques, con todos los elementos que lo componen.

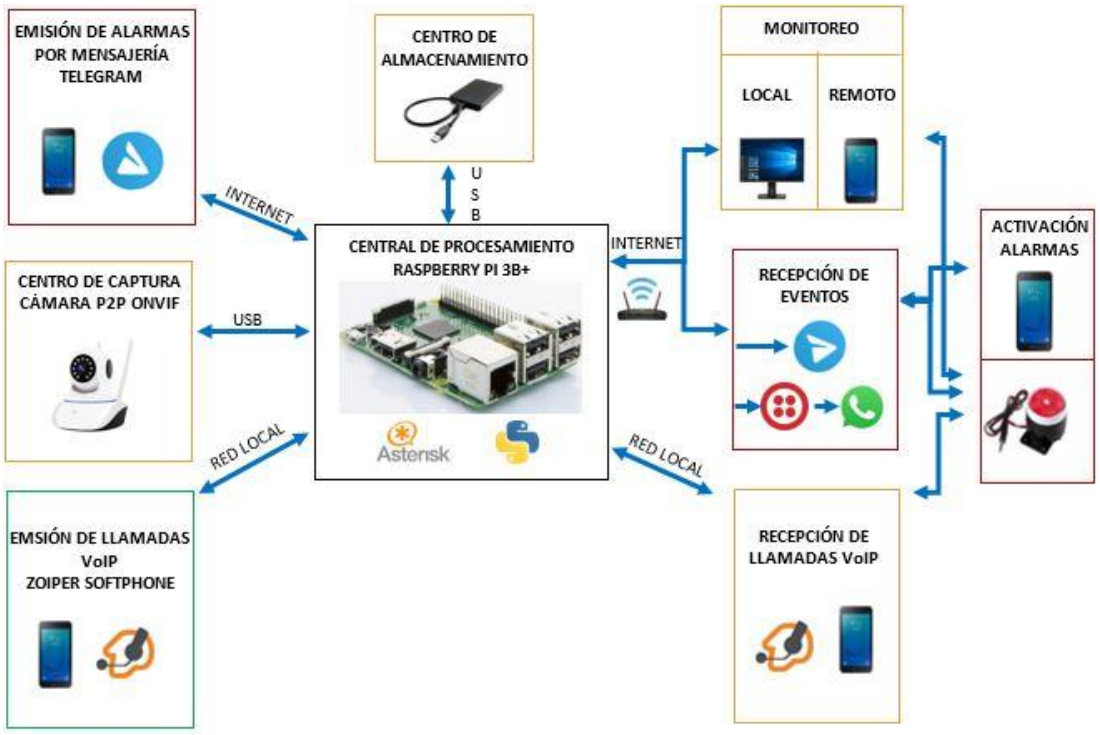


Figura N° 42. Diagrama de Bloques del Sistema de Alarma Comunitaria Integral.

Elaborado por: Investigadora

En la figura anterior, se presenta las secciones que componen a todo el sistema de alarma comunitaria, a continuación se describe cada una de ellas:

En la central de procesamiento se tiene toda la configuración del sistema de alarma, el sistema de video vigilancia IP y el servicio de VoIP; además gestiona el proceso de captura de imagen, grabación y almacenamiento de video, almacenamiento de alarmas generadas, registro de usuarios a través de números telefónicos, monitoreo local y remoto, control del sistema y activación de alarmas.

En la sección de emisión de alarmas, los usuarios del mercado que son registrados acceden a la activación del sistema, emitiendo mensajes Telegram de alarma o alerta en función de las necesidades que requieran, sistema que funciona en el horario de 5am a 9pm.

En el centro de captura, se coloca una cámara wifi, que tiene dos modos de funcionamiento. En el horario de 5am a 9pm realiza solo monitoreo, mientras que en

el horario de 9:01pm a 4:59am monitorea con detección de movimiento y los datos capturados son enviados al centro de procesamiento.

En la sección emisión de llamadas VoIP, los usuarios se comunican a través de la red local, por medio de configuraciones realizadas en los teléfonos celulares, estableciendo conexión con la central VoIP.

En el centro de almacenamiento se guardan los videos grabados por detección de movimiento.

En la sección recepción de eventos, provenientes de la central de procesamiento, si el mensaje emitido fue Alerta se envía un comunicado masivo hacia Telegram y WhatsApp de toda la comunidad registrada en el sistema, si emiten un comunicado de Alarma, se envía el mensaje y la imagen del acto vandálico capturada por la cámara en ese instante, a través de un comunicado masivo hacia Telegram y WhatsApp de todos los usuarios y a la UPC más cercana; además activando la sirena por el lapso de 1 minuto.

En la Recepción de Llamadas VoIP, los usuarios pueden receptar las llamadas realizadas por otros usuarios que se encuentren dentro de la red local, además se recibe la llamada de alarma generada por detección de movimiento, la cual fue configurada en la central de procesamiento junto al buzón de voz para activar o desactivar el sistema y la sirena.

En la sección Activación de alarmas, se tiene a los teléfonos celulares que reciben los mensajes de advertencia y la sirena como medio disuasivo.

En la sección Monitoreo Local y Remoto, se presentan visualizaciones generadas por la cámara a través de una página web, usando internet o red local, además muestra ingresos de usuarios al sistema, activación e historial de alarmas.

2. Diagrama de Conexiones

En la figura 43, se ilustra el diagrama de conexiones de todos los elementos electrónicos necesarios para el desarrollo del proyecto.

Como elemento general se usó la raspberry pi 3B+ para el centro de procesamiento, a cual va conectado: la cámara IP P2P Onvif para el monitoreo, a través de cable Ethernet, con la finalidad de tener una conexión establece sin pérdidas de señal; el Disco Duro para el almacenamiento de videos a través de cable USB 2.0; la sirena para alertas de eventos vandálicos que ocurran dentro del mercado, conectada en el puerto GPIO17 pin 11; el router a través de cable Ethernet para proveer de internet a la Raspberry Pi y a diferentes equipos para la visualización del monitoreo, tanto local como remoto del sistema de alarma y video vigilancia IP.

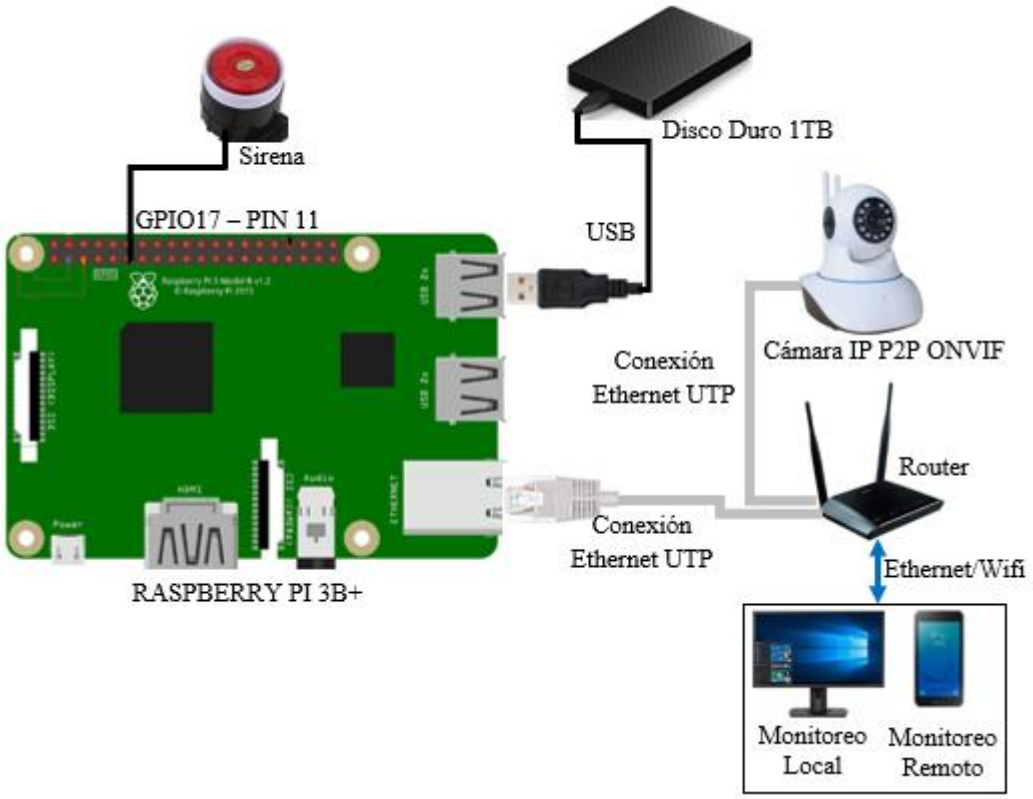


Figura N° 43. Diagrama de Conexiones del Sistema de Alarma Comunitaria Integral.

Elaborado por: Investigadora

3. Diagramas de Flujo

El sistema diseñado tiene dos modos de funcionamiento, en base a los horarios de apertura del mercado, con esta característica el sistema tomará decisiones para trabajar: en Solo Monitoreo y Alarma por mensajería ó en Monitoreo con Alarma por Detección de Movimiento.

Inicialmente, se tiene la actualización del Frame y en base a ello el modo de funcionamiento, si se encuentra en el horario de 5am a 9pm se dirige al case Alarma por mensajería y Solo monitoreo, procediendo a la activación del sistema en general. Ingresa al condicional Alarma; si fue lo emitido se envía mensajes telegram, whatsapp, captura de imagen y activación de sirena; caso contrario se dirige al condicional Alerta, y se envía solo mensajes telegram y whatsapp a todos los usuarios, si no sucede esto regresa al condicional inicial alarma, hasta receptar señales de ejecución, manteniéndose en el ciclo durante el horario establecido.

Si no se encuentra en el condicional horario de 5am a 9pm, se dirige al case Alarma por mensajería y Solo Monitoreo, activando la Detección por Movimiento e ingresando al condicional Detección, si se activa, realiza grabación, almacena en el disco duro los videos grabados en ese instante y activa la sirena. Una vez ejecutada la acción anterior, se procede a la activación de llamada VoIP por red local. En la figura 44, se presenta el diagrama de flujo de todo el sistema.

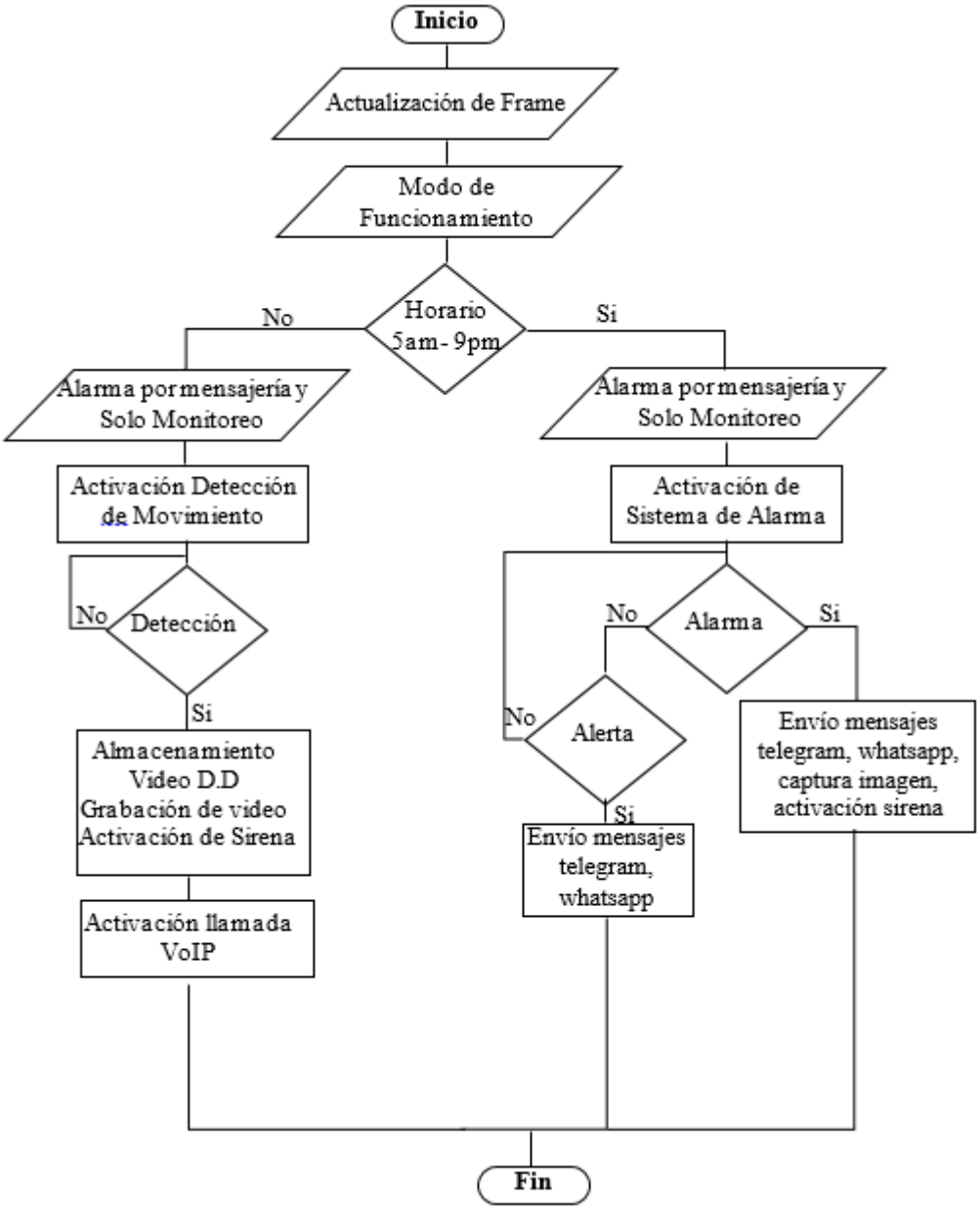


Figura N° 44. Diagrama de Flujo del Sistema de Alarma Comunitaria.

Elaborado por: Investigadora

4. Diseño lógico del Sistema

- **Tabla de direccionamiento**

Al realizar un prototipo que trabaja en base a una red de datos ya sea cableada o wifi, es necesario el direccionamiento de los dispositivos conectados a la red, en la tabla 14, se presenta la asignación IP a cada dispositivo.

Tabla 14. Direccionamiento IP de Dispositivos para la conexión Local.

Dispositivo	Dirección IP	Máscara de Red	Gateway
Raspberry pi	192.168.0.100	255.255.255.0/24	192.168.0.1
Cámara IP	192.168.0.102	255.255.255.0/24	192.168.0.1
Monitoreo	192.168.0.100	255.255.255.0/24	192.168.0.1

Elaborado por: Investigadora

2.2.6. Diseño del Sistema de Alarma Comunitaria Integral

El prototipo de sistema de alarma comunitaria integral, fue implementado en una Raspberry Pi 3 modelo B+, que cumple con funciones de video vigilancia mediante detección de movimiento y alarma física a través de una salida digital de la tarjeta, además envía y recibe alarmas, tanto locales, como remotas por medio de mensajería Telegram, WhatsApp y llamadas telefónicas IP utilizando el software Asterisk, que viene incluido en FreePBX.

El sistema operativo de la Raspberry Pi como se mencionó anteriormente, está basado en Debian, cuya distribución de raspbian fue tomada de la página "raspberry-asterisk.org", el cual viene incluido con Asterisk, FreePBX y Python 3.5.

Una vez descargado el sistema operativo, se procedió a montar en la tarjeta microSD de 64GB como una imagen ".iso", a través de Win32DiskImager, previo paso a la instalación del sistema en la tarjeta, a continuación en la figura 45, se muestra el proceso de montado.

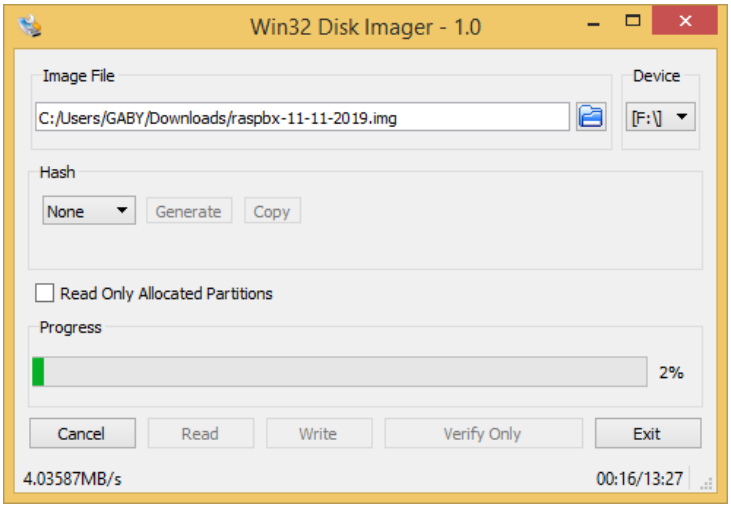


Figura N° 45. Montado imagen raspbx en microsd.

Elaborado por: Investigadora

Python fue instalado en el dispositivo, a través del comando: "sudo apt-get install python3-pip", en conjunto a las liberías de Flask, Gevent, Opencv y Twilio, requeridas por la aplicación, usando los siguientes comandos: "sudo apt-get install flask-pip", "sudo apt-get install gevent-pip", "sudo apt-get install opencv-pip" y "sudo apt-get install twilio-pip", en la figura 46, se ilustra la instalación de uno de ellos.

```
root@raspbx:~# sudo apt-get install python3-pip
Reading package lists... Done
Building dependency tree
Reading state information... Done
```

Figura N° 46. Instalación de python3 en Raspberry Pi.

Elaborado por: Investigadora

1. Diseño del servidor Web

El servidor web fue configurado en la tarjeta, a través del lenguaje de programación Python y la librería flask. En la documentación de flask recomienda no usar el servidor de pruebas integrado con la librería, por lo que la interfaz WSGI (Web Server Gateway Interface), se conecta con la librería gevent, siendo un servidor non-blocking que permitió alojar la aplicación programada, emplea hilos (threads) diferentes para servir a las distintas solicitudes (request). En la figura 47, se presenta la integración de flask y gevent en Python para formar el servidor web. Cabe recalcar que la programación se realizó usando el software Visual Studio Code.

```
from flask import Flask, render_template, request, send_from_directory, Response
from gevent.pywsgi import WSGIServer#sirve al servidor flask
from gevent.pool import Pool
import gevent
```

Figura N° 47. Integración de flask y gevent en Python para formación del servidor web.

Elaborado por: Investigadora

En base al diseño del servidor web, se desarrolló la aplicación tanto del sistema de alarma como el sistema de video vigilancia por detección de movimiento. El sitio web incluye dos páginas, una a disposición de los usuarios finales para controlar la alarma y monitorear las cámaras, y la otra para la administración, en la que se pueden agregar usuarios y configurar el sistema, todos estos archivos ubicados en la carpeta denominada stactic y templades.

Las rutas implementadas en el servidor flask son “/”, como referencia a la interfaz de usuario. Se usó dos formas para realizar request al servidor, emplenado peticiones tanto GET como POST; al recibir una request de tipo GET se envía la página en HTML, con la request de tipo POST se revisa que se hayan llenado los formularios con el usuario y contraseña válidos, para ser procesados por el servidor. Aquí es donde se puede activar o desactivar las alarmas o requerir un enlace de feed de video. En la figura 48, se puede observar el método get y post para petición de la página web en base a un index html y el método post para llenar el formulario.

```
@app.route('/', methods=['GET', 'POST'])
def index():
    if flask.request.method == "GET":
        return render_template('index.html')
    if flask.request.method == "POST":
        pswd = flask.request.form['pswd']
        usuario = flask.request.form['Usuario']
        if usuario in db['usuarios']:
            if db['usuarios'][usuario] != pswd:
                return 'contraseña incorrecta'
        else:
            return 'usuario no existe'
```

Figura N° 48. Método get y post para petición de la página web para usuarios

Elaborado por: Investigadora

La ruta ‘/administrador’ se empleó para la interfaz de administración, de igual forma con una request de tipo GET se envía el código en HTML que es la página web de administración y con la request de tipo POST se verifica la contraseña de ingreso, procediendo así a la configuración del servidor, validado el ingreso, abre funciones de: agregar usuarios, números telefónicos, y tipos de números por telegram o whatsapp, mediante las siguientes líneas de comandos: “elif flask.request.form [‘accion’]== numeros Emergencia”, “if flask.request.form[‘agregar’]==’agregar’:”, además cada número puede ser eliminado, mientras que todos los ingresos se guardan en la carpeta Folder. La ruta “/video_feed/<urlgen>” se usó para servir el feed de video de las cámaras; mientras que para imágenes y archivos estáticos se empleó la ruta “/static/<path:path>”. En la figura 49, se muestra la configuración de la página de administración para la visualización de video.

```python
@app.route('/video_feed/<urlgen>')
def video_feed(urlgen):
    return Response(gen(urlgen),
                    mimetype='multipart/x-mixed-replace; boundary=frame')

@app.route('/administrador', methods=['GET', 'POST'])
def administrador():
    if flask.request.method == "GET":
        return render_template('administrador.html')
    if flask.request.method == "POST":
        pswd = flask.request.form['pswd']
        if pswd != db['adminKey']:
            return 'error'
        if flask.request.form['accion'] == 'pswd':
            return 'correcta'
        elif flask.request.form['accion'] == 'alarma':
            db['alarma'] = not db['alarma']
        elif flask.request.form['accion'] == 'numerosEmergencia':
            if flask.request.form['agregar'] == 'agregar':
                db['numerosEmergencia'].append(
                    [flask.request.form['tipo'], flask.request.form['numero']])
            else:
                for eachNumber in db['numerosEmergencia']:
                    if flask.request.form['numero'] == eachNumber[1]:
                        db['numerosEmergencia'].remove(eachNumber)
        elif flask.request.form['accion'] == 'adminKey':
            db['adminKey'] = flask.request.form['adminKey']
            return 'reload'
        elif flask.request.form['accion'] == 'saveFolder':
            db['saveFolder'] = flask.request.form['saveFolder']
```

Figura N° 49. Configuración de la página de administración.

Elaborado por: Investigadora

Para archivos que deben mantenerse, se usó un archivo .pickle que guarda una variable objeto de nombre db, a través de la instalación de la librería estándar pickle, propia del lenguaje de programación Python, la cual toma una variable (objeto) y la serializa para poder guardarla en un archivo, siendo leído y transformado en una variable. En la figura 50, se observa como el código implementado en Python, primero analiza la existencia de un archivo de nombre data.pickle y de no existir lo crea y guarda los valores por defecto, como la contraseña inicial, de la interfaz de administración "xxxxxx"

```python
if os.path.exists('data.pickle'):
    print('Leyendo Db')
    with open('data.pickle', 'rb') as f:
        db = pickle.load(f)
    print('db Cargada')
else:
    db = {}
    db['usuarios'] = {}
    db['camaras'] = {}
    db['saveFolder'] = ''
    db['adminKey'] = '[redacted]'
```

Figura N° 50. Creación de archivo data.pickle.

Elaborado por: Investigadora

- **Interfaz de Usuario para el Control de la Alarma y Monitoreo**

Al visitar la dirección del servidor con el puerto de escucha “192.168.1.100:8080”, se muestra la página de inicio de sesión al sistema, en donde se ingresa el usuario y la contraseña, las mismas que deben ser creadas previamente en la interfaz de administración. En la figura 51, se presenta la página de inicio.

Figura N° 51. Página de Inicio al Sistema de Alarma Comunitaria.

Elaborado por: Investigadora

Al ingresar el usuario y contraseña correctos, se logra acceder a las opciones de monitoreo de la cámara, al control de la alarma y al registro de actividades. La interfaz de usuario es una aplicación web de una sola página, es decir la transferencia de la página en HTML del servidor al cliente. Las siguientes interacciones del usuario con el servidor se realizan mediante el envío de “xhtmlrequest”, y las respuestas del servidor se procesan en el navegador empleando javascript. En la figura 52, se ilustra la pantalla del menú principal de las acciones a las cuales el usuario puede ingresar.

Figura N° 52. Menú principal de usuarios para acceso al sistema.

Elaborado por: Investigadora

En la figura 53 y 54, se observa el acceso tanto a las cámaras, como a la activación, desactivación y envío de mensajes de alerta, respectivamente.

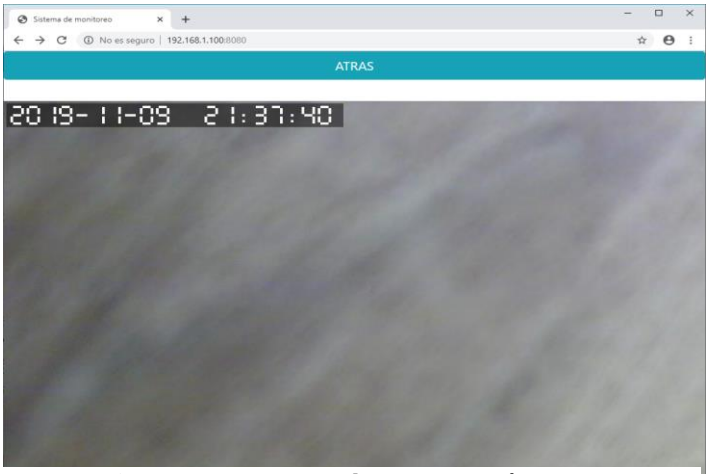


Figura N° 53. Acceso de usuarios a cámaras.

Elaborado por: Investigadora

Figura N° 54. Acceso de usuarios a la Activación de alarmas.

Elaborado por: Investigadora

- **Interfaz de Administración**

En la interfaz de administración, se presentan las diferentes entradas del formulario, que permiten modificar la configuración del servidor, en la figura 55, se muestran estos parámetros.

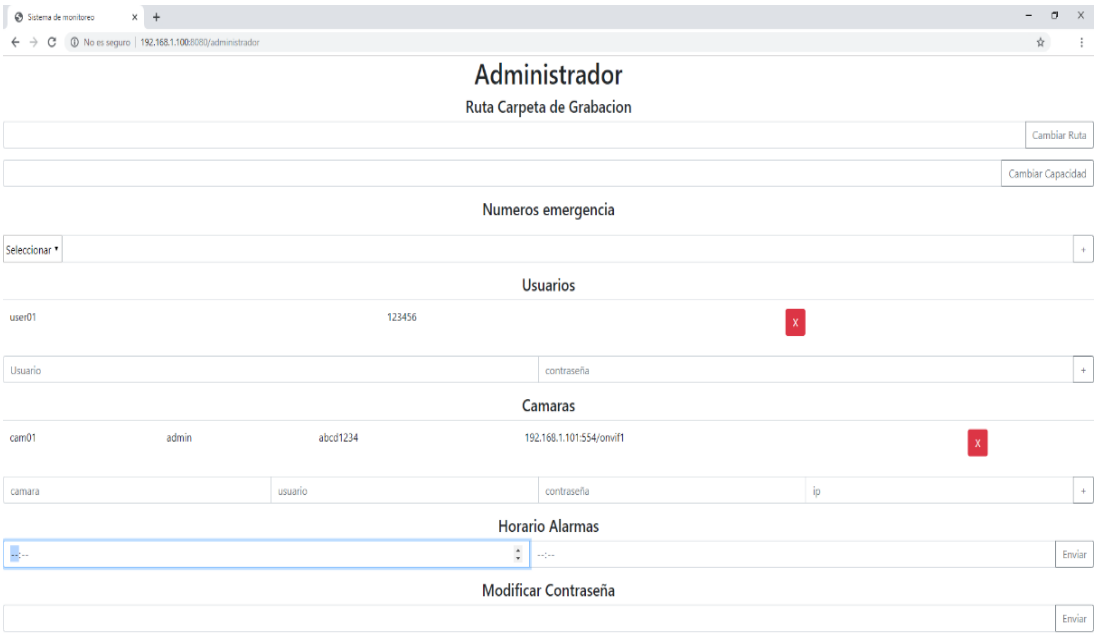


Figura N° 55. Interfaz de Administración.

Elaborado por: Investigadora

2. Diseño del Sistema de Detección de Movimiento

El manejo de las cámaras se lo realizó a través de una clase que implementa un objeto Camera, el cual posee los siguientes métodos: "get_frame" que sirve para obtener el último frame procesado y responder con una imagen codificada como jpg; "motionDetection" método encargado de realizar la detección de movimiento, siendo inicializado en la creación del objeto y ejecutado en un thread permanente de forma paralela para grabar, e "imageRefresh" método que se encarga de obtener los frames de la cámara, para ser usados por los demás métodos, además es ejecutado en su propio thread de forma permanente. En la figura 56 y 57, se observan los métodos y los threads respectivamente utilizados para el sistema de video vigilancia por detección de movimiento.

```
def get_frame(self):
    self.rimage = cv2.imencode('.jpg', self.imagen)[1].tobytes()
    return self.rimage

def motionDetection(self):
    while self.execute:
        imStatic=self.imagen
        gray = cv2.cvtColor(imStatic, cv2.COLOR_BGR2GRAY)
        gray = cv2.GaussianBlur(gray, (21, 21), 0)
```

Figura N° 56. Método motionDetection. Conversión de imagen a escala de grises.

Elaborado por: Investigadora

```
self.thread1 = threading.Thread(target=self.motionDetection)
self.thread1.start()
self.thread2 = threading.Thread(target=self.imageRefresh)
self.thread2.start()
```

Figura N° 57. Threads como ejecución en segundo plano de motionDetection.

Elaborado por: Investigadora

La detección de movimiento se implementó utilizando el principio de substracción entre el último frame obtenido y el fondo o imagen sin movimiento, una vez realizada la substracción se procedió a la conversión a escala de grises mediante “cv2.cvtColor”, y a través de “cv2.GaussianBlur” un filtro gaussiano suavizando la imagen. Para obtener el fondo se realizó una suma ponderada con pesos entre el fondo y el último frame, en donde el fondo inicial es el primer frame obtenido; proceso que permitió obtener un fondo que cambia de forma dinámica y no se mantiene estático, a través del uso de operaciones “cv2.addWeighted” y “cv2.mean” que presenta opencv en Python. Además esta librería se usó para obtener el stream de la cámara y usarlo en el script. En la figura 58, se ilustra el proceso de detección de movimiento en base a las operaciones de opencv.

```
def motionDetection(self):
    while self.execute:
        imStatic=self.imagen
        gray = cv2.cvtColor(imStatic, cv2.COLOR_BGR2GRAY)
        gray = cv2.GaussianBlur(gray, (21, 21), 0)
        if self.background is None:
            self.background=gray
        else:
            self.background = cv2.addWeighted(self.background,0.95,gray,0.05,0.0)
        diff_frame = cv2.absdiff(self.background, gray)
        changeValue = 0
        for item in cv2.mean(diff_frame):
            changeValue += item*item
        if self.imagenes < 50:
            self.imagenes+=1
            changeValue=0
```

Figura N° 58. Proceso detección de movimiento usando cv2.cvtColor y cv2.absdiff

Elaborado por: Investigadora

Después de obtener una detección de movimiento se generó un archivo de video que fue almacenado en la carpeta especificada en la página de administración, esta carpeta se encuentra ubicada en un disco duro externo, para lo cual se realizó el proceso de montado usando los siguientes comandos y en el orden establecido:

- raspbx-upgrade: Actualización del sistema operativo.
- sudo apt-get install ntfs-3g: Instalación del tipo de Sistema de archivos que maneja el disco duro externo, por lo general es ntfs-3g.
- sudo blkid: Verificación de la unidades conectadas a la Raspberry Pi.
- sudo fdisk –l: Verificación de la capacidad que tiene el disco duro, con el tipo de archivos que maneja.
- cd /media, sudo mkdir VIDEOS: Ingresar a la carpeta media y dentro de esta crear otra carpeta llamada VIDEOS.
- /media/ sudo nano /etc/fstab: Dentro de la carpeta media, editar el fichero fstab para que el dispositivo monte el disco duro cada vez que sea encendido.
- Cd/media/VIDEOS/: Dentro de la carpeta donde fue montado el disco duro, se creó otra carpeta denominada VIDEOS-MONITORIZACION para guardar los videos (mkdir VIDEOS-MONITORIZACION).
- sudo chmod 755 /media/VIDEOS: Configuración de permisos a la carpeta.
- sudo reboot: Reiniciar la tarjeta, para que realice los cambios efectuados.
- La ruta de almacenamiento de los videos es: /media/VIDEOS/VIDEOS-MONITORIZACION.

En la figura 59, se presenta la modificación de parámetros dentro del archivo fstab, junto a la carpeta creada media/VIDEOS, para el montado del disco duro.

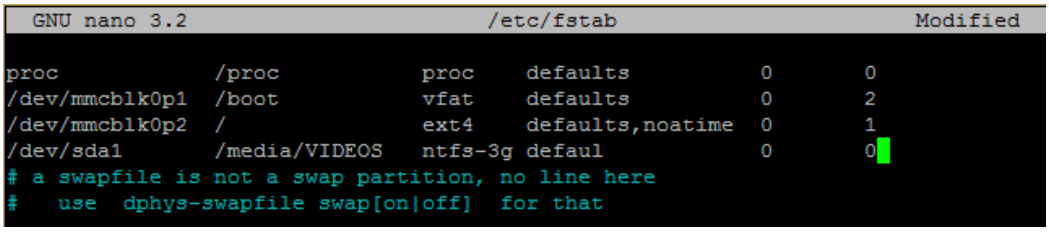


Figura N° 59. Montado de Disco Externo en la Raspberry Pi.

Elaborado por: Investigadora

3. Sistema de Alarma mediante Mensajería Telegram

Otra de las partes que fue programada es el sistema de alarma mediante mensajería, en donde se usó la sentencia "def" para la creación del objeto alarma a través de mensajería Telegram, y se empleó un Bot con el nombre SanJuanSeguraBot, el sufijo Bot debido a las reglas que establece telegram para la creación de API's.

