UNIVERSIDAD NACIONAL DE CHIMBORAZO
FACULTAD DE INGENIERÍA
CARRERA ELECTRÓNICA Y TELECOMUNICACIONES

Título: Implementación de una plataforma IOT integrada a la alarma comunitaria para reforzar la seguridad en el barrio La Merced de Yaruquies de la ciudad de Riobamba

Trabajo de Titulación para optar al título de Ingeniera en Electrónica y Telecomunicaciones

Autor:
Mendoza Sánchez Jessica Mariela

Tutor:
Msc. José Luis Jinez tapia

Riobamba, Ecuador. 2023

DERECHOS DE AUTORÍA

Yo, Jessica Mariela Mendoza Sánchez, con cédula de ciudadanía 172112309-7, autora del trabajo de investigación titulado: Implementación de una plataforma IOT integrada a la alarma comunitaria para reforzar la seguridad en el barrio La Merced de Yaruquies de la ciudad de Riobamba, certifico que la producción, ideas, opiniones, criterios, contenidos y conclusiones expuestas son de mí exclusiva responsabilidad.

Asimismo, cedo a la Universidad Nacional de Chimborazo, en forma no exclusiva, los derechos para su uso, comunicación pública, distribución, divulgación y/o reproducción total o parcial, por medio físico o digital; en esta cesión se entiende que el cesionario no podrá obtener beneficios económicos. La posible reclamación de terceros respecto de los derechos de autora de la obra referida, será de mi entera responsabilidad; librando a la Universidad Nacional de Chimborazo de posibles obligaciones.

En Riobamba, a los 08 días de noviembre de 2023

Jessica Mariela Mendoza Sánchez
C.I:172112309-7

DICTAMEN FAVORABLE DEL TUTOR Y MIEMBROS DE TRIBUNAL

Quienes suscribimos, catedráticos designados Tutor y Miembros del Tribunal de Grado para la evaluación del trabajo de investigación **Implementación de una plataforma IOT integrada a la alarma comunitaria para reforzar la seguridad en el barrio La Merced de Yaruquies de la ciudad de Riobamba**, presentado por **Jessica Mariela Mendoza Sánchez**, con cédula de identidad número 172112309-7, certificamos que recomendamos la APROBACIÓN de este con fines de titulación. Previamente se ha asesorado durante el desarrollo, revisado y evaluado el trabajo de investigación escrito y escuchada la sustentación por parte de su autor; no teniendo más nada que observar.

De conformidad a la normativa aplicable firmamos, en Riobamba 08 de noviembre de 2023

Marlon Danilo Basantes Valverde, PhD.
PRESIDENTE DEL TRIBUNAL DE GRADO

Firma

Antonio Manuel Meneses Freire, PhD.
MIEMBRO DEL TRIBUNAL DE GRADO

Firma

Luis Patricio Tello Oquendo, PhD.
MIEMBRO DEL TRIBUNAL DE GRADO

Firma

José Luis Jinez Tapia, Msc.
TUTOR

Firma

CERTIFICADO DE LOS MIEMBROS DEL TRIBUNAL

Quienes suscribimos, catedráticos designados Miembros del Tribunal de Grado para la evaluación del trabajo de investigación **Implementación de una plataforma IOT integrada a la alarma comunitaria para reforzar la seguridad en el barrio La Merced de Yaruquies de la ciudad de Riobamba,** presentado por Jessica Mariela Mendoza Sánchez, con cédula de identidad número 172112309-7, bajo la tutoría de Msc. José Luis Jinez Tapia; certificamos que recomendamos la APROBACIÓN de este con fines de titulación. Previamente se ha evaluado el trabajo de investigación y escuchada la sustentación por parte de su autor; no teniendo más nada que observar.

De conformidad a la normativa aplicable firmamos, en Riobamba 08 días de noviembre de 2023

Presidente del Tribunal de Grado
PhD. Marlon Danilo Basantes Valverde

Firma

Miembro del Tribunal de Grado
PhD. Antonio Manuel Meneses Freire

Firma

Miembro del Tribunal de Grado
PhD. Luis Patricio Tello Oquendo

Firma

CERTIFICACIÓN

Que, Jessica Mariela Mendoza Sánchez con CC: **172112309-7**, estudiante de la Carrera **Electrónica y Telecomunicaciones, NO VIGENTE,** Facultad de **Ingeniería;** ha trabajado bajo mi tutoría el trabajo de investigación titulado " **Implementación de una plataforma IOT integrada a la alarma comunitaria para reforzar la seguridad en el barrio La Merced de Yaruquíes de la ciudad de Riobamba**", cumple con el 2%, de acuerdo al reporte del sistema Anti plagio **URKUND**, porcentaje aceptado de acuerdo a la reglamentación institucional, por consiguiente autorizo continuar con el proceso.

Riobamba, 01 de noviembre de 2023

Msc. José Luis Jinez Tapia
TUTOR TRABAJO DE INVESTIGACIÓN

DEDICATORIA

Dedico con todo mi corazón este trabajo a mis pequeños hijos, Maickel y Jorge el principal motivo para haber seguido esta lucha constate, muchas veces fueron los que me impulsaban a ponerme de pie y seguir luchando por esta meta, a mi esposo, que ha sido mi principal motor para nunca darme por vencida, con sus consejos y apoyo incondicional me motivó a seguir pese a todas las adversidades, a mi madre que con su apoyo me ha impulsado a seguir adelante, a mi padre que, aunque a la distancia me ha apoyado a ser mejor cada día.

Y a mis hermanos que con sus consejos y apoyo no me han dejado darme por vencida,

Jessica Mariela Mendoza Sánchez

AGRADECIMIENTO

Un agradecimiento profundo a Dios por permitirme llegar hasta este punto de mi vida, rodeada de millón de bendiciones.

Cada día me levantó y le agradezco por tenerme con vida y disfrutar de todas las metas alcanzadas que junto a mi pequeña familia de mis dos hijos y mi esposo hemos construido.

Un agradecimiento inmenso a mi querida Universidad, por permitirme seguir está carrera maravillosa, a cada uno de mis profesores que con su guía he adquirido muchos conocimientos y un especial agradecimiento a mi Tutor Mgs Jose Luis Jinez Tapia por la paciencia y el apoyo prestado para la realización de este trabajo.

Jessica Mariela Mendoza Sánchez

ÍNDICE GENERAL

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

El presente trabajo de titulación trata acerca de la Implementación de una plataforma IOT integrada a la alarma comunitaria para reforzar la seguridad en el barrio La Merced de Yaruquies de la ciudad de Riobamba.

Este proyecto nace a partir de varios delitos que se vinieron cometiendo en este barrio y se inició con un proyecto de resguardo ciudadano, que consistía en realizar rondas durante la noche, esto se realizó durante 1 mes. Transcurrido ese tiempo las personas empezaban a no salir por temor a represarías ya que estos delincuentes vivían cerca de la zona, se instaló una sirena comunitaria que se accionaba mediante un botón, pero la misma al poco tiempo fue desactivada debido al mal uso que se dio, ya que el botón se encontraba en un lugar muy bajo y al alcance de los niños.

Por estos hechos surge la idea de contar con un sistema automatizado, el cual permite tener un control de lo que sucede en la zona las 24 horas del día mediante cámaras de seguridad y en el caso de haber un posible indicio de robo o daño a la propiedad ajena se active la alarma comunitaria desde una aplicación móvil y así evitar riesgos hasta que se puedan concentrar la mayoría de habitantes y la policía de la Parroquia.

El sistema se compone de un conjunto de cuatro cámaras de seguridad integradas en una plataforma para ser administradas y monitoreadas, al mismo tiempo controlar alertas de seguridad y poder accionar una alarma comunitaria mediante la misma aplicación, con autenticación en tiempo real en Firebase para evitar problemas por parte de niños o de usuarios que hagan mal uso de la misma.

La alarma comunitaria se trabajó mediante módulos Esp32, para ser automatizada mediante una aplicación creada en app inventor y por medio de un botón accionarla en cuestión de segundos y alertar a los usuarios de posibles hurtos.

El sistema de video vigilancia se lo realizó mediante la plataforma Motioneye que sirvió para integrar las cuatro cámaras de seguridad y configurarlas de acuerdo a las necesidades requeridas por los usuarios del barrio La Merced. Estas cámaras fueron configuradas para que a partir de las 23:00 hasta las 06:00 emitan alertas con capturas de imágenes. El sistema permanecerá grabando las 24 horas del día en un grabador que en este caso es una Raspberry Pi conectada a un disco Duro Externo de 2 TB.

Palabras claves: Esp32, Motioneye, plataforma, cámaras.

ABSTRACT

The present work focuses on implementing an IOT platform integrated to the community alarm to enhance security in the La Merced neighborhood in Yaruquies in the city of Riobamba.

This project was born from several crimes that were being committed in this neighborhood and began with a citizen protection project, which consisted of making rounds during the night, this was done for 1 month. After that time, people started not to go out for fear of reprisals because these criminals lived near the area. A community siren was installed and activated by a button, but it was soon deactivated due to misuse, as the button was located in a very low place and within reach of children.

For these facts, the idea of having an automated system arises, which allows to have a control of what happens in the area 24 hours a day through security cameras and in the case of a possible indication of theft or damage to the property of others, the community alarm is activated from a mobile application and thus avoid risks until the majority of inhabitants and the police of the parish can be concentrated.
The system comprises four security cameras integrated into a platform for administration and monitoring, simultaneously enabling security alerts and activation of a community alarm through the same application, real-time authentication via Firebase is employed to prevent misuse by children or unauthorized users.

The community alarm was developed using Esp32 modules, to be automated by means of an application created in app inventor and by means of a button to activate it in a matter of seconds and alert users of possible thefts.

The video surveillance system was implemented using the Motioneye platform, facilitating the integration of the four cameras and configuring them according to the La Merced neighborhood users' needs. These cameras were configured so that from 23:00 to 06:00 they emit alerts with image captures. The system will remain recording 24 hours a day in a recorder that in this case is a Raspberry Pi connected to a 2 TB external hard disk.

Keywords: Esp32, Motioneye, platform, cameras.

Firmado electrónicamente por:
MARIO NICOLAS
SALAZAR RAMOS

Revised by
Mario N. Salazar
CCL English Teacher

1. CAPÍTULO I. INTRODUCCIÓN

1.1 Antecedentes

La tecnología ha dado un importante avance mediante el cual se han podido desarrollar nuevas formas de comunicación y transferencia de información entre las personas, además se ha logrado ampliar el rango de interacción de este tipo de sistemas dentro de los que se incluyen cosas y objetos que se encuentran en el medio, mediante el cual se logra que las personas, objetos y aplicaciones informáticas interactúen mediante una red de comunicación continua.

Las IOT (Internet de las Cosas) ha logrado aprovechar dichos avances tecnológicos mediante la inclusión de nuevos elementos para insertar dispositivos inteligentes en diversos lugares para así poder capturar, guardar y administrar información, logrando tener acceso desde cualquier lugar en tiempo real. Es por ello que en el campo de aplicación del internet de las cosas se requiere el desarrollo de aplicaciones especializadas en las necesidades de las personas tomando en cuenta que cada individuo se encuentra en una red de comunicación y requiere información de diferentes entornos y objetos.

Hoy en día el Internet de las Cosas está enfocado a entornos comunes (hogar, lugar de estudio, lugar de trabajo, etc.) para abarcar un mercado más amplio, este proyecto va enfocado a la incorporación de la alarma comunitaria con la plataforma IOT de seguridad inteligente donde se podrán administrar cámaras de vigilancia, sensores de presencia, alarmas de multitud barrial, sistemas de predicción de seguridad y la activación de distintos elementos de alerta y disuasión mediante internet.

El software de aplicación de gestión de seguridad está diseñado y capacitado para responder a los numerosos controles para el tratamiento de la información (fotos, videos, alarmas, sensores) que contiene y que son totalmente configurables según los requerimientos de la sociedad, además permitir la automatización de la plataforma o del sistema IOT.

La plataforma inteligente IOT permitirá el monitoreo en tiempo real de activos y espacios físicos posteriormente revisar la información recopilada para identificar indicadores de seguridad y planificar medidas de seguridad. Cada vez que se detecte los indicadores de incidencia de seguridad la tasa de recopilación de documentos aumenta proporcionando información para un análisis más preciso y creíble. Mediante el sistema inteligente se podrá almacenar y acceder a datos de video que se caractericen por las cuatro V de Big Data: Volumen, Velocidad, Variedad y Veracidad, permitiendo tener una arquitectura de video vigilancia de manera transparente y rentable, mediante el análisis de las señales de video vigilancia se podrá permitir un análisis predictivo, lo que facilita a los operadores o usuarios anticipar incidentes de seguridad y prepararse proactivamente para ello.

Con la realización de este trabajo se busca reforzar la seguridad del barrio La Merced, haciendo que la plataforma inteligente IOT trabaje las 24 horas del día, realizando así un prototipo eficaz con un grado de confiabilidad alto. Esta plataforma inteligente permite integrarse de manera flexible con otros sistemas de seguridad hacia un enfoque analítico holístico de seguridad y vigilancia

El barrio La Merced de la Parroquia de Yaruquies cuenta con tiendas pequeñas, un colegio abandonado que se ha convertido en un punto de encuentro para delincuentes, personas a beber alcohol, y, hasta para la venta y consumo de droga, además alrededor del barrio existe una capilla donde se concentran estas personas para beber y donde es un punto clave para vigilar las casas que quieren asechar. Este tipo de situaciones se ha dado aviso a la Policía Comunitaria de la Parroquia, pero no han podido aplicar las respectivas acciones ya que según los agentes no cuentan con las pruebas pertinentes para iniciar con el procedimiento. Por lo mencionado se ve la necesidad de además de contar con una alarma comunitaria contar con un grupo de cámaras en puntos estratégicos en este sector.

1.2 Planteamiento del Problema

En la actualidad se han implementado proyectos de alarmas comunitarias en diferentes barrios de la ciudad, esto se ha convertido en una necesidad debido al incremento de la delincuencia, pero cabe recalcar que al presionar este tipo de alarmas parte de la población no acuden a estos llamados porque no saben el motivo por el cual se accionó la alarma o por no arriesgarse a represalias por parte de los delincuentes.

Actualmente el barrio La Merced de Yaruquies cuenta con una alarma comunitaria, que se ha accionado en casos de robo, durante la pandemia se dieron un sin número de casos de hurto en el barrio, se acudía al llamado y se concentraban en una esquina, luego la gente se distribuía a las diferentes esquinas para resguardar que los delincuentes no puedan huir, pero lamentablemente no se pudo llegar a encontrar a estas personas debida a que no se conocía el punto exacto donde se hizo el llamado de auxilio, esto debido al factor tiempo hasta que la gente se reúnan el encargado de la alarma diga desde donde fue el llamado y todos se distribuyan para buscar, el ladrón huía fácilmente.