El proceso de creación del Bot se realizó dentro de la app de telegram, escribiendo a la cuenta BotFather, una vez creado el Bot se obtiene un token, con el cual se puede controlar. En la figura 60, se muestra el proceso de creación del Bot, para ello se busca en la mensajería telegram BotFather e inicio de conversación.

Figura N° 60. Creación de Bot a través de BotFather telegram.

Elaborado por: Investigadora

Seguidamente, se crea un nuevo bot con "/newbot", en donde se colocó el nombre SanJuanSeguraBot, generando así un token con el que ya se puede trabajar. En la figura 61, se presenta de creación del Bot.

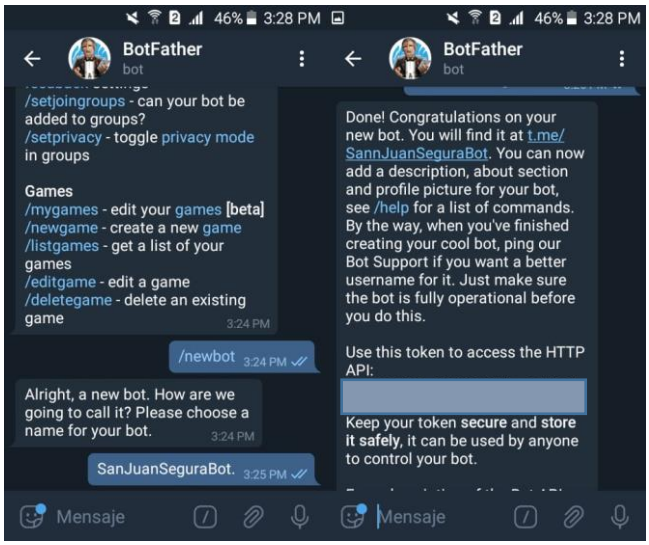


Figura N° 61. Creación del nuevo bot SanJuanSeguraBot y generación del Token

Elaborado por: Investigadora

Una vez se obtuvo el token de telegram, se procedió a realizar la configuración en Python para el control del sistema de alarma. Para ello se estableció una clase denominada telegramHandler, que permitió manejar la mensajería telegram; dentro de esta clase se creó el objeto token del bot de telegram y a su vez funciones de esa clase para el envío de los mensajes, usando la sentencia "def sendMessage(self, mensajeTelegram, sendID)"; necesariamente se generó un thread de la función anteriormente creada, para la ejecución en segundo plano, en caso se detengan las demás funciones. En la figura 62, se muestra la programación realizada.

```
class telegramHandler(object):
    def __init__(self, bottoken):
        self.bottoken = bottoken
        self.actualizaciones = []
        self.loadAlertas()
        self.execute = True
        self.thread1 = threading.Thread(target=self.checkAlertas)
        self.thread1.start()

    def sendMessage(self, mensajeTelegram, sendID):
        threadsm = threading.Thread(target=self.sendMessagethread(mensajeTelegram, sendID))
        threadsm.start()
        print('send msj')
```

Figura N° 62. Clase telegramHandler para envio de mensajes a través del Bot.

Elaborado por: Investigadora

Para que los usuarios y miembros de la UPC puedan interactuar con el servidor, a través, de mensajería telegram, se crearon dos chats para los grupos. Una vez creados, se copió el ID de cada chat para colocarlos en la página de administración y que el servidor trabaje en conjunto al token del bot con los IDs de cada chat.

El ID de los chats pueden ser visualizados, a través, de mensajes que son enviados al bot, accediendo a la dirección: "https://api.telegram.org/bot[token]/getUpdates" y, copiando el token emitido por el bot en lugar de la palabra "bot[token]", quedando así: https://api.telegram.org/xxxxxxxxxxxxxxxxxxxxxxxx/getUpdates, la cual responde con un objeto JSON y siendo procesado en Python para ver actualizaciones caso de existir. El sistema implementado hace una request cada 10 segundos hacia la dirección citada anteriormente usando la librería urllib que es parte de las librerías estándar de Python. En la figura 63, se puede observar la programación del envío de mensajes usando el bot.

```
def sendMessagethread(self, mensajeTelegram, sendID):
    values = {'chat_id': sendID,
              'text': mensajeTelegram
              }
    data = urllib.parse.urlencode(values)
    data = data.encode('ascii')
    msjurl = 'https://api.telegram.org/bot'+self.bottoken+'/sendMessage'
    req = urllib.request.Request(msjurl, data)
    with urllib.request.urlopen(req) as response:
        html = response.read()
    print(mensajeTelegram)
```

Figura N° 63. Envío de mensajes con ID, usando librería urllib, a través de threads.

Elaborado por: Investigadora

- **Creación del Grupo SanJuanSegura**

Una Vez generado el token, para el envío de mensajes e interacción con el servidor, se crearon dos grupos, al primer chat SanJuanSegura se agregó a tres usuarios del mercado y al Bot creado inicialmente, para que todos los usuarios reciban los mensajes tanto de Alarma como de Alerta, y en el segundo chat SanSeguraUPC, se agregaron números policiales en conjunto con el Bot para recibir solo mensajes de Alarma. En la figura 64, se ilustra la creación de los grupos.

Figura N° 64. Creación del grupo de chat usuarios y UPC en Telegram

Elaborado por: Investigadora

Una vez creados los grupos, se copió el IDE de cada chat, para que el servidor interactúe de acuerdo a los mensajes emitidos por cada usuario, este IDE puede ser visualizado, al ingresar a la URL:

"https://api.telegram.org/xxxxxxxxxxxxxxxxxxxxxxxx/getUpdates"

Con el Token asignado por el BotFather, y dentro de esta página se puede observar el IDE de cada Chat, como se presenta en la figura65.

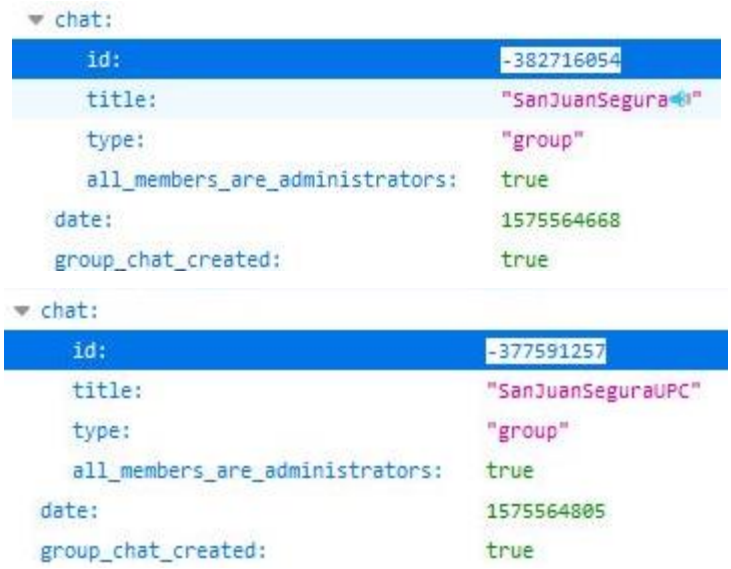


Figura N° 65. IDES de los chats para interacción con el servidor.

Elaborado por: Investigadora

Los IDES copiados fueron ingresados a la página de administración del sistema. En la figura 66, se presenta el ingreso de cada IDE y un número de whatsapp para la recepción de mensajes tanto de alerta como de alarma.

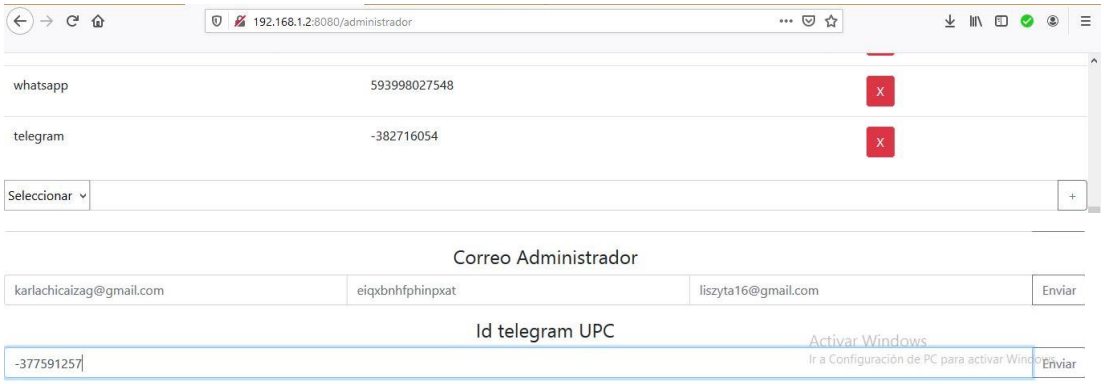


Figura N° 66. Ingreso de IDE de los dos grupos para interacción del Bot con el servidor.

Elaborado por: Investigadora

4. Recepción de mensajes de alerta a mensajería WhatsApp

Para que el servidor creado emita mensajes de alerta activados por los usuarios mediante telegram a WhatsApp, se empleó la plataforma twilio, que permitió enviar mensajes desde un número provisto por la plataforma, la cual mantiene una librería de Python.

Con la importación del módulo Cliente de twilio.rest, se creó un objeto cliente, a través del "account_sid" y el "token" autorizado que se obtiene de la plataforma. Como argumentos del método se ingresa el número desde el cuál se envía (provisto por la plataforma), el número objetivo y el mensaje a enviar. En la figura 67, se muestra el proceso de envió de mensajes de alerta o alarma a WhatsApp.

```
account_sid = "[redacted]"
auth_token = "[redacted]"

client = Client(account_sid, auth_token)
mensajewhatsapp = client.messages.create(
    to=numerowhats,
    from_='[redacted]',
    body=logmensaje)
```

Figura N° 67. Envío de mensajes de alerta a WhatsApp usando token de twilio.

Elaborado por: Investigadora

5. Configuración correo electrónico

Cuando el sistema haya detectado movimiento, a más de emitir las alertas por medio de mensajería, se configuró un correo electrónico que reciba la imagen captada en ese momento. Para ello se usó la librería ygmail un cliente GMAIL /SMTP, que fue empleado en la clase alarma, para emitir la imagen desde el correo Gmail del administrador de la página, hacia el correo de la persona encargada de la seguridad del mercado. En la figura 68, se presenta la configuración.

```
yag = yagmail.SMTP(db['correoApp'], db['passwordCorreo'])
yag.send(db['correoAdministrador'], 'Correo Alarma Comunitaria', [logmensaje,'imagenSend.jpg'])
```

Figura N° 68. Configuración correo electrónico para envío de imagen usando ygmail.

Elaborado por: Investigadora

6. Configuración de Llamada Asterisk

El software Asterisk junto con FreePBX, se ejecutan de forma paralela al servidor de monitoreo y control. Una forma sencilla de realizar llamadas automáticas en Asterisk es mediante el uso de archivos de llamadas o call files. Un archivo de llamada que se coloque en la carpeta /var/spoll/Asterisk/outgoing es procesado de forma automática por Asterisk.

Para realizar las llamadas mediante Python se configuró un archivo de extensión .call en el directorio del servidor, colocando el canal (extensión) a la cual se va a llamar, en este caso la extensión 707 perteneciente al guardia de seguridad, en conjunto con el mensaje que se vaya a reproducir, este archivo se envió a la carpeta "/var/spool/Asterisk/outgoing", para ser ejecutado, en caso de recibir un mensaje de ALARMA, configuración mostrada en la figura 69.

C: > Users > GABY > Desktop > calls > hw.call

```
1  Channel: Local/707@from-internal
2  Application: Playback
3  Data: Alarma-Intruso-Acceso-Mercado
```

Figura N° 69. Archivo de llamada Asterisk hw.call

Elaborado por: Investigadora

7. Configuración del Servidor Asterisk VoIP

FreePBX posee una interfaz gráfica para la configuración de llamadas telefónicas IP, a esta página se añadieron las extensiones para cada usuario. Para ello se ingresó a la dirección del servidor asterisk, 192.168.1.100, con usuario y contraseña admin, colocando extensiones formato PJSIP, con su respectivo usuario y contraseña. En la figura 70, se presentan las extensiones creadas para tres usuarios del mercado San Juan.

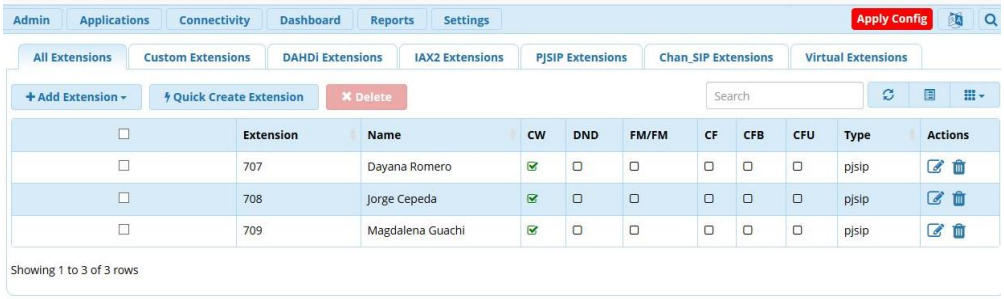


Figura N° 70. Extensiones PJSIP creadas en FreePBX, para 3 usuarios del mercado.

Elaborado por: Investigadora

Creadas las extensiones, se procedió a la configuración de los zoiper para cada usuario, estableciendo así la telefonía IP. En la figura 71, se ilustra la extensión 707 perteneciente al usuario Dayana Romero, junto a la dirección del servidor y la contraseña establecida en FreePBX. Para el usuario Jorge Cepeda se usó la extensión 708 y para el usuario Magdalena Guachi la extensión 709, como se presenta en la figura 72.

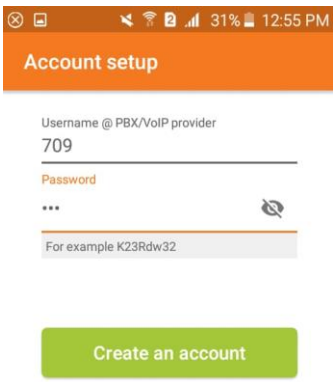


Figura N° 71. Configuración de teléfono zoiper usuario Magdalena Guachi, extensión 709.

Elaborado por: Investigadora

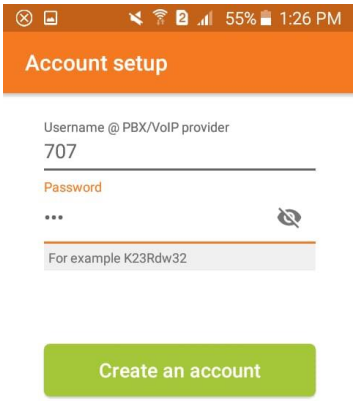


Figura N° 72. Configuración de teléfono zoiper usuario Dayana Romero, extensión 707.

Elaborado por: Investigadora

Para que la aplicación app.py creada en Python sea iniciada, al ejecutar la Raspberry Pi de forma automática, sin tener que levantar el servidor, se utilizó el comando ">crontab –e" lanzando un archivo .sh ubicado en el directorio del script, en donde se colocó la ruta del script del proyecto, seguido del comando "launcher" para lanzar el script.sh. En la figura 73, se muestra la configuración realizada.

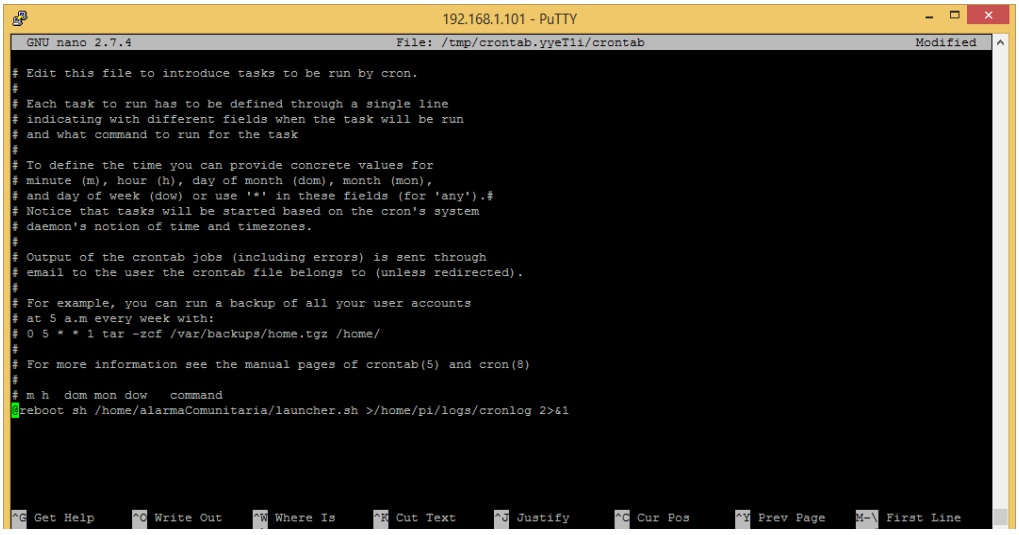


Figura N° 73. Configuración de archivo crontab para ejecución de script al iniciar el sistema.

Elaborado por: Investigadora

2.2.7. Diseño Sistema de Alimentación

Para la implementación del sistema de alarma comunitaria y video vigilancia IP en el mercado “San Juan”, se diseñó un sistema de alimentación y un sistema de respaldo de energía. El sistema de alimentación consta de una fuente de energía de 12V 5A, que por medio del circuito de potencia se alimentó: a un relé de 12V para activación de la sirena, a la Raspberry y al ventilador como sistema de refrigeración para el centro de procesamiento.

La alimentación de la Raspberry y ventilador, fue a través de conversores DC DC Step Down 3A LM2596, un regulador conmutado, que presenta altos niveles de eficiencia energética, debido al uso de conmutadores y almacenadores, con excelencia de regulación de línea y bajo voltaje de rizado, como se observa en la figura 74.

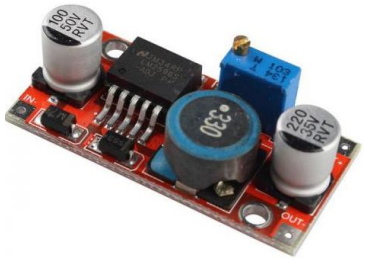


Figura N° 74. Regulador DC DC LM2596 3A.

Elaborado por: Investigadora

A continuación, en la figura 75, se presenta el diseño del circuito de alimentación para la Raspberry Pi de 5V 2.5A, para un ventilador de 5 V 0.23A y para la sirena de 12V 180mA, además se adicionó un circuito de respaldo de energía usando una batería de 12V 4A, y en la figura 76, se observa el circuito de activación de la sirena de 12V, a través de un relé y del puerto GPIO 17 de la Raspberry Pi.

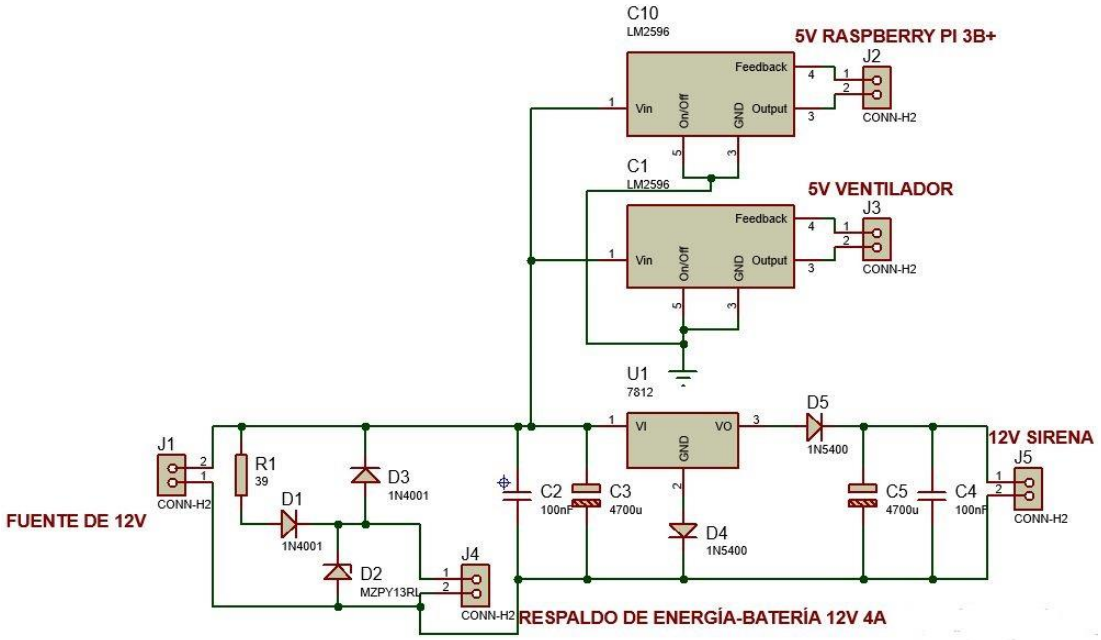


Figura N° 75. Circuito de Alimentación y Respaldo de Energía.

Elaborado por: Investigadora

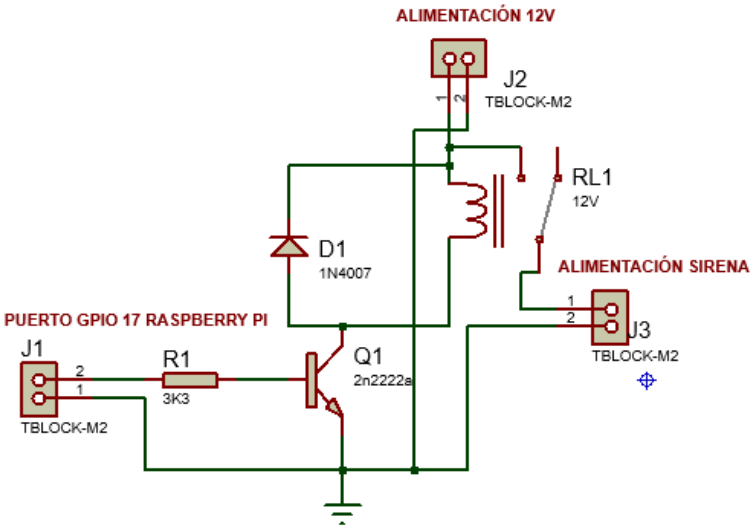


Figura N° 76. Circuito de activación de sirena 12V.

Elaborado por: Investigadora

2.2.8. Cálculo del Ancho de Banda

1. Ancho de Banda de Sistema de Video Vigilancia IP

Para el diseño de la red wifi es necesario calcular el ancho de banda del prototipo del sistema de video vigilancia, esto se realiza en base a varios parámetros tanto de la cámara IP que se seleccionó como del servidor flask.

Es necesario calcular el tamaño de la imagen en base a la resolución y al tipo de compresión que emplea la cámara, para el cálculo del ancho de banda, cabe mencionar que la cámara que se seleccionó usa un códec de video H.264-v50, con ello teniendo un tamaño de imagen o cuadro de 9Kbytes, garantizando así una mejor resolución para mostrar las imágenes.

- **Tamaño de un cuadro incluyendo encapsulamiento [39]**

Un paquete TCP/IP sobre Ethernet, presenta un tamaño máximo de datos de 1500 bytes que se puede transportar; de esta trama al retirar tanto la cabecera IP, como la cabecera TCP, se obtiene los datos útiles de la capa de Aplicación TCP, como se muestra a continuación:

$$T_{real.inf} = Tamaño.máx\ datos - cabecera\ IP - cabecera\ TCP$$

$$T_{real.inf} = 1500\ bytes - 20\ bytes - 20\ bytes$$

$$T_{real.inf} = 1460\ bytes$$

Con el tamaño de información o datos útiles obtenidos anteriormente y el tamaño de cuadro de 9Kbytes de acuerdo a la compresión H.264-V50, se calculó el número de tramas que se necesitan para la transmisión de un cuadro.

$$\#tramas\ para\ envio\ de\ un\ cuadro = \frac{tamaño\ de\ cuadro}{T_{real.inf}} * \frac{1024\ bytes}{1Kilobyte}$$

$$\#tramas\ para\ envio\ de\ un\ cuadro = \frac{9\ Kilobytes}{1460\ bytes} * \frac{1024\ bytes}{1Kilobyte} = 7tramas$$

A través del número de tramas, se calculó la sobrecarga por encapsulamiento, como se muestra a continuación:

$$Sobr. = 7 * [20bytes(cab.IP) + 20bytes(cabe.TCP) + 18bytes(encab + col.eth)]$$

$$Sobr. = 7 * [20 + 20 + 18]$$

$$Sobr. = 406bytes * \frac{1Kilobyte}{1024\ bytes} = 0.396\ Kbytes$$

Obteniendo así el tamaño real de un cuadro de 1920x720 pixeles igual a:

$$Tamaño\ real\ de\ un\ cuadro = (2Kbytes + 0.396Kbytes) * \frac{8bits}{1byte} = 19.17Kbits$$

- **Ancho de banda necesario para la transmisión de video**

Una vez calculado el tamaño real de un cuadro, se procedió a obtener el ancho de banda necesario para la transmisión de video, cabe recalcar que en el servidor flask se configuró el parámetro cuadros por segundo (fps), asignando 5fps, esta asignación fue baja para que el streaming de video no demande de un gran ancho de banda.

A continuación se presenta el cálculo del ancho de banda para la transmisión de video a 5fps:

$$AB_{5fps} = 19.17\frac{Kbits}{cuadro} * \frac{5\ cuadros}{seg} = 95.85Kbps$$

Obteniendo así un ancho de banda aproximado para la transmisión de cinco cuadros por segundo de 95.85Kbps

- **Cálculo de espacio de memoria para almacenamiento de video [40]**

Para la determinación del espacio de memoria que se requiere para el almacenamiento de video, se tomó en cuenta el tiempo de actualización, en este caso se realizó para un mes, en donde el periodo de funcionamiento es de 1728000 segundos o las 480 horas, con ello se procedió a determinar el espacio de memoria suficiente:

$$Espacio\ de\ memoria = Perido\ de\ func. mensual * AB_{5fps}$$

$$Espacio\ de\ memoria = 1728000s * 95.85Kbps * \frac{1Mbit}{1024Kbits} * \frac{1Gbit}{1024Mbits}$$

$$Espacio\ de\ memoria = 157.95Gbits$$

$$Espacio\ de\ memoria = 157.95Gbits * \frac{1Byte}{8bits} = 19.74Gbytes$$

El espacio de memoria mínimo que se requiere para almacenamiento de video en la Raspberry Pi es de 19.74Gbytes.

- **Cálculo de datos consumido por el sistema de video vigilancia [40]**

Para el envío de video streaming de forma remota, a través de internet, desde el servidor flask instalado en la Raspberry hacia el usuario, se requiere de datos, que provee un router instalado en el mercado a los diferentes equipos que existentes dentro de el.

Previamente calculado el ancho de banda aproximado para el sistema de video vigilancia de acuerdo al período de funcionamiento, se procedió a calcular los datos necesarios para el funcionamiento del sistema mensualmente.

$$Datos\ de\ video\ vigilancia = Perido\ de\ func.mensual * AB_{5fps}$$

$$Datos\ de\ video\ vigilancia = 1728000s * 95.85Kbps * \frac{1Mbit}{1024Kbits} * \frac{1byte}{8bits}$$

$$Datos\ de\ video\ vigilancia = 20218.36Mbytes$$

El consumo de datos mensualmente que utilizará el sistema de video vigilancia es de 20218.36Mbytes aproximadamente, este valor se utilizará posteriormente para el cálculo de megas necesarias para la implementación de una red wifi dentro del mercado.

2. Ancho De Banda De Servicio VoIP [40]

Dentro del mercado San Juan, no existe el servicio de telefonía para la comunicación entre diferentes locales o áreas administrativas existentes, es por ello que se desarrolló el servicio de VoIP, aprovechando el servicio de internet que se va a diseñar.

Para el cálculo del ancho de banda requerido, que permita una buena comunicación se tomó en cuenta dos parámetros primordiales como son la señalización y el audio; además se debe tener en cuenta los siguientes aspectos:

- Tipo de códec
- Número de usuarios
- Encapsulamiento de trama de voz en capa 2

- **Determinación de la trama de voz**

Para transmitir voz sobre una red de datos se arman paquetes, y el ancho de banda necesario para esta transmisión, depende de la sobrecarga que generen los paquetes armados.

Una vez que la señales de voz análoga es digitalizada, pasa a ser encapsulada por el protocolo RTP, posteriormente por el protocolo UDP y este a su vez por el protocolo IP debido a que viaja típicamente sobre Ethernet; además para el cálculo de la trama de voz es necesario determinar la carga útil del códec a emplear. A continuación en la tabla 15, se muestra el encapsulamiento para una trama de voz, en donde el servidor VoIP Asterisk usa un códec G.726, con una carga útil de 80 bytes, en un tiempo de 20ms.

Tabla 15. Encapsulamiento de la Trama de Voz.

Cabecera Ethernet (20 bytes)	Cabecera IP (20 bytes)	Cabecera UDP (8 bytes)	Cabecera RTP (12 bytes)	Carga útil del códec (80 bytes)

Elaborado por: Investigadora

Con los valores de la tabla 15 presentados se calcula la trama de voz como sigue:

$$Trama\ de\ voz = cab.eth + cab(IP + UDP + RTP) + carga\ útil\ de\ códec$$

$$Trama\ de\ voz = 20bytes + (20 + 8 + 12)bytes + 80bytes$$

$$Trama\ de\ voz = 140bytes$$

Como siguiente punto se calcula el ancho de banda total requerido para una llamada, cabe recalcar que al usar un códec G.726 se envía 50 tramas por segundo, obteniendo así:

$$AB_{total\ VoIP\ 1\ llamada} = Trama\ de\ voz * \#tramas\ por\ segundo$$

$$AB_{total\ VoIP\ 1\ llamada} = 140bytes * \frac{50\ tramas}{1s}$$

$$AB_{total\ VoIP\ 1\ llamada} = 7000\ bytes\ por\ segundo$$

$$AB_{total\ VoIP\ 1\ llamada} = 7000\ bytes\ por\ segundo * \frac{8bits}{1byte}$$

$$AB_{total\ VoIP\ 1\ llamada} = 56Kbps$$

Entonces el ancho de banda necesario para establecer una llamada a través de la red Ethernet es de 56Kbps, valor que servirá para obtener el ancho de banda total y con ello realizar el diseño de la red wifi para el mercado San Juan.

Otro de los parámetros a calcular es el número máximo de llamadas que se pueden realizar simultáneamente, cabe recalcar que la Raspberry Pi soporta hasta un máximo de 10 llamadas simultáneas, obteniendo así un ancho de banda total de:

$$AB_{total\ 10\ llamadas} = 56Kbps * 10\ llamadas$$

$$AB_{total\ 10\ llamadas} = 560Kbps$$

Obteniendo así un ancho de banda total al ocurrir 10 llamadas simultáneamente de 560 Kbps.

3. Ancho De Banda Total

En base al análisis realizado en los apartados anteriores sobre el ancho de banda necesario para el funcionamiento del prototipo de un sistema de alarma comunitaria integral, compuesto por un sistema de video vigilancia IP, servicio de VoIP y la generación de alarmas en base al uso de mensajería instantánea WhatsApp y Telegram, se calcula el ancho de banda total del prototipo, se tomó en cuenta que las mensajerías usadas para el sistema de alarma, se analizan en apartados posteriores en base al número de usuarios y a la frecuencia de utilización.

Tabla 16. Ancho de Banda Total para el prototipo.

ÍTEM	SERVICIOS	ANCHO DE BANDA (KBPS)
SERVICIOS	Video vigilancia IP	95.85
	VoIP (Voz sobre IP 10 llamadas simultáneas)	560
ANCHO DE BANDA TOTAL		**655.85**

Elaborado por: Investigadora

En la tabla 16, se observó que se tiene un ancho de banda total, tanto del sistema de video vigilancia IP y del servicio VoIP de 655.85Kbps, dato que en apartados posteriores se usará para el cálculo del ancho de banda total.

2.2.9. Diseño del Sistema de Video Vigilancia

1. Análisis del sistema de video vigilancia mediante visitas de campo

Para el diseño de un sistema de video vigilancia CCTV que pueda ser implementado en el mercado "San Juan" fue necesario realizar vistas de campo y en conjunto con los planos adquiridos del lugar, se evaluaron las áreas a cubrir, en donde se estableció la ubicación de las diferentes cámaras, el cableado y la localización de los equipos conectados hacia las cámaras.

Como se muestra en la figura 28, en el subsuelo se encuentra el garaje para el acceso vehicular, cuenta con una garita del guardia (recaudación), el área de reciclaje, área de limpieza, la cámara de transformación, cuarto de bombeo y bodega. Además el acceso a este nivel tanto vehicular como peatonal es por medio de una sola entrada principal frente a la calle Urbina, mientras que el acceso solo peatonal es desde el primer nivel hacia el subsuelo es a través del ascensor y de las gradas.

En el primer nivel, como se ilustra en la figura 29, se dispone de seis locales comerciales externos, puestos de expendio de frutas, hortalizas, legumbres, lácteos, cárnicos. Se tiene cuatro accesos con puertas de vidrio, denominados de la siguiente forma: al norte con el acceso 1 frente a la calle Montalvo, al sur con el acceso 2 frente a la calle Flores, al este con el acceso 3 frente a la calle Rocafuerte y al oeste con el acceso 4 frente a la calle Urbina. Además se tiene un acceso por medio del ascensor y por medio de las gradas.

En el Segundo nivel, como se presenta en la figura 30, se encuentra el registro de la propiedad, almacenes de ropa y bisutería, abarrotes, ferreterías, artesanías y el patio de comidas. El acceso a este nivel es por medio del ascensor y de las gradas.

En el tercer nivel, como se muestra en la figura 31, se encuentra la administración, consultorio médico, guardería, salón de uso múltiple, patio de comidas rápidas y áreas comunes. El acceso a este nivel es solo por medio de las escaleras.

El sistema de seguridad de video-vigilancia contará con dos niveles de seguridad, según la visita de campo realizada, uno de alta prioridad y otro de baja prioridad.

En la tabla 17, se muestra los diferentes pisos con el nivel de seguridad y el número de cámaras correspondientes para cada área a cubrir. Entre los pisos con nivel de seguridad baja son el tercer y segundo nivel, mientras que el subsuelo y el primer nivel son considerados como áreas que dependen de un alto nivel de seguridad, debido a que en el subsuelo se tiene el acceso tanto vehicular como peatonal, mientras que en el primer nivel se tiene el acceso solo de personas hacia los niveles superiores y además se tiene locales comerciales exteriores, que poseen una cantidad elevada de mercadería.

Una vez analizado el nivel de seguridad para cada piso, con la finalidad de tener un control de la mercadería expuesta al público, almacenes en bodega, y diferentes áreas de servicio a la comunidad pillareña como son: el registro de la propiedad, consultorio médico, entre otras oficinas, se ha establecido el número de cámaras. Para el nivel subsuelo se consideró conveniente usar tres cámaras para la zona de garaje y acceso vehicular; para el primer nivel se tiene siete cámaras, cuatro cámaras para el control de las zonas de acceso de personas, dos cámaras para la seguridad de los locales comerciales exteriores que se encuentran frente a las calles Rocafuerte y Urbina y una cámara en las escaleras de acceso al nivel; para el segundo nivel se tiene seis cámaras, dos cámaras ubicadas en las escaleras de acceso del norte y del sur, dos cámaras para el control de almacenes de bodega y dos cámaras para el control de la zona de comidas y demás oficinas aledañas a esta área; y finalmente para el tercer nivel se usó dos cámaras, una cámara ubicada en las únicas escaleras de acceso y una cámara para el control del acceso hacia las diferentes oficinas.

Tabla 17. Número de cámaras de acuerdo al nivel de seguridad de cada nivel.

Piso	Áreas	Nivel de seguridad	N° de cámaras
Subsuelo	• Acceso: Vehicular, peatonales • Garaje	Alto	3
Primer Nivel	• Accesos: Peatonales	Alto	7

	• Locales comerciales externos • Pasillos		
Segundo Nivel	• Accesos peatonales • Almacenes de bodega • Patio de comidas y oficinas aledañas	Medio	6
Tercer Nivel	• Acceso peatonal • Acceso a consultorio médico, guardería, administración y salón de uso múltiple	Medio	2
TOTAL DE CÁMARAS			**18**

Elaborado por: Investigadora

2. Requerimientos del sistema de video vigilancia

El sistema de seguridad de video vigilancia CCTV propuesto para el mercado "San Juan" en base al análisis realizado, consta de 18 cámaras distribuidas en áreas estratégicas para el control del mismo. La localización de los equipos principales como es el NVR, Switch, accesorios necesarios para la conexión, el rack y el monitoreo local estarán ubicados en el área de seguridad en el segundo nivel del mercado, el monitoreo remoto se lo ubicó en el área de acceso al garaje, controlado por el guardia. En base a lo descrito anteriormente se procede a la selección de parámetros y equipos para el diseño del sistema de video vigilancia, antes de ello se menciona a la tecnología CCTV IP, que se usó para el diseño del sistema, debido a los requerimientos iniciales.

Tecnología CCTV IP

El diseño propuesto para que sea implementado en el mercado "San Juan", será basado en la tecnología IP, ya que presenta varias ventajas con respecto a los sistemas tradicionales como son los análogos.

Entre las ventajas que presentan los sistemas CCTV utilizando tecnología IP es la calidad de la imagen, debido a que las imágenes que son capturadas por las cámaras mantienen el mismo formato digital; además que manejan un amplio rango de resolución sin tener pérdidas de la calidad de imagen. Para la transmisión de video, audio y alimentación PoE por lo general se usa cable UTP y la característica principal

que lleva con respecto a los sistemas análogos, es que utilizan el ancho de banda de la red, permitiendo una conexión a internet y con ello estableciendo una conexión remota.

Selección del Medio de Transmisión

En este tipo de sistemas de video vigilancia usando tecnología IP, existen dos opciones para los medios de transmisión de información en una red local, una por cable de par trenzado y otra por medio de fibra óptica. En la tabla 18, se analizó los cables más usados para estos sistemas.

Tabla 18. Cables como medio de transmisión en sistema de video vigilancia IP.

Tipo de Cable	**UTP cat.5e**	**UTP cat.6**	**Fibra óptica**
Descripción del cable	Cobre de 4 pares	Cobre de 4 pares	Vidrio, de 2 fibras
Frecuencia	100 MHz	250 MHz	
Velocidad de transmisión	1000Mbps	1000Mbps	1Gbps
Ancho de banda por segundo	1000Mbps	1000Mbps	1Gbps
Atenuación mín.	22dB	19.8dB	0.2-3.0dB/Km
Tipo de conector	RJ45	RJ45	ST o SC
Longitud máxima de cable	100 metros	100 metros	2Km(multimodo) 100Km(monomodo)
Inmunidad al ruido	Buena	Buena	Excelente
Facilidad de instalación	Excelente	Excelente	Buena
Costo por conexión	Muy Bajo	Muy Bajo	Alto
Red Soportada	1000 BASE-T	1000 BASE-TX	Multimodo: 1000BASE-SX, 1000BASE-LX, 1000BASE-LH

Elaborado por: Investigadora

De acuerdo al análisis se escogió el cable par trenzado UTP, debido a su flexibilidad, a la velocidad de transmisión, la distancia del cableado horizontal y sobre todo el costo. Se usó el estándar Gigabit Ethernet (1000 Mbit/s), cable UTP categoría 6, par trenzado

de cobre, impedancia de 100 ohms, velocidad de 1000 Mbps con un aislamiento de polietileno y desempeño de hasta 300MHz. Para su implementación se realizó el diseño mediante cableado horizontal entre las cámaras que existen en los diferentes pisos hacia el Switch principal.

Tomando en cuenta las normas del cableado horizontal regidas por la norma ANSI/TIA-568.1-D [41], se tienen distancias máximas de 100 m entre el Switch y las cámaras IP; para la conexión entre los equipos de red se usará conectores RJ45 categoría 6 regidos por la norma T568B de ponchado. En la tabla 19, se presenta tres marcas de cable utp categoría 6 que actualmente se destacan en el mercado nacional.

Tabla 19. Características de cables UTP cat.6 marca NEXXT y AMP

Tipo de Cable	**Cable UTP cat.6 NEXXT para interiores**	**Cable UTP cat.6 AMP para interiores**
Número de pares	4	4
Calibre de conductor	23 AWG	23 AWG
Frecuencia de operación	250MHz o mas	250MHz o mas
Tipo de revestimiento	LSZH	LSZH
Material conductor	Cobre sólido pulido	Cobre sólido
Atenuación máx. a 250MHz	32.8dB/100m	32.8dB/100m
Distancia máxima de enlace	90 metros	100 metros
Color	Gris	Blanco
Rollo	305 metros	305 metros
Costo	$158.00	$187.00
Disponibilidad en la ciudad	Si	No

Elaborado por: Investigadora

De acuerdo a la comparativa que se realizó de las dos marcas más sobresalientes en el mercado nacional con sus respectivas características técnicas, se escogió el cable utp cat.6 para interiores marca NEXXT, debido al costo y a la disponibilidad en la ciudad de Ambato.

Selección del dispositivo de monitoreo

Las cámaras IP hoy en la actualidad son los equipos más usados debido a sus grandes funcionalidades, ya que permiten captar y transmitir imágenes directamente a través de la red datos que se tenga instalada. En la tabla 20, se realizó el análisis técnico de diferentes cámaras IP de acuerdo a tres marcas más predominantes en el mercado nacional.

Tabla 20. Características de cámaras Hikvisión, Dahua, Axis.

Dispositivo /Características			
Marca	Hikvision	DAHUA	AXIS
Modelo	DS-2CD1041-I	DH-IPC-HFW1431S	P1435-LE
Tipo	Bullet	Bulle	Bullet
Sensor de imagen	1/3”	1/3”	1/2.8”
Resolución	4Mp(2688x1520) pix	4Mp(2688x1520)pix	1080p
Tipo de lente	2.8mm	2.8mm	3mm
Ángulo de visión	105.8°	104°	95°
Compresión	H.264, H.264+, MJPEG	H.264, H.265	H.264, MPEG, JPEG
Video bit rate	32Kbps a 16Mbps	32Kbps a 10.24Mbps	-
Visión nocturna	Si	Si	Si
Rango de IR	Hasta 30m	Hasta 30m	Hasta 30m
Frame Rate (fps)	20fps	20fps	50fps
Enfoque remoto	Si	Si	Si
Alimentación PoE	Si	Si	Si
Costo	$107	$128	$570
Otras características	• Detección de movimiento • Múltiples protocolos: TCP/IP, IPv6, FTP, HTTP, HTTPS, DHCP • Estándar ONVIF • Protección IP67 • Monitoreo móvil a través de Hik-Connect o iVMS-4500 • Uso para edificaciones	• Detección de movimiento • Múltiples protocolos: TCP/IP, IPv6, FTP, HTTP, HTTPS, DHCP • Estándar ONVIF • Protección IP67 • Software de Gestión Smart PSS, DSS, DMSS • Control remoto para IOS, Android • No hay interfaz de video y audio	• Detección de movimiento • Múltiples protocolos: TCP/IP, IPv6, FTP, HTTP, HTTPS, DHCP • Zoom remoto • API abierta para integración de software • Software de gestión Axis • Notificaciones por correo electrónico.

	interiores y exteriores • Alimentación 12VDC	• Protección IP67 • Red Ethernet RJ45 (10/100 Base-T) • Alimentación 12VDC	

Elaborado por: Investigadora

Para este diseño se eligió cámaras IP Hikvision modelo DS-2CD1041-I para interiores y exteriores, con ello dando cobertura a las zonas deseadas y siendo las mejores para su instalación. En el Anexo B se puede observar las características técnicas de la cámara seleccionada.

Selección del equipo de grabación y almacenamiento

Al ser un sistema que trabaja con tecnología IP es necesario utilizar un equipo denominado NVR (Grabador de Video en Red), el mismo que permitirá recibir las imágenes digitales y transmisiones de video usando la red y con ello ofreciendo visualizaciones remotas; la visualización y gestión del NVR se realiza a través de la red usando una PC por medio de conexión remota. En la tabla 21, se presenta un análisis comparativo de las especificaciones técnicas de tres equipos NVR.

Tabla 21. Comparativa equipos NVR, marca Hikvision, Dahua, Axis

Dispositivo /Características			
Marca	HIKVISION	DAHUA	AXIS
Modelo	DS-7732NI-E4	DH-NVR4232-4K	Grabador AXIS Camera Station S1032. Versión 1
Número de canales	32	32	32
Interfaces de Red	Ethernet: 10/100/1000Base-T	Ethernet: 10/100/1000Base-T	Ethernet: 10/100/1000Base-T
NVR estándar	Si	Si	Si
Procesador	-	Procesador doble núcleo	Intel, Xeon E5-2407 v2, 2.40 GHz, 10 MB caché
Almacenamiento	2 x 6 TB para cada Disco	2 x 12 TB para cada Disco	4 x 3 TB (9 TB espacio libre después de RAID)

Velocidad de grabación	160Mbps	192Mbps	192Mbps
Gestión remota	Si	Si	iDrac 7 Express
Compresión de video	• H.264 • H.264+	• H.264 • H.265 • MJPEG	• H.264 • Motion JPEG
Conectores	• 2 USB 2.0 • 1 USB 3.0 • 1 RJ45 • 1 HDMI • 1 VGA • 1 Salida de video y audio	• 1 USB 2.0 • 1 USB 2.0 • 1 puerto RS232 • 1 puerto RS485 para control PTZ • 2 puertos SATA III de hasta 12 TB • 1 Ethernet RJ45	• 4 USB 2.0 • 2 VGA • puerto serie (DB9) • 2 Ethernet (RJ45) • 2 tomas de corriente
Alimentación	100-240V	100-240V	100-240V
Otras características	• Búsqueda por detección de movimiento y eventos de alarmas. • Múltiples protocolos ONVIF, TCP, UDP, RTP, IPv6	• Máximo acceso de usuarios 128 • Control móvil iPhone, iPad, Android	• Activación de eventos por detección de movimiento por video • Activación de alarmas
Costo	$437.00	$395.00	$7.533

Elaborado por: Investigadora

El equipo que se seleccionó para este diseño fue el NVR de Hikvision modelo DS-7732NI-E4 de 32 canales debido a las 18 cámaras IP que se van a utilizar, con un disco duro de 6TB, 2 puertos USB de 2.0 con una compresión de video H.264. Además posee puertos VGA, HDMI para la grabación y reproducción local del video, otra forma de reproducción es de forma remota a través de conexión internet [42]. Una de las características opcionales es trabajar en búsqueda por detección de movimiento generando alarmas en base al modo de grabación.

Selección de dispositivo de almacenamiento

Estos dispositivos son un componente fundamental dentro de un sistema de video vigilancia para el almacenamiento digital de las imágenes, en conjunto con el NVR ya que este siempre está activo grabando lo que las cámaras IP captan, además otra característica de selección es su tiempo de funcionamiento 24 horas diarias 7 días de la semana y 365 días al año, y que sea compatible con el NVR seleccionado; a

continuación en la tabla 22, se muestra un cuadro comparativo de discos duros más usados en un sistema de video vigilancia.

Tabla 22. Comparativa de dos discos duros internos para almacenamiento de video.

Dispositivo /Características	**DISCO DURO**	**DISCO DURO**
Marca	Western Digital Purple	Seagate SkyHawk
Modelo	WD40PURZ	ST4000VX007
Capacidad formateado	4TB	4TB
Formato	3.5 pulgadas	-
Interfaz del DD	Serial ATA-600	Serial ATA-600
Firmware	AllFrame 4K	ImagePerfect
Cumple con RoHS	Si	Si
Cámaras admitidas	Hasta 64	Hasta 64
Velocidad de transferencia	Búfer-huésped: 6Gb/s Huésped a: 150MB/s	Hasta 190MB/s
Carga de trabajo anualizada	180TB/año	180TB/año
Costo	$144.00	$160.00

Elaborado por: Investigadora

Para el diseño del sistema se ha seleccionado un disco duro Western Digital Purple modelo WD40PURZ de 4TB con un total de cámaras admitidas de 64, firmware AllFrame 4K, su interfaz Serial ATA-600 compatible con el NVR seleccionado [43], además es seleccionado presentar un costo asequible.

Selección del equipo intermediario Switch

Este dispositivo permitirá gestionar la red del sistema de video vigilancia, en la tabla 23, se observa la comparativa de dos tipos de Switch con sus respectivas características técnicas, para la selección del más óptimo.

Tabla 23. Comparativa de equipos intermediarios Switch, marca Cisco y HP.

Dispositivo /Características		
Marca	CISCO	HP
Modelo	SG200-10FP	HPE 2915
Puertos	8 x 10/100/1000 +2 Gigabit SFP	8 x 10/100/1000
Tecnología PoE	Si	Si
Protocolo de Gestión Remota	SNMP, RMON, HTTP,	SNMP
RAM	128 MB	128 MB

Memoria FLASH	16 MB	32 MB
Estándar	IEEE 802.3, 802.3u, 802.1D, 802.3af, 802.1q	IEEE 802.3, 802.3u, 802.3ab,802.1q 802.1D, 802.3af
Interfaces	8 x 10BASE-T/100BSE-TX/1000BASE-T, RJ45, PoE	8 x 10BASE-T/100BSE-TX/1000BASE-T, RJ45, PoE
Alimentación	110VAC: 60Hz	110VAC: 60Hz
Costo	$400.00	$841.00

Elaborado por: Investigadora

Los Switch seleccionados fueron de la marca CISCO modelo SG200-10FP de 10 puertos con 8 puertos PoE 10/100/1000, utilizados como dispositivos centrales, que permiten interconectar hasta 8 cámaras IP del subsuelo, del primer nivel segundo nivel y tercer nivel, en el segundo nivel se ubicó un Switch central de 8 puertos al cual se conectaron los 3 switch y este hacia el NVR; mientras que el dispositivo de grabación se conectó hacia la red local e internet, formando así una topología en árbol, además que permite la alimentación de cada una de las cámaras. Los cuatro Switch cuentan con 6 puertos RJ45, que al contar con la tecnología PoE reduce los costos de equipo y de instalación ya que ofrece datos y alimentación eléctrica a través del cable Ethernet existente para las interconexiones [44]. En el Anexo C se puede observar las características técnicas del dispositivo.

Alimentación a través de Ethernet

La alimentación PoE (Power Over Ethernet) es una tecnología que incluye la alimentación eléctrica a la estructura LAN. En la tabla 24, se muestra el estándar 802.3af, el mismo que establece las clases de potencia para los diferentes dispositivos, en este caso se hizo énfasis en las cámaras IP, la cual pertenece a la clase 2, con una potencia máxima en PSE (Equipo de Abastecimiento de Energía) de 7W [45].

Tabla 24. Clases de potencia que usa el estándar 802.3af

Estándar	Clase	Potencia Máxima En PSE	Potencia Máxima En PD (100m)	Dispositivos
802.3af	0	15.4 W	0.44 a 12.94 W	-
802.3af	1	4 W	0.44 a 3.84 W	Teléfonos IP
802.3af	2	7 W	3.84 a 6.49 W	Cámaras IP, Access Point

802.3af	3	15 W	6.49 a 12.95 W	Cámaras PTZ, Access Point

Elaborado por: Investigadora

Selección del equipo de visualización

Para la visualización del video, así como también la configuración y gestión de los equipos, se requiere de pantallas que se conecten hacia el NVR, en la tabla 25, se presenta un cuadro comparativo de los tipos de pantallas de visualización.

Tabla 25. Comparativa de Monitores marca Samsung y Hikvision

Dispositivo /Características	**MONITOR**	**MONITOR**
Marca	SAMSUNG	HIKVISION
Modelo	S24F350FHU	24MP48HQ
Pantalla	24”	24”
Resolución	1920 x 1080 (Full HD)	1920 x 1080 pixeles
Puertos	• 1 HMI • 1 VGA	• 1 HMI • 1 D-Sub
Accesorios	• Cable de alimentación de 1.5m • Cable VGA	• Cable de alimentación de 1.5m • Cable HDMI
Alimentación	110, 220 VAC	110, 220 VAC
Costo	$142.00	$292,00

Elaborado por: Investigadora

Mediante el cuadro comparativo realizado se seleccionó un monitor de la marca Samsung modelo S24F350FHU de 24 pulgadas, compatible con la conexión VGA y HDMI del NVR seleccionado anteriormente.

Selección del dispositivo de Red

Para el diseño del sistema de video vigilancia IP es necesario que en la unidad de administración ubicada en el segundo nivel del mercado, se requiera de un dispositivo proveedor de internet, con la finalidad que este pueda dar conectividad de internet al Switch general, y se pueda acceder al control remoto. En la tabla 26, se tiene un cuadro comparativo de los diferentes dispositivos de red, que existen en el mercado.

Tabla 26. Comparativa de dispositivos de red. Routers marca Lynksys, Asus y TP-Link.

Dispositivo /Características			
Marca	LINKSYS	ASUS	TP-LINK
Modelo	EA6200	90IG0471-BO3100	ARCHE C7
Frecuencia	2.4GHz 5GHz	2.4GHz 5GHz	2.4GHz 5GHz
802.11a/b/g/n/ac	Si	Solo n, ac	Si
Velocidad de datos	Hasta 300Mbps para 2.4GHz Hasta 867Mbps para 5GHz	Hasta 300Mbps para 2.4GHz Hasta 450Mbps y 750Mbps para 5GHz	Hasta 450Mbps para 2.4GHz Hasta 1300Mbps para 5GHz
Puertos LAN/WAN	Puertos 10/100/1000 4 LAN 1 WAN	Puertos 10/100/1000 1 ADSL 2 WAN	4 puertos LAN 10/100/1000Mbps 1 WAN
Puerto USB	1 USB 3.0	No	2 USB 2.0
Antenas	2 internas de 2.4GHz 2 internas de 5GHz	3 antenas externas de 5GHz	3 antenas externas de 5GHz 3 antes internas de 2.4GHz
Seguridad	WEP, WAP, WPA2	WEP ,WPA-PSK,WPA2-Enterprise,WPA2-PSK,WPS	WEP,WPA / WPA2,WPA-PSK/ WPA2-PSK
Soporte DDNS	Si	Si	Si
Port forwarding	Si	Si	Si
Alimentación	12 VDC, 2A	12 VDC, 2A	12VDC / 1.5A
Costo	$409.00	$70.00	$86.00

Elaborado por: Investigadora

Para el sistema de administración se ha seleccionado el router TP-LINK modelo ARCHE C7, cuya característica principal es contar con una seguridad WPA2-PSK, por su compatibilidad de una multitud de estándares inalámbricos, además por la velocidad de transmisión que ofrece en la banda de los 5GHz de hasta 1300Mbps y por su costo accesible para el diseño del sistema [46].

3. Diseño esquemático del sistema de Video-Vigilancia IP

El diseño del sistema de video vigilancia en base a la tecnología IP para el mercado San Juan, consta de 18 cámaras IP que monitorearan el área a cubrir, cuatro Switch

PoE de 10 puertos cada uno, un dispositivo NVR para la grabación, como medio de transmisión cable UTP categoría 6, un monitor para la observación del video y un equipo de red para el acceso a internet. Cada Switch del subsuelo, del primer y segundo nivel consta de 10 puertos RJ 45 con alimentación mediante cable de red, ideales para trabajar con cámaras IP. Estos dispositivos fueron identificados por diferente nomenclatura de acuerdo a los niveles del mercado, los cuales se detallan más adelante, las cámaras se conectarán a estos equipos, permitiendo así la transmisión de datos y su propia alimentación. Los Switch de cada nivel a su vez se conectan a un Switch general que se encuentra en el área de seguridad ubicado en el segundo nivel, a este se conectó el router (para el acceso remoto) y a su vez al equipo de grabación. En la figura 77, se presenta el esquema general del sistema de video vigilancia IP.

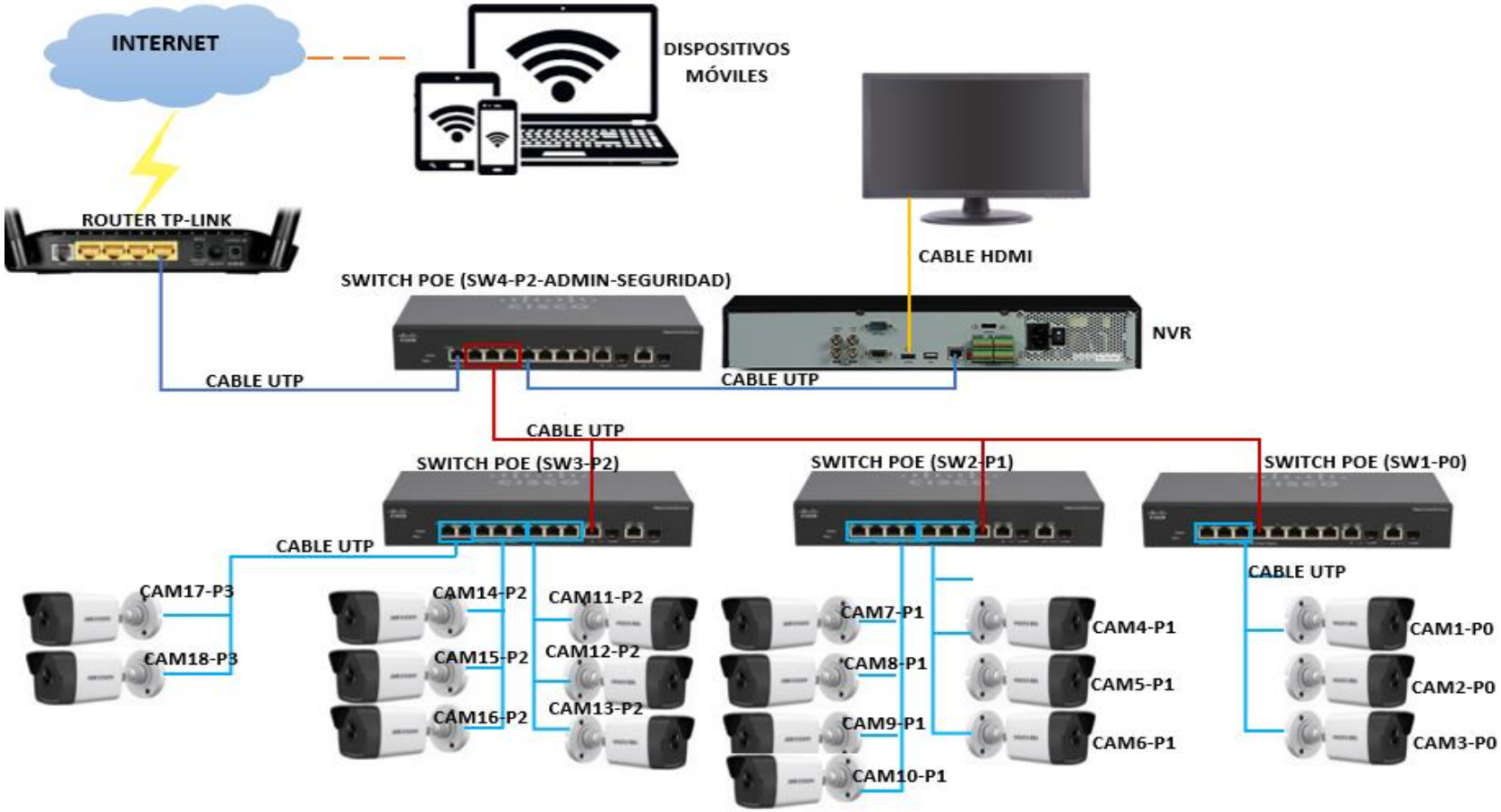


Figura N° 77. Esquema General del Sistema de Video Vigilancia IP para el Mercado San Juan

Elaborado por: Investigadora

4. Características de Elementos usados en el sistema

Para el diseño del sistema de video vigilancia en base a tecnología IP para el mercado "San Juan" se utilizó los siguientes elementos que se detallarán a continuación en la tabla 27, presentando las características técnicas de cada uno de ellos.

Tabla 27. Características de equipos usados en el sistema de video vigilancia IP.

Equipo	Características técnicas	Función	Cantidad
Cámara **Marca:** Hikvision **Modelo:** DS-2CD1041-I	• Cámara IP tipo Bullet. • Resolución de video de hasta 4 megapíxeles.	Captura de imágenes y de video para el control local y remoto dentro del mercado.	18
NVR **Marca:** Hikvision **Modelo:** DS-7732NI-E4	• 32 canales. • Ancho de banda de entrada de 200Mbps y de salida de 160 Mbps.	Graba y visualiza el video de forma local y remota.	1
Switch **Marca:** Cisco **Modelo:** SG200-10FP	• Switch Cisco con tecnología PoE. • 10 puertos RJ45 LAN, 8 con tecnología PoE y 2 Gigabit.	Equipo administrable para la interconexión de las cámaras de diferentes niveles hacia el NVR,	4
Router **Marca:** TP-LINK **Modelo:** ARCHE C7	• Frecuencias de 2.4 y 5GHz. • Estándares inalámbricos 802.11a/b/g/n/ac. • Velocidad de datos hasta 1300Mbps. • 4 puertos LAN 10/100/1000Mbps. • Seguridad WEP, WPA, WPA2-PSK.	Equipo proveedor de internet al Switch para acceso remoto.	1
Disco Duro **Marca:** Western Digital Purple **Modelo:** WD40PURZ	• Capacidad de 4TB • Formato 3.5" • Interfaz serial ATA-600 • Hasta 64 Cámaras • Firware AllFrame 4K • Carga de trabajo anualizada 180TB/año	Equipo de almacenamiento de imágenes durante 24 horas, 7 días a la semana, 30 días al mes.	1
Monitor **Marca:** Samsung **Modelo:** S24F350FHU	• Pantalla de 24 pulgadas. • 1 entrada HDMI y VGA. • Resolución de 1920 x 1080p.	Visualiza el video capturado de forma local en el área de seguridad (segundo nivel).	1
Pantalla LCD **Marca:** Samsung **Modelo:** 5 SMART WIFI	• Pantalla led wifi • Puerto HDMI y USB • Resolución de 1920 x 1080p.	Visualiza el video capturado de forma remota en el área de acceso a garaje (subterraneo).	1

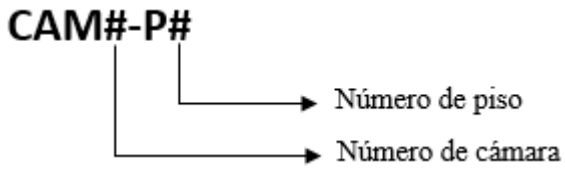
Cable de cobre par trenzado UTP **Marca:** NEXXT	• Cable UTP • Soporta velocidades Gigabit Ethernet de hasta 1 Gbps. • Distancia máxima de 100m.	Medio de transmisión de video y medio de suministro de energía hacia cámaras. Cableado Horizontal.	694,92 metros (3 bobinas)
Conectores RJ45 cat.6 **Marca:** NEXXT **Modelo:** AW102NXT04	• Conectores machos para cableado estructurado. • De material termoplástico.	Interfaz física de conexión de cables de red en cableado estructurado.	44 conectores
Protector de conector RJ45 **Marca:** DELTA	• Protector de plástico • Soporta cableado categoría 6.	Interfaz física de conexión de cables de red en cableado estructurado.	44 Protectores
Manguera corrugada	• De materia plástico polipropileno. • Diámetro de 6,8mm y 23mm.	Canalización del cableado horizontal.	• 87 metros de 6,8mm • 5 metros 23mm
Canaleta plástica PVC **Marca:** Dexson	• De material plástico de 39x18mm con capacidad de 12 cables cat.6	Canalización del cableado horizontal.	694,92m (350 canaletas de 2m)

Elaborado por: Investigadora

5. Diseño físico del sistema de Video Vigilancia IP

Para el diseño se usó el software AutoCAD, un software que permitió realizar el diseño de la ruta del cableado para la conexión de las cámaras hacia los diferentes dispositivos que se ubicaron en el cuarto de telecomunicaciones (Área de Administración). Así como también se indicó la ubicación de las cámaras en los diferentes niveles del mercado.

Las cámaras dentro del diseño estarán identificadas de acuerdo a la norma ANSI/EIA/TIA 606-C clase 1, debido a que es un estándar de administración para infraestructuras de telecomunicaciones específicamente para edificios comerciales [47], cubriendo las necesidades del mercado que es atendido por una sola sala de equipos, el cual se encuentra ubicado en el área de administración. A continuación, se presenta la identificación de cada una de las cámaras que se ubicarán en cada nivel del mercado.



Cada variable significa:

CAM#: Número de cámara, para este caso depende del número de cámaras que existan en cada nivel del mercado.

P#: Número de piso, al existir cuatro pisos se tendrá: piso 0 (subterráneo), piso 1 (primer nivel), piso 2 (segundo nivel), piso 3 (tercer nivel).

En la figura 78, se ilustra el diseño físico del sistema de video vigilancia para el nivel subterráneo, en donde se muestra la colocación de las cámaras y del cableado hacia el centro de seguridad ubicado en el segundo nivel del mercado, junto con las canaletas para la conexión de los diferentes puntos del sistema CCTV mediante cable UTP. Los demás planos se encuentran en el Anexo D.

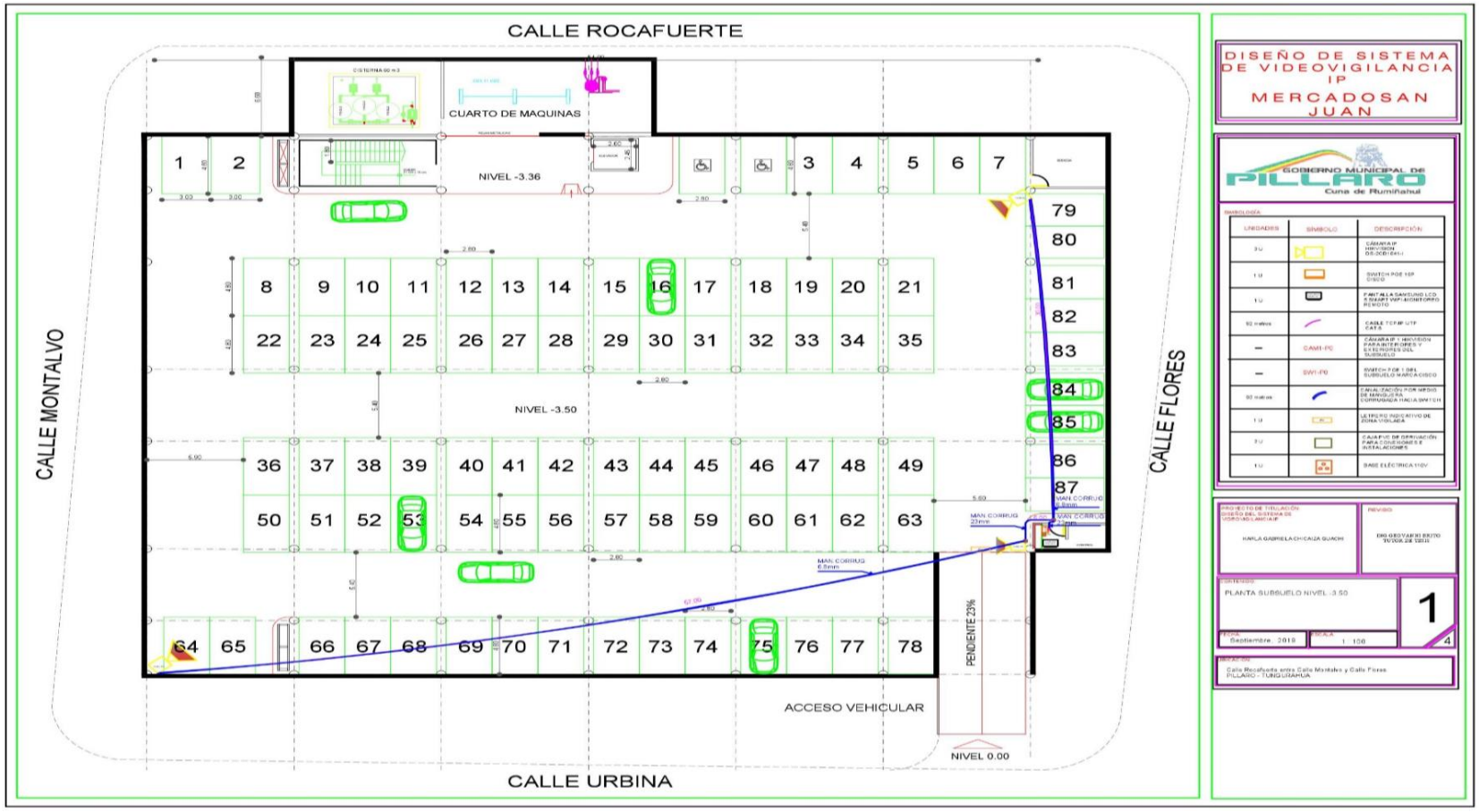


Figura N° 78. Plano de Diseño de Sistema de Video Vigilancia IP nivel Subterráneo.