Hoy en día incluso la alarma comunitaria del barrio la Merced se encuentra desactivada ya que cuando esta fue instalada, el botón de encendido fue dejado en un punto muy bajo y dentro de este hogar había niños pequeños los cuales llegaron a activar esta alarma muchas veces tan solo por juego, entonces la encargada decidió desactivarla, las escusas era que nadie se quiso hacer cargo para volver a reubicar esta alarma.

Al realizar una encuesta acerca de la delincuencia en este barrio, la gente afirma que se sienten muy inseguras, se han seguido dando actos delictivos, pero ya no existe organización por parte de los habitantes del barrio, y que necesitan una reorganización para volver activar esta alarma comunitaria y como no si a esta se le da un valor agregado

como es la integración de una plataforma inteligente la cual puede contribuir para reforzar la seguridad del barrio y poder tener un registro de los datos recopilados.

Teniendo en cuenta que la seguridad de la información recopilada es un aspecto fundamental dentro de la industria y todos los sectores económicos, se busca que este sistema inteligente este protegido contra hurtos o filtración de información, gracias a la integración de los dispositivos con el internet de las cosas se puede reducir que una persona tenga que estar presente de forma física junto a los dispositivos donde llega la información para transferirla de forma manual, ya que al enlazar el internet de las cosas con dispositivos inteligentes móviles se puede acceder en cualquier lugar a toda hora a esta información.

1.3 Objetivos

1.3.1 General

- Implementar una plataforma IOT integrada a la alarma comunitaria para reforzar la seguridad en el barrio La Merced de Yaruquies de la ciudad de Riobamba

1.3.2 Específicos

- Diseñar la plataforma de Seguridad IOT con todos los parámetros compatibles con la alarma comunitaria.
- Determinar los puntos estratégicos para la ubicación de los elementos y componentes de la plataforma.
- Implementar la red IOT mediante Protocolos de seguridad tomando en cuenta transmisión, velocidad, cobertura, confiabilidad y predicción
- Diseñar la interfaz para la visualización y el análisis del sistema de seguridad en tiempo real.

2. CAPÍTULO II. MARCO TEÓRICO

En esta sección se abordarán las definiciones de cada fase que conforman la plataforma IoT para el barrio La Merced de Yaruquies de la ciudad de Riobamba, ya que es indispensable tener claro cada concepto de las herramientas y componentes del proyecto, para un mejor entendimiento en cada etapa.

2.1 Historia de los Sistemas de Video vigilancia

Iniciando desde la creación de las primeras cámaras hasta en la actualidad el reconocimiento facial, la historia de la video vigilancia nos ayuda a entender cómo surgió esta herramienta y cuáles han sido sus avances hasta la actualidad. Las cámaras cinematográficas aparecen en 1880, pero no fue hasta el año 1942 que fueron usadas como un elemento de seguridad en un circuito cerrado, estos primeros sistemas solo contaban con cámaras en blanco y negro que estaban conectadas a monitores, y que además fueron creadas para monitorear el lanzamiento de cohetes espaciales [1].

Al inicio la video vigilancia requería un circuito cerrado que continuamente esta monitoreado por un humano para su funcionamiento, cuando llegaron las cintas de video lo que hizo posible grabar lo que sucedía en las cámaras, entonces, en la década de los 60’s la video vigilancia se hizo más común y las cámaras se ubicaban en sitios estratégicos como en lugares públicos [1][2].

Casi una década después los bancos y tiendas empezaron a usar estos sistemas de video vigilancia como medida de seguridad para evitar robos, dos décadas después se viene mejoras tecnológicas [2], permitiendo una mejor visión en situaciones con poca luz y el tamaño de las cámaras se reducen, lo que hizo que esta tecnología se adentrará a los hogares como un método de seguridad para las familias.

Luego en los años 90’s se da el lanzamiento de las cámaras IP, lo que es un avance grandioso ya que estas cámaras se conectan a una red de internet sin la necesidad de utilizar un computador [2], haciendo que los usuarios puedan revisarlas constantemente desde cualquier dispositivo con conexión a internet.

En la actualidad la video vigilancia se ha convertido en una herramienta indispensable para negocios y en muchos casos gobiernos enteros en cuanto a la seguridad, siendo así el último avance el reconocimiento facial.

Los sistemas de video vigilancia basados en DVR y en nube son igual de vulnerables a intrusiones maliciosas, en la actualidad las empresas de cámaras de video vigilancia trabajan en hardware y software, permitiendo que las soluciones de seguridad sean de menor costo asequibles a los usuarios, siendo más seguras y permitiendo un mayor control de lo que sucede en los hogares, trabajos, colegios o lugares abiertos (aeropuertos o parques) [3].

2.2 Seguridad Ciudadana

Debemos de conceptualizar a la seguridad ciudadana debido a que este proyecto está enfocado en solventar uno de los problemas más graves de la sociedad, el cual es la inseguridad.

Se entiende como Seguridad Ciudadana a la acción integrada que desarrolla el Estado mediante la colaboración de la ciudadanía y el apoyo de organizaciones públicas, cuyo principio fundamental es asegurar la convivencia y desarrollo pacífico, así como la erradicación de violencia.

2.3 Sistemas De Seguridad Física (SSF o PSS, Physical Security System)

La seguridad física de una manera particular se vuelve ardua porque las operaciones en sí son realizadas por los usuarios y pueden crear vulnerabilidades, ya sea de manera intencional o desacertada, por lo que es importante que los gerentes de seguridad de la información hagan cumplir las políticas de seguridad como parte de la norma.

En términos generales, los sistemas de seguridad no suelen ser un único servicio aislado, sino una combinación de elementos físicos y electrónicos que juntos forman las herramientas adecuadas para intentar proteger la integridad de las personas, los bienes físicos y los lugares a través de una ubicación estratégica, teniendo así diversos dispositivos para detectar presencia e intrusión no autorizada.

Hoy en día, los sistemas de seguridad están altamente automatizados, basados en un conjunto de sensores y tecnologías de comunicación, así como software de gestión que evalúan situaciones de riesgo potenciales y pueden reaccionar de forma autónoma o actuar como apoyo del personal de seguridad

La video vigilancia permite grabar imágenes que capturan las cámaras, así como permite visualizar en tiempo real lo que está sucediendo en el lugar donde se encuentran instaladas estas cámaras, este tipo de sistemas son muy útiles para empresas, negocios, supermercados, escuelas, colegios, permitiendo tener vigilados estos lugares, logrando evitar robos, llegando a disminuir los niveles de inseguridad.

Al hablar de video vigilancia decimos que son sistemas de seguridad que son utilizados para evitar robos y tener seguridad en hogares, oficinas, escuelas, lugares públicos, etc. Este tipo de sistemas están conformadas por un conjunto de cámaras, las cuales se encargan de captar y grabar imágenes.

2.4 Circuito Cerrado de Televisión

CCTV Circuito Cerrado de Televisión se lo puede definir como una combinación de varios dispositivos (cámaras, monitores), los cuáles mediante la infraestructura correcta para su interconexión, permite visualizar y llevar un registro en video de las situaciones que ocurren en el entorno determinado y así poder minimizar los riesgos de inseguridad.

Además, este tipo de sistemas sirven para el control o supervisión de procesos industriales o logísticos y del control de tráfico para el sector de la salud y diferentes ámbitos académicos.
Estas cámaras permiten transmitir su señal mediante un cable coaxial a un grabador de video DVR, el cuál es el encargado de la gestión y control de estas imágenes.

Este sistema puede estar compuesto por un conjunto de cámaras de vigilancia interconectadas a uno o varios monitores de video o también a televisores, mismos que reproducen las imágenes, para obtener mayores beneficios del sistema se interconectan por red otros dispositivos como videos o computadoras.

Cada vez estos sistemas eran más conocidos y utilizados en los espacios públicos para la prevención de actos delictivos, ya que estos sistemas sirven para alertar de forma inmediata a la policía y así su rápida intervención y hace que las personas se sientan más seguras en estos lugares, sin embargo, los costos de los CCTV tienen un costo elevado. Un ejemplo de ello es que entre los años 1992 y 2002 en el Reino Unido se gastó más de 250 millones de libras en este tipo de sistemas [10].

Los CCTV son el complemento perfecto en cualquier sistema de alarmas para registrar el momento exacto que sucedió el percance, existiendo sistemas muy complejos pero fáciles de interpretar y manejar, mismos que permiten grabar continuamente, detectar movimientos, temperaturas, además de detectar objetos faltantes o sobrantes. Estos sistemas se apoyan en software de video analítica, algunos incorporados en las mismas cámaras y otras instaladas mediante el equipo de video vigilancia en el cuarto de control.

Con el avance de la tecnología los tipos de CCTV van expandiéndose y desarrollándose, es así como en la actualidad tenemos los sistemas analógicos y digitales, al hablar de analógicos decimos tecnología con cables y los sistemas digitales ya no necesitan cables y la forma de operación varia, ambas tecnologías utilizan básicamente los mismos.
El modo de operación es el mismo las imágenes son enviadas a los monitores y depende del sistema estas son enviadas por cable o vía inalámbrica, mismas que son observadas por un personal autorizado y calificado en tiempo real, que a su vez son grabados en DVR o NVR.

En los sistemas de CCTV las aplicaciones más frecuentes que están relacionadas con estándares de seguridad en los diferentes sectores inician con aplicaciones sencillas de tipo residencial hasta aplicaciones más complejas como vigilancia ciudadana.

Otro de los campos de aplicación de los CCTV es la medicina, así por ejemplo en las salas de cuidados intensivos o en el área de psiquiatría y se usan además en cirugías asistidas de forma remota.

Dentro del sector productivo son utilizados para controlar líneas de producción y supervisión de temperatura, flujo, presión, etc. Siendo de gran utilidad para ingenieros de control de procesos, optimizando el tiempo sin tener la necesidad de estar en sitios remotos.

En el campo académico se usa para implementar centros de simulaciones y transmitir en tiempo real a una o varias salas de diversos grupos de interés.

En un sistema moderno en el que a las cámaras se pueden inspeccionar remotamente desde una sala de control, donde es posible configurar el enfoque, la inclinación, panorámica y zoom las cuales son conocidas como PTZ (Pan-Tilt-Zoom) [10] [11], estas incluyen visión nocturna, así como contar con funciones asistidas por un ordenador y detección de movimiento, por lo que permite al sistema ponerse en estado de alerta al contar con movimientos delante de las cámaras.

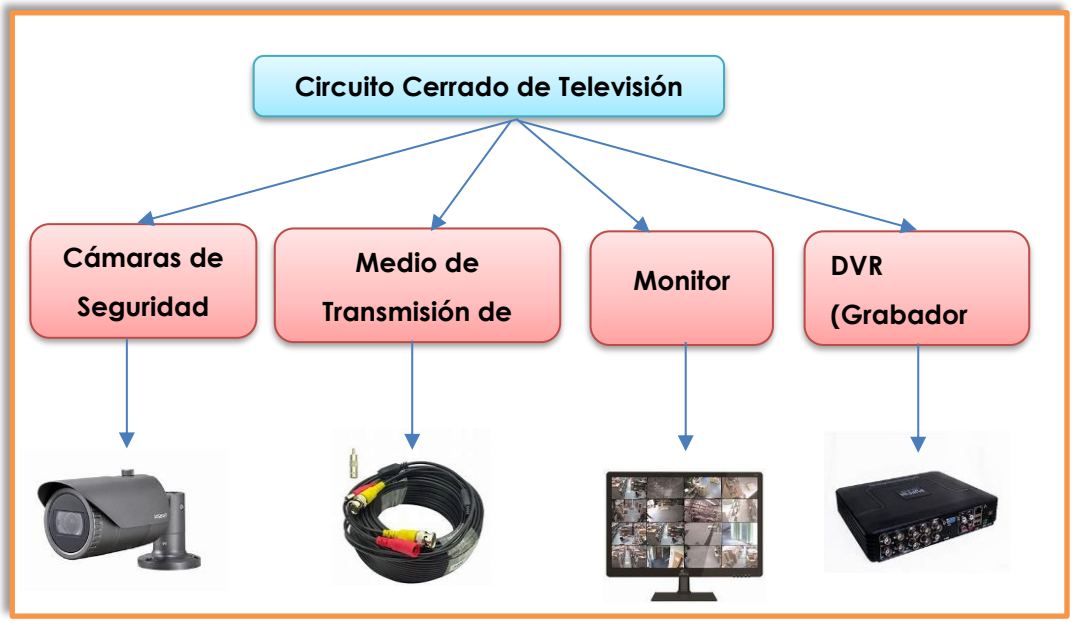
2.5 Componentes Principales de un CCTV

Las cámaras de seguridad son dispositivos que emiten la señal de video, estas permiten capturar las imágenes, pueden ser diversas dependiendo el tipo de aplicación, función y especificaciones técnicas.

Las cámaras fijas más comunes cuentan con:

- **Box**, cuenta con una forma que asemeja a una caja.
- **Domo**, tiene una forma redonda, que es similar a una bola.
- **Bullet**, es un lente con una forma cilíndrica.

Figura 1. Componentes Principales de un CCTV Analógico



Fuente: *Autor*

Medios de transmisión de Imagen, se trata de un conjunto de elementos como cableado, ductos y conectores indispensables y definidos por los fabricantes para la correcta transmisión de las señales de video emitidas por las cámaras, esto cuando el medio de transmisión sea físico, ya que también existen medios de transmisión inalámbricos, estas se envían por señales de radio y en estos casos se usan elementos como antenas y radios. Según la tecnología del sistema y especificaciones para cada implementación se usa cable coaxial, cable par trenzado o cable UTP.

Monitor, es un dispositivo de visualización de video, en donde se despliega las imágenes emitidas por las cámaras de seguridad.