Elaborado por: Investigador

El cableado de cada cámara va hacia el cuarto de telecomunicaciones (CUARTO DE SEGURIDAD DEL MERCADO), ubicado en el segundo nivel, para ello se aplica el estándar ANSI/TIA 569.D con respecto al espacio y recorrido del cable dentro de edificios comerciales, como en este caso para el Mercado “San Juan”.

En el subsuelo se tiene tres cámaras, una ubicada a la entrada del garaje y dos ubicadas dentro del lugar para la vigilancia de los vehículos. Dentro del primer nivel se colocaron siete cámaras, una ubicada en las gradas hacia este nivel, cuatro ubicadas en las puertas principales de ingreso al mercado, una ubicada en el exterior del mercado frente la calle Urbina y una frente a la calle Rocafuerte, para protección de locales comerciales externos. En el segundo nivel se ubicaron seis cámaras, dos ubicadas en las gradas de acceso a este nivel, una ubicada en el área de venta de ropa, una en la zona de comidas, una en el área de servicios a la comunidad y una en el área de venta de bisutería y demás productos. Para el tercer nivel se usó dos cámaras, una ubicada en la zona de acceso a locales comerciales y una en el acceso a las zonas de guardería, administración y consultorio médico.

6. Diseño lógico del sistema de Video Vigilancia IP

El mercado “San Juan” contará con el ISP DATAIR; para el diseño del sistema de video vigilancia IP, es necesario mantener una red fuera del alcance de otras redes por cuestión de seguridad y rendimiento, en este aspecto se segmenta la red mediante el manejo de diferentes VLANs, se hace uso de una VLAN para el acceso remoto que se asigna al NVR. Se usó la VLAN 20: 172.16.20.0, con una máscara 255.255.255.0; mientras que para el direccionamiento local de las cámaras se usó una dirección IP clase C: 192.168.1.0, máscara 255.255.255.0

En la tabla 28, se observa la distribución de las direcciones IP para el sistema:

Tabla 28. Direccionamiento lógico a equipos del sistema de Video vigilancia IP, usando VLANs.

Direccionamiento IP			
Red LAN1			
Dirección IP	192.168.1.64		
Máscara	255.255.255.0		
Gateway	192.168.1.1		
Dispositivo	**Dirección IP**	**Máscara**	**Gateway**
CAM1-P0	192.168.1.2	255.255.255.0	192.168.1.1

CAM2-P0	192.168.1.3	255.255.255.0	192.168.1.1
CAM3-P0	192.168.1.4	255.255.255.0	192.168.1.1
CAM4-P1	192.168.1.5	255.255.255.0	192.168.1.1
CAM5-P1	192.168.1.6	255.255.255.0	192.168.1.1
CAM6-P1	192.168.1.7	255.255.255.0	192.168.1.1
CAM7-P1	192.168.1.8	255.255.255.0	192.168.1.1
CAM8-P1	192.168.1.9	255.255.255.0	192.168.1.1
CAM9-P1	192.168.1.10	255.255.255.0	192.168.1.1
CAM10-P1	192.168.1.11	255.255.255.0	192.168.1.1
CAM11-P2	192.168.1.12	255.255.255.0	192.168.1.1
CAM12-P2	192.168.1.13	255.255.255.0	192.168.1.1
CAM13-P2	192.168.1.14	255.255.255.0	192.168.1.1
CAM14-P2	192.168.1.15	255.255.255.0	192.168.1.1
CAM15-P2	192.168.1.16	255.255.255.0	192.168.1.1
CAM16-P2	192.168.1.17	255.255.255.0	192.168.1.1
CAM17-P3	192.168.1.18	255.255.255.0	192.168.1.1
CAM18-P3	192.168.1.19	255.255.255.0	192.168.1.1
Red LAN2			
VLAN 20	172.16.20.0		
Máscara	255.255.255.0		
Gateway	172.16.20.1		
Dispositivo	**Dirección IP**	**Máscara**	**Gateway**
NVR	172.16.20.2	255.255.255.0	172.16.20.1

Elaborado por: Investigadora

7. Cálculo de capacidad de disco duro [48]

La capacidad de disco duro es otro de los aspectos más importantes para un funcionamiento óptimo en el diseño de un sistema de video vigilancia IP. Para este cálculo se basa en parámetros como la resolución de las cámaras, método de codificación, número de canales a usar y el número de frames por segundo (fps).

Forma matemática

Para el cálculo de la capacidad de disco duro se requiere de los siguientes parámetros:

- Capacidad para un segundo de video para una cámara expresado en bytes ó bit rate de video expresado en kbps.
- Velocidad de grabación (fps).
- Porcentaje de actividad de la escena.

A continuación, se presenta la forma matemática para el cálculo de la capacidad de disco duro:

$$\boldsymbol{Espacio\ de\ DD\ para\ 1\ seg = video\ bit\ rate * fps * \%actividad}$$

Datos entregados por el fabricante de la cámara DS-2CD1041-I:

- Video bit rate: 32 Kbps
- Velocidad de grabación: 20fps.
- % de actividad: 60% (0.6) debido a que en el horario de 9:00 pm a 5:00 pm, no se tiene gran cantidad de movimientos de escenas.

$$Espacio\ de\ DD\ para\ 1\ seg = 32kbps * (20fps) * (0.6)$$

$$Espacio\ de\ DD\ para\ 1\ seg = 348\ kbps\ para\ 1\ cámara$$

$$Espacio\ de\ DD\ para\ 1\ seg\ total = 348\ kbps * 18\ canales\ (\#cámaras)$$

$$Espacio\ de\ DD\ para\ 1\ seg\ total = 6912kbps$$

ó

$$Espacio\ de\ DD\ para\ 1\ seg\ total = \frac{6912kbps}{8} = 864KB$$

Pasando a Mega Bytes por hora se tiene:

$$Espacio\ de\ DD\ para\ total = \frac{864KB}{1024} = 0.84375KB * 3600seg = \frac{3037.5MB}{h}$$

Capacidad de disco para grabar un día:

$$Espacio\ de\ DD\ para\ total = \frac{3037.5MB}{h} * \frac{24}{día} = \frac{72900MB}{día} = \frac{0.68TB}{día}$$

De acuerdo a los cálculos se tiene que el espacio de disco duro total para las 18 cámaras y grabando un día se requiere una capacidad de 0.7 TB; como se tiene un NVR de 6 TB, permite almacenar ocho días lo que graban las cámaras IP.

La capacidad de almacenamiento calculada anteriormente, se puede aumentar, activando la función grabación por detección de movimiento al NVR, con ello incrementándose la capacidad de grabación 3 veces más, es decir un tiempo de 24 días.

8. Cálculo del ancho de banda [48]

El ancho de banda y la red, para el diseño de un sistema de video vigilancia IP son parámetros importantes a calcular ya que de esto depende el manejo de grandes cantidades de video, asegurando un sistema que trabaje eficientemente sin tener problemas a futuro.

Para el cálculo del ancho de banda requerido por el sistema IP a implantarse en el mercado San Juan, se determina en base a las especificaciones técnicas de las cámaras a usar.

Anteriormente, se calculó el espacio para un segundo de video de 6921 Kbps, al ser bps, indica que es el ancho de banda total de las 18 cámaras IP.

$$BW = 6912\ Kbps = 6{,}75\ Mbps$$

9. Presupuesto de diseño del sistema de Video Vigilancia IP

En la tabla 29, se muestra el presupuesto total del sistema de Video Vigilancia IP para todo el mercado San Juan.

Tabla 29. Presupuesto Total del Sistema de Video Vigilancia.

Presupuesto de diseño del sistema de Video Vigilancia IP para el Mercado "San Juan"				
Ítem	**Detalle**	**Cantidad**	**Precio Unitario**	**Precio Total**
1.	Cámara HIKVISION DS-2CD1041-I	18 U	$107.00	$1926.00
2.	NVR HIKVISION DS-7732NI-E4	1 U	$437.00	$437.00
3.	Switch CISCO SG200-10FP	4 U	$400.00	$1600.00
4.	Router TP-LINK ARCHE C7	1 U	$86.00	$86.00
5.	Disco Duro	1 U	$144.00	$144.00
6.	Monitor SAMSUNG S24F350FHU	1 U	$142.00	$142.00
7.	Pantalla LCD SAMSUNG 5 SMART WIFI	1 U	$600.00	$600.00
8.	Cable UPT cat.6 AMPXL	694.92 metros (3 bobinas de 300 metros)	$0.52	$474.00

9.	Conectores RJ45 cat.6 NEXXT AW102NXT04	44 U	$0.25	$11.00
10.	Protector de conector RJ45 DELTA	44 U	$0.10	$4.40
11.	Manguera corrugada	• 87 metros de 6,8mm • 5 metros 23mm	$1.00	$92.00
12.	Canaleta plástica PVC DEXSON	694,92m (350 canaletas de 2m)	$3.50	$700.00
13.	Caja de derivación PVC 15x11x7cm	10 U	$9.00	$90.00
	Letreros de zona de vigilancia	2 U	$15.00	$30.00
14.	Regulador de voltaje Tripp-lite	1 U	$45.00	$45.00
15.	Rack Mural 500mm FAYSER AMP	1 U	$235.00	$235.00
Sub-Total				$6616.40
Imprevistos 10%				$661.64
TOTAL				**$7278.04**

Elaborado por: Investigadora

2.2.10. Diseño de la Red de Datos

1. Parámetros para el diseño de la Red Inalámbrica

El mercado San Juan es un mercado de 8.260,37 m^2, que cuenta con cuatro plantas, a las cuales se pretende dar cobertura inalámbrica wifi. Actualmente al no contar con una red de datos se realiza el diseño de la misma, en donde se ha identificado en cada planta zonas estratégicas para la instalación de equipos, que permitan cubrir la totalidad de áreas requeridas, a continuación se presentan los planos generales del mercado para establecer las características de la red inalámbrica y con ello determinar las herramientas y dispositivos necesarios para el diseño de la red.

Además, se contratará un proveedor de servicio de internet, y por medio de este realizar el diseño de la red inalámbrica para dar cobertura a todas las instalaciones del mercado, con la finalidad de que los usuarios tengan acceso a este servicio y puedan hacer uso

del sistema de alarma comunitaria y del sistema de video vigilancia IP que se ha diseñado en beneficio de la comunidad.

A continuación, se presentan los requerimientos necesarios para el diseño de la red inalámbrica W-FI necesaria para dar cobertura a todo el mercado.

- Conexión permanente de los dispositivos móviles a la red inalámbrica wifi creada.
- Determinar políticas de uso para que los usuarios que sean designados a conectarse a la red utilicen la tecnología solo para el sistema de alarma comunitaria y video vigilancia en casos de emergencia.
- Los equipos y dispositivos deberán ser configurados de acuerdo a las normas establecidas que se encuentren dentro de los servicios prestados con el desarrollo del proyecto.
- La red creada debe tener un identificador SSID y una clave para el acceso a la misma desde diferentes dispositivos móviles.

2. Descripción de la estructura física de los pisos y paredes de cada nivel

- **Nivel Subterráneo:** Es un área con menos obstáculos posibles y consta de varias columnas circulares construidas de hormigón armado al igual que el piso y sus paredes. Po estas razones se considera como el área con un bajo índice de pérdida de señal, en este nivel se ve la necesidad que solo la recaudación de acceso al garaje cuente con conexión a internet es por ello que se colocará un solo punto de acceso.
- **Primer Nivel:** En el primer nivel existen cubículos para el expendio de productos los mismos que están construidos a base de hormigón al igual que el piso y las paredes, las puertas de ingreso fueron hechas de vidrio y su techo de hormigón con una parte libre de obstáculos hacia la segunda planta. Se ve la necesidad de colocar dos puntos de acceso, para dar cobertura a toda la planta.
- **Segundo Nivel:** Este nivel consta de tres áreas, un área en donde existen cubículos para el sector de comidas, en la segunda área existen locales de ropa, ferreterías y bisutería, mientras que en la tercera área se encuentran las oficinas de registro de la propiedad todas ellas construidas a base de hormigón al igual de las paredes y el techo, el piso fue construido de hormigón y cerámica, parte de las paredes son de

vidrio, de acuerdo a estas características se ve la necesidad de colocar igual tres puntos de acceso.

- **Tercer Nivel:** Esta área consta de 4 oficinas que fueron construidas de hormigón armado, el piso es de cerámica, las ventanas de vidrio, existen escritorios y equipos de cómputo. De acuerdo a las características se ve la necesidad de colocar dos puntos de acceso.

Dentro del mercado "San Juan" existen gran cantidad de locales comerciales destinados a la venta de diferentes productos, como se puede mostrar en la tabla 30.

Tabla 30. Número de locales comerciales por Nivel.

Nivel	Local Comercial	N° De Locales	Host
Subsuelo	PARQUEADEROS	1	-------
	BODEGA	1	-------
	CONTROL DE ACCESO	1	1
Primer Nivel	FRUTAS	36	-------
	LEGUMBRES Y HORTALIZAS	116	-------
	GRANOS	30	-------
	CARNES	12	-------
	SERVICIO TÉCNICO	1	2
	CENTRO DE BELLEZA	1	-------
	SERVIPAGOS Y WESTERN UNION	1	1
	PELUQUERÍA HOLLYWOOD	1	-------
	CYBERNET	1	1
	ALMACÉN DEPORTIVO HEITEX	1	1
	LOCAL DE ARRENDAMIENTO 1	1	-------
	LOCAL DE ARRENDAMIENTO 2	1	-------
Segundo Nivel	LOCALES DE COMIDA	30	-------
	REFRESCOS Y BATIDOS	2	-------
	FERRETERÍA	2	-------
	ABARROTES	20	-------
	ROPA	20	-------
	BISUTERÍA	11	-------
	LÁCTEOS	4	-------
	SERVICIO REGISTRO DE LA PROPIEDAD	1	4
Tercer Nivel	ADMINISTRACIÓN	1	4
	SALA DE REUNIONES	1	-------
	MÉDICO	1	1
	GUARDERÍA	1	-------
	SEDE BARRIAL	1	-------

TOTAL	300	15

Elaborado por: Investigadora

Como se pudo observar, existen trecientos locales comerciales funcionando, y dentro de ellos quince máquinas que se usan para diferentes actividades.

3. Necesidades de los clientes

Hoy en la actualidad la utilización de la tecnología es primordial, debido a la necesidad de adquirir información, permitiendo así el desarrollo de la sociedad, es por ello que actualmente el uso de dispositivos tecnológicos que se conecten a una red y a internet es una necesidad que tanto los propietarios, como los clientes y visitantes del mercado "San Juan" requieren, en este caso para dar aviso y alertar a toda la comunidad cuando se presenten actos vandálicos dentro y fuera del mismo.

Al visitar el mercado "San Juan" se pudo observar que no existe una red propia, para conexión a internet; además se observó que tanto los propietarios como los clientes, hacen uso de diferentes dispositivos móviles como tablets, celulares, laptops, e incluso computadores de escritorio, en donde cada uno de ellos buscan tener acceso a una conexión, por ello es necesario realizar el diseño de la red inalámbrica wifi.

Principalmente los locales comerciales tanto del exterior como del segundo nivel y tercer nivel, actualmente disponen de una conexión a internet, a través de conexiones ADSL entregadas por empresas como CNT, CLICKNET y DATAIR, respectivamente, o mediante el uso de módems inalámbricos con tecnologías 3.5G y 4G, ofrecidas por empresas como, CNT, CLARO y MOVISTAR respectivamente.

Ante este análisis se planteó la solución que se presenta en la figura 79.

El mecanismo usado para ver las necesidades de los clientes, con respecto al uso de un sistema de alarma comunitaria y del acceso a internet, se realizó mediante una visita de campo al lugar del desarrollo del proyecto, además de la utilización de información de fuentes primarias, como fue el municipio y la administradora de mercados, determinando así ciertos parámetros para el diseño de la red inalámbrica wifi.

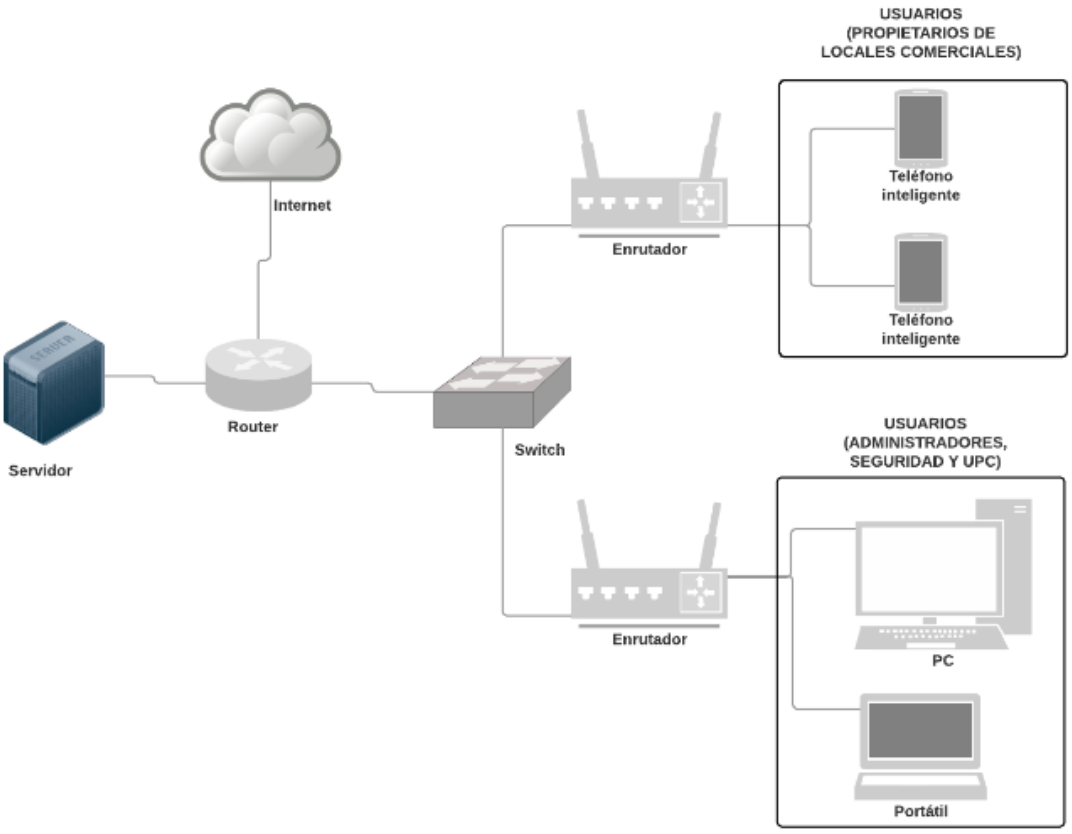


Figura N° 79. Esquema general de la Red Wifi.

Elaborado por: Investigadora

4. Clasificación de los Usuarios

Fijos

El mercado "San Juan" consta de trecientos locales comerciales, por lo que se tendrá un aproximado de trecientos usuarios fijos que se conectarán a la red inalámbrica. Cabe señalar que la mayor concentración de locales comerciales se encuentran entre el primer y segundo nivel.

Visitantes

Estos usuarios son aquellos que se conectarán a la red wifi de forma esporádica, para conocer el número de visitantes se basó en datos proporcionados tanto por los propietarios de los locales comerciales, como de la administradora del mercado San Juan, además la constatación del número de personas se logró a base de visitas de campo realizadas en los días lunes, miércoles, jueves y domingos, en un horario de 11:00am a 14:00pm, y de 15:00pm a 18:00pm, se realizó en estos horarios y días

debido a que son días en donde se produce la feria de varios productos, acudiendo vendedores y compradores en general.

En base a los datos analizados, se obtuvo un promedio de docientas personas visitantes, considerando que la mayoría son esporádicos. Mientras que en ciertos días y horas pico se tiene un 28% de afluencia del total de visitas, es decir de cincuenta y cinco visitantes dentro y fuera del mercado San Juan, siendo el primero y segundo nivel de mayor afluencia de personas visitantes, para los demás niveles se tiene un porcentaje del 36% para cada nivel tanto subterráneo como tercer nivel. Como se observa en la tabla 31, se tiene el número de usuarios que se conectan de forma simultánea, de la siguiente forma:

En el subterráneo, existen ochenta y ocho lugares de aparcamiento, es decir ochenta y ocho personas visitantes, de entre ellas se tiene quince visitantes que concurren y tres usuarios fijos en el área de control de acceso, teniendo un total de dieciocho usuarios concurrentes.

Para el primer nivel se tiene alrededor de noventa usuarios visitantes conectados en ciertos días y horas pico, que de acuerdo con el porcentaje de afluencia para este nivel se tienen quince usuarios concurrentes y doscientos dos usuarios fijos, de los cuales se tienen veinticinco usuarios conectados, obteniendo así un total de cuarenta usuarios concurrentes.

Para el segundo nivel se tiene alrededor de treinta usuarios visitantes en ciertos días y horas pico, de acuerdo al porcentaje de afluencia para este nivel se tienen diez usuarios concurrentes y noventa usuarios fijos, de los cuales de acuerdo al porcentaje se tienen veinte usuarios conectados, con un total de treinta usuarios concurrentes.

En el tercer nivel existe un total de cinco usuarios fijos conectados simultáneamente, cuarenta usuarios visitantes en horas pico, de acuerdo al porcentaje de afluencia se tiene diez usuarios visitantes conectados simultáneamente, con un total de quince usuarios concurrentes.

Tabla 31. Predicción del total de usuarios fijos y visitantes a la Red.

Características	USUARIOS DEL MERCADO SAN JUAN		VISITANTES DEL MERCADO SAN JUAN		TOTAL DE USUARIOS
Piso	**Usuarios fijos por piso**	**Usuarios conectados simultáneamente**	**Usuarios visitantes**	**Usuarios conectados**	**Usuarios Simultáneos**
Subterráneo	3	3	40	15	18
Primer Nivel	202	25	90	15	40
Segundo Nivel	90	20	30	10	30
Tercer Nivel	5	5	40	10	15
TOTAL DE USUARIOS CONECTADOS					**103**

Elaborado por: Investigadora

De acuerdo al análisis realizado se tiene un total de usuarios conectados simultáneamente en todo el mercado de ciento tres personas.

5. Análisis del ancho de banda total para el diseño de la red

Para el diseño de una red wifi, se procedió a realizar el análisis del tráfico de red, en donde se calculará la cantidad de datos que son enviados y recibidos por los usuarios y las páginas que frecuentemente visitan.

Ancho de banda de Aplicaciones más usadas

Calculo de la capacidad consumida por aplicaciones más usadas.

- **Video Streaming y YouTube:** YouTube al ser un sitio web que permite subir videos y a su vez visionar los mismos, es una de las páginas más conocidas y buscadas en internet. Por medio de la herramienta WebSite Optimization se logró medir el tiempo de carga de un video de youtube, con una resolución de 480 pixeles, ya que la mayoría de estos presentan esta calidad, a continuación en la figura 80, se presentan los resultados del tamaño de un video analizado:

URL:	https://www.youtube.com/watch?v=Nw17-YBCQ_E&feature=youtu.be
Title:	5a - Redes Neuronales: Matlab - YouTube
Date:	Report run on Fri Oct 11 18:20:36EDT2019

Total HTTP Requests:	12
Total Size:	578972 bytes

Figura N° 80. Análisis de ancho de banda consumido de video de Youtube.

Elaborado por: Investigadora

Los resultados de tiempo de descarga para el video se lo realizaron mediante una conexión DSL 710, ya que la mayoría de los locales comerciales hacen uso de esta conexión, teniendo así un tiempo de carga de 5.47 segundos.

$$AB_{youtube} = \frac{578972\ Bytes}{5.47s} * \frac{1\ KB}{1024Bytes} * \frac{8bits}{1\ Byte} = 826{,}91Kbps$$

- **Redes Sociales:** Otro de los sitios web más usados es la red social Facebook, como medio de comunicación y entretenimiento, se considera a esta red social para el análisis de tráfico, puesto que es la más usada en el país, así como también la mensajería instantánea WhatsApp.

  En la figura 81, se muestran los tiempos de navegación en Facebook, usando la conexión DSL710, debido a que es la forma de conexión que poseen varios de los lugares, teniendo así un tiempo de carga de 0.40 segundos.

URL:	https://www.facebook.com/gamavisionecu/
Title:	Redirecting...
Date:	Report run on Fri Oct 11 19:37:39EDT2019

Total HTTP Requests:	2
Total Size:	588 bytes

Figura N° 81. Tiempos de navegación de Facebook.

Elaborado por: Investigadora

$$AB_{Facebook} = \frac{588\ Bytes}{0.40s} * \frac{1\ KB}{1024Bytes} * \frac{8bits}{1\ Byte} = 11.48Kbps$$

- **Descargas:** Se toma a consideración las descargas, ya que en el segundo nivel se encuentran oficinas destinadas al servicio de la comunidad con respecto al registro de la propiedad, en donde descargan fichas, información que proviene del municipio; entre otros, en donde un usuario descarga archivos de un tamaño

promedio de 10MB, en un tiempo de 5 minutos, datos obtenidos al realizar descargas directamente desde las oficinas.

$$AB_{Descargas} = \frac{10240\ KBytes}{1\ descarga} * \frac{8bits}{1Bytes} * \frac{1\ descarga}{5\ min} * \frac{1\ min}{60s} = 273.1Kbps$$

Obteniendo así una tasa de descarga de 273Kbps

- **Correo electrónico:** Debido a que es un mercado en donde existen varias oficinas, como el registro de la propiedad, médico, administración y locales comerciales externos que emiten facturas a través de este medio; en base a pruebas realizadas específicamente en las oficinas de registro de la propiedad, se envían archivos de un tamaño de 1.5MB en promedio, en un tiempo aproximado de 1 minuto.

$$AB_{correo} = \frac{1536\ KBytes}{1\ correo} * \frac{8bits}{1Bytes} * \frac{1\ correo}{1\ min} * \frac{1\ min}{60s} = 204.8Kbps$$

- **Mensajerías Instantáneas:** El sistema de alarma comunitaria que se desarrolló, fue en base al uso de mensajerías instantáneas de Telegram y WhatsApp, es por ello que se analiza el tráfico de datos que generan, para el diseño de la red inalámbrica wifi.

  La compañía SOSTariffe, realizó pruebas de las apps más usadas como son Telegram, WhatsApp y Messenger, con la finalidad de conocer el tráfico que generan por hora, para ello dividió el consumo de cada app en bajo, medio y alto [49], a continuación en la tabla 32, se presenta el consumo de megas de acuerdo al envío y a la recepción de mensajes e imágenes:

Tabla 32. Consumo de megas de Mensajerias Telegram y Whatsapp.

Tipo de archivo / **Tipo de consumo**	**MENSAJES**		**IMÁGENES**	
	Enviados	**Recibidos**	**Enviados**	**Recibidos**
Consumo Bajo	20	20	2	5
Consumo Medio	40	40	5	10
Consumo Alto	100	100	20	50

Elaborado por: Investigadora

WhatsApp: De acuerdo a las pruebas realizadas por la compañía, se tiene que WhatsApp tiene un consumo bajo de 0.65Mbps, consumo medio de 1.39Mbps y

6.23Mbps de consumo alto, para nuestro diseño se tomó un consumo bajo, debido al uso que se le da en sistema de alarma, ya que solo permitirá a los usuarios recibir mensajes de alerta permitiendo conocer eventos anormales que puedan ocurrir dentro y fuera del mercado; además de acuerdo a la tabla 2 se puede observar que se puede emitir y recibir 20 mensajes por hora, una cantidad suficiente para los que los usuarios en casos de emergencia se puedan comunicar entre sí.

$$AB_{WhatsApp} = 0.65Mbps = 665.6Kbps$$

Telegram: Este tipo de mensajería al igual que WhatsApp tiene sus ventajas, esto en base al consumo de datos; de acuerdo a las pruebas realizadas, se obtuvo que tiene un consumo bajo de 0.42Mbps, consumo medio de 0.87Mbps y 3.75 Mbps de consumo alto, debido a que es la herramienta principal para la emisión y recepción de mensajes de alerta sobre acontecimientos vandálicos, se tomó un consumo medio de 0.87Mbps.

$$AB_{Telegram} = 0.87Mbps = 890.88Kbps$$

Una vez calculado el ancho de banda de las aplicaciones más usadas, se procede a calcular el ancho de banda total, que resulta de la suma del ancho de banda necesario para el funcionamiento del prototipo del sistema de alarma comunitaria integral, más el ancho de banda del diseño real del sistema de video vigilancia IP que pueda ser implementado en el mercado, más el ancho de banda de las aplicaciones que los usuarios podrían usar con mayor frecuencia; a continuación en la tabla 33, se observa el ancho de banda total necesario para el diseño de la red wifi:

Tabla 33. Ancho de Banda Total para Diseño de la Red Wifi.

ÍTEM	APLICACIÓN	ANCHO DE BANDA (Kbps)
SERVICIOS PROTOTIPO	Video vigilancia IP	95.85
	VoIP (Voz sobre IP 10 llamadas simultáneas)	560.00
SERVICIOS DE DISEÑO PARA IMPLEMENTACIÓN	Video Vigilancia IP (Transmisión de video de 18 cámaras IP)	1725.30
	Red social Facebook	11.48
	Mensajería WhatsApp	665.60
	Mensajería Telegram	890.88
	Correo electrónico	204.80
	Descargas	273.10
	Video streaming y YouTube	826.91
ANCHO DE BANDA TOTAL		**5253.92Kbps = 5.13Mbps**

Elaborado por: Investigadora

Como se observa en la tabla 33 se obtuvo un ancho de banda total de 5.13 Mbps, para cada usuario como un ancho de banda máximo que puede tener, tomando este valor para horas pico; cabe recalcar que este ancho de banda lo usaría si se encuentra navegando al mismo tiempo en todos los servicios que se presentan en la tabla 37, caso que no sucedería, por ende a cada usuario se le asignará la media del ancho de banda total, como se muestra a continuación:

$$AB_{necesario.usuario} = \frac{5253.92Kbps}{9} = 583.77Kbps = 0.57Mbps$$

Obteniendo así un ancho de banda necesario para cada usuario como mínimo de 0.57Mbps, multiplicando para los 300 usuarios se obtuvo un ancho de banda total necesario de 171.026Mbps.

Índice de simultaneidad

El uso de internet, se da en base a las necesidades que tienen las personas, ya sea para entretenimiento o actualización de conocimientos, accediendo de forma aleatoria. Debido a que es inseguro conocer la conectividad de los usuarios al mismo tiempo y al diferente uso de información, se presenta un índice de simultaneidad, este índice permite calcular el número de usuarios conectados simultáneamente en la red, y se determina como 1/n, en donde n es el número de usuarios conectados simultáneamente, existen índices de simultaneidad dentro del país desde 0.1 a 0.5 [50].

En base a este índice de simultaneidad, se estima que existe una baja probabilidad de que los 300 usuarios se conecten a la red al mismo tiempo, de acuerdo a una visita de campo que se realizó, se estimó que existen por lo general 103 usuarios conectados simultáneamente de los 300 usuarios, con ello obteniendo un factor de simultaneidad de 0.23; es decir que el 23% del total de usuarios se conectarán al servicio al mismo tiempo, dentro de los 300 usuarios que se estima tener en la red de datos, a continuación se presenta la velocidad de transmisión necesaria para cubrir todo el mercado, la cual será contrata a un ISP:

$$V_{Tx} = V_{TT} * índice\ de\ simultaneidad$$

Donde:

V_{TX}: Es la velocidad de contratación de un ISP para la navegación en la red wifi total.

V_{TT}: Es la velocidad total de la red.

$$V_{Tx} = 171.026Mbps * 23\%$$

$$V_{Tx} = 39.57 = 40Mbps$$

Obteniendo así un plan ce contratación de internet de 40Mbps, en donde los usuarios concurrentes tendrán una velocidad máxima en horas pico de 397.67Kbps y una velocidad mínima de 204.80Kbps para cada usuario.

El parámetro anteriormente calculado es necesario en el desarrollo del diseño de la red wifi para el mercado San Juan, permitiendo dar cobertura a todo el área que requiere de este servicio.

En base a la velocidad requerida, se requiere la contratación de una empresa proveedora de internet, ya sean CNT, DATAIR y CLICKNET, empresas que brindan este tipo de servicio dentro del cantón Santiago de Píllaro.

A continuación en la tabla 34, se presenta una comparativa de los planes de servicio de internet de las empresas mencionadas anteriormente:

Tabla 34. Planes de Internet, empresas CNT, DATAIR y CLICKNET.

EMPRESA	VELOCIDAD	TECNOLOGÍA	PRECIO
CNT	50 Mbps	Fibra solo Ambato	$57.00
DATAIR	40 Mbps	Fibra	$156.80
CLICKNET	Ofrece solo hasta 6 M	Fibra	$49.99

Elaborado por: Investigadora

6. Banda de frecuencia utilizada para el mercado

Se concluyó que el Mercado San Juan se encuentra ubicado en una zona rodeada de viviendas, por lo que la banda de los 2,4 GHz se supone que estará saturada, y este al ser un centro de mercadeo que se encuentra dividido por plantas y para dar mayor área de cobertura se requiere colocar Access point de gran capacidad para dar cobertura a

todo el lugar, en base a ello se optó por escoger la banda de los 5 GHz para interconectar los AP's entre los diferentes pisos, una banda que ofrece más canales con ello reducir la interferencia co-canal y tener una mejor calidad de señal. Mientras que para emitir la señal wifi a los clientes desde los Access Point se usó la frecuencia de los 2.4Ghz, una banda que permite tener mayor área de cobertura y que además varios equipos móviles se puedan conectar a la red.

En base a este análisis se opta por trabajar con equipos de doble banda; es decir que trabajen en la banda de 5GHz para interconectarse entre sí y que trabajen en la banda de los 2.4GHz para emitir la señal a los usuarios.

En base a las bandas de frecuencia seleccionadas, se utilizó el estándar IEEE 802.11ac ofreciendo una velocidad máxima de 1.3Gbps con compatibilidad de los estándares 802.11b/g/n y el estándar 802.11g con una velocidad máxima de 54Mbps; de acuerdo a estas características y las presentadas a continuación se realiza el diseño de la red wifi.

7. Cálculo del número de APs basado en la capacidad de usuarios

Para la determinación de la capacidad total necesaria en la red se estimó el número de los posibles usuarios conectados en cada una de las plantas del mercado como se analizó en la tabla35. El número de puntos de acceso serán además de acuerdo a la zona de cobertura [51].

Para el cálculo se basó en los siguientes parámetros de inicio:

- **Ce:** Capacidad efectiva de un AP, de los 54 Mbps los 22 Mbps es la velocidad de transmisión y recepción de datos.
- **N:** Número máximo de usuarios por cada nivel.
- **Fs:** Factor de simultaneidad. Número máximo de usuarios que usan simultáneamente la red inalámbrica, se utiliza un factor de 23% para todas las zonas
- **Cg:** Capacidad garantizada por usuario. Tasa mínima de transferencia que se garantiza a un usuario en este caso de 204.80Kbps
- **Fe:** Factor de escalabilidad. Se usó un factor del 10%
- **C:** Capacidad necesaria por cada nivel del mercado.

A continuación se presenta el número de puntos de acceso necesarios para cada nivel, usando un factor de simultaneidad para todos los niveles del 23%, como se usó en cálculos anteriores:

Nivel Subterráneo

- En este nivel se conectarán 43 usuarios

N= 43 usuarios

- Con un Fs del 23%

$$C = N.Fs.Cg = 43 * 0{,}23 * 204.80 = 1.98 Mbps$$

- Asumiendo un factor de escalabilidad del 10% y que el reparto de carga entre los AP es equilibrado, es necesario:

$$C * Fe/_{Ce} = {}^{1.98 * 1{,}1}/_{22} = 0.1 \ (1\ PUNTO\ DE\ ACCESO)$$

Primer Nivel

- En este nivel se tiene 292 usuarios

N= 292 usuarios

- Con un Fs del 23%

$$C = N.Fs.Cg = 292 * 0.23 * 204.80 = 13.43\ Mbps$$

- Asumiendo un factor de escalabilidad y que el reparto de carga entre los AP es equilibrado, es necesario:

$$C * Fe/_{Ce} = {}^{13.43 * 1{,}1}/_{22} = 0.67\text{Mbps} \ (1\ PUNTO\ DE\ ACCESO)$$

Segundo Nivel:

- Entre usuarios fijos y visitantes se tiene 120 usuarios

N= 120 usuarios

- Fs de 23%

$$C = N.Fs.Cg = 120 * 0{,}23 * 204.80 = 5.52\ Mbps$$

- Asumiendo un factor de escalabilidad y que el reparto de carga entre los AP es equilibrado, es necesario:

$$C * Fe/_{Ce} = {}^{5.52 * 1{,}1}/_{22} = 0.276 \ (1\ PUNTO\ DE\ ACCESO)$$

Tercer Nivel:

- 4 locales como son: área administrativa (5 usuarios aprox.), consultorio médico (3 usuarios aprox.), centro gerontológico (5 usuarios aprox.), y guardería (5 usuarios aprox.).

N= 45 usuarios

- Tomando un Fs del 23%

$$C = N.Fs.Cg = 45 * 0{,}23 * 204.80 = 2.07\ Mbps$$

- Asumiendo un factor de escalabilidad y que el reparto de carga entre los AP es equilibrado, es necesario:

$$C * Fe/Ce = 2.07 * 1{,}1/22 = 0{,}10\ \ (1\ PUNTO\ DE\ ACCESO)$$

De acuerdo a los cálculos realizados sobre el número de Access point en base a la cantidad de usuarios, se tiene una aproximación teórica de cuantos son necesarios para cubrir todo el área; cabe recalcar que además depende de la capacidad, la distancia de cobertura de los Access point que se vayan a seleccionar posteriormente y de la estructura física del mercado; a continuación en la tabla 35, se observa el número mínimo de AP's a utilizar:

Tabla 35. Número mínimo de APs a usar.

Nivel	Fs	Cg(Kbps)	N	Fe	C(Mbps)	Total de AP's
Subsuelo	23%	204.80	43	10%	1.98	1
Primero	23%	204.80	292	10%	13.43	1
Segundo	23%	204.80	120	10%	5.52	1
Tercero	23%	204.80	45	10%	2.07	1
TOTAL DE AP'S EN EL MERCADO						4

Elaborado por: Investigadora

8. Simulación de la red wifi dentro y fuera del mercado

Tras haber analizado en el apartado anterior la estructura interna y externa de cada uno de los niveles del mercado, se determinó que existen áreas en donde se requiere un número más alto de Access point, que los determinados en base al ancho de banda y a la cantidad de usuarios concurrentes. Para ofrecer un nivel mínimo de potencia de -70dBm, establecido por el indicador de la señal recibida o RSSI, es necesario ocupar

un número más alto de Access point, con la finalidad de evitar interferencias, así como la pérdida de señal y las desconexiones de los usuarios tanto fijos como visitantes mientras se trasladan de un nivel a otro.

Para el diseño en base a la cobertura, es necesario el estudio previo de la infraestructura del mercado, debido a que, los materiales de construcción y la ubicación de los dispositivos influyen en el rendimiento de la conexión wifi, es por ello que en zonas donde existen barreras de mayor atenuación, se opta por cambiar la ubicación del dispositivo, con ello garantizando mejor calidad de la señal y mayor área de cobertura.

A continuación, en la tabla 36, se ilustra el tipo de obstrucciones con las diferentes atenuaciones a la señal:

Tabla 36. Atenuación de la señal por Tipo de Material.

Tipo de Material	**Calidad de la señal**	**Atenuación en dB a 2.4GHz**
Vidrio	Débil	3
3 Puertas de madera	Débil	3
Bloque	Intermedio	5
Ladrillo	Intermedio	6
Muro de hormigón	Intermedio	8
Ser humano	Intermedio	8
Columna de hormigón	Elevado	15
Agua	Elevado	7dBm
Metal	Muy Elevado	37

Elaborado por: Investigadora

De acuerdo a lo expuesto anteriormente y con la finalidad de determinar el número de Access point y su ubicación, se procede a realizar el diseño de la red wifi usando el software de simulación WI-FI Designer de XIRRUS, un software libre existente en el mercado, que permite calcular y ubicar los Access point dentro del mercado, en base a un análisis de mapas de calor, indicando los tipos de materiales que existan dentro del lugar. Este software tiene una desventaja, ya que para la simulación solo existen equipos de la marca XIRRUS, pero que al final dan la idea de cuantos equipos usar, y con ello establecer una comparativa entre los equipos de UniFi que se van a usar en el diseño real; además se compara el número de equipos usados en el software y el número de equipos calculados en base a la cantidad de usuarios y el ancho de banda.

Subsuelo: En la figura 82, se observa la propagación de la señal wifi en el interior del subsuelo, como resultado del software de simulación se observa que en base a la propagación de la señal se requiere solo de 1 AP, debido a que es un área libre solo para garaje con la menor cantidad de obstáculos, además es un solo equipo, ya que es un área en donde menor cantidad de usuarios existen o se van a conectar a la red wifi, las demás simulaciones se presentan en el ANEXO E.

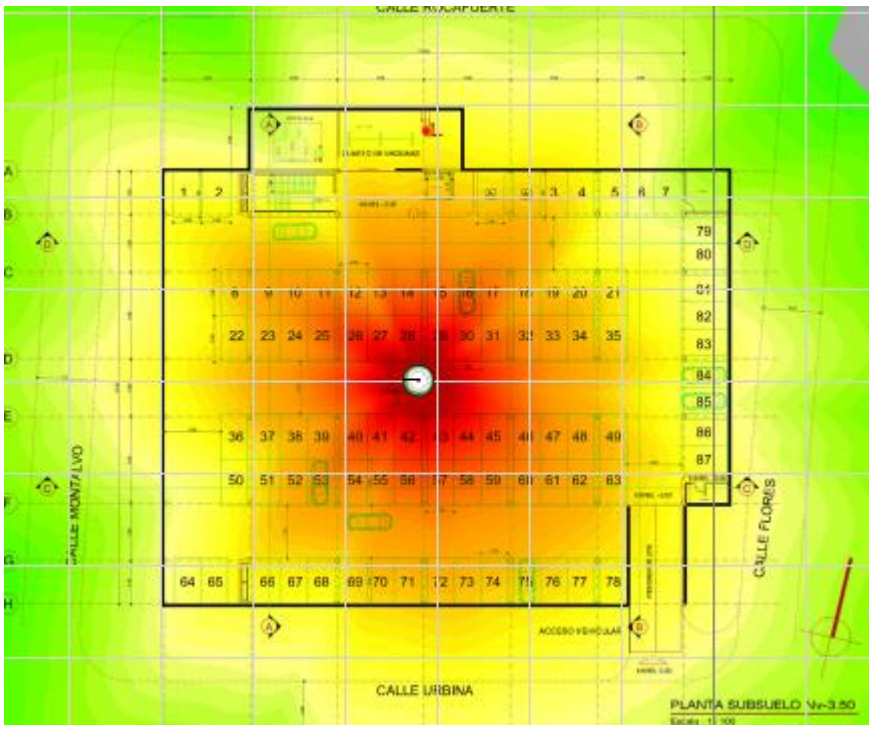


Figura N° 82. Señal wifi usando 1 AP y software XIRRUS.

Elaborado por: Investigadora

Las características de la señal, con la calidad de la misma hasta los -70dBm, que es una medida mínima, en base a los colores establecidos por el software, son mostradas en la tabla 37.

Tabla 37. Calidad de señal en software XIRRUS.

Calidad de señal	Características
-30dBm	Es una señal ideal, 99% de calidad.
-40dBm	Tasa de transmisión elevada, considerando una señal estable.
-50dBm	Tasa de transmisión elevada, considerando una señal de calidad estable.
-60dBm	Estabilidad de conexión de un 80%, señal de calidad buena

-70dBm	Estabilidad de conexión propensa a atenuaciones, señal de calidad baja.

Elaborado por: Investigadora

Resultados De La Simulación en XIRRUS

Una vez efectuadas las simulaciones para determinar la cantidad de Access point para dar cubertura wifi a todo el mercado San Juan, se obtuvieron una serie de datos que ayudaron a realizar un mejor diseño de la red. Se debe indicar que los AP's usados en el simulador son de la marca XIRRUS, mientras que los usados en el diseño real son de la marca UniFi.

En el caso de la simulación se usó el Access Point XR-630 de doble banda, con velocidades de hasta 1.3Gbps, estándar 802.11ac, con capacidad de conexión concurrente de 240 usuarios y con 6 antenas integradas, lo que permite tener mayor rango de cobertura [52].

9. Análisis de access point en base a capacidad de usuarios y cobertura

En la tabla 38, se observa un resumen del número de Access point calculados por medio de la capacidad de usuarios y en base a la cobertura mediante el software de simulación XIRRUS.

Tabla 38. Comparativa de access point en base a capacidad de usuarios y cobertura.

NIVEL	**AP's (cálculos teóricos)**	**AP's (simulación)**
Subsuelo	1	1
Primer Nivel	1	2
Segundo Nivel	1	3
Tercer Nivel	1	2
TOTAL	4	8

Elaborado por: Investigadora

En base a los cálculos realizados para la banda de los 2.4GHz, se obtuvo una diferencia de 4 AP's en relación al cálculo teórico usando la capacidad de usuarios. Esto debido a que el simulador toma en cuenta la estructura interna de cada nivel, obteniendo una mayor cantidad de Access point.

10. Selección de equipos para el diseño de la red wifi

Una vez determinado ciertos parámetros para el diseño de la red wifi que requiere el mercado “San Juan”, se procede a la selección de los equipos necesarios, en el caso que el municipio decida optar por implementar el diseño de la red.

a) Red de Transporte

La red de transporte es el servicio contratado a la empresa proveedor de internet DATAIR, con una velocidad de 40Mbps y a través de fibra óptica, con ello garantizando la calidad de la señal.

b) Red de Acceso

Selección de Puntos de Acceso

Estos puntos de acceso inalámbrico permiten interconectar dispositivos de comunicación inalámbrica y con ello formar una red inalámbrica, que a su vez se pueden conectar a una red LAN cableada para un mayor rendimiento, además se pueden interconectar entre sí para formar una red más grande, realizando un proceso de roaming. En la tabla 39, se muestra diferentes puntos de acceso con sus marcas y características.

Tabla 39. Comparativa de APs marca Unifi, Cisco, Linksys.

Dispositivo /Características			
Marca	UniFi	Cisco	Linksys
Modelo	UAP AC PRO	WAP371	LAPAC1200
Bandas de frecuencias	2.4GHz 5GHz	2.4GHz 5GHz	2.4GHz 5GHz
Velocidad de transferencia	2.4GHz: 450Mbps 5GHz: 1300Mbps	2.4GHz: 450Mbps 5GHz: 1300Mbps	2.4GHz: 450Mbps 5GHz: 1200Mbps
Ambiente	Interior/exterior	Interior	Interior
Seguridad Wifi	WEP, WPA-PSK, WPA- WPA/WPA2	WPA/WPA2	WPA/WPA2
Estándares soportados	802.11 a/b/g/n/r/k/v/ac	802.11 n/ac	802.11 a/b/g/n/ac
Puertos	1 puerto USB 2.0	-	-
Alimentación PoE	Si	Si	Si
Máxima Potencia Tx	2.4GHz: 22dBm 5GHz: 22dBm	2.4GHz: 12dBm 5GHz: 18dBm	2.4GHz: 12dBm 5GHz: 18dBm

Antenas	2.4GHz: 3dBi 5GHz: 3dBi	-	2.4GHz: 1.7dBi 5GHz: 1.9dBi
Interfaz de red	2 interfaces 10/100/1000Ethernet	1 interfaz 10/100/1000Ethernet	1 interfaz 10/100/1000Ethernet
Conexión de usuarios	250 usuarios concurrentes	64 usuarios concurrentes	-
Distancia de cobertura	Hasta 120 metros	-	-
Costo	$230.00	$250.00	$150.00

Elaborado por: Investigadora

De acuerdo al análisis realizado sobre tres modelos de Access point, se escogió el Access point de marca UniFi modelo UAP AC PR, que trabaja en doble banda, con el estándar 802.11ac; además muestra la cantidad de usuarios concurrentes y la distancia de cobertura máxima que ofrece este equipo. Es ideal para el diseño de la red dentro y fuera del mercado, por su potencia de transmisión y por las ganancias de las antenas transmisoras que son de 3dBi, óptimas debido a la infraestructura física que presenta el área a cubrir.

c) Red de Distribución

Selección de Switch

En este aparatado se realiza el análisis de tres marcas de Switch, equipos necesarios para interconectar los Access point seleccionados anteriormente, obteniendo así la comunicación entre todos los dispositivos a través de comunicación wifi.

En la tabla 40, se presenta la comparativa de los switches, haciendo énfasis en el número de puertos, tecnología PoE, y el soporte de estándares.

Tabla 40. Comparativa de switches marcas Unifi, Cisco y HP.

Dispositivo /Características			
Marca	UniFi	Cisco	HP
Modelo	US-24-250W	WS-C2960X-24PD-L	2530-24G-POE+ J9773A
Número de puertos	24 puertos 10/100/1000 Mbps RJ45	24 puertos 10/100/1000 Mbps RJ45	24 puertos 10/100/1000 Mbps RJ45
Soporte PoE	Si	Si	Si
Rendimiento	26Gbps	95.2Mbps	56Gbps
Soporte de estándares 802.11 a/b/g/n/ac	Si	Si	Si
Soporte QoS	Si	Si	Si
Máximo de VLANs	255	-	-
Soporte SSH	Si	Si	Si
Soporte Telnet	Si	Si	Si
Costo	$230.00	$2500.00	$2100.00

Elaborado por: Investigadora

En base al análisis realizado sobre los diferentes equipos, se escogió el Switch de la marca UniFi modelo US-24-250W, debido a la fácil configuración, la contabilidad con los Access point seleccionados anteriormente, a la disponibilidad en el mercado y a su costo asequible.

Selección de Router

En la tabla 41, se ilustra el análisis de tres tipos de routers, en base a las marcas establecidas anteriormente, con la finalidad de seleccionar el más óptimo para interconectar la red interna con la red externa wifi que otorga el ISP DATAIR.

Tabla 41. Comparativa de Routers marcas, Unifi, Cisco y HP

Dispositivo /Características			
Marca	UniFi	Cisco	HP
Modelo	USG-PRO-4	RV130	MSR931 (JG514A)
Interfaz de red	1 puerto serial RJ45	-	1 puerto serial RJ45
Puerto Serie de Consola	2 puertos 10/100/1000 LAN RJ45	4 puertos 10/100/1000 LAN RJ45	4 puertos 10/100/1000 LAN RJ45
Puertos de Datos	2 Puertos de 1 Gbps RJ45/SFP Combinación WAN	1 Puerto de 1 Gbps RJ45	1 Puerto de 1 Gbps RJ45
Procesador	Dual-Core 1 GHz	-	-
Sistema de memoria	2 GB RAM	-	128MB
Soporte SSH	Si	Si	Si
Soporte Telnet	Si	Si	Si
Costo	$350	$173	$650

Elaborado por: Investigadora

Una vez comparada las características técnicas de los equipos, se seleccionó el router de la marca UniFi modelo USG-PRO-4, por la fácil administración, monitoreo, seguridad avanzada, compatibilidad con los switches y Access point anteriormente seleccionados y por el soporte de VLAN's.

11. Diseño Esquemático de la Red Cableada

Una vez elaborado el análisis y selección de los equipos necesarios, se procede a realizar el diseño de la red wifi; al ser el diseño para un mercado de cuatro niveles, un área grande, y ofrecer una calidad de señal wifi alta, se vio la necesidad de interconectar los Access Point mediante cableado vertical hacia el cuarto de seguridad, que se encuentra ubicado en el segundo nivel, junto a los equipos del sistema de video vigilancia IP. La alimentación de estos equipos se realiza por medio de cable Ethernet, usando la tecnología PoE, con ello reduciendo costos y facilitando la implementación.

Como se observa en la figura 83, se sitúa el Switch y el Router de seguridad de la red en el cuarto de seguridad del mercado en el segundo nivel, junto a la ONT equipo proveedor de internet por parte de la empresa DATAIR. Se toma esta decisión ya que en ese nivel existen más Access point y además debido a que la longitud máxima del cable de red Ethernet que alimenta a estos equipos es reducida.

El cableado vertical entre los niveles se realiza al igual que el cableado del sistema de video vigilancia IP diseñado anteriormente, con la finalidad de reducir instalaciones y por ende costos.

El cable de color naranja de 1Gbps del Switch se conecta al router y por medio de este se empaquetan los datos provenientes de los 8 puntos de acceso; cabe recalcar que se está usando Access point de doble banda con la finalidad de tener una mejor calidad de la señal, debido a este parámetro se establece conexión a través de la banda de los 5GHz, ya que es una banda que posee más canales y no provocan interferencial co-canal entre los diferentes equipos situados en cada nivel y además enlazándoles por medio de cable, para minimizar pérdidas en la señal.

El cable de color azul señala la conexión entre el proveedor de servicio de internet y el router, permitiendo el acceso a internet con un ancho de banda de 40Mbps.

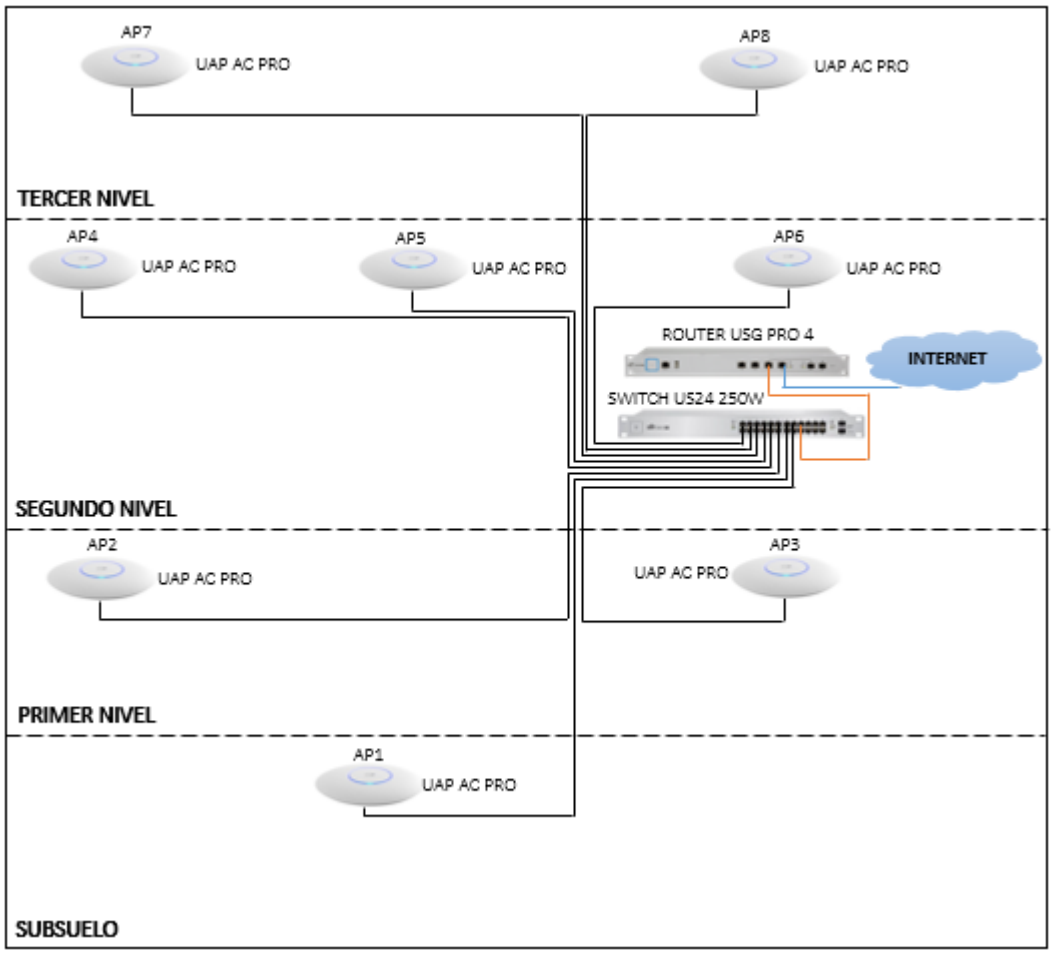


Figura N° 83. Diseño Esquemático de la Red Cableada entre access point.

Elaborado por: Investigadora

En la figura 84, se observa el diseño físico de la red wifi dentro del mercado San Juan, con sus respectivas rutas, en donde se muestra la colocación de los Access Point, Switch, Router y el cableado hacia el cuarto de seguridad, junto con las canaletas para la interconexión de los diferentes dispositivos, usando cable UTP categoría 6 1000 BASE-TX. Además se toma en cuenta el número de Access point calculados en base a la cobertura mediante el software XIRRUS. Para el primer nivel, segundo nivel y tercer nivel, se presenta en el ANEXO F.

Nivel Subterráneo

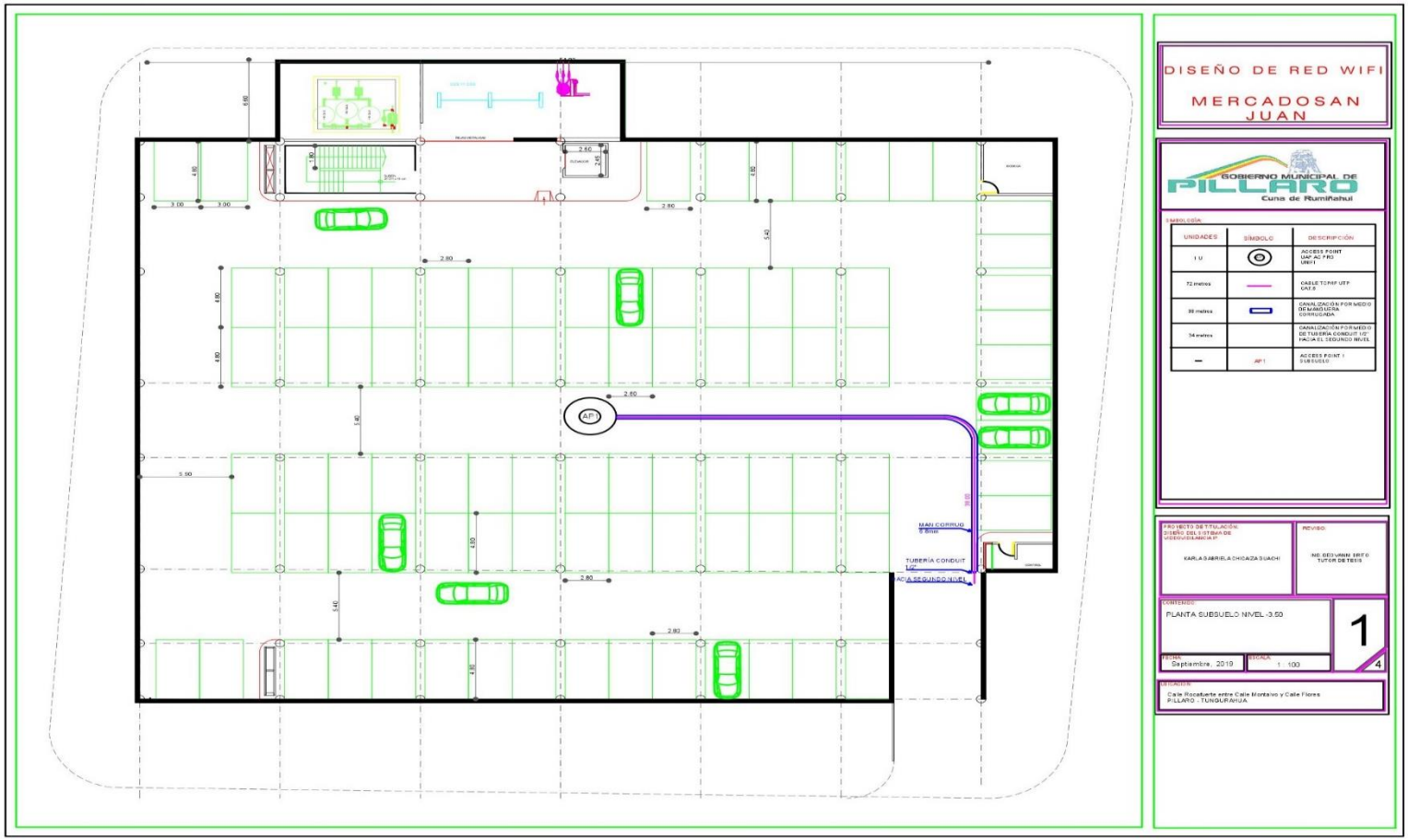


Figura N° 84. Diseño de red Wi-Fi - Nivel Subterráneo.

Elaborado por: Investigadora

12. Diseño Lógico de la Red

Como se analizó anteriormente el cálculo del ancho de banda total y en base a este el plan de contratación de internet de 40Mbps a través de fibra óptica, se procede a subdividir las megas contratadas en: 10Mbps destinados para el sistema de video vigilancia IP más prototipo, 10Mbps para navegación de los usuarios visitantes y los 20Mbps para navegación de los usuarios fijos del mercado, con ello garantizando un óptimo uso del ancho de banda total contratado, y evitando la saturación de la red.

En base a la división de las megas, se procede a la creación de VLAN's; en donde se tiene la VLAN 10 para los usuarios fijos del mercado, la VLAN 20 para el sistema de video vigilancia IP, que ya fue direccionada en el apartado anterior y la VLAN 30 para los usuarios visitantes.

La distribución de las direcciones IP para la VLAN 10 y VLAN 30, se lustra en la tabla 42.

Tabla 42. Direccionamiento lógico y creación de VLANS-Red de datos.

Subred	**Nombre de VLAN**	**Host**	**Máscara**	**Gateway**	**Rango direccionamiento**
Usuarios Visitantes	VLAN2	50	255.255.255.0 /24	192.168.2.1	192.168.2.2 - 192.168.2.50
Usuarios Fijos	VLAN3	100	255.255.255.0/24	192.168.3.1	192.168.3.2 - 192.168.3.200
Sistema de Video Vigilancia	VLAN20	2	255.255.255.0/24	172.16.20.1	172.16.20.2-172.16.20.3
	VLAN1	30	255.255.255.0/24	192.168.1.1	192.168.1.2 – 192.168.1.30

Elaborado por: Investigadora

13. Presupuesto Total del Diseño de la Red Wifi

Tabla 43. Presupuesto Total para implementación de Red Wi-Fi.

Presupuesto Total				
Ítem	**Detalle**	**Cantidad**	**Precio Unitario**	**Precio Total**
1.	Access Point UniFi UAP AC PRO	8 U	$230.00	$1840.00
2.	Switch PoE UniFi US24 250W	1 U	$230.00	$230.00
3.	Router Unifi USG PRO 4	1 U	$350.00	$350.00

4.	Cable UTP cat.6	481 metros (2 bobinas de 300 metros)	$0.52	$316.00
5.	ConectOres RJ45 cat.6 NEXXT AW102NXT04	16 U	$0.25	$4.00
6.	Protector de conector RJ45 DELTA	16 U	$0.10	$1.60
7.	Manguera Corrugada de 23 mm	38 metros	$1.00	$38.00
8.	Tubería conduit de 1/2"	34 metros	$0.67	$22.78
9.	Canaleta plástica PVC DEXSON	46 metros (23 canaletas de 2m)	$3.50	$80.50
10.	Respaldo de Energía UPS Apc Br1000g Pro 1000va 600w	1 U	$260.00	$260.00
11.	Configuración e Instalación	12 horas	$60.00	$720.00
Sub-Total				$3214.88
Imprevistos 10%				$321.488
TOTAL				**$3536.37**

Elaborado por: Investigadora

2.3. PRESUPUESTO DEL PROTOTIPO

El presupuesto del prototipo de Sistema de Alarma Comunitaria se presenta en la tabla 44, en donde se encuentran los materiales y equipos usados con la cantidad, y que es necesario detallar cada elemento para el establecimiento del costo final.

Tabla 44. Presupuesto de elaboración del Prototipo.

Presupuesto					
Ítem	**Unidad**	**Descripción**	**Cantidad**	**Valor Unitario**	**Valor Total**
1	c/u	Kit Completo Raspberry Pi 3B+	1	$95	$95
2	c/u	Cámara IP	1	$45	$45
3	c/u	Router Tp-Link TL WR840N	1	$18	$18
4	c/u	Cable HDMI	1	$20	$20
5	c/u	Tarjeta MicroSD	1	$30	$30
6	c/u	Disco Duro Hitachi	1	$140	$140
7	c/u	Cable de red	3	$3	$9
8	horas	Internet	300	$0.50	$150
9	c/u	Batería seca 12V 4A	1	$25	$25
10	c/u	Fuente de 12V 5A	1	$20	$20
11	c/u	Ventilador 5V	1	$6	$6
12	c/u	Kit de equipamiento electrónico	1	$45	$45
13	c/u	Kit de Herramientas electrónicas	1	$50	$50

14	c/u	Case	1	$25	$25
15	c/u	Otros (Materiales para elaboración del prototipo)	1	$10	$10
Sub-Total					$688
Imprevistos del 10%					$68.80
TOTAL DEL PROTOTIPO					$756.80

Elaborado por: Investigadora

2.4. MÉTODOS

La modalidad del presente proyecto se basa en una investigación aplicada ya que se hizo uso de los conocimientos adquiridos durante toda la formación superior con la finalidad de buscar una de las mejores opciones y dar cumplimiento a los objetivos planteados para el desarrollo del proyecto; además se hará uso de las siguientes modalidades:

2.4.1. Investigación Bibliográfica

Debido a que se vio la necesidad de buscar información que provengan de tesis, artículos científicos, libros, así como también páginas web que permitieron la programación de los dispositivos electrónicos a utilizar.