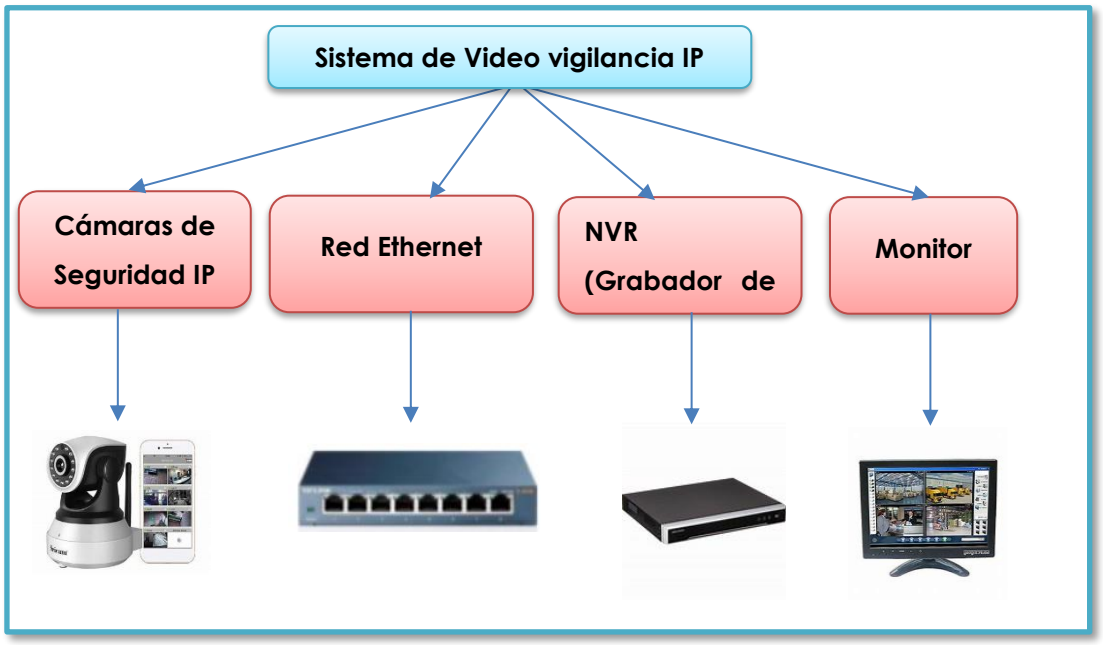
DVR, dispositivo cuya función es digitalizar, grabar y almacenar en su memoria interna las imágenes captadas por las cámaras de seguridad, para manipular esta información se requiere de un software que permite su interacción. Este software se debe configurar para poder elegir las cámaras a visualizar, manipular y descargar imágenes, realizar acercamientos, entre otras funciones. Además, algunos DVR más avanzados cuentan con la capacidad de detectar rostros con mucha nitidez, también se puede ahorrar el consumo de energía y el almacenamiento, logrando evitar falsas alarmas.

A los DVR se les puede conectar un tipo de kit de alarma que sirva como un método persuasivo y alerta contra intrusos, añadiendo sensores de movimiento que detecten ciertas señales y activen el sistema. Este tipo de dispositivos se debe configurar por cámara y cuando detecta movilidad se encienden y activan todos los recursos disponibles.

Un DVR brinda la posibilidad de grabar sonidos que obtienen las cámaras de seguridad que cuentan con esta funcionalidad, además mediante un micrófono externo que se lo puede vincular directo a un canal especifico de una cámara.

2.6 Sistemas de Video vigilancia IP

Figura 2. Componentes Principales de un CCTV Digital



Fuente: *Autor*

Estos sistemas se caracterizan de los CCTV porque la transmisión de imágenes se las realizar mediante una red TCP/IP, misma que puede ser cableada o inalámbrica y la grabación se la realiza mediante Cámaras IP, este tipo de sistemas son utilizados para aplicaciones como el reconocimiento facial o reconocimiento de matrículas, etc.

Además de ser un sistema más sencillo y económico que un CCTV, debido a que aprovecha las redes informáticas empresariales, esto quiere decir que utiliza el mismo cableado para la comunicación de datos, acceso a internet, sin necesitar una infraestructura para el cableado coaxial determinada para dicha red de video vigilancia.

Hoy en día la mayoría de las instalaciones más modernas están cambiando la tecnología analógica CCTV por la video vigilancia IP, debido a sus ventajas como versatilidad, funcionalidad, optimización y sencillez de las infraestructuras. Entre los avances más significativos de este tipo de tecnología además de eliminar el tendido de cables por sus capacidades inalámbricas, tenemos la alta resolución de imagen que ofrecen las cámaras IP, la incorporación de sistemas de inteligencia para el tratamiento de gestión de eventos

y video , permite capturar video y almacenarlo a pocos frames por segundo, además de habilitar la grabación en determinadas circunstancias, esto mediante sensores de movimiento en un determinado lugar o franjas horarias.

En cuanto a resolución, esta tecnología va acompañada de altas tasas de comprensión para evitar consumos excesivos de ancho de banda y espacio de almacenamiento en los NVR respecto a los formatos de video que se utilizaban como Motion JPEG, MPEG-4.

A diferencia de los sistemas de video vigilancia analógico los sistemas IP no necesitan de una red de cableado, ya que estas son inalámbricas y los NVR tienen mayor capacidad para guardar las imágenes y manipularlas de acuerdo con la necesidad del usuario.

2.6.1 Cámaras IP

Este tipo de cámaras capturan el video/audio de forma digital, además de que pueden ser fijas o móviles, mismas que transmiten estas imágenes al grabador de vídeo en red NVR mediante cables o red de datos IP de forma inalámbrica, se puede también enviar estas imágenes de forma directa a los servidores de video en red.

En la actualidad ciertos modelos de cámaras IP llevan incorporado una ranura para tarjetas MicroSD donde se puede almacenar las imágenes, en este caso la capacidad de almacenamiento está limitada a 128Gb y en este caso solo graban las imágenes en caso de detectar movimientos, esto con la finalidad de economizar espacio. Es por ello por lo que se recomienda añadir un videograbador NVR para registrar las imágenes que permita instalar hasta dos discos duros, logrando aumentar la capacidad de registro y además proteger las grabaciones de posibles robos, otro de los beneficios de conectar estas cámaras a un NVR es que el flujo de transmisión de datos se va a poder gestionar mejor, evitando así posibles saturaciones en la red, los niveles de protección contra ataques son superiores además de contar con mayor calidad e integración con distintos sistemas de seguridad [12].

2.7 Regulaciones respecto a las CCTV

Al trabajar con cámaras de seguridad hay que guiarse en ciertos principios o normas establecidas a nivel mundial, mismos que tienen el fin de proteger a las personas, es por ello por lo que a continuación se mencionará cada una de estas regulaciones.

Proporcionalidad de los objetivos perseguidos y métodos de procesamiento de datos.

Información acerca de la capacitación y grabación de las imágenes, sobre todo cuando se utilicen con fines lícitos y legítimos.

Cuando se utilice video vigilancia no debe existir algún tipo de medio invasivo.

Si se instalan cámaras de seguridad en lugares privadas, están no pueden obtener imágenes de lugares públicos.

Se debe poner un cartel aprobado en la instrucción 1/2006 en un lugar visible [8].

El cartel amarillo debe ser homologado según la Ley Orgánica 15/1999, los demás carteles son solo informativos y se pueden poner, pero no son oficiales [8].

La información de las zonas vigiladas ya sean exteriores o interiores deben ser visibles desde cualquier acceso a estos espacios.

2.8 Internet de las Cosas (IoT, Internet of Things)

El internet de las cosas representado por sus siglas IoT, se refiere al conjunto de dispositivos electrónicos físicos, los cuales reciben y transfieren datos mediante redes inalámbricas, siendo mínima la intervención humana. Permitiendo una conexión entre estos dispositivos desde cualquier lugar sea desde el hogar oficina, el automóvil, desde cualquier lugar, llegando a intercambiar datos y así obtener resultados de manera automática.

IoT es un término ampliamente utilizado para un conjunto de tecnologías, sistemas y principios de diseño asociados con la ola emergente de cosas conectadas a internet. En muchos aspectos, puede parecer lo mismo que la comunicación M2M (machine to machine, máquina a máquina en español) ya que se conectan sensores y otros dispositivos a sistemas de tecnología de la información y la comunicación a través de redes cableadas o inalámbricas, Sin embargo, en contraste con M2M, el concepto de IoT también se refiere a la conexión de dichos sistemas y sensores a Internet, así como al uso de tecnologías generales de Internet [5] [6].

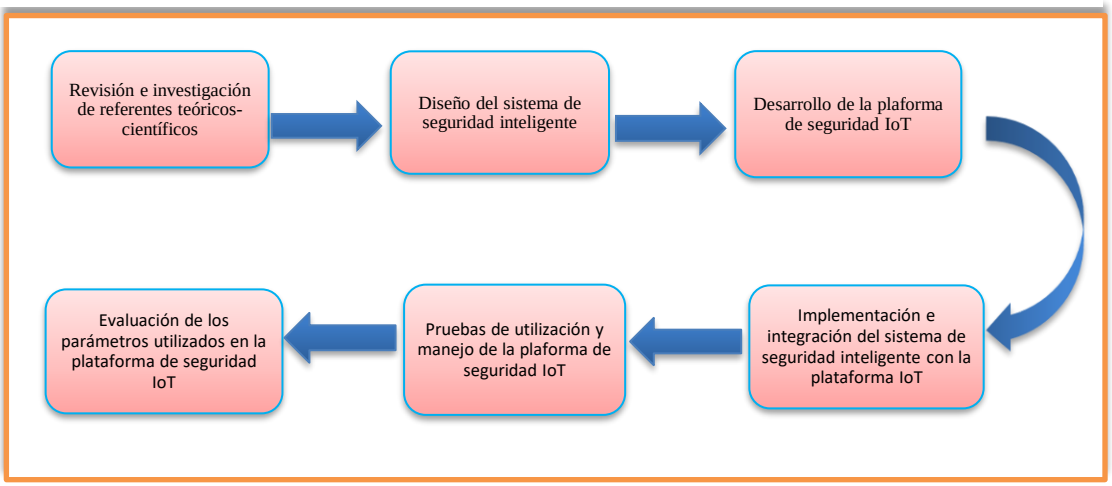
El Internet de las Cosas es una red de objetos físicos de dispositivos, instrumentos, vehículos, edificios y otros elementos equipados con electrónica, circuitos, software, sensores y conexiones de red que permiten a estos objetos recopilar e intercambiar datos. IoT permite la detección remota y el control de dichos dispositivos a través de la infraestructura de red existente, creando oportunidades para una integración más directa del mundo físico en los sistemas informáticos, aumentando la eficiencia y la precisión. El concepto de una red de dispositivos inteligentes se discutió ya en 1982, cuando una máquina de Coca Cola modificada en la Universidad Carnegie Mellon se convirtió en el primer dispositivo en red capaz de informar su inventario y si una bebida recién llenada estaba fría. Kevin Ashton, es un pionero británico de la tecnología conocido por haber inventado el término "Internet de las Cosas" para describir un sistema en el que internet está conectado al mundo físico a través de sensores ubicuos [7].

La tecnología IoT puede lograr que objetos o cosas puedan ser convertidas en objetos inteligentes. El desarrollo constante que se puede evidenciar hasta el momento son las

viviendas inteligentes, automatizadas siendo estas las primeras con la conectividad a internet permitiendo así la amplia conectividad de cada uno de los componentes de la casa. Entre los más destacables se puede encontrar electrodomésticos, entre una variedad que se localizan en lugares específicos como lo son equipos de la red eléctrica, los equipos logísticos, los equipos médicos y los equipos agrícolas, a raíz de esto se logra obtener la integración sistemática del entorno humano y natural [8] [9].

Para ofrecer una plataforma de calidad, en la cual se pueda interactuar con los conocimientos teóricos, se presenta en la Figura 1 el diagrama general del proyecto, el cual está enfocado en establecer parámetros por los cuales regirse para su desarrollo.

Figura 3. Diagrama general del proyecto



Fuente: *Autor*

Para la realización de este proyecto, cada temática está relacionada a los sistemas de seguridad IoT, dichos contenidos estarán plasmados en la plataforma virtual, estableciendo el esquema que se presenta en la Figura 1. Dicho esquema presenta el procedimiento que se debe seguir para abordar una determinada temática o la explicación de cierto concepto, empezando desde la investigación para luego pasar al diseño, comprobación, modelación, e implementación. El resultado obtenido ofrecerá adaptabilidad para extender la población que se pretende abarcar, así como la implementación de nuevos dispositivos a la plataforma de seguridad IoT.

2.8.1 Características IoT

Al hablar del Internet de las Cosas este permite adaptarse a cualquier dispositivo o sistema que transmite información, mediante la interacción de sensores extraer y manipular en

términos operativos analizando gran cantidad de datos. Es por ello que debemos tener ciertas características muy presentes como:

Sensibilidad, las máquinas requieren de sensores para lograr interpretar la realidad a su alrededor, lo que facilita el monitoreo, detección, recopilación de datos y otras funciones que se vinculan al Internet de las cosas.

Interacción, Al usar un sistema IoT se hace posible la comunicación entre la realidad, sistemas y usuarios, logrando así avances significativos como casas inteligentes, granjas automatizadas, robots que facilitan tareas cotidianas, entre muchos otros.

Conectividad, Los sistemas IoT permiten obtener mayor potencial al aumentar la compatibilidad y el acceso a la red.

Seguridad, al integrar una gran cantidad de dispositivos conectados a la red, la necesidad de protegerlos de ataques cibernéticos aumenta, es por ello por lo que la ciberseguridad y arquitectura son indispensables para este tipo de proyectos.

2.9 Arquitectura IoT

Una tecnología IoT está compuesto por varios elementos como sensores, dispositivos e interfaces electrónicos los cuáles recopilan, procesan y envían datos como ciertos comandos a los monitores de punto final.

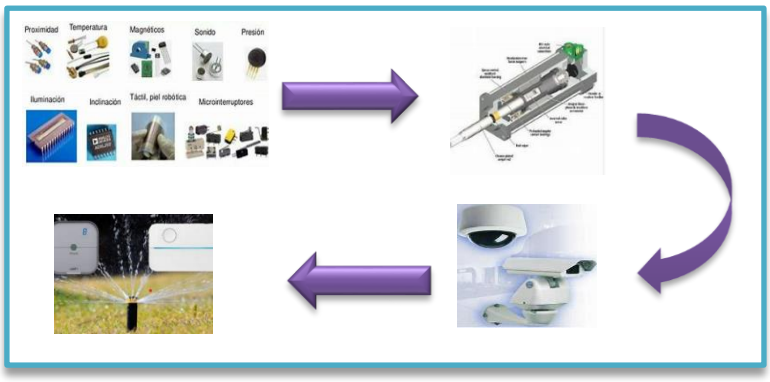
Para ordenar estas partes móviles y establecer la estructura final IoT se requiere de una arquitectura IoT, la cual indica como conectar y operar estos dispositivos dentro del sistema, tanto el software en la nube y la red de sensores, y la solución de problemas inesperados dentro del sistema IoT se realiza dentro de la arquitectura IoT.
Para un funcionamiento básico se requiere de tres capas de elementos en un sistema IoT, como:

- Sensores, dispositivos, actuadores, etc., que se encuentran bajo la capa de percepción.
- LAN, Wi-Fi, 4G, 5G, etc., que se encuentran en la capa de red.
- Una interfaz gráfica de usuario que conforma la capa de aplicación.

La arquitectura de un sistema IoT están conformadas por varias capas que se desempeñan como medios digitales mediante los cuales los datos del sensor llegan a la aplicación de la nube. Para luego de este proceso esta aplicación en la nube tome decisiones de acuerdo con el flujo de trabajo preestablecido para estos dispositivos finales.
Finalmente, estas decisiones viajan hacia los dispositivos finales a través de la misma capa.

2.9.1 Capa sensorial/ de percepción

Figura 4. Componentes de la capa de Percepción del sistema IOT



Fuente: *Autor*

Esta capa está compuesta por dispositivos de punto final, los que son encargados de recopilar los datos del universo físico, para luego las aplicaciones digitales analicen los datos obtenidos.
En esta capa los objetos del mundo real se mantienen en permanente contacto, esta también es llamada capa física, compuesta por elementos como lo son:

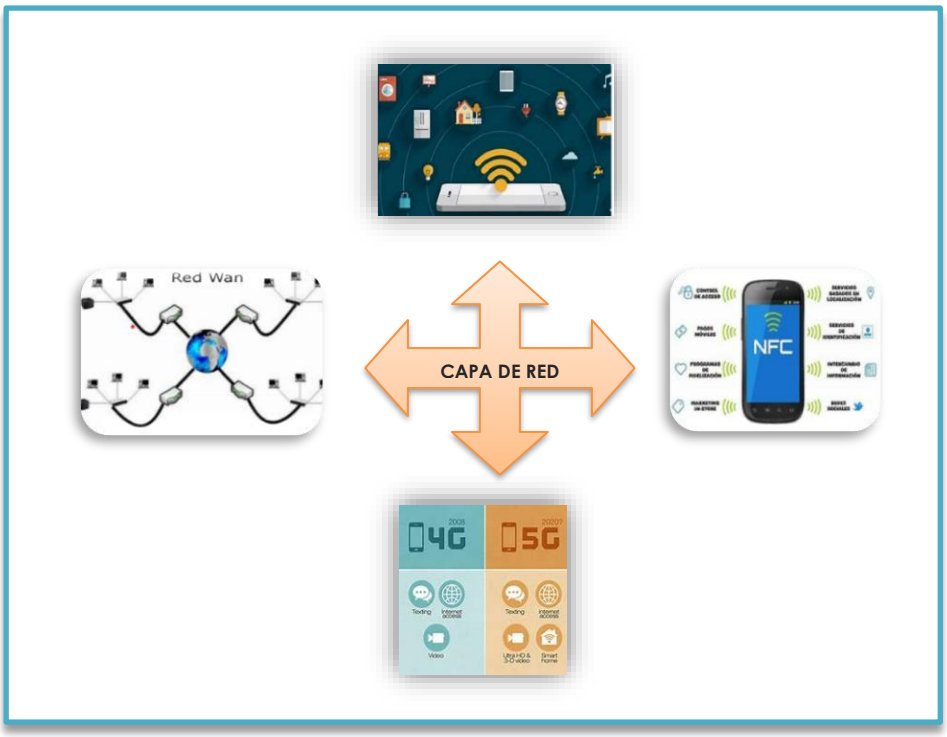
- **Sensores de velocidad**, presencia, identificación por radiofrecuencia, químicos, temperatura, movimiento, etc.
- **Actuadores y brazos robóticos**.
- **Cámaras de seguridad**, sistemas de acceso a puertas y ventanas, etc.
- **Termostatos**, rociadores de agua, elementos de calefacción, etc.

2.9.2 Capa de Red/datos

Esta capa cumple con la función del transportar los datos entre todas las capas dentro de una arquitectura IoT, además de definir la topología de red para los dispositivos dentro de esta tecnología, aplicaciones en la nube y la base de datos.
Las partes que conforman esta capa son las puertas de enlace de internet, las puertas de enlace de red e intranet y los sistemas de adquisición de datos. Los dispositivos físicos para los protocolos de conectividad de red pueden ser:

- Wi-Fi
- Redes de área amplia (WAN)
- 4G LTE/5G
- Bluetooth de bajo consumo
- Comunicación de campo cercano (NFC)

Figura 5. Componentes de la capa de Red del sistema IOT



Fuente: *Autor*

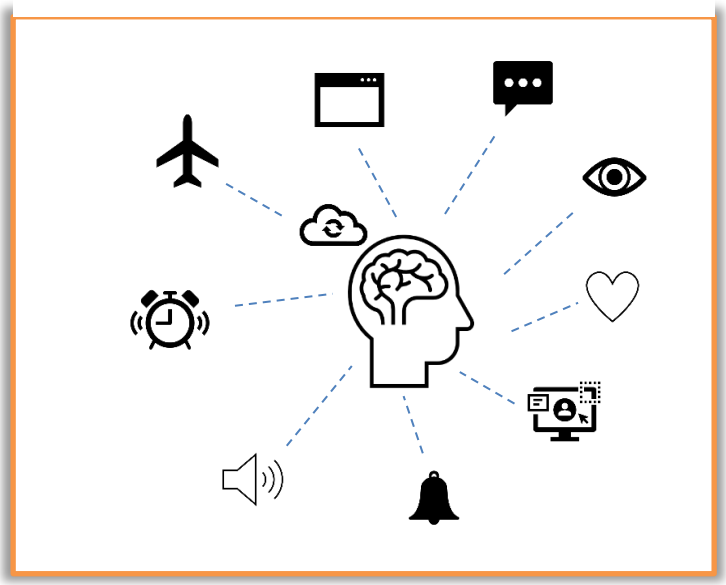
Mediante esta capa, los dispositivos de punto final y aplicaciones en la nube se comunican entre sí. Los datos de los sensores viajan a través de la capa de red para lograr llegar a otras capas.

2.9.3 Capa de Procesamiento de Datos

Esta capa es la encargada de procesar y almacenar los datos antes de ser transferidos a un centro de datos, incluyendo análisis de borde en cuanto a informática perimetral, inteligencia artificial (IA)y las máquinas de aprendizaje (ML) [14].

Además de ser la capa encargada de tomar, anular o mejorar el sistema tomando decisiones ad-hoc en la capa de aplicación, siendo esta una característica fundamental para el control humano en las máquinas inteligentes.

Figura 6. Componentes de la capa de Procesamiento de Datos del sistema IOT



Fuente: *Autor*

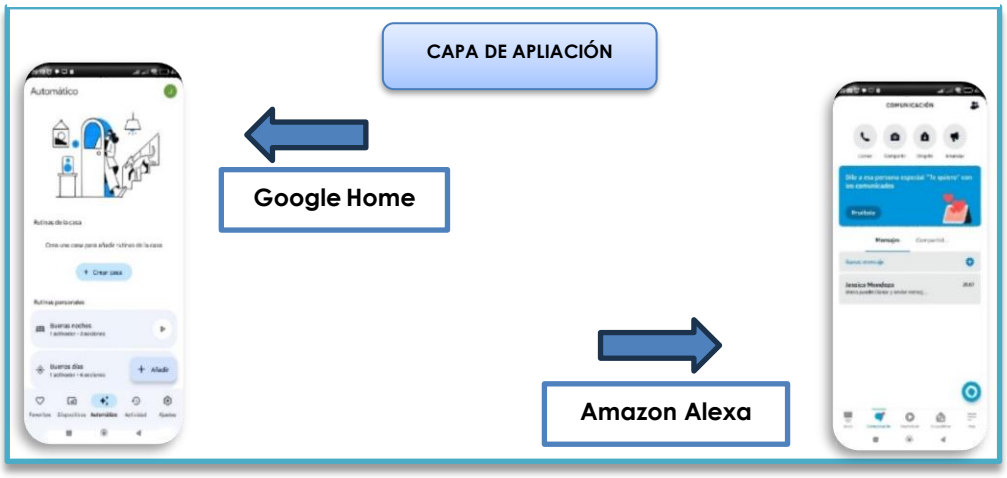
2.9.4 Capa de Aplicación

Dentro de los sistemas IoT la mayoría de ellos funcionan sin intervención humana, entre ellas Google Home, Amazon Alexa, etc., pero estos necesitan de una interfaz gráfica de usuario para añadir IoT workflows, cambiar parámetros, añadir dispositivos, etc. Esto es lo que conforma la capa de aplicación, esta capa requiere de algunos parámetros como:

- Comunicación con gran cantidad de sensores y dispositivos de punto final desde una pantalla pequeña.
- Añadir nuevos dispositivos a un sistema IoT ya existente sin la necesidad de cerrar toda la operación comercial.
- Observar y monitorear el sistema y de servicio a los dispositivos cuando haya una alerta en el tablero.
- Crear nuevos workflows o reglas específicas dentro de los sistemas IoT.
- Crear y guiarse mediante un acuerdo de nivel de servicio (SLA).
- Omitir los problemas ocasionados por comandos de voz.

En cuanto al campo industrial, estos sistemas necesitan específicamente de un tablero centralizado en una pantalla de un computador para observar todos los sistemas IoT, dentro de este tablero se puede interactuar con uno o todos los sistemas IoT logrando así pausar, detener o reiniciar los dispositivos.

Figura 7. Componentes de la capa de Aplicación del sistema IOT



Fuente: *Autor*

2.9.5 Capa de Negocios

Figura 8. Compontes de la capa de Negocios del sistema IOT

Fuente: *Autor*

Esta capa es la encargada de convertir los datos recopilados en información procesable, los gerentes, directivos, encargados pueden usar estos informes, ya que les ayuda a tomar decisiones y así poder mejorar la productividad.
En esta capa se incluyen fundamentalmente integraciones de aplicaciones comerciales, así como ERP (Planificadores de recursos empresariales, BI (Inteligencia empresarial), aplicaciones de visualización de datos, etc.
Los analistas de datos pueden procesar estos datos y lograr establecerlos dentro de una herramienta de BI como Cuadro, Power BI, etc., para tener presente el rendimiento global del sistema IoT, además de crear pronósticos que se basan en la capacidad de producción actual y futura de las necesidades del mercado.

2.10 Protocolo IoT

En el campo de las telecomunicaciones los protocolos IoT se definen como el conjunto de normas y reglas que permiten intercambiar información a dos dispositivos, facilitando así la comunicación Machine2Machine.

Estos protocolos sirven para la comunicación entre máquinas, como la comunicación entre humanos idiomas, gestos o el lenguaje corporal. Es como los humanos requieren hablar el mismo idioma para entenderse, los dispositivos requieren utilizar los mismos protocolos IoT para poder intercambiar información.

Estos protocolos de comunicación IoT cumplen con varias funciones es así como:

- Facilitar la escalabilidad, añadiendo o eliminando dispositivos al sistema IoT sin afectar la estructura general.
- Garantizar la seguridad de las comunicaciones en entornos vulnerables como la ciberseguridad y en el campo industrial.
- Proporcionan un sencillo acceso a los dispositivos, existiendo o no problemas de latencia o ciertos cortafuegos, etc.

Por la variedad de dispositivos IoT existentes en la actualidad, se han creado diferentes protocolos IoT para la gestión de la comunicación en diferentes ámbitos, estos se dividen en:

2.10.1 Protocolos de acceso a la red

Estos se encuentran en la capa inferior, permitiendo la conexión entre dos máquinas. Estos protocolos son el medio comunicación, es aquí donde entran las redes Ethernet, Wi-Fi, 3G, 4G, 5G, etc.

2.10.2 Protocolos de Transmisión

Son utilizados para codificar la información que se envía a través de las redes 3G, 5G, Wi-Fi, entre otras, estos protocolos son el lenguaje específico para transmitir información, dentro de estos protocolos IoT encontramos dos familias importantes como son:

- **Protocolos informáticos**, son los que se utilizan para transmitir información a internet.
- **Protocolos OT (industrial),** utilizados para la comunicación en equipos industriales. Cuando se comunica los dispositivos IoT con internet, los protocolos más utilizados son MQTT, CoAP y HTTP, este tipo de protocolos son flexibles en cuanto a comunicación [15].

2.10.2.1 MQTT (Transporte de Telemetría MQ)

Este protocolo sigue el modelo publicación-suscripción, el cual permite la comunicación entre una gran cantidad de dispositivos, el cual funciona mediante un servidor central llamado bróker que es el encargado de recibir los mensajes de los dispositivos emisores para así distribuirlos entre los receptores. Este tipo de, mensajes se organizan de manera jerárquica mediante etiquetas.

2.10.2.2 CoAP (Constrained Aplication Protocol)

es un protocolo de software que permite que sensores y actuadores de baja potencia, se comuniquen de manera interactiva mediante internet. Utiliza el modelo REST de HTTP, además de otros requerimientos como la multidifusión, una baja sobrecarga y el soporte de UDP.

En cuanto a los despliegues de comunicación industrial y comunicación industrial IoT se trabajan mediante protocolos enfocados a las operaciones, estos protocolos están orientados a que un dispositivo controlador PLC logre comunicación con otra máquina que ejecuta órdenes [15].

En el campo industrial existen protocolos específicos como IEC102 y el IEC104 que son para los contadores eléctricos y el MBUS para contadores de agua [16].

2.10.2.3 Advanced Messaging Queuing Protocol (AMQP)

Se define como un protocolo de estándar abierto que trabaja en la capa de aplicaciones de un sistema de comunicación, determina el comportamiento del servidor que provee los mensajes y el cliente de mensajería llegando al punto en que las implementaciones de diferentes proveedores llegan a ser interoperables, está diseñado para aplicaciones corporativas, de mayor rendimiento y redes de baja latencia.

2.10.2.4 Extensible Messaging and Presence Protocol (XMPP)

Es un protocolo de estándar abierto que está basado en XML pensado inicialmente para aplicaciones de mensajería instantánea, en la actualidad se usa para diálogos, llamadas de voz y video, así como tele presencia.

2.10.2.5 Data Distribution Service (DDS)

Es un protocolo de publicación/suscripción que se utiliza para comunicación en tiempo real de máquina a máquina (M2M), se basa en una arquitectura sin bróker y que utiliza multidifusión para obtener una excelente calidad de QoS y mayor confiabilidad en sus aplicaciones.

3. CAPÍTULO III. METODOLOGÍA

3.1 Tipo de investigación

El tipo de investigación que se aplicará en el presente trabajo es de carácter exploratorio y experimental, ya que permite descubrir todas las afirmaciones o pruebas existentes del fenómeno con relación a sistemas de seguridad IoT, para fortalecer la seguridad en el barrio la Merced de Yaruquies de la ciudad de Riobamba, brindando apoyo mediante un sistema inteligente con cámaras, sensores. Tarjetas RFID. donde puedan ser controladas mediante un software fácil y manipulable para los moradores de este barrio.