2.4.2. Investigación de Campo

Se hizo uso de esta investigación debido a que se realizó el estudio en el mercado San Juan, un lugar en donde puedan ocurrir situaciones extrañas en cuanto a la seguridad ciudadana, con ello se obtuvo información que ayudó al desarrollo del proyecto.

CAPÍTULO III

RESULTADOS Y DISCUSIÓN

3.1. ANÁLISIS Y DISCUSIÓN DE RESULTADOS

En este capítulo se presentan los resultados obtenidos durante la investigación; para el desarrollo del proyecto de sistema de alarma comunitaria, se realizó un análisis de la activación de las alarmas y del funcionamiento de la cámara IP como sistema de monitoreo y detección de movimiento. Además se efectuó un análisis del historial de las alarmas almacenadas de acuerdo al tiempo de activación y de la presentación de video en 720 pixeles.

3.1.1. Análisis del ingreso de datos a página web

a) Configuración del funcionamiento del Sistema

En base a la programación desarrollada en python para el diseño de la página web del administrador, se logró realizar el ingreso de los diferentes datos para acceder a la configuración del sistema, a través de los archivos: data.pickle usado en la serialización de los datos ingresados; archivo template para el diseño de la página web y archivo app.py donde se encuentra la configuración general; ubicados en la carpeta alarmaComunitaria. El prototipo fue implementado en el área administrativa del mercado, cuyas direcciones IP de los dispositivos fueron modificadas a la red existente en el lugar, usando la dirección IP: 192.168.1.2 en el área administrativa, y la dirección 192.168.0.100 en el Local N°01, que permitieron el acceso al sistema.

En el navegador se digitó la dirección IP, seguido del puerto de comunicación y del dominio "administrador", como sigue: "192.168.1.2:8080/administrador", modificando los siguientes parámetros:

Colocación de la ruta de almacenamiento de Videos grabados en caso de detección de movimiento, junto a la capacidad de almacenamiento del Disco Duro externo, como se presenta en la figura 85.

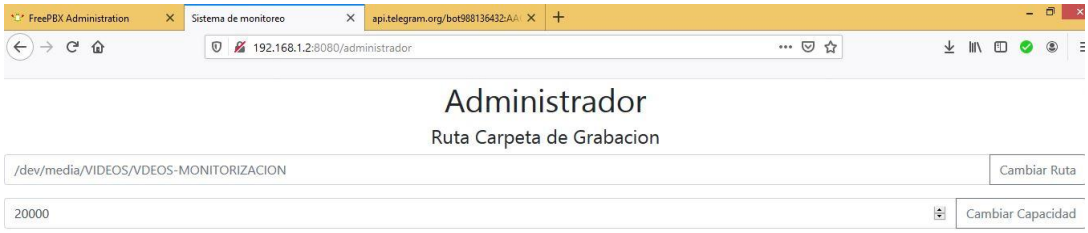


Figura N° 85. Ingreso de carpeta de grabación y espacio de almacenamiento.

Elaborado por: Investigadora

Ingreso de los ID del grupo de usuarios del centro comercial y del grupo policial, a la sección números de emergencia y a la sección ID telegram UPC, como se presenta en la figura 86 y 87 respectivamente.

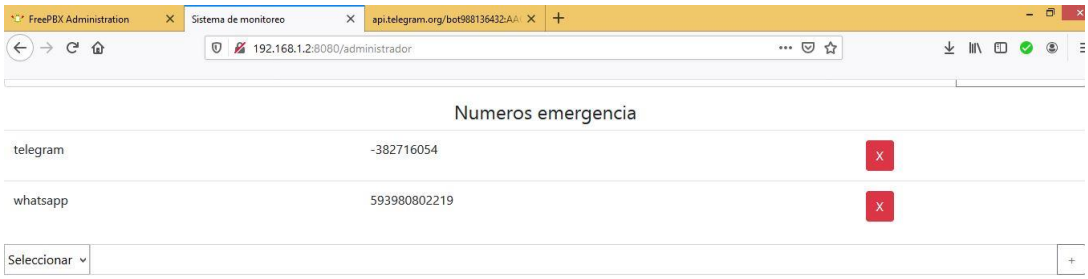


Figura N° 86. Ingreso de ID de grupo de usuarios.

Elaborado por: Investigadora

Figura N° 87. Ingreso de ID de grupo UPC.

Elaborado por: Investigadora

Otro de los parámetros ingresados, fueron los beneficiarios, en este aspecto se registraron a los usuarios y contraseñas por su número de cédula, y a uno de ellos como user01, en la figura 88, se muestran el registro inicial.

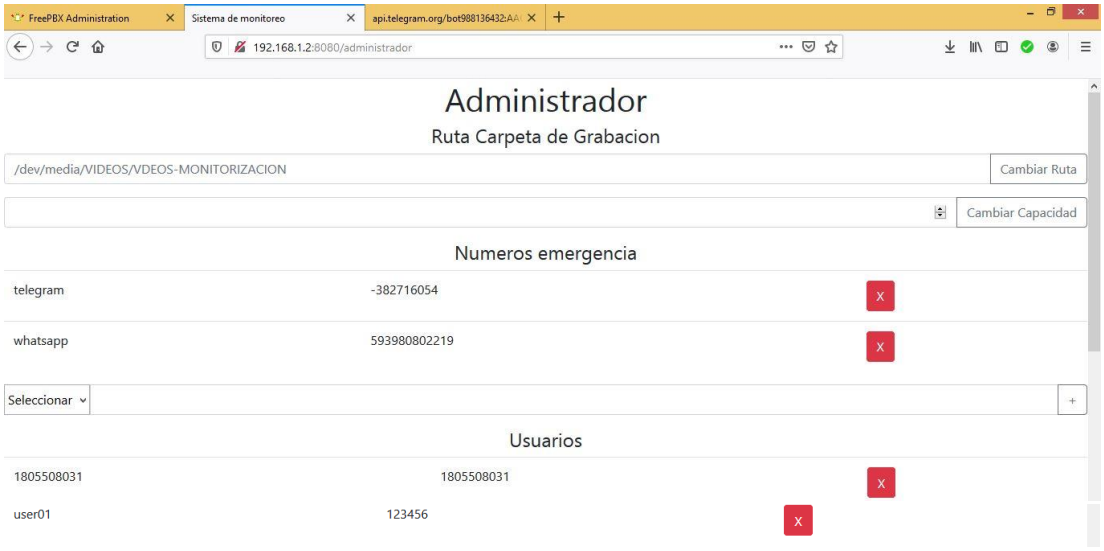


Figura N° 88. Ingreso de usuarios al sistema.

Elaborado por: Investigadora

Para que el prototipo funcione como sistema de monitoreo, se ingresó a la sección de cámaras, en donde se colocó: el nombre del dispositivo “cam1”; el usuario “admin”; contraseña “abcd1234”, dirección IP “192.168.1.102” y el protocolo que usa el equipo “onvif1”. Además trabaja automáticamente a través, de dos horarios, para tener una mejor visión del funcionamiento, se colocó en la sección horario un tiempo de 21pm a 4:59am, sistema empleado para monitoreo en base a detección de movimiento. En la figura 89, se presenta los campos ingresados.

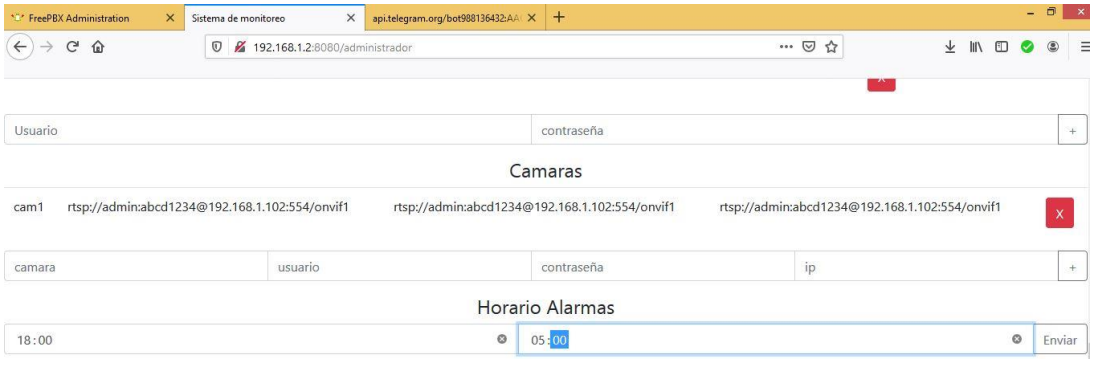


Figura N° 89. Configuración de cámara y horario de funcionamiento

Elaborado por: Investigadora

Ingreso de correo electrónico para el envío de capturas de imagen en caso de alarma por detección de movimiento; llenando los campos dirección de correo electrónico como medio de envío en este caso a través del correo: karlachicaizag@gmail.com, la

contraseña establecida en el servidor y el correo del usuario encargado de la seguridad de ingreso al mercado a quién se enviará las imágenes: liszyta16@gmail.com, como se muestra en la figura 90.

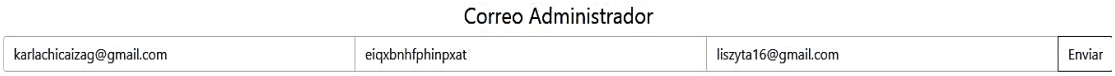


Figura N° 90. Ingreso de correo gmail del administrador de la seguridad del mercado.

Elaborado por: Investigadora

Previa las configuraciones realizadas, se ingresó al funcionamiento del sistema.

b) Ingreso de usuarios al Sistema zona Administrativa

El funcionamiento del sistema con sus respectivas pruebas, fue desarrollado, en diferentes lugares, una en la zona de administración y otra en los locales exteriores del mercado. En esta sección se presentan las pruebas realizadas en el área de administración, cuyo acceso al sistema, los usuarios ingresaron al navegador usando la dirección: 192.168.1.2:8080, con su respectivo usuario y contraseña, previamente configurados, en la figura 91, se presenta el ingreso al sistema.

Figura N° 91. Ingreso al sistema con usuario y contraseña.

Elaborado por: Investigadora

Una vez ingresado al sistema, los usuarios accedieron a, las cámaras, alarmas e historial de eventos. En la figura 92, se observa el ingreso a la cámara de monitoreo desde un teléfono Android, mientras que en la figura 93, se visualiza el video desde una pc de las oficinas del área de administración del mercado.

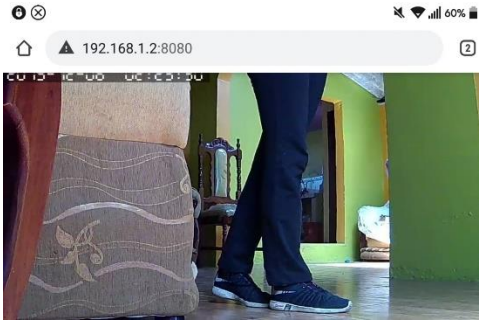


Figura N° 92. Monitoreo remoto a través de teléfono Android.

Elaborado por: Investigadora

Figura N° 93. Monitoreo local a través de PC de oficina de administración.

Elaborado por: Investigadora

Dentro de la página además, se puede activar o desactivar la alarma y enviar mensajes de alerta en caso de presentarse actos delictivos, los beneficiarios de esta forma de activación son aquellos que no posean un teléfono celular y en su local tengan dispositivos de escritorio. En la figura 94, se ilustra el envío de este mensaje y recepción de alerta a través de telegram y whatsapp, incluyendo el remitente con fecha y hora.

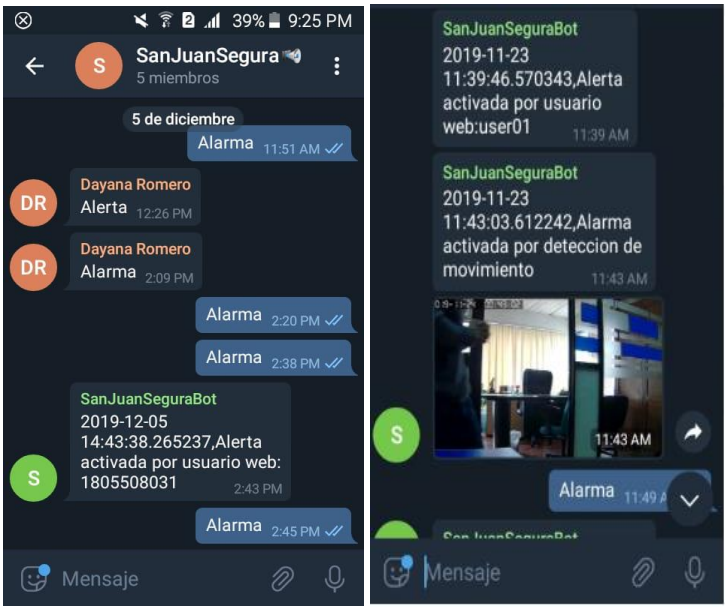


Figura N° 94. Activación de Alerta desde PC y reenvío a chat de usuarios telegram.

Elaborado por: Investigadora

c) Ingreso de usuarios al Sistema Local externo del mercado N°01

La propietaria del local ingresó a la página web, a través del usuario user01 mediante una computadora, en donde se le indicó el funcionamiento del sistema, como se presenta en la figura 95 y 96 respectivamente.

Figura N° 95. Acceso de usuario user01 del local N°01 del mercado.

Elaborado por: Investigadora

Figura N° 96. Capacitación de acceso al sistema a propietaria del local comercial.

Elaborado por: Investigadora

3.1.2. Activación de Alerta por mensajería Telegram

a) Pruebas de Alertas zona Administración del mercado

Las alertas fueron activadas mediante mensajería Telegram, y enviadas de forma masiva a los usuarios registrados, en la figura 97, se observan las alertas emitidas, con las siguientes palabras de activación del sistema:

- **Alerta:** Comunicado masivo a todos los usuarios, sin activación tanto de la sirena como del envío de notificaciones a UPC.
- **Alarma:** Comunicado masivo a todos los usuarios incluyendo a UPC con activación de sirena por 1 minuto y desactivación de la misma, por ingreso a la página web.

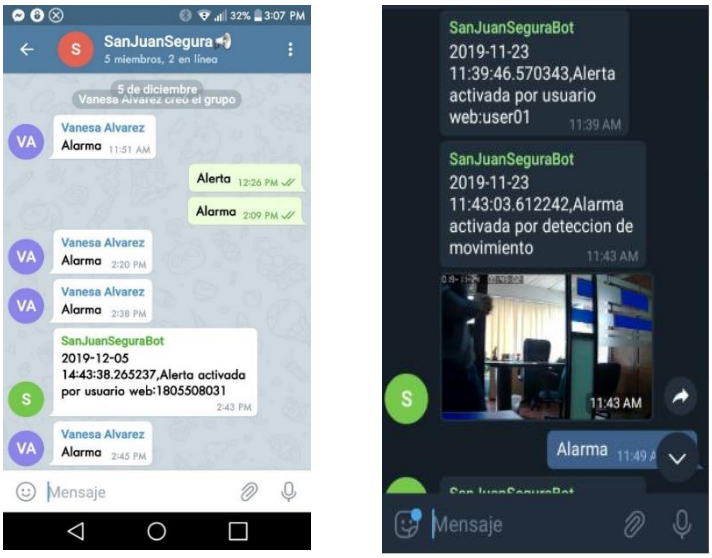


Figura N° 97. Activación de Alerta por mensajería telegram por user01.

Elaborado por: Investigadora

b) Prueba de Alertas Local Exterior N°01 del mercado

Para estas pruebas se instaló en el teléfono de una de las personas que trabaja dentro del local comercial la aplicación de mensajería Telegram, para luego ser añadido al chat del sistema SanJuanSegura; proceso que fue realizado para que demás usuarios accedan y puedan hacer uso del sistema, como se ilustra en la figura 98.

Figura N° 98. Instalación de Telegram a usuario del local N°01 del mercado.

Elaborado por: Investigadora

Una vez instalada la aplicación de mensajería, el usuario envió y recibió notificaciones del sistema de alarma, en casos de emergencia, usando las palabras citadas anteriormente, como se presenta en la figura 99.

Figura N° 99. Activación de Alertas y Alarmas por mensajería Telegram de usuario Bayardo Rosero.

Elaborado por: Investigadora

3.1.3. Activación de Alarma por Detección de Movimiento Administración

Las Alarmas fueron activadas en el horario de 18:00pm a 5:00am a través del sistema detector de movimiento, en donde al observar un objeto en movimiento, emitió un mensaje de alarma, junto a la captura de imagen del instante en que el objeto fue detectado, activando la sirena y el almacenamiento de videos en el disco externo,

dispositivo que fue programado para la eliminación de un 10% de los videos más antiguos al llegar al 99% de almacenamiento. En la figura 100, se presenta el mensaje de alarma con el objeto detectado, mientras que en la figura 101, se muestra la recepción del mensaje a WhatsApp con el usuario y la fecha de emisión en el área de administración, en la figura 102 se presenta los videos grabados y almacenados en el disco externo por detección de movimiento, y en la figura 103 la notificación de mensajes de detección de movimiento fuera del local comercial N°01, recalcando que estas pruebas se realizaron en el día cambiando el horario del mismo en la página del administrador, para observar el funcionamiento del sistema.

Figura N° 100. Recepción de alarmas y alertas a WhatsApp

Elaborado por: Investigadora

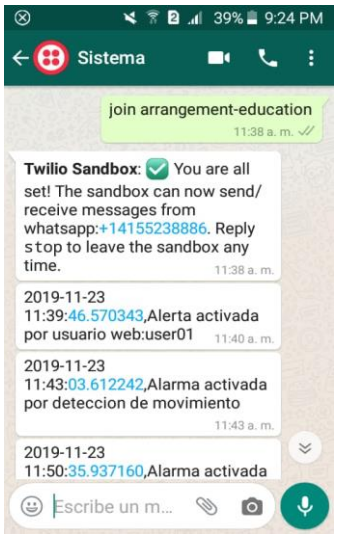


Figura N° 101. Alarma recibida por detección de movimiento.

Elaborado por: Investigadora

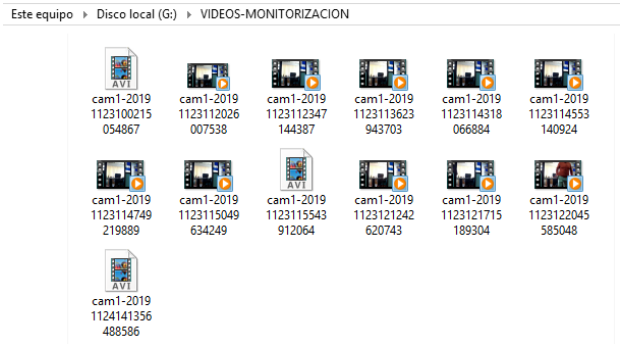


Figura N° 102. Almacenamiento de videos por detección de movimiento en disco externo.

Elaborado por: Investigadora

Figura N° 103. Notificación de Alarma por detección de movimiento, con captura de imagen de local N°01.

Elaborado por: Investigadora

Además la notificación de Alarmas por detección de movimiento, fueron enviadas al correo de la administradora del mercado, como se ilustra en la figura 104.

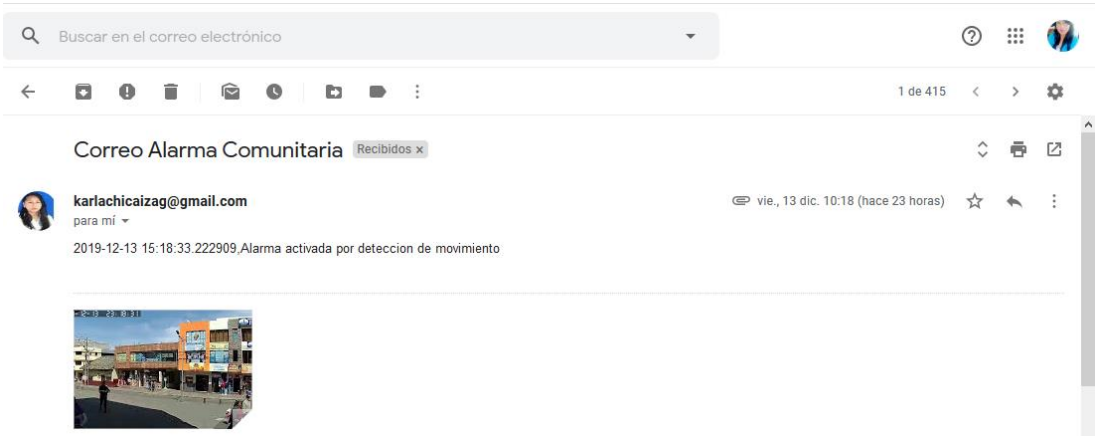


Figura N° 104. Notificación de Alarma por correo electrónico a persona encargada de seguridad del mercado.

Elaborado por: Investigadora

3.1.4. Resultado Final del Proyecto

Las pruebas realizadas por el prototipo de Sistema de Alarma Comunitaria fueron satisfactorias, en la figura 105 se puede observar el prototipo armado, el cual consta de una Raspberry Pi 3B+ como el centro de procesamiento, los sistemas de: alimentación de 12V, respaldo de energía, monitoreo, comunicación, alarma y almacenamiento, que en conjunto permitieron el funcionamiento de todo el prototipo.

Figura N° 105. Prototipo armado Sistema de Alarma Comunitaria, vista Superior.

Elaborado por: Investigadora

En la figura 106, se presenta la estructura final del Sistema de Alarma, con la cámara IP, sirena, circuitos de alimentación, respaldo de energía y almacenamiento, en funcionamiento.

Figura N° 106. Prototipo final en funcionamiento, vista frontal.

Elaborado por: Investigadora

En la figura 107, se observa el monitoreo fuera del mercado San Juan, a través de un teléfono Android, por medio del ingreso de usuarios a la página web creada y en la figura 108, se presenta la instalación del prototipo en el local exterior N°01 del lugar perteneciente al señor Luis Chimborazo.

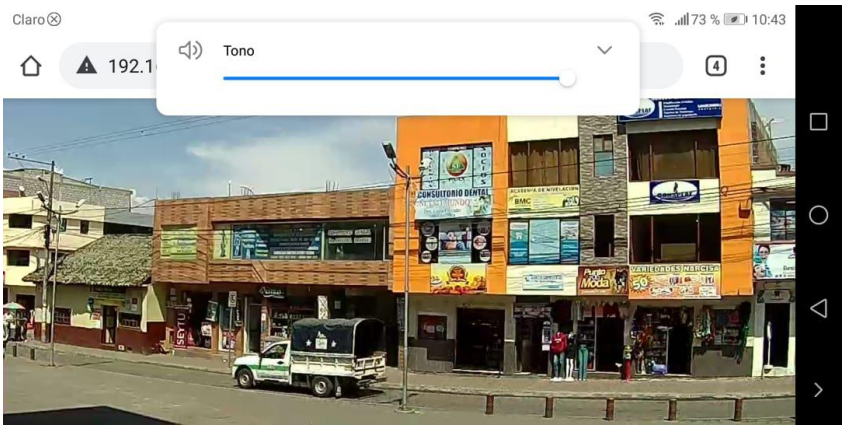


Figura N° 107. Monitoreo local del exterior del mercado a través de página web

Elaborado por: Investigadora

Figura N° 108. Implementación de Prototipo en el Local N°01 del mercado San Juan.

Elaborado por: Investigadora

Otro de los parámetros fundamentales son los tiempos de recepción de notificaciones tanto de Alarmas como de Alertas a los beneficiarios, a través de mensajería Telegram, WhatsApp, página web y por detección de movimiento. A continuación, en la tabla 45, se presentan los tiempos de recepción de mensajes desde un usuario notificador Telegram, obteniendo un tiempo promedio de 0.57milisegundos en receptar mensajes

de Alerta, mientras que las recepciones de mensajes de Alarma en un tiempo promedio de 0.67 milisegundos.

Tabla 45. Tiempo promedio de recepción de alarmas en base a Telegram-Telegram.

Tiempos de Respuesta del Sistema de Alarma Comunitaria por mensajería Telegram		
Muestras	**Alerta (milisegundos)**	**Alarma (milisegundos)**
1	0.60	0.62
2	0.62	0.76
3	0.40	0.80
4	0.56	0.54
5	0.70	0.64
Promedio	0.57	0.67

Elaborado por: Investigadora

En la tabla 46, se tienen los tiempos de recepción de Alarmas emitidas desde la Página web a Mensajería Telegram y WhatsApp, obteniendo como tiempo promedio de recepción de mensajes de Alarma Telegram de 2.004 segundos, mientras que la recepción de alarmas WhatsApp de 2.544 segundos, son tiempos estables por la conexión a Internet, obteniendo así una calidad óptima de la señal.

Tabla 46. Tiempos de recepción de Alarmas de Página web a Mensajería Telegram y WhatsApp

Tiempos de Respuesta del Sistema de Alarma Comunitaria por Página Web		
Muestras	**Tiempo Telegram (s)**	**Tiempo WhatsApp (s)**
1	1.20	2.54
2	2.01	2.38
3	1.56	3.24
4	3.02	1.89
5	2.23	2.67
Promedio	2.004	2.544

Elaborado por: Investigadora

Otro de los tiempos a tomar en cuenta son: recepción de mensajes de Alarma por detección de Movimiento tanto a Telegram como a WhatsApp y el envío de mensaje con captura de imagen a correo electrónico. En la tabla 47, se presentan tiempos promedios de 8,09 segundos en la recepción de mensajes Telegram, 5,18 segundos a WhatsApp y 8,99 segundos a correo electrónico, cabe recalcar que estos tiempos son mayores por el procesamiento de la central al captar imagen y enviar hacia los diferentes medios.

Tabla 47. Tiempos de Respuesta del Sistema de Alarma Comunitaria por Detección de Movimiento.

Tiempos de Respuesta del Sistema de Alarma Comunitaria por Detección de Movimiento			
Muestras	**Tiempo Telegram (s)**	**Tiempo WhatsApp (s)**	**Tiempo Correo Electrónico (s)**
1	8,34	5.67	8,90
2	6,76	4.56	9,24
3	7,56	5,78	8,14
4	8,45	4,56	9,16
5	9,34	5,34	9,52
Promedio	8,09	5,18	8,99

Elaborado por: Investigadora

CAPÍTULO IV

CONCLUSIONES Y RECOMENDACIONES

4.1. CONCLUSIONES

- La configuración de todo el sistema de alarma fue montado sobre la tarjeta Raspberry Pi como centro de procesamiento, en la ejecución del servidor, se logró tener un óptimo rendimiento al ejecutar todas las tareas designadas en la programación, con lo que mostró ser un sistema confiable al momento de ser implementado, otra de las ventajas que se obtuvo fue la optimización de memoria ya que los videos captados por la cámara se almacenaron en un disco externo, lo que permitió que el servidor no se colapse, optimizando la capacidad de procesamiento.

- Los dispositivos que conforman el sistema de alarma y video vigilancia IP son de tecnología ONVIF, es decir que el sistema puede funcionar con la instalación de diferentes tipos de cámaras, sean cámaras IP, cámaras web, o las dos, ya que el sistema fue diseñado para trabajar con cualquier marca de dispositivos, pero siempre hay que verificar la compatibilidad con la Raspberry Pi 3B+.

- Las características y funcionalidades del computador de placa reducida respecto a otros sistemas de alarma tiene una gran ventaja, ya que al tener acceso a puertos GPIO, se puede conectar más dispositivos para enriquecer al sistema de alarma, debido a que puede soportar mejoras, sin afectar su funcionamiento.

- El desarrollo de las alarmas y alertas a través de las aplicaciones Telegrama y WhatsApp permiten que el sistema sea una herramienta funcional, ya que no se necesita la instalación de otras aplicaciones en los teléfonos de los usuarios, sino más bien aprovechar las redes sociales de uso cotidiano para el control y notificación de eventos delictivos que puedan suceder dentro y fuera del mercado.

- El sistema de alarma comunitaria cumplió con las necesidades del mercado, emitiendo los mensajes oportunos, en tiempos adecuados e informando a toda la

comunidad de estar en Alerta y comunicando a las autoridades encargadas de la seguridad del sector, trayendo así la satisfacción de los usuarios al conocer que el sistema ayuda a estar en alerta y a disuadir posibles hechos atentados contra la vida humana.

- El proyecto además contó con el diseño del sistema de video vigilancia IP y red wifi para todo el mercado, usando equipos de marcas registradas para un óptimo funcionamiento, al contar con los planos elaborados en AutoCAD, el Alcalde del cantón obtuvo una mejor visión de la implementación, con sus respectivos costos y beneficios.

4.2. RECOMENDACIONES

- Para que la placa tenga un óptimo funcionamiento, es necesario colocar los disipadores y ventilador, sobre el procesador ya que la placa está ejecutando todas las funciones al mismo tiempo.

- El prototipo al ser un sistema que ayuda a evitar hechos vandálicos, es probable que pueda sufrir daños por personas involucradas en estos actos, por ello es recomendable colocarlo en un lugar seguro, específicamente en un pequeño rack de comunicaciones.

- Un sistema de alarma comunitaria siempre debe tener un circuito de alimentación y respaldo de energía para el funcionamiento continuo, en caso de existir cortes eléctricos, para el diseño adecuado de estos sistemas alimentadores se debe tomar en cuenta el consumo tanto de voltaje como amperaje de cada dispositivo, y que al final de la implementación no existan fallos principalmente en el funcionamiento del computador de placa reducida.

- Si se requiere del aumento de cámaras IP, es necesario realizar un análisis del consumo de ancho de banda, con la finalidad de evitar problemas con el sistema de activación, desactivación, notificación de alarmas y el sistema detector de movimiento, además lo más recomendable para el incremento de estos dispositivos es preciso usar un hub con alimentación propia, debido a la limitación de los puertos que presenta el router TP-LINK usado.

BIBLIOGRAFÍA

[1] Zhaoxia W, Hanshi W, Lizhen L, Wei S, JingLi L, «Community Alarm System Design Based on MCU and GSM,» *International Conference on Computer Science and Network Technology*, vol. 4, nº 16090191, pp. 859-862, 2015.

[2] Villalba, Freddy René Aguilar, «Desarrollo de un Prototipo de Alarma Multimodal Comunitaria Utilizando el Protocolo Ipv6 y GPRS para Smart Cities con Monitoreo en Tiempo Real,» Junio 2017. [En línea]. Available: http://dspace.espoch.edu.ec/handle/123456789/7516. [Último acceso: 30 Marzo 2019].

[3] Llagua, Evelyn, «Sistema de Monitoreo de Alarmas mediante Mensajería SMS e Interface hacia un computador para la Recepción de Eventos de Emergencia,» Septiembre 2017. [En línea]. Available: http://repositorio.uta.edu.ec/jspui/handle/123456789/27122. [Último acceso: 30 Marzo 2019].

[4] S. Sruthy, S. George, «WiFi enabled home security surveillance system using Raspberry Pi and IoT module,» *IEEE International Conference on Signal Processing, Informatics, Communication and Energy Systems (SPICES)*, pp. 1-6, 2017.

[5] Gómez, Boris, «Estudio de Sistemas de Alarma Comunitaria. Caso de Estudio Conjunto Residencial Ruiseñor 2,» 2018. [En línea]. Available: http://repositorio.puce.edu.ec/handle/22000/15072. [Último acceso: 30 Marzo 2019].

[6] Victor O, Etinosa N, Praise J, Morgan K, Uzairue S, «Implementation of a Community Emergency Security Alert System,» *International Journal of Innovative Science and Research Technology*, vol. 3, pp. 475-482, 2018.

[7] A. S. Jenny Pontón, «Seguridad Ciudadana,» de *Nuevas problemáticas en seguridad ciudadana*, Quito, Flacso Ecuador, 2008, pp. 24-30.

[8] Victor O. Matthews, Etinosa Noma-Osaghae, UzairueStanley Idiake, Morgan Kubiat Enefiok, Praise Jude Ogukah, «Implementation of a

Community Emergency Security Alert System,» *International Journal of Innovative Science and Research Technology*, vol. 3, pp. 1-4, 2018.

[9] F. Carrión, «Lla Violencia en Ecuador,» [En línea]. Available: http://www.flacso.org.ec/docs/artvioecu.pdf. [Último acceso: 25 Agosto 2019].

[10] Ministerio del Interior, «Seguridad Ciudadana - Solidaridad Ciudadana,» Febrero 2015. [En línea]. Available: https://www.ministeriointerior.gob.ec/wp-content/uploads/2015/04/SEGURIDAD-CIUDADANA-SOLIDARIDAD-CIUDADANA.pdf. [Último acceso: 07 Marzo 2019].

[11] Instituto Nacional de Estadísticas y Censos, «Compendio Estadístico de Seguridad Ciudadana 2014 - 2016,» 12 Marzo 2017. [En línea]. Available: www.ecuadorencifras.gob.ec/.../web.../COMPENDIO_ESTADISTICO_%1F2014.xlsx. [Último acceso: 07 Marzo 2019].

[12] Diario La Hora, «Baja Índice Delincuencial en el Cantón Santiago de Píllaro,» 02 Abril 2018. [En línea]. Available: https://lahora.com.ec/tungurahua/noticia/1102146781/baja-indice-delincuencial-en-pillaro-. [Último acceso: 07 Marzo 2019].

[13] Julián. Fernández, «Seguridad Electrónica,» de *Circuito cerrado de televisión y seguridad electrónica*, España, Paraninfo, 2018, pp. 2-10.

[14] Juan. Uribe, Wilmar Gómez, «Modelo de Integración Tecnológica del Subsistema de Alarmas Comunitarias con los Sistemas de Seguridad y Emergencias (SIES),» 2013. [En línea]. Available: https://repository.javeriana.edu.co/bitstream/handle/10554/15574/GomezRodriguezWilmarAlejandro2013.pdf?sequence=2. [Último acceso: 25 Marzo 2019].