3.2 Deductivo- Inductivo

En esta etapa se identifican las posibles fuentes de información almacenada en los servidores informáticos, con referencia a los sistemas de seguridad IoT, con el objetivo de verificar los resultados de emisión y recepción de las evidencias digitales, con el fin de mejorar la eficiencia y la efectividad del proceso de preservación, recolección y revisión de datos, considerando que este método permite tener conclusiones particulares en base a la realidad, y así demostrar las causas y consecuencias de los problemas de inseguridad en el barrio La Merced de Yaruquies de la ciudad de Riobamba.

3.3 Fuentes de información

Para realizar el presente trabajo de investigación se realizará una revisión metódica de documentos de acuerdo a la enseñanza de sistemas de seguridad IOT, teniendo en cuenta que la información y la base de datos se obtendrá mediante la revisión de libros, artículos científicos, informes, catálogos, prototipos de bibliotecas virtuales como: ProQuest, e-libro, Scopus, SCIMAGO, IEEE., y así mismo se considerará que toda la información que se obtendrá en esta investigación debería basarse en tecnología IoT y software como Python, con una información actual con el fin de respaldar la veracidad de la información en los últimos 10 años.

Así como la recolección de información por medio de una encuesta segmentada donde se reconocerá cada una de las necesidades de los habitantes del barrio La Merced de Yaruquies en cuanto al sistema de video vigilancia y monitoreo, logrando cumplir con las expectativas que los habitantes tienen frente al prototipo propuesto.

3.4 Instrumentos de investigación

Los instrumentos de investigación que se utilizaran para la elaboración del presente estudio, es el uso de análisis documentales y procedimientos experimentales.

- Análisis de documentos: adquiriendo en su mayoría publicaciones científicas, revistas y manuales con el fin de fundamentar la viabilidad del proyecto.
- Procedimientos experimentales: El concepto se basa en el uso del contexto de prueba y error para definir los resultados que nos permitan identificar su correcto funcionamiento que cuya información se puede obtener mediante encuestas a los moradores de barrio la Merced de Yaruquies, uso y manipulación del sistema de seguridad IOT.

3.5 Población y muestra

Para la realización del trabajo de investigación se ha tomado en cuenta como población al número estimado de moradores del barrio la Merced de Yaruquies de la ciudad de Riobamba y para la muestra se ha considerado el número de moradores que existen en 2 manzanas, es entonces que el tipo de muestreo que se aplicará es del tipo no probabilístico debido a que se está eligiendo por conveniencia el grupo de estudio. Por lo cual se especifican dichos datos a continuación:

3.5.1.1 Población

Se describe como el número aproximado de moradores presentes en el barrio la Merced de Yaruquies de la ciudad de Riobamba, de la cual conforman 160 moradores.

3.5.1.2 Muestra

se presenta como la cantidad de moradores que habitan en las 2 manzanas principales del barrio la Merced de Yaruquies de la ciudad de Riobamba, de lo que se conoce existen 50 moradores que serán el grupo para considerarse para la realización del proyecto de investigación.

3.5.1.3 Formula

$$n = \frac{z^2 * p * q * N}{z^2 * p * q + (N-1) * E^2}$$ Ecuación 1

n= muestra
N= Población
p= probabilidad de que un miembro de la población esté en la muestra (0.5)
q= probabilidad de que un miembro de la población no esté en la muestra (0.5)
E= error (0.05)
Z= valor normalizado con la confiabilidad (1.96)

$$q = 1 - p$$
$$q = 1 - 0.5$$
$$q = 0.5$$
$$n = \frac{(1.96)^2 * 0.5 * 0.5 * 160}{(1.96)^2 * 0.5 * 0.5 + (160 - 1) * (0.05)^2}$$
$$n = \frac{153{,}664}{1{,}3579}$$
$$n = 113$$

3.6 Operacionalización de las variables

Tabla 1. Análisis de Variables

Variables independientes			
Variables	**Concepto**	**Indicadores**	**Técnicas e instrumentos**
• Diseño del sistema de seguridad inteligente para el barrio la Merced de la ciudad de Riobamba	• Información proponente acerca de los sistemas de seguridad mediante tecnología IoT	• Video vigilancia • Acceso • Indicadores Remotos	• Cámaras • Sensores • Tarjetas RFID
• Plataforma de seguridad IoT	• Periodicidad en que los moradores ingresan a la plataforma IoT. • Periodo de tiempo que dedica a interactuar con la plataforma.	• Servidores • Páginas Web • Dispositivos Móviles	• Matlab • Python • ThingSpeak

Fuente: *Autor*

3.7 Análisis de requerimientos

3.7.1 Elementos y Dispositivos requeridos para el sistema de comunicación IOT

3.7.2 Cámaras de Seguridad

Para este sistema se ha decidido trabajar con cámaras IP de la marca HIKVISION tipo Domo para exteriores DS-2CD1123GOE-I de 2MP y cámara Tubo DS-2CD1021-I, que a continuación se detallarán sus características:

Para la elección de cámaras de seguridad para el sistema de debe tomar en cuenta los siguientes parámetros:

En el sistema de video vigilancia se va a utilizar cámaras IP POE, las cuáles cuenten con un alcance de aproximadamente unos 200 metros para poder detectar personas e identificarlas, mismas que estén en la capacidad de soportar las diferentes condiciones climáticas que se presenten para no alterar su correcto funcionamiento, otro de los factores a tomar en cuenta es la visibilidad de las cámaras es por ello que se va a utilizar dos diferentes tipos de cámaras donde una de ellas cuenta con visión nocturna mientras que el otro tipo de cámara soporta un estándar mayor en cuanto a calidad de video e imágenes. Es por ello que para el diseño del CCTV se consideró utilizar las siguientes cámaras que se visualizan en el siguiente cuadro detallado.

Tabla 2. Características cámaras Hikvision

 **Características cámara IP HIKVISION Domo DS-2CD1123GOE-I**	
Modelo	DS-2CD1123GOE-I
Sensor de Imagen	1/2.7”Progressive Scan CMOS
Resolución	1920 x1080
Iluminación Mínima	Color: 0.01 Lux @(F2.0, AGC ON), B/W: 0 Lux with IR
Protocolos	Tcp/ip, ICMP,HTTPS, FTP, DHCP, DNS, DDNS, RTP, RTSP, RTCP, NTP, UPnP, SMTP, IGMP, 802.QX, QoS, IPv6, Bonjour, IPv4, UDP, SSL/TLS
Lente Longitud Focal	2.8mm, horizontal FOV 112.1º, vertical FOV 60.0º, diagonal FOV 132.2º 4mm, horizontal FOV 90.2º, vertical FOV 48.6º, diagonal FOV 107.6º
Rango de ajuste	Pan:0º to 355º, tilt: 0º to 75º
Rango IR	Hasta 30 (m)
Fuente de Alimentación	12 VDC POE
Nivel de protección IP	IP67
Compresión de video	Main Stream: H.265/H.264/H.264+/H.265+ Sub-Stream: H.265/H.264/MJPEG
Software Cliente	iVMS-4200, Hik-Connect
 **Características cámara IP HIKVISION Tubo DS-2CD1021-I**	
Modelo	DS-2CD1021-I
Sensor de Imagen	1/2.8”Progressive Scan CMOS
Resolución	1920 x1080
Iluminación Mínima	Color: 0.01 Lux @(F1.2, AGC ON), 0 Lux with IR
Protocolos	Tcp/ip, ICMP,HTTPS, FTP, DHCP, DNS, DDNS, RTP, RTSP, RTCP, NTP, UPnP, SMTP, IGMP, 802.QX, QoS, Ipv6, Bonjour

Lente Longitud Focal	Lente Longitud Focal
Rango de ajuste	2.8mm, @F2.0, horizontal field of view 105.8º,4mm @F2.2, horizontal field of view 83.6º, 6mm @F2.0, horizontal field of view 55º
Rango IR	Hasta 30 (m)
Fuente de Alimentación	12VDC POE
Nivel de protección IP	IP67
Compresión de video	Main Stream: H.264/H.264+ , Sub-Stream: H.264/MJPEG
Software Cliente	iVMS-4200, Hik-Connect

Fuente: *Autor*

3.7.2.1 Altura de Colocación

Para contar con un sistema óptimo de video vigilancia se debe tomar en cuenta factores importantes como la altura de la ubicación de las cámaras, iluminación, ángulos, así como también puntos muertos. La altura correcta en áreas externas puede variar entre los 4 y 5 metros, y en áreas internas contar con una altura máxima de hasta 3 metros.

Tomando en cuenta estas consideraciones se colocarán las cámaras a 4 metros de altura, ya que son cámaras exteriores, y además se contarán con un soporte metálico para la colocación de componentes adicionales utilizados para el sistema.

3.7.2.2 Sensor, tipo de lente y ángulo de visión de las cámaras

En el diseño del sistema se utilizará 3 cámaras HIKVISION tipo domo y una cámara tubular, todas con una resolución de 2 megapíxeles para imágenes claras y detalladas, en este caso la cámara tipo Bullet cuenta con un rango de lente de 2.8mm, un sensor de 1/2.8" con escaneo progresivo, cuenta con visión nocturna para procesar una vigilancia efectiva con poca luz, al ser una cámara tipo tubo de lente variable permite un ángulo de cobertura de 90 a 30º, con una mayor distancia de visibilidad. En cambio, las cámaras tipo domo cuentan con un rango de lente de 2.8mm, un sensor de 1/2.7" con escaneo progresivo, este tipo de cámaras cuentan con un ángulo de ajuste de acuerdo a las necesidades de los usuarios.

3.7.2.3 Tipo de Comprensión

La compresión de video la podemos definir como el proceso de codificación y decodificación de una cámara, en este caso la compresión de la cámara tipo Bullet es H.264 el cuál es un estándar que permite una transmisión con mejor calidad de video full

Motion y requiere menor ancho de banda y latencia en comparación con los estándares tradicionales.
Para las cámaras tipo domo cuentan con el estándar H.264 y H.265, en este caso estas cámaras cuentan con dos tipos de comprensión, como se mencionó anteriormente el estándar H.264 permite una transmisión de mejor calidad mientras que el estándar H.265 permite una codificación de video de alta eficiencia, uno de los principales objetivos de este estándar es brindar mejor calidad de video con alta resolución en un menor espacio y así no saturar las conexiones de internet.

3.7.2.4 Condiciones Climáticas

Las cámaras tipo domo elegidas para el sistema cuentan con protección IP66, lo que significa el grado de resistencia del dispositivo frente a factores como el polvo, agua y cambios climáticos. Estos equipos que cuentan con esta protección son herméticos al polvo y logran soportar potentes chorros de agua, es por ello que este tipo de cámaras que cuentan con esta protección son recomendables para instalaciones exteriores.

Mientras que la cámara tipo Bullet cuenta con protección IP67, el cuál es un estándar de alto nivel de protección para el polvo y agua, estas cámaras al contar con este tipo de protección están 100% protegidos y cuentan con una resistencia comprobada de estar sumergidas bajo un metro de agua de hasta 30 minutos sin alterar su correcto funcionamiento [17].

3.7.2.5 Visión Nocturna

En la actualidad las cámaras de seguridad están incorporadas con un sistema de infrarrojos que ayudan a tener una mejor visualización por la noche, así como también es espacios con poca iluminación, en este caso los dos tipos de cámaras elegidas en el diseño del sistema cuenta con una iluminación infrarroja (IR) de hasta 30m.

3.7.2.6 Alimentación a través de Ethernet (POE)

Para la alimentación de nuestro sistema de cámaras se tomó la alternativa de hacerla mediante Ethernet (POE), el cuál es una alimentación a través de Ethernet, esto significa que la corriente eléctrica necesaria para el funcionamiento de estos dispositivos será a través de los cables de datos, remplazando así los cables de alimentación.
Este método reduce significativamente el número de cables, ya que solo se realizará el tendido de una sola red tanto para datos como para alimentación será llevada por un mismo cable, y al utilizar esta tecnología reducen en un grado significativo interferencias entre ellos, esto debido a que los datos y la electricidad son transportados en extremos opuestos del espectro de frecuencias. Es así como la electricidad utiliza una frecuencia de

60 Hz o menos y la transmisión de datos trabaja con frecuencias altas de entre 10 a los 100 millones de hercios.

3.7.2.6.1 Ventajas de tecnología POE

- Suministro Simultáneo de datos y alimentación: quiere decir que con un solo cable se puede suministrar energía y conectividad a los dispositivos en este caso las cámaras IP.

- Conectar dispositivos en áreas de difícil acceso: Las cámaras de seguridad normalmente son ubicadas en zonas de difícil acceso (exteriores de edificios, techos, paredes de altura considerable, etc.) los mismos que no cuentan con acceso a una fuente de alimentación. Por lo que POE brinda la facilidad de conectar y alimentar a estos dispositivos mediante un cable Ethernet con un puerto RJ-45.

- Rentabilidad: En cuanto a costos de instalación se reducen con esta tecnología debido que solo se requiere un cable para datos y alimentación, también en canalización y mano de obra, ya que reduce el tiempo de instalación debido a que es una sola red.

- Instalación Sencilla de dispositivos: Con POE la instalación de equipos en lugares que no cuenten con alimentación para tomas de corriente será fácil y se podrá realizar la instalación en cualquier lugar.

- Fiabilidad: Para las operaciones comerciales la pérdida de energía causa pérdidas de dinero y tiempo, pero en las redes LANs suelen contar con protección a fallos eléctricos mediante un sistema de alimentación ininterrumpida, por lo que los dispositivos conectados mediante POE se mantendrán encendidos y conectados todo el tiempo, así exista un corte de energía en la red principal.

3.7.2.7 Cálculo del ancho de banda y capacidad de almacenamiento

Mediante el formato de compresión de las cámaras que van a ser utilizadas, la calidad de grabación y la resolución se puede obtener un promedio de la imagen, entonces lo primero que se va a calcular es la cantidad de bytes por segundo de video utilizando los fotogramas por segundo (FPS) o también conocida como velocidad de grabación, siendo la calidad de grabación 20 FPS ya que se ocupa la compresión de video H.265+, la resolución de 1920, el promedio de porcentaje de actividad continuo será del 100% ya que habrá una grabación continua las 24 horas del día en los 7 días de la semana.

$$Espacio\ para\ 1\ segundo\ de\ video = FPSxBytesx\%Actividad = [Bps]$$
$$Espacio\ para\ 1\ segundo\ de\ video = 20FPSx1920x100\%$$
$$Espacio\ para\ 1\ segundo\ de\ video = 4KB$$ Ecuación 2

Una vez obtenido la cantidad de bytes por segundo de video podemos calcular el ancho de banda aplicando la siguiente fórmula:

$$BW = Espacio\ para\ 1\ segundo\ de\ video x 8 = [bps]$$
$$Bw = 20FPSx4KBx100\%x8$$
$$BW = 640kbp \quad \text{Ecuación 3}$$

Luego de obtener el ancho de banda se puede calcular la capacidad de almacenamiento del disco duro del videograbador del sistema.

$$Capacidad\ de\ almacenamiento = BWx3600sx24h = [GB]$$
$$Capacidad\ de\ almacenamiento = 640kbpx360osx24h$$
$$Capacidad\ de\ almacenamiento = 55.3GB \quad \text{Ecuación 4}$$

Una vez realizado los cálculos concluimos que para el sistema que de seguridad IOT se requiere de:

Tabla 3. Resultados cálculo ancho de banda y capacidad de almacenamiento de cámaras

Número de cámaras	Ancho de banda	Capacidad de almacenamiento por día
1	640 kbps	55.3 GB
4	2.56 Mbps	0.22 TB

Fuente: *Autor*

3.7.3 Raspberry Pi

Conocido como un mini ordenador, con funcionalidades muy avanzadas, con precios asequibles para los usuarios, esta placa surge en el Reino Unido con la finalidad de incentivar aprendizajes de informática en colegios e instituciones superiores, los modelos de Raspberry pi conformados por 40 pines que pueden ser utilizados tanto de entrada como salida, en la actualidad existen los modelos Pi Zero, PI1, Pi2, PI3 y Pi4, próximo a ser lanzado el modelo PI5, el cual contará con funciones más avanzadas en cuánto a elementos y capacidades del mismo hardware, esta placa está conformada por:
Procesador Central (CPU): este es un procesador interno Broadcom System on chip, es decir que tanto el audio como el hardware están integrados en un mismo chip.

Procesador Gráfico: Esta parte de la placa contiene estándares de compresión que están entre MPEG-2 hasta H.265.

Módulo de memoria RAM: En esta parte contiene un único módulo de memoria RAM, donde dependía del modelo se trabajaba con memorias desde los 4 GB hasta en la actualidad soportar modelos de 128 GB, cabe recalcar que para el proyecto se trabajó con una memoria de 32 GB, debido a que ciertas librerías no funcionan de la manera correcta según la SD que utilice el sistema.

Conector RJ45: permite conectividad directa de la Raspberry hacia la PC, los primeros modelos de esta placa no contaban con módulos Wi-fi integrados, hoy en día esta es una opción que ayuda a trabajar los proyectos de una manera más rápida y mejor y así poder ubicar la Raspberry de acuerdo a las necesidades del proyecto.

Buses USB: estos buses permiten la interconexión entre la Raspberry y otros dispositivos externos.

Salida Digital de Video +Audio HDMI: este es un puerto capaz de soportar tanto señales de audio como de video, lo que quiere decir que con un solo cable conectado a una pantalla es posible generar las dos señales, obteniendo una conexión digital eficiente y de alta calidad para visualizar imágenes.

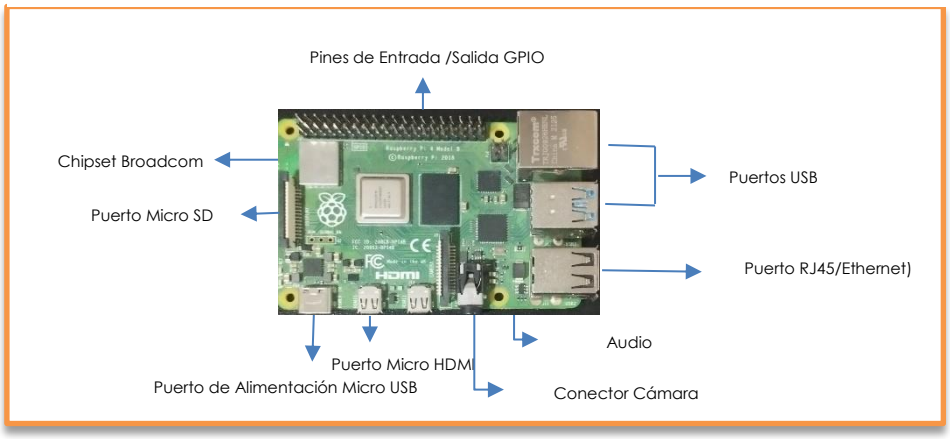
Salida Analógica de audio estéreo: este conector será necesario utilizarlo en el determinado caso que el display no contenga algún puerto de entrada HDMI.

Salida Analógica de video RCA: este componente fue diseñado para conectar dispositivos de pantalla con la Raspberry Pi, sin embargo, puede existir interferencias, fallas, resolución de baja calidad y limitada.

Conector de Alimentación micro USB: Para encender la Raspberry se cuenta con un conector micro USB tipo C de 5V, de un promedio de 700 mA de consumo, esta placa carece de botón de encendido y apagado, una vez conectado a este puerto la Raspberry se iniciará inmediatamente.

Lector de tarjetas SD: este micro ordenador no cuenta con un disco duro como generalmente los ordenadores comunes, es por esto que trabaja a través de un lector para memorias SD, por ello es importante adicionar una SD que tenga la capacidad de almacenamiento para albergar el sistema operativo, por lo general es recomendable trabajar con SD de 32 GB, ya que al trabajar con una de mayor capacidad se requiere realizar ciertas configuraciones para trabajar con librerías específicas.

Figura 9. Esquema General de una Raspberry Pi y sus elementos



Fuente: *Autor*

3.7.4 Disco duro 2TB

En este proyecto se utilizó un disco duro externo tipo SATA el cual permite almacenar información, este tipo de dispositivo se lo puede llevar fácilmente y conectar o desconectar desde otro dispositivo que se desee usar los archivos almacenados en el mismo, en este caso la Raspberry Pi se utilizó junto al disco duro para hacer un servidor NAS local para almacenar videos e imágenes de las cámaras de seguridad de este proyecto.

Figura 10. Disco Duro externo 2TB

Fuente: *Autor*

3.7.5 Switch POE

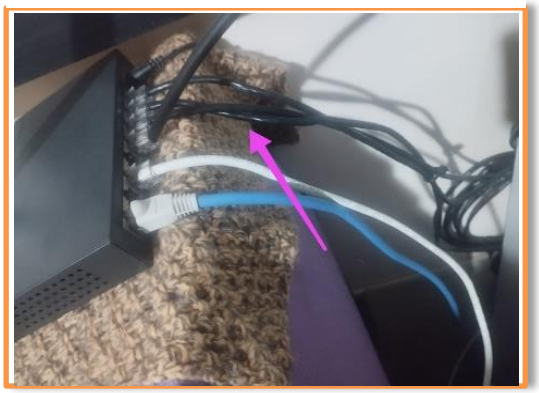
Como se mencionó anteriormente la alimentación de las cámaras se va a realizar mediante tecnología POE para ello se requería conectar las cámaras a puertos POE en un switch, por lo que se adquirió un switch tp-link Gigabit de 8 puertos, el cual contiene 4 puertos Poe requeridos para la conexión de las cámaras, con la utilización de este switch se garantizó una conexión óptima de los dispositivos.
La tecnología POE está basada en los estándares IEEE 802.3, estos estándares definen como debe ser la operatividad de equipos conectados a la red entre ellos y garantizar la interoperabilidad mundial [18].

Figura 11. Switch POE tp-link

Fuente: *Autor*

3.7.6 Cable UTP cat 6 exteriores 100% cobre

Figura 12. Cable UTP cat 6 100% cobre



Fuente: *Autor*

Para enlazar los equipos terminales que en este caso son las cámaras con el switch se decidió utilizar cable UTP cat 6 para exteriores 100% cobre y así garantizar pérdidas en los enlaces, al utilizar este tipo de cable se logró realizar las conexiones a largas distancias sin tener ningún tipo de problema en la instalación y visualización de las cámaras, mediante este tipo de cable se transportó energía y datos para el sistema de cámaras.

Los dispositivos mencionados anteriormente se podrían tomar como el punto de inicio para la implementación del sistema, pero no obstante se trabajó con otros componentes como son:

3.7.7 Sirena

Las sirenas son componentes necesarios dentro de un sistema de seguridad ya sea en el hogar, negocio, escuelas, edificios, parques, ya que estos dispositivos emiten un sonido de alta potencia permitiendo así advertir a la ciudadanía de un posible evento de hurto o emergencia.

Figura 13. Sirena 110V

Fuente: *Autor*

3.7.8 Módulos ESP32

Este módulo que está integrado de Wi-fi y Bluetooth, permite trabajar en un sin número de aplicaciones, su temperatura de funcionamiento está entre -40ºC y 125ºC, es muy utilizado para aplicaciones IOT, con un bajo consumo de energía, trabaja a 5V, trabaja como un sistema independiente o puede ser utilizado como dispositivo esclavo de un software anfitrión, los lenguajes de programación utilizados son Arduino IDE, Python o LUA.

Figura 14. Módulo ESP32

Fuente: *Autor*

3.7.9 Extensor tp-link Wi-fi TL-WA855RE

Este dispositivo de tamaño pequeño, permite extender el área de conexión Wi-Fi en áreas a las que el router no llega su señal, es fácil de usar e implementar, requiere de conexión a un toma corriente, lo demás es configurarlo a la red a la que se va a conectar, definirlo como un nombre de red, este puede ser diferente al de la red local y la contraseña se la puede establecer solo para este dispositivo, entonces para acceder a esta nueva red se debe acceder ingresando los datos de usuario y contraseña que se le asignará al momento de configurarlo.

Figura 15. Extensor tp-link

Fuente: *Autor*

3.7.10 Sensor PIR

Son dispositivos ópticos que se utilizan para detectar el movimiento en determinadas áreas, estos trabajan en las variaciones de la radiación electromagnética en el entorno, y el rango de luz infrarroja, estos dispositivos se activan al detectar un movimiento enviando un pulso para indicar para informar que se ha detectado una persona o un objeto en movimiento en el área colocado.

Figura 16. Sensor PIR

Fuente: *Autor*

3.7.11 Pantalla LCD

Una pantalla LCD es un dispositivo de cristal líquido, utilizado para visualizar imágenes fijas o en movimiento, estas pantallas tienen una luz de fondo las que alimentan de luz de fondo a cada pixel ubicado en la cuadrícula rectangular, estos píxeles están conformados por un subpíxel (rojo, verde o azul), que se activa o desactiva cuando se requiere.

Figura 17. Pantalla LCD

Fuente: *Autor*

3.7.12 Soporte Metálico

Los soportes metálicos son colocados en paredes o techos, que permite dar mejor ángulo de visibilidad para las cámaras y así ubicarlas para dar el enfoque deseado en la instalación, entonces depende de la ubicación de las cámaras se requiere el brazo con medidas específicas. Para este sistema se realizó un previo diseño con las medidas necesarias para ubicar las cámaras de seguridad y las cajas con los dispositivos adicionales al sistema como se puede apreciar en la siguiente figura.

Figura 18. Soporte Metálico

Fuente: *Autor*

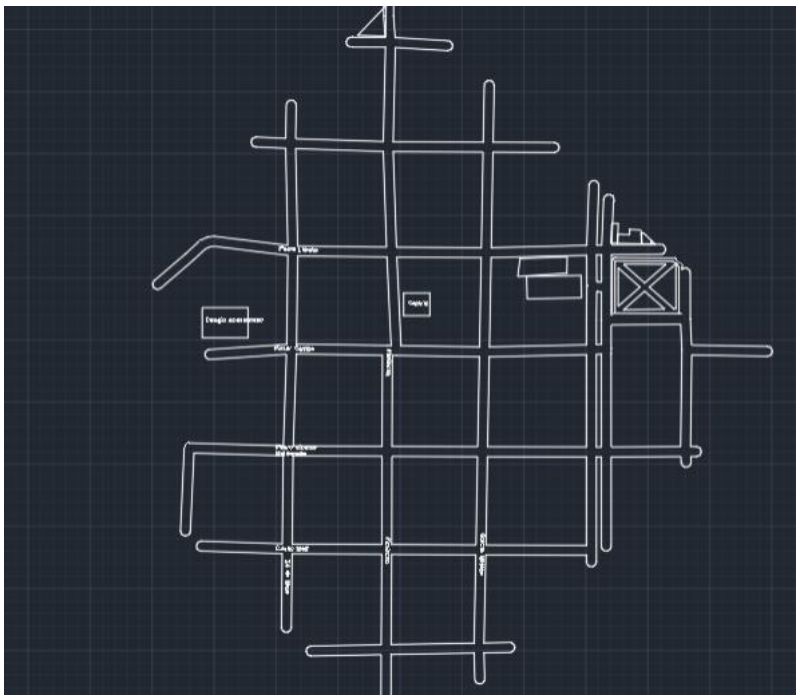
3.8 Diseño del Sistema de comunicación IoT

3.8.1 Estudio y Asignación de puntos estratégicos para ubicación de las cámaras de seguridad

Para iniciar con el diseño de nuestro sistema lo primero que procedemos es realizar un estudio del área geográfica a cubrir en el barrio La Merced de Yaruquies, como apreciamos en la siguiente figura, el área a cubrir es de una manzana (cuatro cuadras), entonces lo que se realizó es un previo análisis de la ubicación de las cámaras de seguridad y se realizó una reunión con los usuarios del barrio para llegar a un acuerdo e indicar los puntos estratégicos donde se van a ubicar cada una de ellas y pedir la aprobación para la posterior ubicación en los lugares determinados.

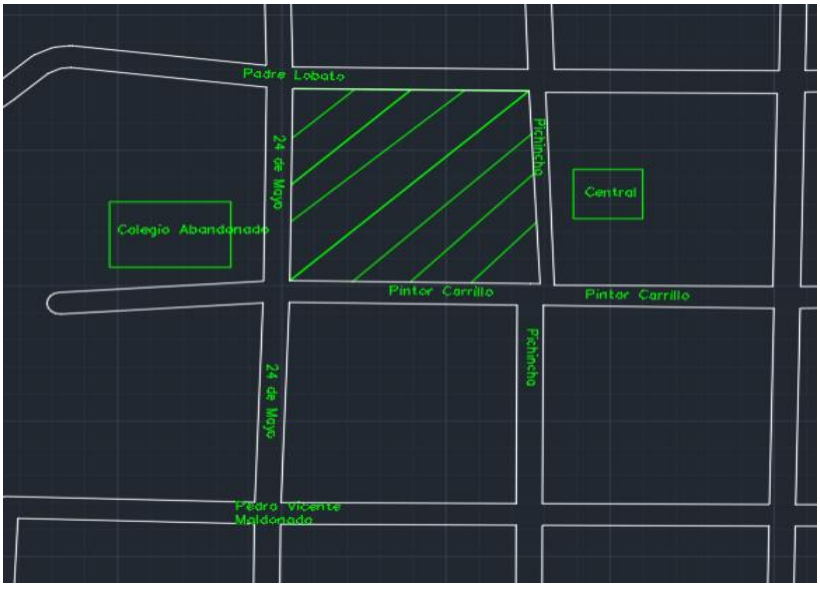
Entonces lo que primero se hace es el diseño de los planos de Yaruquies y así ubicar el Barrio la Merced que es el objeto de estudio.