[15] J. Andreu, «Comunicaciones Inalámbricas,» de *Redes inalámbricas (Servicios en red)*, Editex, 2011, pp. 212-215.

[16] Clanar Internacional, «Comunicaciones Inalámbricas,» de *Internet y Redes Inalámbricas*, Perú, pp. 6-30.

[17] Carlos. Miranda, «Red WLAN,» de *Sistemas informáticos y redes locales*, España, Paraninfo, 2014, pp. 145-148.

[18] Jordi. Salazar, «Redes Inalámbricas,» [En línea]. Available: https://upcommons.upc.edu/bitstream/handle/2117/100918/LM01_R_ES.pdf. [Último acceso: 26 Agosto 2019].

[19] Ignacio. Herreros, Josep. Nolla. Xavier Muñoz, «Tecnología Wifi,» de *Manual de Derecho de las Telecomunicaciones*, España, LegalLink, 2006, pp. 202-210.

[20] José. Carballar, «Estándar 802.11,» de *Wi-Fi. Instalación, Seguridad y Aplicaciones*, España, Copyright, 2014, pp. 28-33.

[21] Izaskun. Pellejero, Amaia. Lesta, Fernando Andreu, «Estándar IEEE 802.11,» de *Fundamentos y Aplicaciones de Seguridad en Redes WLAN: Fundamentos y Aplicaciones de Seguridad*, España, Marcombo, 2006, pp. 21-30.

[22] Edwin. Hurtado, «Diseño e Implementación de un Prototipo que permita Telefonía IP, Servicio de Acceso a Iinternet,» Febrero 2018. [En línea]. Available: https://bibdigital.epn.edu.ec/handle/15000/19151. [Último acceso: 25 Agosto 2019].

[23] Miriam. Mingarro, «Aplicación para Transmisión de Datos en Internet de las Cosas,» 26 Julio 2018. [En línea]. Available: http://oa.upm.es/53559/1/TFG_MIRIAM_LAINA_MINGARRO.pdf.. [Último acceso: 25 Marzo 2019].

[24] Paula. Nieto, Paúl. Rojas, Nicolás. Villanueva, Carina Flores, «Comparación de protocolos en seguridad de mensajeríainstantánea - WhatsApp v/s Telegram,» Agosto 2018. [En línea]. Available: http://profesores.elo.utfsm.cl/~agv/elo322/1s18/projects/reports/SeguridadWhatsapp_Telegram.pdf. [Último acceso: 24 Agosto 2019].

[25] Carmen Janeth, «Estrategias Didácticas basadas en Aplicaciones de Mensajería Instantánea WhatsApp Exclusivamente para Móviles y el uso de la Herramienta para Promover el Aprendizaje Colaborativo,» 2 Julio 2013. [En línea]. Available: http://servicio.bc.uc.edu.ve/educacion/eduweb/v7n2/art09.pdf. [Último acceso: 25 Marzo 2019].

[26] Francisco. García, «Sistema de Video Vigilancia IP,» de *Videovigilancia: CCTV usando vídeos IP*, España, Vertice, 2011, pp. 13-24.

[27] Roberto. Junghanss, «Componentes y característicasde un Sistema de CCTV,» [En línea]. Available: http://www.rnds.com.ar/articulos/037/RNDS_140W.pdf. [Último acceso: 26 Agosto 2019].

[28] Tecnología, «Estándar de compresión de video H.264,» [En línea]. Available: http://www.rnds.com.ar/articulos/044/RNDS_140W.pdf. [Último acceso: 27 Agosto 2019].

[29] Axis Communications, «Guía técnica de vídeo IP.,» [En línea]. Available: https://www.microsa.es/biblioteca/Axis/Axis%20_%20Gu%EDa%20t%E9cnica%20de%20v%EDdeo%20IP.pdf. [Último acceso: 26 Agosto 2019].

[30] Gemma. Antón, Jorge. Rodríguez, Octavio Romero, Jaime Mondé, Julio Concejero, María Romero, Francisco Castillo, «Servicio de VoIP,» de *Servicios en Red*, España, Paraninfo, 2010, pp. 192-211.

[31] mheducation, «Servicio de voz sobre IP,» [En línea]. Available: https://www.mheducation.es/bcv/guide/capitulo/8448171330.pdf. [Último acceso: 28 Agosto 2019].

[32] Julio. López, «Servicio VoIP,» de *VoIP y Asterisk: redescubriendo la telefonía*, España, Ra-Ma, 2014, pp. 18-30.

[33] Quarea Voz Datos IP, «FreePBX, Gestor Web para Asterisk,» [En línea]. Available: https://www.quarea.com/es/freepbx-gestor-web-asterisk. [Último acceso: 30 Agosto 2019].

[34] Bernard. Pérez, «Manejo de Asterisk,» de *Asterisk PBX: Aprende a crear y diseñar soluciones de telefonía IP desde cero*, 2014, pp. 60-70.

[35] Manuel. Carrasco, «Alarmas sonoras,» de *Sistemas de detección y alarma*, España, 2016, pp. 28-30.

[36] tp-link, «Router Inalámbrico,» [En línea]. Available: https://www.tp-link.com/es/home-networking/wifi-router/tl-wr840n/. [Último acceso: 20 Octubre 2019].

[37] Arkaitz. Lázaro, Abel. Velasco, «Discos Duros,» [En línea]. Available: https://www.infor.uva.es/~cevp/FI_II/fichs_pdf_teo/Trabajos_Ampliacion/Discos_Duros.pdf. [Último acceso: 01 Octubre 2019].

[38] Code Visual Studio, «Code editing Redefined,» [En línea]. Available: https://code.visualstudio.com/. [Último acceso: 24 Agosto 2019].

[39] Revelo. Guevara, «http://repositorio.utn.edu.ec/bitstream/123456789/7064/1/04%20RED%20085%20TRABAJO%20GRADO.pdf,» 30 Marzo 2016. [En línea]. [Último acceso: 25 Agosto 2019].

[40] Alvaro. Valladares, «Diseño e implementación de un prototipo que permita telefonía IP, servicio de acceso a Internet, video vigilancia y geolocalización, en una unidad articulada del sistema de transporte Río Coca – Aeropuerto,» 05 Enero 2018. [En línea]. Available: http://bibdigital.epn.edu.ec/handle/15000/19151. [Último acceso: 25 Agosto 2019].

[41] Standards Informant, «Standards Informant,» [En línea]. Available: https://blog.siemon.com/standards/ansitia-568-c-1-commercial-building. [Último acceso: 18 Septiembre 2019].

[42] Hikvision, «NVR DS-7716/32NI-E4,» [En línea]. Available: https://www.montersi.pl/pliki/ds-7716ni-e4-karta-17834.pdf. [Último acceso: 20 Septiembre 2019].

[43] Western Digital, «Hoja de Datos de WD Purple,» [En línea]. Available: https://media.flixcar.com/f360cdn/Western_Digital-3807284878-esn_spec_data_sheet_2879-800012.pdf. [Último acceso: 20 Septiembre 2019].

[44] Cisco, «Hoja de Datos Switch serie 200,» [En línea]. Available: https://www.cisco.com/c/dam/en/us/products/collateral/switches/small-business-100-series-unmanaged-switches/data_sheet_c78-634369_Spanish.pdf. [Último acceso: 21 Septiembre 2019].

[45] College, Diseño de la WLAN de Wheelers Lane Technology, «Power-over-Ethernet,» [En línea]. Available: (Power Sourcing Equipment. [Último acceso: 15 Septiembre 2019].

[46] TP-LINK, «TP-LINK,» [En línea]. Available: https://www.tp-link.com/es/home-networking/wifi-router/archer-c7/. [Último acceso: 18 Septiembre 2019].

[47] Standard Informant, «ANSI/TIA-606-C: Administration Standard for Telecommunications Infrastructure,» [En línea]. Available: https://blog.siemon.com/standards/ansitia-606-c-administration-standard-

for-telecommunications-infrastructure. [Último acceso: 22 Septiembre 2019].

[48] Shiraki. Mitugi, «Almacenamiento y Ancho de Banda,» de *Seguridad Electrónica CCTV*, 2018, pp. 49-55.

[49] «WhatsApp, Telegram o Messenger,» 03 Septiembre 2019. [En línea]. Available: https://www.movilzona.es/2017/05/08/whatsapp-telegram-o-messenger-que-app-consume-mas-datos/. [Último acceso: 08 Mayo 2017].

[50] Juan. Cacuango, «DISEÑO DE UNA RED WIFI PARA PROVEER SERVICIO DE INTERNET INALÁMBRICO EN LA ZONA URBANA NORTE DEL CANTÓN CAYAMBE,» [En línea]. Available: http://repositorio.utn.edu.ec/bitstream/123456789/5991/3/ART%C3%8DCULO.pdf. [Último acceso: 10 Septiembre 2019].

[51] José. Murillo, «Diseño e implantación de una red inalámbrica unificada en el Colegio Nuestra Señora de Fátima de Valencia,» 2015. [En línea]. Available: https://riunet.upv.es/bitstream/handle/10251/57385/MURILLO%20-%20Dise%C3%B1o%20e%20implantaci%C3%B3n%20de%20una%20red%20inal%C3%A1mbrica%20unificada%20en%20el%20Colegio%20Nuestra%20Se%C3%B1ora%20de%20....pdf?sequence=1. [Último acceso: 15 Septiembre 2019].

[52] XIRRUS, «Xirrus XR-630 Wireless Access Point,» [En línea]. Available: https://www.bluechipit.com.au/media/product_spec/XIRRUS_XR630_041414.pdf. [Último acceso: 16 Septiembre 2019].

ANEXOS

ANEXO A

DATASHEET DE RASPBERRY PI 3B+

Specifications

Processor	Broadcom BCM2387 chipset. 1.2GHz Quad-Core ARM Cortex-A53 802.11 b/g/n Wireless LAN and Bluetooth 4.1 (Bluetooth Classic and LE)
GPU	Dual Core VideoCore IV® Multimedia Co-Processor. Provides Open GL ES 2.0, hardware-accelerated OpenVG, and 1080p30 H.264 high-profile decode. Capable of 1Gpixel/s, 1.5Gtexel/s or 24GFLOPs with texture filtering and DMA infrastructure
Memory	1GB LPDDR2
Operating System	Boots from Micro SD card, running a version of the Linux operating system or Windows 10 IoT
Dimensions	85 x 56 x 17mm
Power	Micro USB socket 5V1, 2.5A

Connectors:

Ethernet	10/100 BaseT Ethernet socket
Video Output	HDMI (rev 1.3 & 1.4 Composite RCA (PAL and NTSC)
Audio Output	Audio Output 3.5mm jack, HDMI USB 4 x USB 2.0 Connector
GPIO Connector	40-pin 2.54 mm (100 mil) expansion header: 2x20 strip Providing 27 GPIO pins as well as +3.3 V, +5 V and GND supply lines
Camera Connector	15-pin MIPI Camera Serial Interface (CSI-2)
Display Connector	Display Serial Interface (DSI) 15 way flat flex cable connector with two data lanes and a clock lane
Memory Card Slot	Push/pull Micro SDIO

Key Benefits

- Low cost
- 10x faster processing
- Consistent board format
- Added connectivity

Key Applications

- Low cost PC/tablet/laptop
- Media centre
- Industrial/Home automation
- Print server
- Web camera
- Wireless access point
- IoT applications
- Robotics
- Server/cloud server
- Security monitoring
- Gaming
- Environmental sensing/monitoring (e.g. weather station)

Figura A. 1. *Características técnicas de Raspberry Pi 3B+.*

ANEXO B

DATASHEET CÁMARA IP HIKVISION

Camera	
Image Sensor	1/3" progressive scan CMOS
Min. Illumination	Color: 0.01Lux @(F1.2,AGC ON),0 Lux with IR
Shutter Speed	1/3s to 1/100,000 s, support slow shutter
Lens	2.8 mm @F2.0, horizontal field of view 105.8°, 4 mm @F2.0, horizontal field of view 83.6° 6 mm @F2.0, horizontal field of view 55°
Lens Mount	M12
Day &Night	IR cut filter with auto switch
3-Axis Adjustment (Bracket)	Pan: 0° to 360°, tilt: -90°to 90°, rotation:0° to 360°
DNR(Digital Noise Reduction)	3D DNR
WDR (Wide Dynamic Range)	Digital WDR
Compression Standard	
Video Compression	Main stream:H.264+/H.264 Sub stream: H.264/MJPEG
H.264 Type	Main Profile/High profile
Video Bit Rate	32 Kbps to16 Mbps
Image	
Max. Resolution	2688 × 1520
Main Stream Max. Frame Rate	50Hz:20fps @(2688 × 1520),20fps @(2304 × 1296),25fps @(1920 × 1080, 1280 × 720) 60Hz: 20fps @(2688 × 1520),20fps @(2304 × 1296), 30fps @(1920 × 1080, 1280 × 720)
Sub-stream Max. Frame Rate	50Hz: 25fps @(640 × 360, 352 × 288) 60Hz: 30fps @(640 × 360, 352 × 240)
Image Settings	Brightness, saturation, contrast, sharpness are adjustable via web browser or client software
Day/Night Switch	Support auto, scheduled
Others	Mirror, BLC (area configurable), region of interest (support 1 fixed region)
Network	
Network Storage	NAS (NFS,SMB/CIFS)
Detections	Motion detection
Alarms	Video tampering, network disconnected, IP address conflicted
Protocols	TCP/IP,ICMP,HTTP,HTTPS,FTP,DHCP,DNS,DDNS,RTP,RTSP,RTCP, NTP,UPnP,SMTP,SNMP,IGMP,802.1X,QoS,IPv6,Bonjour
Standard	ONVIF(PROFILE S,PROFILE G),PSIA,CGI,ISAPI
General Function	Anti-flicker, heartbeat, mirror, password protection, privacy mask, watermark, IP address filter
Interface	
Communication Interface	1 RJ45 10M/100M self-adaptive Ethernet port
General	
Operating Conditions	-30 °C to60 °C (-22 °F to140 °F), humidity: 95% or less (non-condensing)
Power Supply	12 VDC ± 25%, PoE (802.3af)
Power Consumption	Max. 5 W/6.5 W (PoE)
Ingress Protection	IP67
IR Range	Up to 30 m
Dimensions	69.1 mm ×66 mm × 172.7 mm (2.7"× 2.6"× 6.8")
Weight	500 g (1.1 lb.)

Figura B. 1. *Características técnicas de cámara Hikvision DS-2CD1041-I*

ANEXO C

DATASHEET SWITCH CISCO SG200-10FP

Función	Descripción
Estándares	IEEE 802.3 10BASE-T, Ethernet IEEE 802.3u 100BASE-TX Fast Ethernet, IEEE 802.3ab 1000BASE-T Gigabit Ethernet, IEEE 802.3ad LACP, IEEE 802.3z Gigabit Ethernet, Control de flujo IEEE 802.3x, IEEE 802.1D (STP), IEEE 802.1Q/p VLAN, IEEE 802.1w RSTP, Autenticación de acceso de puerto IEEE 802.1X, IEEE 802.3af, RFC 768, RFC 783, RFC 791, RFC 792, RFC 793, RFC 813, RFC 879, RFC 896, RFC 826, RFC 854, RFC 855, RFC 856, RFC 858, RFC 894, RFC 919, RFC 922, RFC 920, RFC 950, RFC 951, RFC 1042, RFC 1071, RFC 1123, RFC 1141, RFC 1155, RFC 1350, RFC 1533, RFC 1541, RFC 1542, RFC 1624, RFC 1700, RFC 1867, RFC 2030, RFC 2616, RFC 2131, RFC 2132, RFC 3164, RFC 2618
IPv6	
IPv6	Modo host IPv6 IPv6 por Ethernet Pila dual IPv6/IPv4 Detección de router y vecinos IPv6 (ND) Configuración automática de dirección sin estado IPv6 Detección de unidad máxima de transmisión (MTU) de ruta Detección de dirección duplicada (DAD) Protocolo de mensajes de control de Internet (ICMP) versión 6 Red IPv6 por IPv4 compatible con el protocolo de direccionamiento automático de túnel dentro de un sitio (ISATAP)
Calidad de servicio de IPv6	Prioriza los paquetes IPv6 en el hardware
Detección Multicast Listener Discovery (MLD)	Entrega paquetes multidifusión IPv6 solo a los receptores requeridos
Aplicaciones IPv6	Web, ping, protocolo simple de tiempo de red (SNTP), protocolo trivial de transferencia de archivos (TFTP), RADIUS, syslog, cliente DNS
Compatibilidad con RFC IPv6	RFC 2463: ICMP versión 6 RFC 3513: arquitectura de direcciones IPv6 RFC 4291: arquitectura de direcciones IPv6 RFC 2460: especificación de IPv6 RFC 2461: detección de vecinos para IPv6 RFC 2462: configuración automática de dirección sin estado de IPv6 RFC 1981: detección de unidad máxima de transmisión (MTU) de ruta RFC 4007: arquitectura de direcciones definidas IPv6 RFC 3484: mecanismo de selección de direcciones predeterminadas RFC 4214: túnel ISATAP RFC 4293: MIB IPv6: convenciones textuales y grupo general RFC 3595: convenciones textuales para etiquetas de flujo IPv6
Administración	
Interfaz de usuario web	Utilidad de configuración de switch integrada para facilitar la configuración de dispositivos basada en la web (HTTP). Admite configuración, tablero del sistema, mantenimiento del sistema y supervisión
Protocolo simple de administración de redes (SNMP)	SNMP versiones 1, 2c y 3 compatibles con capturas y modelo de seguridad basado en el usuario para SNMP versión 3

Figura C. 1. *Características Técnicas de Switch modelo SG200-10FP*

ANEXO D

PLANOS DISEÑO DE SISTEMA DE VIDEO VIGILANCIA IP

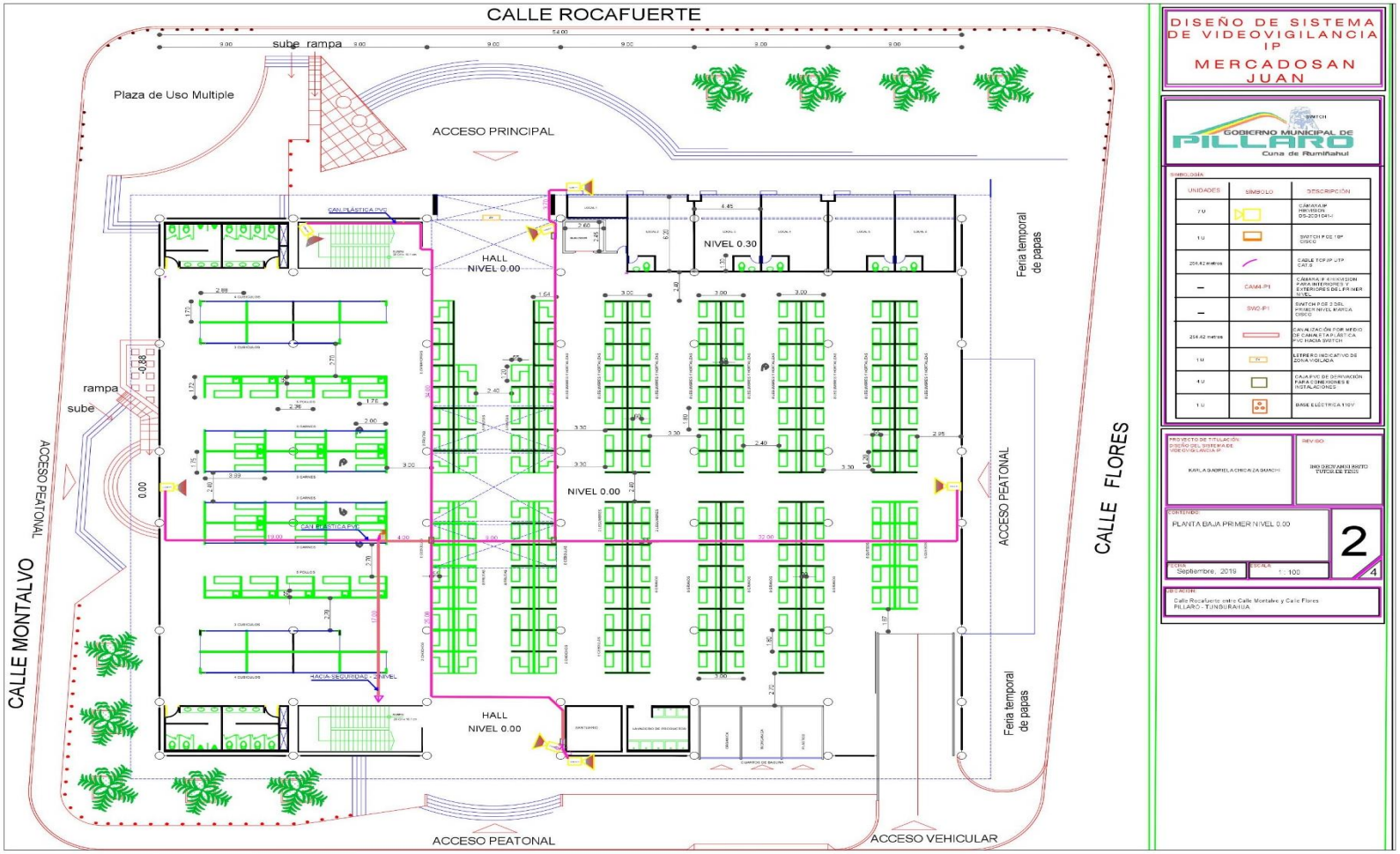


Figura D. 1. *Plano Sistema Video Vigilancia IP. Primer Nivel*

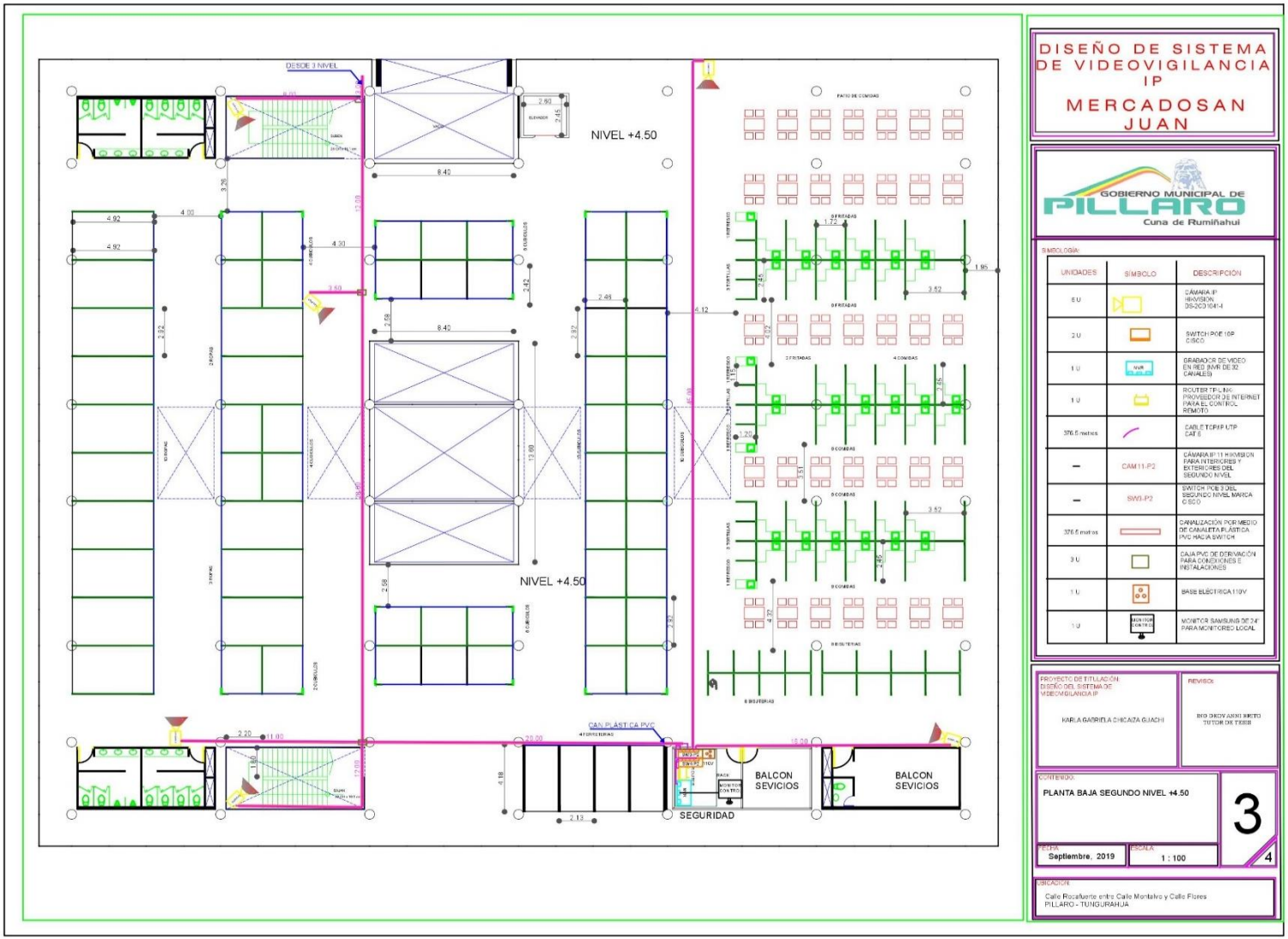


Figura D. 2. *Plano Sistema Video Vigilancia IP. Segundo Nivel.*

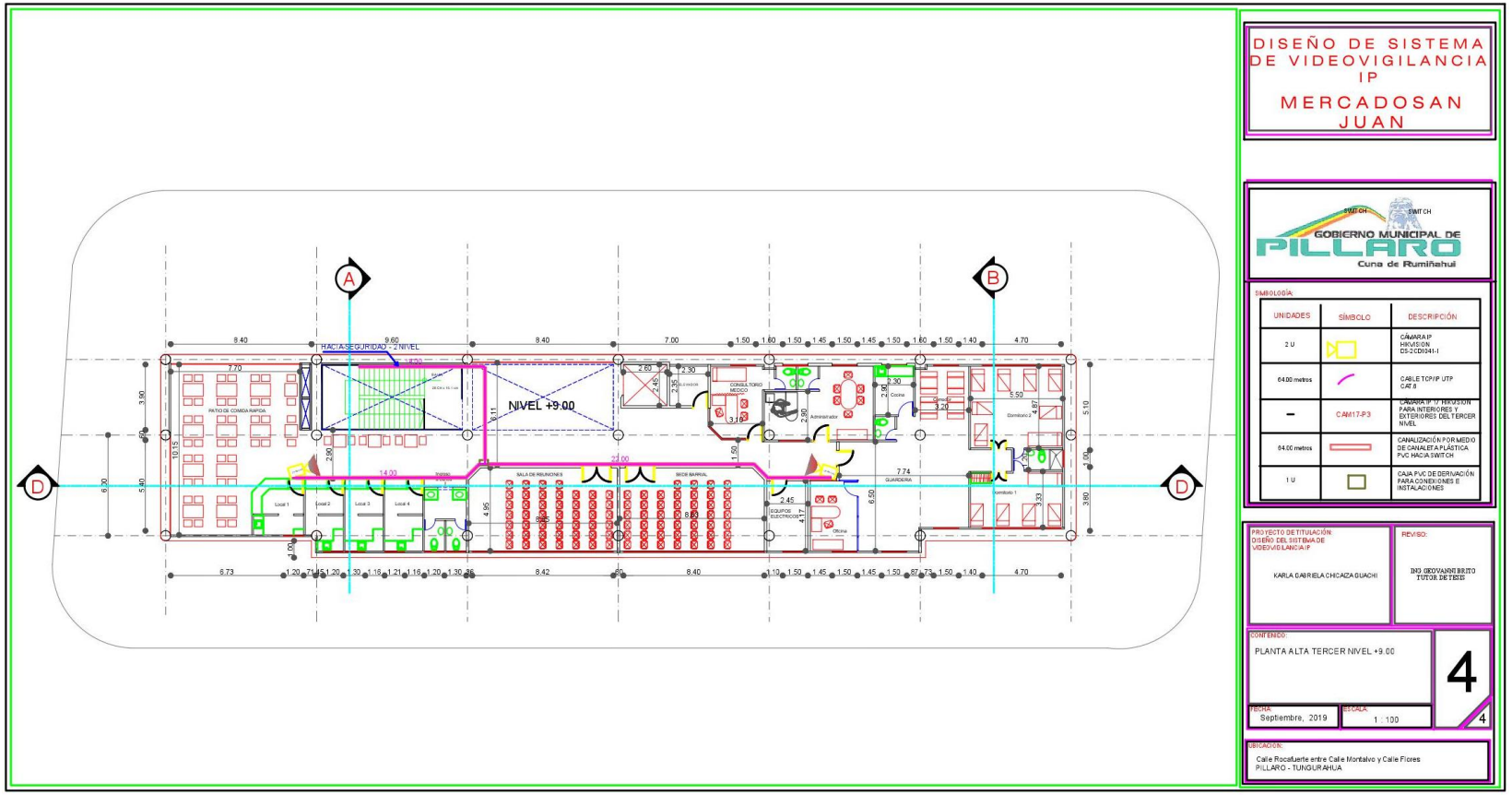


Figura D. 3. *Plano Sistema Video Vigilancia IP. Tercer Nivel*

ANEXO E

SIMULACIÓN DE COBERTURA WIFI SOFTWARE XIRRUS

En la figura E.1 se observa como el simulador muestra la colocación de dos Access point, para cubrir toda el área requerida; además en este nivel al igual que en el segundo nivel, se tiene más cantidad de usuarios fijos y visitantes, llegando a la conclusión que es adecuado colocar dos equipos.

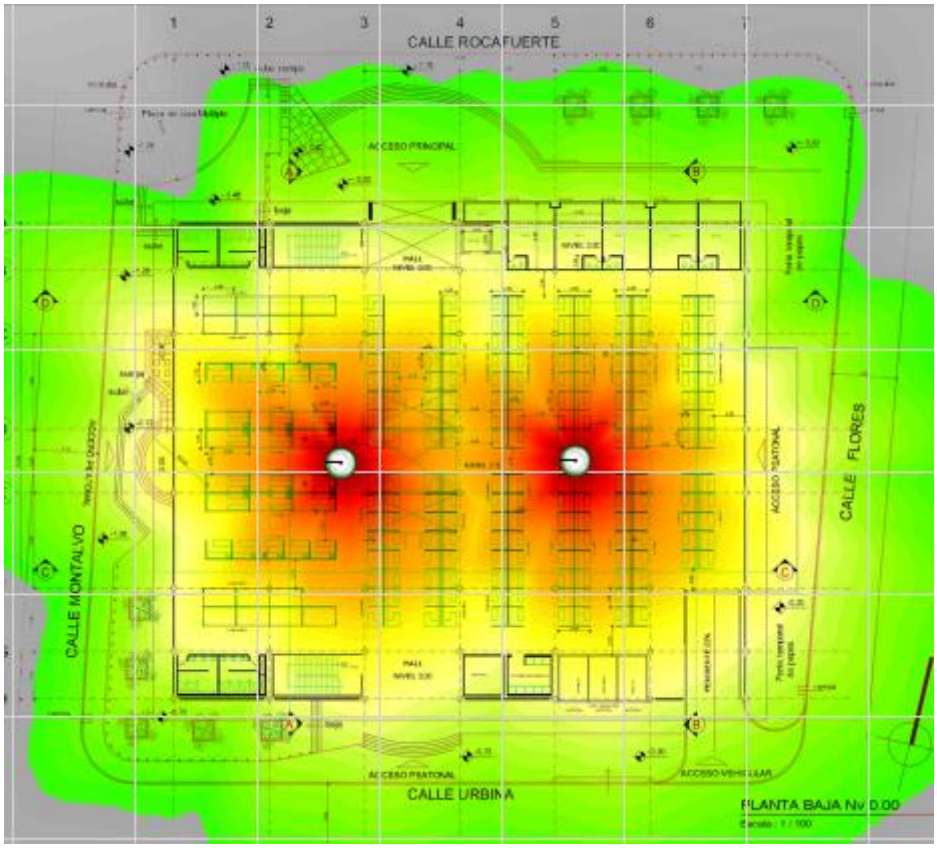


Figura E. 1. *Simulación de cantidad de Access Point por cobertura. Software XIRRUS Primer Nivel.*

En la figura E.2 se observa el área de cobertura de la señal inalámbrica simulada, en base a la ubicación de tres Access point, debido a que es un área en donde existe mayor cantidad de obstáculos (paredes y cubículos de hormigón), con este número de equipos se certifica la calidad de la señal en todo el nivel.