Figura 19. Planos AutoCAD de Yaruquies



Fuente: *Autor*

Figura 20. Planos AutoCAD Barrio La Merced



Fuente: *Autor*

Como se aprecia en la imagen se va a instalar cuatro cámaras siendo el nodo principal en las calles Pichincha y Pintor Carrillo, teniendo un enfoque hacia la calle Pichincha, la segunda cámara se va a ubicar en la calle Pichincha en la casa esquinera teniendo un enfoque hasta el final de la calle Pichincha con la intersección de la calle Maldonado, la tercera cámara se va a ubicar en la calle 24 de mayo en la casa esquinera de 4 pisos con un enfoque hacia el colegio abandonado el cual es un punto clave ya que ahí se da reuniones de antisociales y además de abarcar la calle 24 de mayo hasta llegar a la intersección con la calle Padre Lobato, y la cuarta cámara se ubicara en la calle Pintor Carrillo en la casa esquinera de 4 pisos dando un enfoque hacia esta calle teniendo un alcance hasta la intersección con la calle García Moreno.
Con la ubicación de estas cámaras en los puntos mencionados se abarcará el área deseada, logrando así tener puntos clave de visualización y protección para esta área determinada.

Figura 21. Estudio de los puntos estratégicos de las cámaras de seguridad Barrio La Merced

Fuente: *Autor*

Para la ubicación de las cámaras se hizo un estudio previo del índice de personas que a diario circulan por estas calles, llegando a determinar así los requerimientos necesarios tanto en cobertura como en funcionalidad de las cámaras, para llegar a tener un modelo confiable, accesible para los usuarios del barrio la Merced de Yaruquies de la ciudad de Riobamba.

3.8.2 Instalación Sistema Operativo Raspberry PI

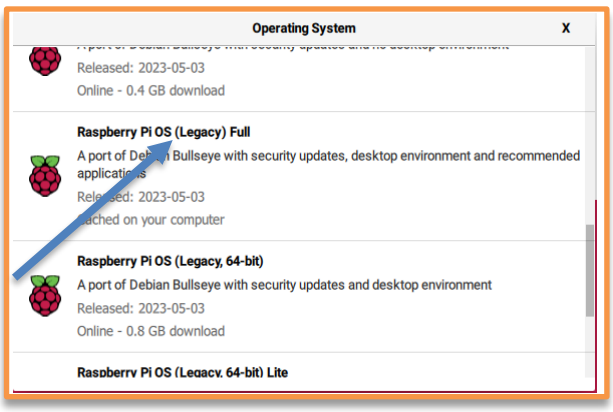
Una vez que se determinó los puntos estratégicos para la ubicación de las cámaras se inició con la parte de diseño del proyecto, para ello se realizó varios estudios para determinar el funcionamiento de la Raspberry Pi y así proceder con la instalación del sistema operativo, se inicia ingresando a la página oficial **Raspberry Pi OS – Raspberry Pi**, para descargar la imagen del sistema operativo y se elige la imagen para Windows, una vez descargada la imagen, se ejecuta como administrador y se realiza su correcta instalación, donde aparecerá la siguiente ventana:

Figura 22. Aplicación para instalar la imagen del sistema operativo de la Raspberry Pi

Fuente: *Autor*

En esta aplicación se determina la imagen del sistema operativo para la Raspberry Pi, para ello se instalará **Debian Bullseye** de 32 bits con escritorio, ya que al iniciar se realizó pruebas con la instalación de **Debian Bookworm** de 32 bits, pero se encontraron varios errores en cuanto a la instalación de las librerías que se requerían para instalar ciertas aplicaciones necesarias para el proyecto que se mencionarán más adelante, esta imagen se instaló en una MicroSD de 32 bits.

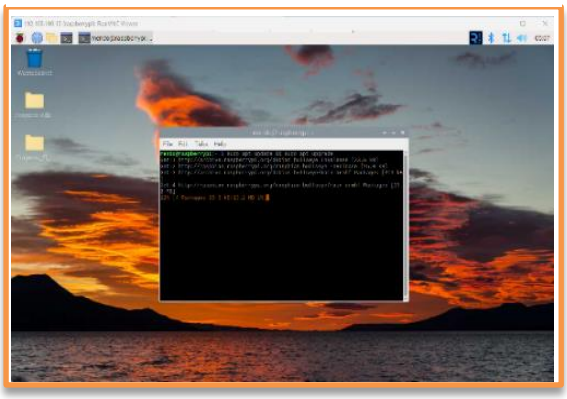
Figura 23. Aplicación para instalar la imagen del sistema operativo de la Raspberry Pi



Fuente: *Autor*

Para arrancar el sistema operativo se coloca la MicroSD en el puerto para SD de la Raspberry Pi e inicia enseguida el proceso, la instalación se la puede realizar de dos maneras mediante una pantalla conectada al puerto microHDMI de la Raspberry junto con mouse y teclado necesarios para las configuraciones iniciales, y el otro método es arrancar la Raspberry mediante conexión remota SSH, donde se configuró la habilitación de VNC server para con la ayuda de VNC Viewer una aplicación descargada de la página oficial de VNC abrir el escritorio de la Raspberry Pi, mediante conexión remota, en este caso se probó la instalación de las dos formas, las cuales funcionan perfectamente, para mayor comodidad se decide trabajar mediante escritorio remoto con VNC Viewer.
Lo primero es iniciar con la actualización e instalación de los repositorios de paquetes utilizando los siguientes comandos en el terminal:

Figura 24. Instalación y actualización de los paquetes del repositorio

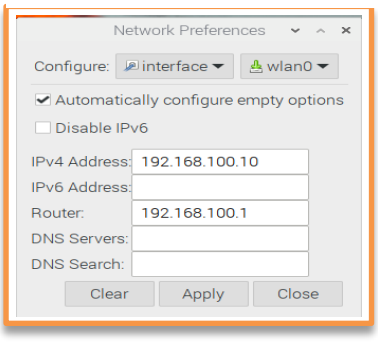


Fuente: *Autor*

3.8.3 Asignación de IP Fija a Raspberry Pi

Para realizar este procedimiento se debe ubicar en la parte derecha de la pantalla de nuestro escritorio remoto, hacemos clic en el símbolo de redes, en este caso está conectado mediante Wi-FI, y al dar un clic derecho nos aparecerá la siguiente ventana:

Figura 25. Asignación de una IP fija a la Raspberry Pi



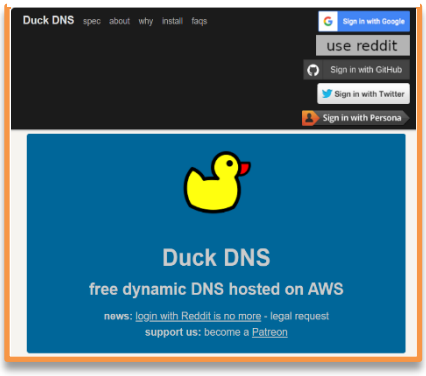
Fuente: *Autor*

En esta ventana asignaremos la IP de la Raspberry que se asignó mediante el router, esta es la 192.168.100.10 e incluimos la IP del router la cuál es 192.168.100.1 y asignaremos los servidores DNS, damos en aplicar y la Raspberry contará con una IP fija.

3.8.4 Configuración de DDNS dinámico

Para la asignación de DNS dinámico existen varias opciones tanto de pago como gratuitas, para la configuración en este caso se ha tomado la opción de trabajar con DuckDNS, es un servicio totalmente gratuito sin anuncios, el proceso para asignación de un DNS dinámico inicia ingresando a la página (https://www.duckdns.org)

Figura 26. Página Principal Duck DNS



Fuente: *Autor*

Donde se nos desplegará esta ventana e ingresaremos con una de las opciones que nos da con twitter, google, GitHub, en este caso se ha elegido ingresar con la cuenta de google.

Al ingresar se abrirá otra ventana donde se debe asignar un nombre de dominio que se encuentre disponible y se introduce, y el sistema da un aviso de si se puede utilizar el nombre elegido, al ser exitosa la acción ya se tendría el dominio creado.

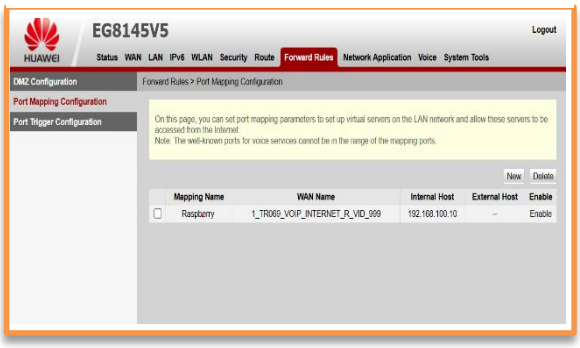
Figura 27. Configuración de Dominio Duck DNS

Fuente: *Autor*

3.8.5 Apertura de puertos en el router

En este caso se cuenta con un router Huawei del proveedor de internet Netlife, donde para ingresar se debe acceder a una página web desde cualquier dispositivo conectado a la red local, en este caso se accedió desde un ordenador a la IP 192.168.100.1, donde al ingresar los datos del usuario y contraseña, para este caso se solicitó estos datos mediante una llamada al proveedor de servicios, una vez que se ingresó al router se procede a ir a la opción Forward Rules y a continuación Port Mapping Configuration, donde añadiremos la ip fija de la Raspberry que debería estar encendida y conectada a la red LAN, para que pueda aparecer al abrir las opciones del dispositivo, se asigna un nombre un puerto y el protocolo necesario para establecer la conexión, hecho damos en aplicar y podremos verificar que la redirección de puertos se encontrará habilitada con el nombre que se asignó, como se puede observar en la imagen a continuación:

Figura 28. Página Principal Router Huawei

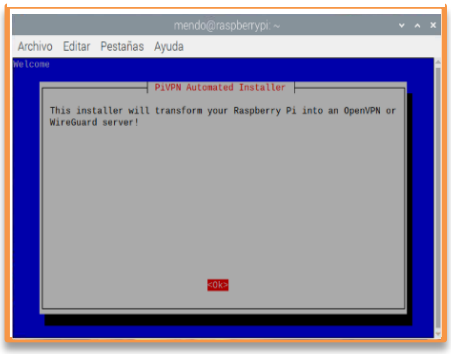


Fuente: *Autor*

3.8.6 Raspberry como servidor VPN

Para ello lo primero fue instalar servidor VPN en la Raspberry, desde el cliente que se vaya a acceder mediante esta VPN se debe instalar un software para poder establecer conexión, si se conecta desde un móvil se debe descargar de Play Store una de las opciones que Play Store cuenta para abrir este tipo de conexiones, en este caso se instaló la aplicación OPenVPN Connect, que es fácil y sencilla de instalar y usar.
Para proceder con la instalación de piVPN se debe ingresar a la consola y escribir el comando **curl -L https://install.pivpn.io | bash,** por lo que inmediatamente iniciará la descarga de paquetes necesarios para la instalación del servidor VPN, una vez que se completó la descarga ira apareciendo varias pantallas donde se deberá ir configurando para el servidor VPN, que a continuación se describirán las más importantes en este proceso.

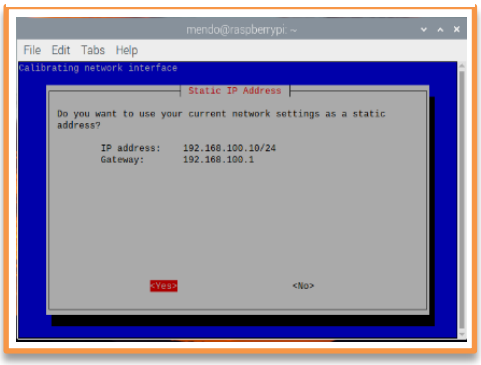
Figura 29. Configuración del servidor VPN



Fuente: *Autor*

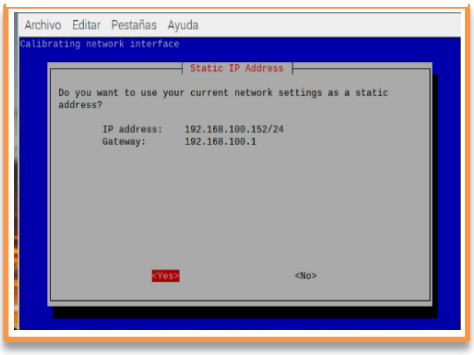
En esta página vemos que inicia la instalación para convertir la Raspberry Pi en un servidor VPN, por consiguiente, se tendrá que asignar una dirección IP fija a la Raspberry, pero en este caso este paso ya se lo realizó con anterioridad teniendo la dirección IP estática de la Raspberry PI 192.168.100.10, el Gateway es la dirección IP del router, se dará en aceptar para continuar con la instalación.

Figura 30. Configuración del servidor VPN



Fuente: *Autor*

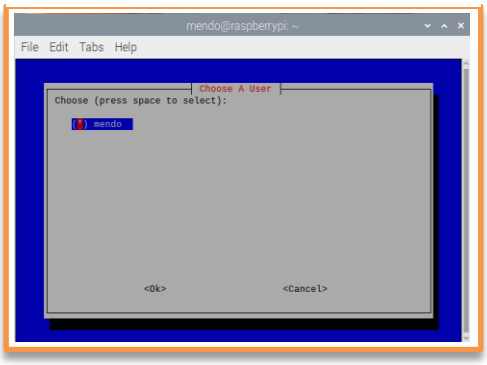
Figura 31. Configuración del servidor VPN



Fuente: *Autor*

Ahora se requiere establecer un usuario local, el mismo que es el usuario de la raspberry pi, dando en OK para aceptar trabajar con esta configuración.

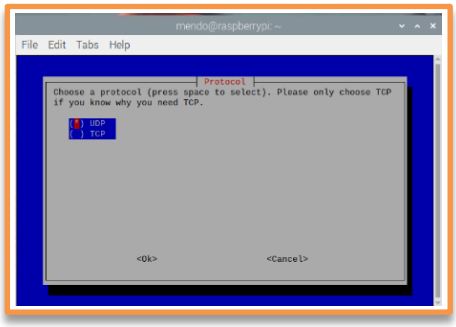
Figura 32. Configuración del servidor VPN



Fuente: *Autor*

A continuación, seleccionamos el protocolo que se va a utilizar, aquí se va a elegir el protocolo UDP, esto se debe a que este protocolo garantiza la entrega de paquetes de una manera más rápida, y por consiguiente se da en OK y continuamos al siguiente paso.