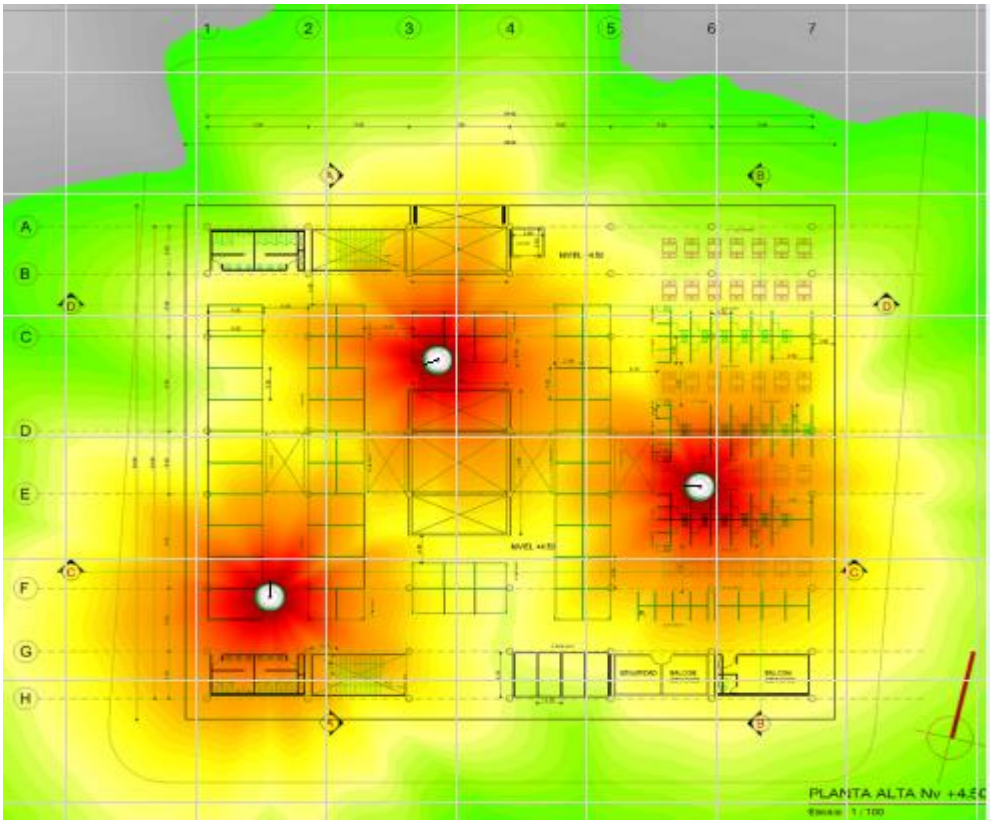


Figura E. 2. *Simulación de cantidad de Access Point por cobertura. Software XIRRUS Segundo Nivel.*

En la figura E.3 se observa la ubicación de dos Access point, que cubren toda el área requerida. Cabe destacar que es un área más administrativa, por ende es necesario que todos los usuarios tengan buena calidad de señal.

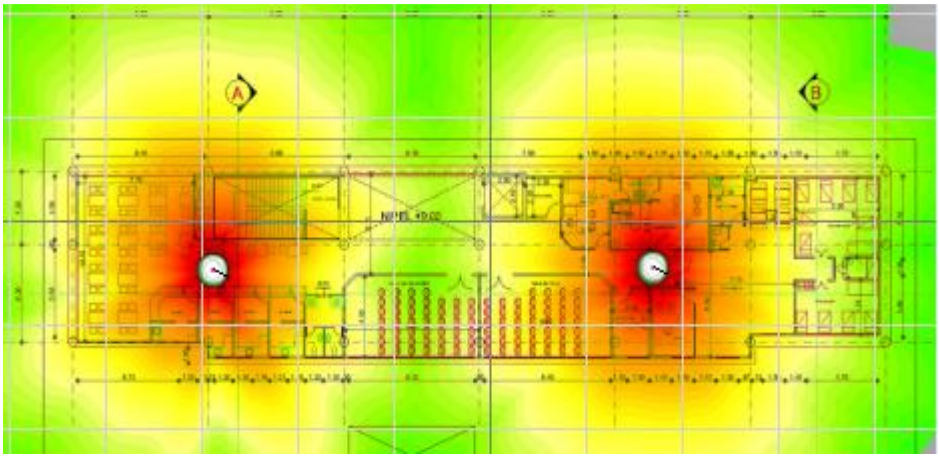


Figura E. 3. *Simulación de cantidad de Access Point por cobertura. Software XIRRUS Tercer Nivel.*

ANEXO F

PLANOS DISEÑO RED WIFI

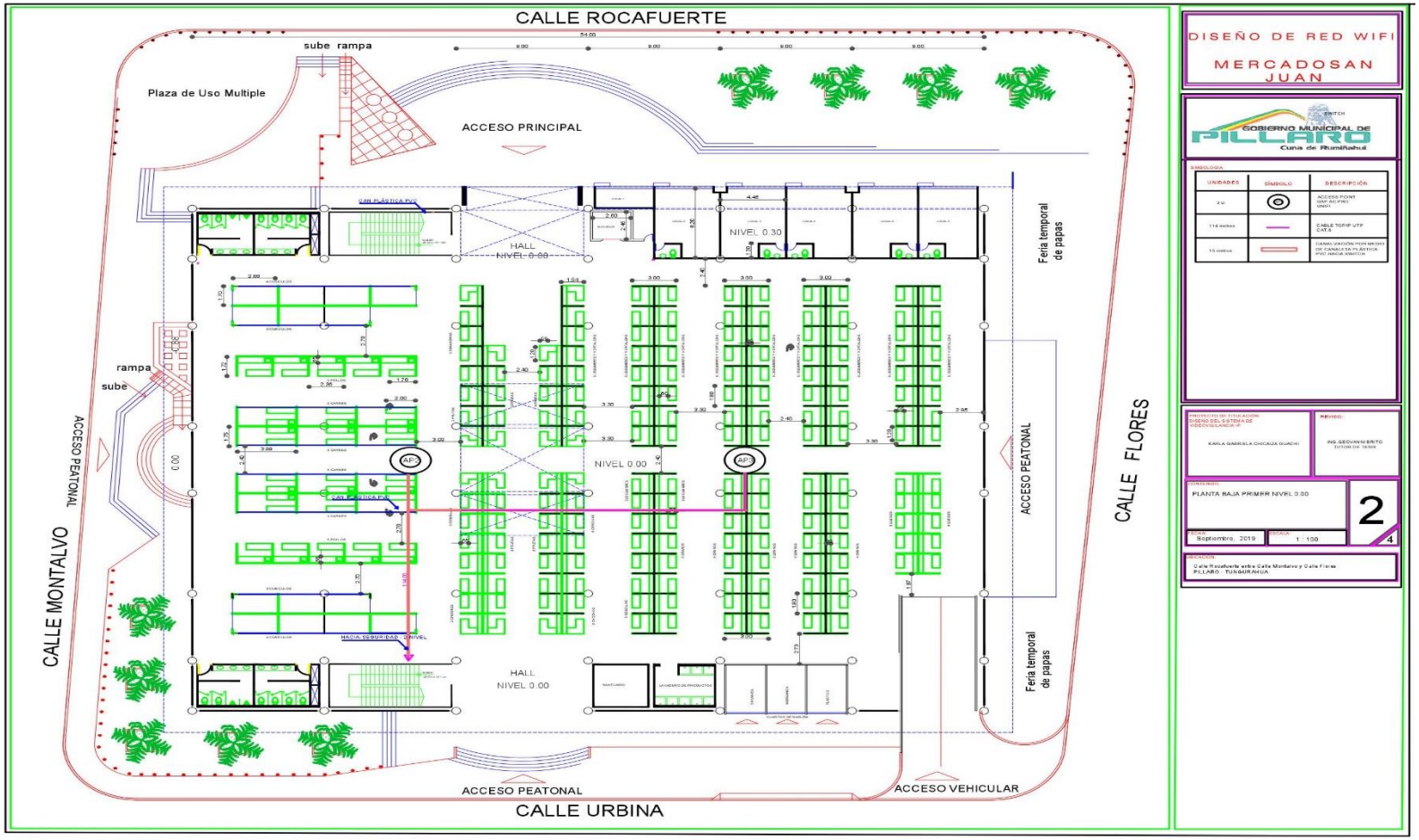


Figura F. 1. *Plano Diseño de Red Wifi Primer Nivel.*

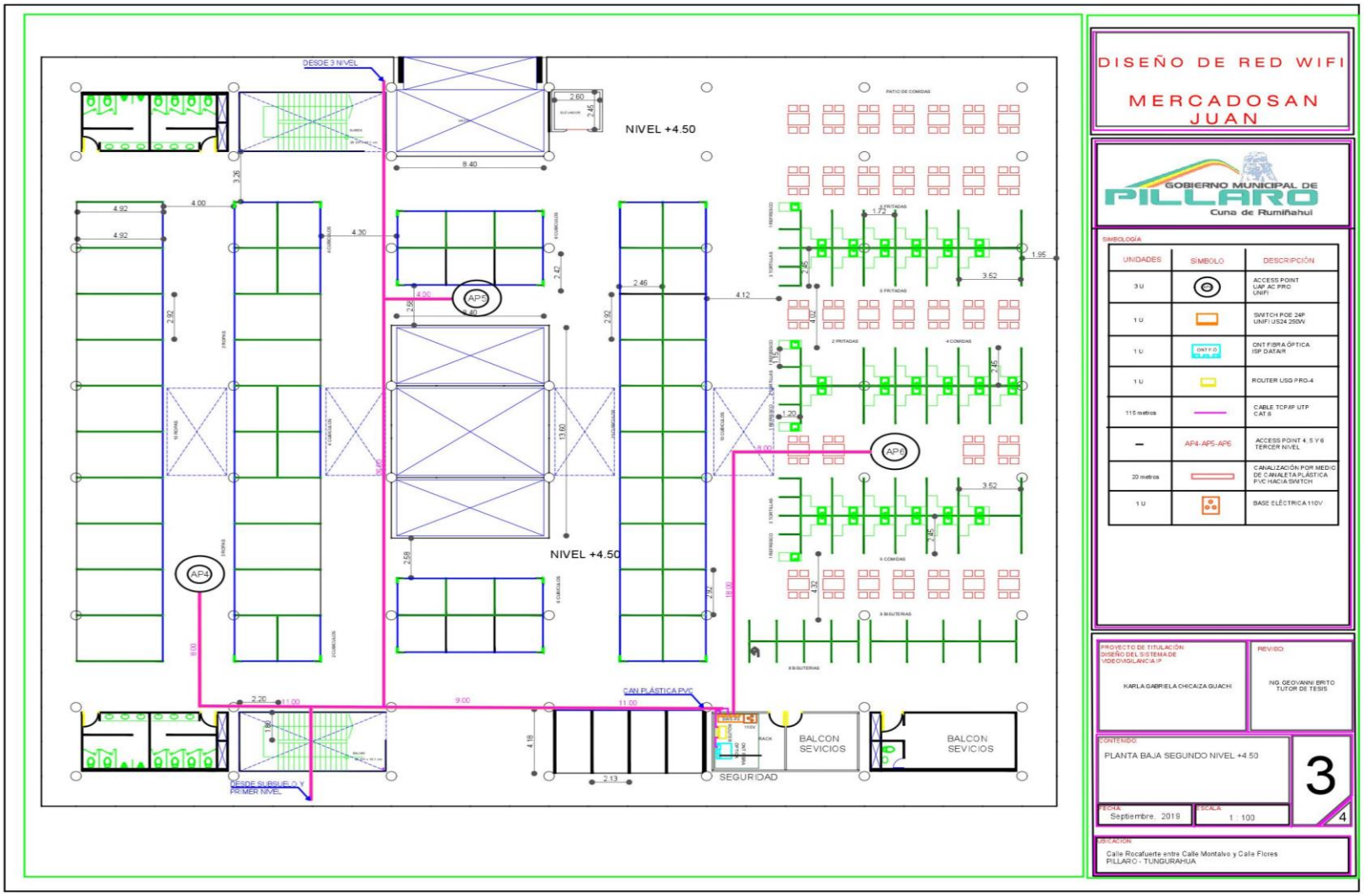


Figura F. 2. *Plano Diseño de Red Wifi Segundo Nivel.*

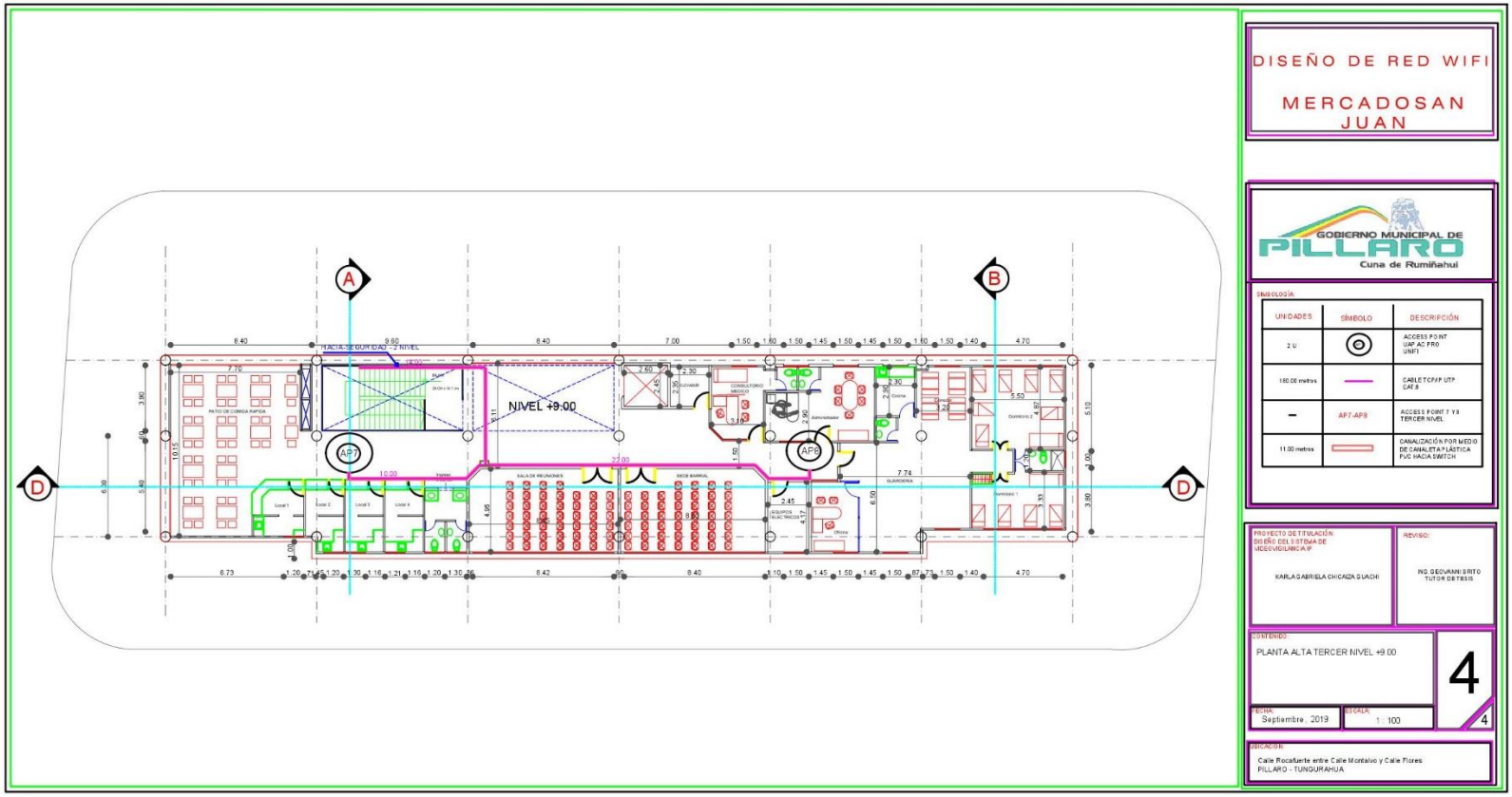


Figura F. 3. *Plano Diseño de Red Wifi Tercer Nivel.*

ANEXO G

PROGRAMACIÓN DEL SISTEMA

Archivo app.py

```
from flask import Flask, render_template, request,
send_from_directory, Response
from gevent.pywsgi import WSGIServer
from gevent.pool import Pool


from twilio.rest import Client
import gevent

import pickle
import json
import cv2
import random
import string
import datetime
import threading
import time
import urllib.request
import urllib.parse
import numpy as np
import shutil
import requests

from gpiozero import LED

#pin para encender o apagar sirena
pinAlarma = LED(17)
os.environ["OPENCV_FFMPEG_CAPTURE_OPTIONS"]                    =
"rtsp_transport;udp"

account_sid = "xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx"
auth_token = "xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx"

client = Client(account_sid, auth_token)

if os.path.exists('data.pickle'):
    print('Leyendo Db')
    with open('data.pickle', 'rb') as f:
        db = pickle.load(f)
    print('db Cargada')
else:
    db = {}
    db['usuarios'] = {}
    db['camaras'] = {}
    db['saveFolder'] = ''
    db['adminKey'] = '123456'
```

```
    db['alarma'] = True
    db['numerosEmergencia'] = []
    db['rango1'] = '18:00'
    db['rango2'] = '06:00'
    db['log'] = ''
    db['size']=4000
    db['correoAdministrador'] = ''
    db['passwordCorreo'] = ''
    db['idUPC'] = ''
    db['correoApp'] = ''
    dbfile = open('data.pickle', 'ab')
    pickle.dump(db, dbfile)
    dbfile.close()
    print('db creada')

def randomString(stringLength=10):
    """Generate a random string of fixed length """
    letters = string.ascii_lowercase
    return    ''.join(random.choice(letters)    for    i    in
range(stringLength))

app = Flask(__name__, static_url_path='')
videoSRCS = {}

class telegramHandler(object):
    def __init__(self, bottoken):
        self.bottoken = bottoken
        self.actualizaciones = []
        self.loadAlertas()
        self.execute = True
        self.thread1                                          =
threading.Thread(target=self.checkAlertas)
        self.thread1.start()

    def sendMessage(self, mensajeTelegram, sendID):
        threadsm                                              =
threading.Thread(target=self.sendMessagethread(mensajeTelegram
, sendID))
        threadsm.start()
        print('send msj')



    def sendImage(self, image, sendID):
        threadsim                                             =
threading.Thread(target=self.sendImagethread(image, sendID))
        threadsim.start()

    def sendImagethread(self,image,sendId):
        print('sendImage')
        imjurl                                                =
'https://api.telegram.org/bot'+self.bottoken+'/sendPhoto'
        ims = cv2.imencode('.jpg',image)[1].tobytes()
```

```
        multipart_form_data = {
            'photo': ('imagen.jpg', ims),
        }
        otherDict={'chat_id': sendId,}
        response                        =requests.post(imjurl,
data=otherDict,files=multipart_form_data)
```

Programación de archivo de video y captura de imagen

```
createVideopath()

alejecutada = False
alarmatiempo = datetime.datetime.now()
sospechaEjecutada = False
sospechatiempo = datetime.datetime.now()
m10 = datetime.timedelta(seconds=300)
pinAlarma.off()
alarmaEncendida=False

def alarma(logmensaje='',imagen=''  ):
    global alejecutada
    global alarmatiempo
    global alarmaEncendida
    if  (datetime.datetime.now()  >  alarmatiempo+m10)  or  not
alejecutada   :

telegram.sendMessage('mensajeUpc:'+logmensaje,db['idUPC'])
        if imagen!='':
            telegram.sendImage(imagen,db['idUPC'])
            cv2.imwrite('imagenSend.jpg', imagen)
            yag        =        yagmail.SMTP(db['correoApp'],
db['passwordCorreo'])
            yag.send(db['correoAdministrador'], 'Correo Alarma
Comunitaria', [logmensaje,'imagenSend.jpg'])

        for item in db['numerosEmergencia']:
            if item[0] == 'telegram':
                telegram.sendMessage(logmensaje, item[1])
                if imagen!='':
                    print('enviaImagen')
                    telegram.sendImage(imagen, item[1])
            if item[0]=='whatsapp':
                numerowhats='whatsapp:+'+item[1]
                mensajewhatsapp = client.messages.create(
                    to=numerowhats,
                    from_='whatsapp:+14155238886',
                    body=logmensaje)
        print('Alarma Ejecutada')
        pinAlarma.on()
        alejecutada = True
        alarmatiempo = datetime.datetime.now()
        agregarLog(logmensaje)
        alarmaEncendida=True
```

Programación de mensaje Alerta

```
def sospecha(logmensaje=''):
    global sospechaEjecutada
    global sospechatiempo
    if (datetime.datetime.now() > sospechatiempo+m10 )  or not
sospechaEjecutada :
        for item in db['numerosEmergencia']:
            if item[0] == 'telegram':
                telegram.sendMessage(logmensaje, item[1])
            if item[0]=='whatsapp':
                numerowhats='whatsapp:+'+item[1]
                mensajewhatsapp = client.messages.create(
                    to=numerowhats,
                    from_='whatsapp:+14155238886',
                    body=logmensaje)

        print('Sospecha Ejecutada')
        sospechaEjecutada = True
        sospechatiempo = datetime.datetime.now()
        agregarLog(logmensaje)
```

Programación Detección de Movimiento

```
        self.background=None
        self.motion=False
        self.execute = True
        self.thread1                                          =
threading.Thread(target=self.motionDetection)
        self.thread1.start()
        self.thread2                                          =
threading.Thread(target=self.imageRefresh)
        self.thread2.start()
        self.tiempoActual=None
        self.d = datetime.datetime(2009, 10, 5, 18, 00)
        self.recording = False
        self.initTime = datetime.datetime(2009, 10, 5, 18, 00)
        self.recordedFrames = 0
        self.framesObject = []
        self.s10 = datetime.timedelta(seconds=10)
        self.frame_width = int(self.camera.get(3))
        self.frame_height = int(self.camera.get(4))
        self.servingUrls=[]


    def get_frame(self):
        self.rimage           =           cv2.imencode('.jpg',
self.imagen)[1].tobytes()
        return self.rimage

    def motionDetection(self):
        while self.execute:
            imStatic=self.imagen
```

```
            gray = cv2.cvtColor(imStatic, cv2.COLOR_BGR2GRAY)
            gray = cv2.GaussianBlur(gray, (21, 21), 0)
            if self.background is None:
                self.background=gray
            else:
                self.background                                    =
cv2.addWeighted(self.background,0.95,gray,0.05,0.0)
            diff_frame = cv2.absdiff(self.background, gray)
            changeValue = 0
            for item in cv2.mean(diff_frame):
                changeValue += item*item
            if self.imagenes < 50:
                self.imagenes+=1
                changeValue=0


rango1      =      datetime.datetime(2015,      12,      1,
int(db['rango1'].split(':')[
                                          0]),
int(db['rango1'].split(':')[1])).time()
                rango2   =   datetime.datetime(2015,   12,   1,
int(db['rango2'].split(':')[
                                          0]),
int(db['rango2'].split(':')[1])).time()
                condicion1 = rango1 < now
                condicion2 = rango2 > now
                if condicion1 | condicion2:
                    alarma(str(datetime.datetime.now()) +
                           ',Alarma activada por deteccion de
movimiento \n',imStatic)
            else:
                self.motion=False
            time.sleep(0.05)

    def imageRefresh(self):
        while self.execute:
            self.ri=False
            _, self.imagen = self.camera.read()
            #if len(self.servingUrls)>0:
            #           self.rimage   =   cv2.imencode('.jpg',
self.imagen)[1].tobytes()
            self.ri=True
            self.tiempoActual=datetime.datetime.now()
            if  self.motion  or  (self.tiempoActual  <  self.d  +
self.s10):
                self.framesObject.append(self.imagen)
                self.recordedFrames += 1
                self.recording=True
                if self.recordedFrames>1000:
                    thread3                                        =
threading.Thread(target=self.grabar)
                    thread3.start()
            elif self.recording:
```

```
                self.recording=False
                thread3 = threading.Thread(target=self.grabar)
                thread3.start()
```

Programación de método GET y POST para ingreso y envío de datos através de página web

```
getCamaras()

@app.route('/', methods=['GET', 'POST'])
def index():
    if flask.request.method == "GET":
        return render_template('index.html')
    if flask.request.method == "POST":
        pswd = flask.request.form['pswd']
        usuario = flask.request.form['Usuario']
        if usuario in db['usuarios']:
            if db['usuarios'][usuario] != pswd:
                return 'contraseña incorrecta'
        else:
            return 'usuario no existe'
        if flask.request.form['accion'] == 'pswd':
            return 'correcta'
        elif flask.request.form['accion'] == 'gVideo':
            returnVideoData = {}
            for camarad in db['camaras']:
                urlgen = randomString(32)
                videoSRCS[urlgen]          =          [camarad,
datetime.datetime.now(),True]
                returnVideoData[camarad] = urlgen
            return json.dumps(returnVideoData)

        elif flask.request.form['accion'] == 'activaAlarma':
            alarma(str(datetime.datetime.now()) +
                   ',Alarma      activada      por      usuario
web:'+usuario+' \n')
            return ''
        elif flask.request.form['accion'] == 'apagaAlarma':
            alarmaApagar(str(datetime.datetime.now()) +
                         ',Alarma    apagada    por    usuario
web:'+usuario+' \n')
            return ''
        elif flask.request.form['accion'] == 'mAlerta':
            sospecha(str(datetime.datetime.now()) +
                     ',Alerta     activada     por     usuario
web:'+usuario+' \n')
            return ''
        elif flask.request.form['accion'] == 'getLog':
            return db['log']
        elif flask.request.form['accion']=='keeplive':
            videoSRCS[flask.request.form['urlofCam']][1]=
datetime.datetime.now()
            return 'ok'
```

```
        return 'post /'

def gen(urlofCam):
    thiscamara = videoSRCS[urlofCam][0]
    s10=datetime.timedelta(seconds=10)
    camaras[thiscamara].servingUrls.append(urlofCam)
    while videoSRCS[urlofCam][2]:
        frame = camaras[thiscamara].get_frame()
        if              datetime.datetime.now()              >
videoSRCS[urlofCam][1]+s10:
            videoSRCS[urlofCam][2]=False
            camaras[thiscamara].servingUrls.remove(urlofCam)
        gevent.sleep(0.04)
        yield (b'--frame\r\n'
               b'Content-Type:  image/jpeg\r\n\r\n'  +  frame  +
b'\r\n')


@app.route('/video_feed/<urlgen>')
def video_feed(urlgen):
    return Response(gen(urlgen),
                    mimetype='multipart/x-mixed-replace;
boundary=frame')


@app.route('/static/<path:path>')
def send_js(path):
    return send_from_directory('static', path)
```

Programación del servidor mediante asignación de IP mas Puerto de escucha, usando WSGI

```
# app.run(debug=True)

pool=Pool(10)

http_server = WSGIServer(('0.0.0.0', 8080), app,spawn=pool)
http_server.serve_forever()
```

ANEXO H

INSTALACIÓN Y PRUEBAS DE FUNCIONAMIENTO DEL PROTOTIPO

Figura H. 1. *Instalación del prototipo en el Local N°01 del mercado San Juan.*

Figura H. 2. *Prototipo Sistema de Alarma Comunitaria Implementado.*

Figura H. 3. *Usuarios agregados al chat Telegram SanJuanSegura.*

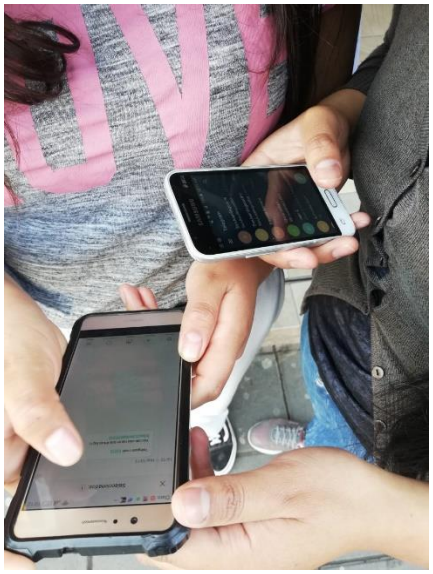


Figura H. 4. *Instalación de mensajería Telegram a usuarios del mercado.*

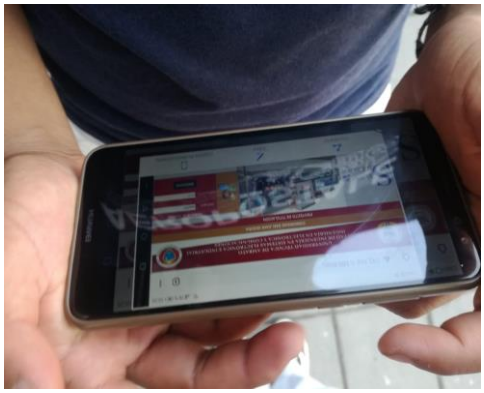


Figura H. 5. *Ingreso a página web del Sistema de Alarma Comunitaria por teléfono Huawei.*

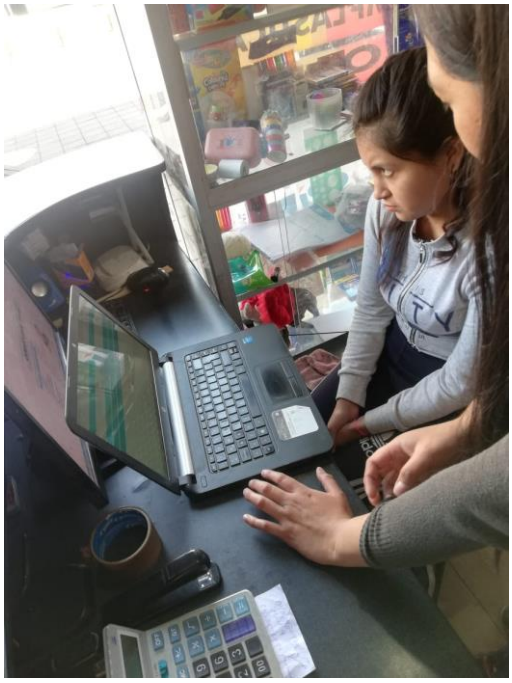


Figura H. 6. *Ingreso a página web del Sistema de Alarma Comunitaria usando Laptop.*

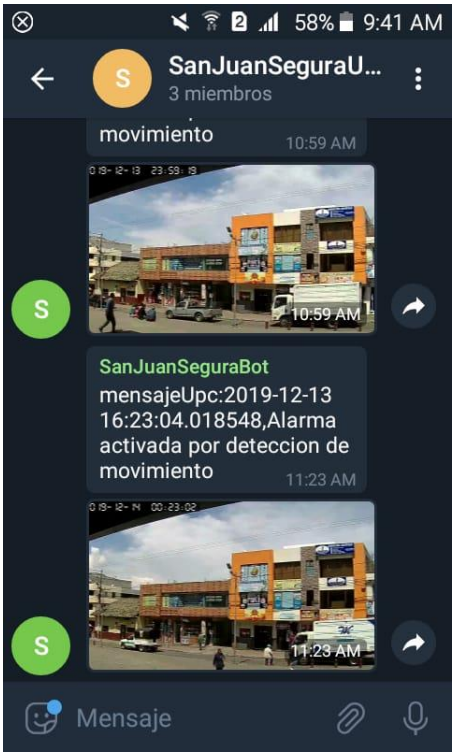


Figura H. 7. *Notificación de Alarmas a la UPC central del cantón.*

Figura H. 8. *Envío y notificación de Alertas y Alarmas a usuarios del mercado.*

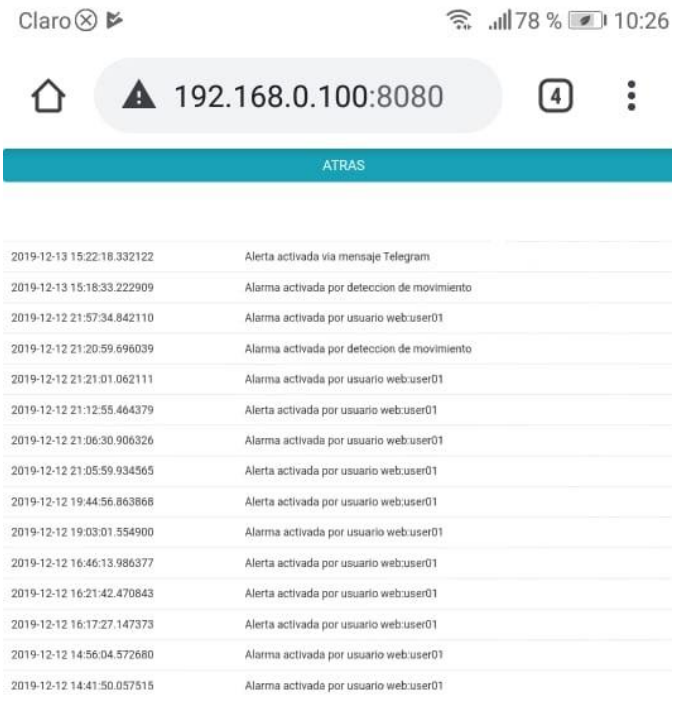


Figura H. 9. *Historial de alarmas emitidas a los diferentes usuarios.*

ANEXO I

ACTA DE IMPLEMENTACIÓN DEL PROTOTIPO

GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL
DEL CANTÓN SANTIAGO DE PÍLLARO

RUC. 1860000720001

Nº 110081

PAPEL OFICIO

ESPECIE VALORADA USD. 1.50

Píllaro 13 de Diciembre del 2019

Ingeniera Mg.

Pilar Urrutia Urrutia

DECANA

Facultad de Tecnologías de la Información, Telecomunicaciones e Industrial

Presente

Señora Decana:

Yo, Enith Lorena Campaña Tamayo en mi calidad de Administradora de Mercados del GADM Santiago de Píllaro, portadora de la Cédula de Identidad No. 1805508023, manifiesto que el prototipo del "Sistema de Alarma Comunitaria para el Mercado San Juan de la ciudad Santiago de Píllaro", ha sido instalado en el local N°01, principalmente por el acceso a internet, local que se encuentra a cargo del Sr. Luis Chimborazo con Cédula de Identidad No.1803837614, el prototipo se encuentra funcionando correctamente con la página web de monitoreo diseñada para el sistema, en conjunto con los planos del diseño de la Red Wifi y Sistema de Video Vigilancia IP, dando cumplimiento al Proyecto de Investigación realizado por la Srta. Karla Chicaiza, portadora de la Cédula de Identidad N° 1805508023, estudiante de Décimo nivel de la Carrera de Ingeniería en Electrónica y Comunicaciones.

Atentamente

Enith Lorena Campaña Tamayo
C.I. 1802406437
Tutora Empresarial

GAD. MUNICIPAL SANTIAGO DE PILLARO
TESORERIA

IMPJGM.05-19.pe

Figura I. 1. *Acta de Implementación del prototipo en el mercado San Juan.*