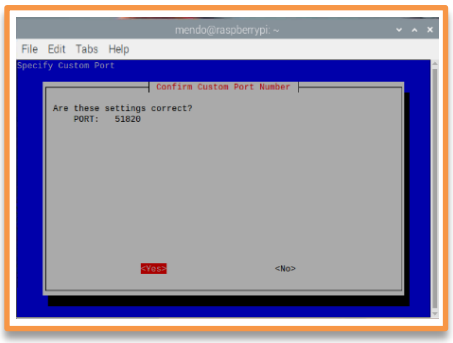
Figura 33. Configuración del servidor VPN



Fuente: *Autor*

Ahora se configurar el mismo puerto que se configuró en el router, en este caso es el puerto 51820 y se confirma que es el puerto correcto.

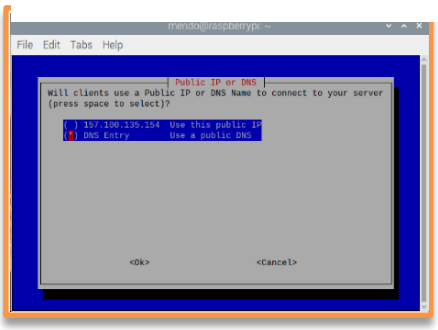
Figura 34. Configuración del servidor VPN



Fuente: *Autor*

Como siguiente paso se debe decidir si se desea trabajar con la ip pública del router o ingresar un dominio del servidor DNS, debido a que como paso inicial se creó un servidor DNS en Duck DNS, entonces se selecciona DNS Entry y se acepta.

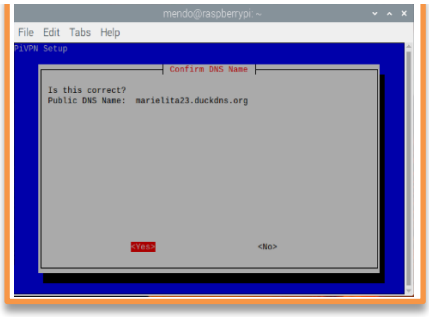
Figura 35. Configuración del servidor VPN



Fuente: *Autor*

En esta ventana se ingresa el nombre de dominio que se creó en el proveedor DNS.

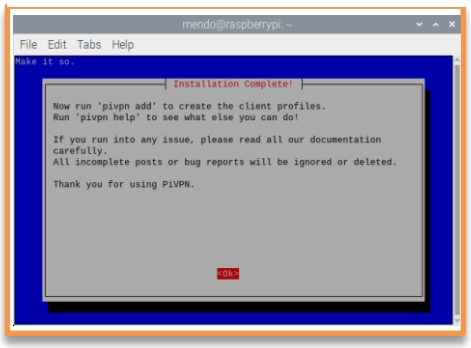
Figura 36. Configuración del servidor VPN



Fuente: *Autor*

En la siguiente imagen se observa un mensaje donde se indica que al ingresar en la consola el comando ***pivpn add,*** *se creará los archivos con extensión. ovpn de los clientes.*

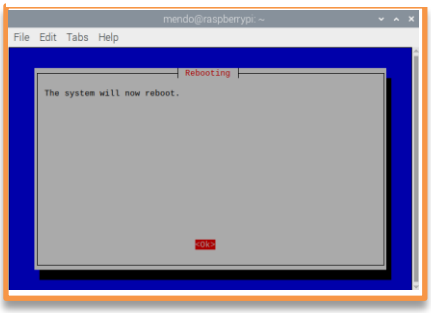
Figura 37. Configuración del servidor VPN



Fuente: *Autor*

El proceso ha finalizado con éxito, donde el último paso es reiniciar la raspberry.

Figura 38. Configuración del servidor VPN



Fuente: *Autor*

Una vez finalizada la instalación del servidor VPN en la raspberry se agregará los clientes necesarios para la conexión desde fuera de la red local, esto se realiza con el comando pivpn add y se comprobará que el túnel hacia el exterior se creó satisfactoriamente.
Una vez finalizado este proceso la Raspberry se convertirá en un servidor VPN

3.8.7 Instalación de Motioneye

Motioneye es una interfaz visual que permite controlar un número de cámaras desde una única interfaz, desde ella se pueden agregar o eliminar cámaras al sistema de video vigilancia, así como configurar las mismas para detección de movimientos, enviar un mensaje de alerta al correo electrónico y ciertas configuraciones adicionales.
Para la instalación de esta plataforma se debe ingresar en la consola de la raspberry pi, y lo primero que se debe hacer es actualizar e instalar repositorios de paquetes con el comando **sudo apt update && sudo apt upgrade**

A continuación, se debe ingresar los siguientes comandos, agregando super usuario para permitir la instalación de las siguientes configuraciones mediante **sudo su.**

Estos comandos permiten instalar los paquetes para movimiento y visualización de imágenes en motioneye.

- **apt-get install motion ffmpeg v4l-utils -y**
  systemctl stop motion
  systemctl disable motion

Estos paquetes son requeridos para motioneye, se deben instalar línea por línea.

- **apt-get install python2 curl -y**
  curl https://bootstrap.pypa.io/pip/2.7/get-pip.py --output get-pip.py

python2 get-pip.py

Mediante esta línea de comando se instalará las dependencias necesarias para los repositorios de motioneye.

- **apt-get install python-dev-is-python2 python-setuptools libssl-dev libcurl4-openssl-dev libjpeg-dev zlib1g-dev libffi-dev libzbar-dev libzbar0 -y**

Con esta instrucción se instalará las dependencias de Python.

- **pip install motioneye**

Ahora se procede a crear un directorio de configuración mediante las siguientes líneas

- **mkdir -p /etc/motioneye**
  cp/usr/local/share/motioneye/extra/motioneye.conf.sample/etc/motioneye/motioneye.conf

Una vez creado el directorio de configuración, se requiere crear el directorio de medios.

- **mkdir -p /var/lib/motioneye**

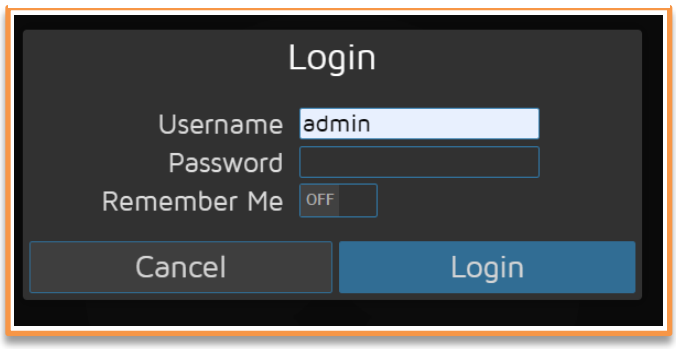
Ahora es momento de crear un script para ejecutar e inicializar el servidor

- **cp/usr/local/share/motioneye/extra/motioneye.systemd-unit-local**
  /etc/systemd/system/motioneye.service
  systemctl daemon-reload
  systemctl enable motioneye
  systemctl start motioneye

Una vez finalizados estos pasos se debe ingresar al navegador e ingresar la IP de la Raspberry PI seguido del puerto del servidor:**8765,** donde aparecerá la siguiente ventana de inicio.

*Para ingresar a la ventana principal en username se debe escribir **admin** y seleccionar login.*

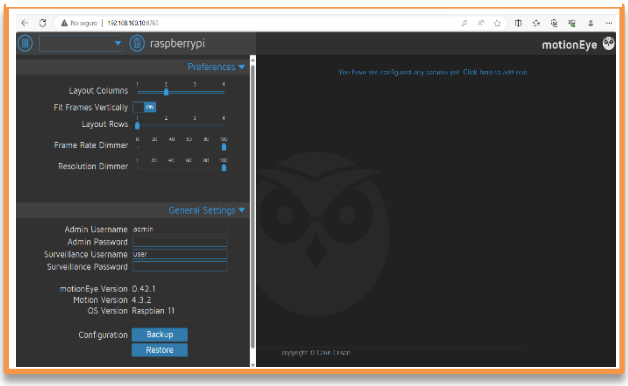
Figura 39. Ventana de Inicio Motioneye



Fuente: Autor

Posteriormente se presentará la siguiente ventana, donde se debe añadir las cámaras a ser configuradas en el sistema de video vigilancia.

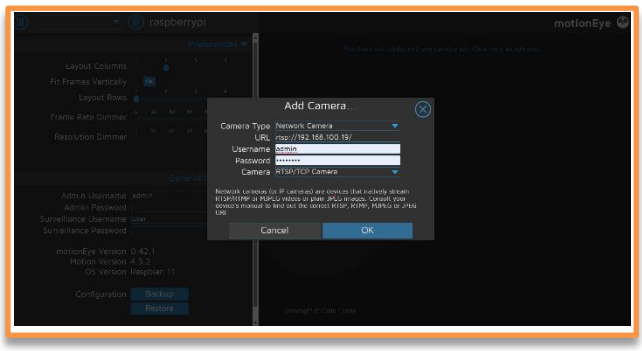
Figura 40. Ventana Principal de Motioneye



Fuente: Autor

Para añadir las cámaras IP, se debe ingresar mediante una dirección IP válida, en este caso se procede agregar de la siguiente manera:

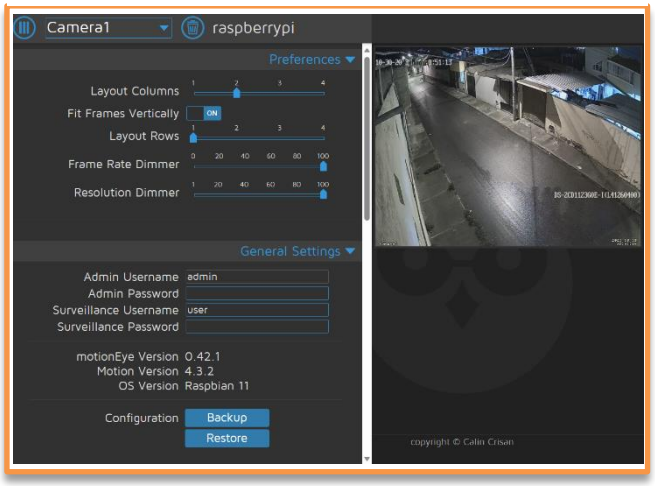
Figura 41. Ventana para añadir cámaras



Fuente: Autor

Como se observa en la imagen anterior, se debe seleccionar cámara de red, para la IP se la busca mediante RTSP, se ingresa el usuario y contraseña configurado en cada cámara y la interfaz se encarga de analizar y buscar la cámara mediante estos datos, se hace clic en OK y la cámara queda añadida a la interfaz, como se observa a continuación.

Figura 42. Cámara de Seguridad añadida a Motioneye



Fuente: Autor

Para añadir las cuatro cámaras que se tiene para el sistema, se procede a realizar el mismo paso anterior, llamando a cada cámara con la IP asignada.

Figura 43. Cámaras de seguridad en Motioneye

Fuente: Autor

Una vez añadidas las cuatro cámaras a motioneye se procede a realizar la configuración para que no exista pérdidas en los videos, tomando en cuenta los siguientes parámetros:

Frame Rate: este factor es la cantidad de imágenes que aparecerán por segundo en la cámara, la elección de este factor dependerá de la calidad de video, por lo general al

trabajar en alta definición el valor puede estar entre 23,9 fps hasta 60 fps, en motioneye el valor límite es de 30 fps, por lo que se irá ajustando hasta obtener la fluidez deseada [19].

Streaming Frame Rate: esta es una característica de las cámaras para transmitir en vivo mediante internet con una buena calidad en cuanto a video y audio, esta característica deberá ser igual al valor de Frame Rate para evitar pérdidas.

Streaming Quality: en este factor se puede determinar la calidad del Streaming de la cámara, en porcentaje.

Streaming Port: es el puerto mediante el que se realizará el Streaming de cada cámara.

Image Quality: la calidad de imagen que se desea, por lo general se quiere tener una imagen con una calidad al 100%, que es el porcentaje más alto.

Capture Mode: en este factor se puede escoger el modo de capturar las imágenes, ya sea este manual, o mediante algún movimiento detectado, como se quiere tener un sistema autónomo se debe configurar para que las imágenes sean capturadas cuando exista movimiento.

Preserve Pictures: este factor permite conservar las imágenes capturadas, ya sea por un día una semana, un mes o por siempre, y se conservará hasta que el usuario decida eliminar estas imágenes, se lo dejará por siempre.

Movie Format: son los tipos de formatos que se le puede dar al video, estos pueden ser avi, MP4, mkv, swf, flv.

Movie Quality: este factor permite configurar la calidad de video que se desea, se puede configurar de acuerdo a las necesidades del usuario, siendo el 100% el valor máximo de calidad de video.

Recording Mode: Este factor permite configurar el modo de capturar el video, este puede ser de forma manual o mediante detección de movimiento.

Preserve Movies: Permite conservar los videos, estos pueden ser por un día, un mes o por siempre.

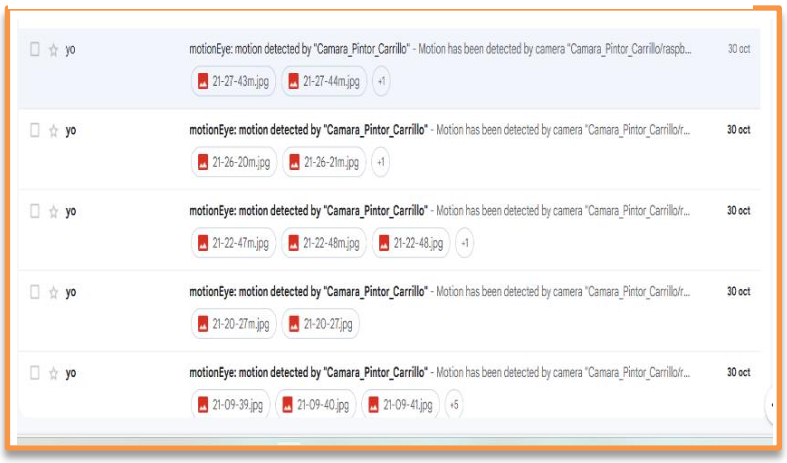
Motion Detecction: permite configurar los parámetros de detección de imágenes y videos, se puede configurar cuantas capturas se van a realizar en cada detección antes y después del movimiento, así como crear un cuadro para capturar las imágenes de los movimientos, estos parámetros deben ser muy bien configurados para evitar capturas innecesarias y emita imágenes o videos ante movimientos falsos, como se observa en la siguiente imagen.

Figura 44. Detección de movimiento en Motioneye

Fuente: Autor

Motion Notifications: mediante este parámetro se puede enviar notificaciones de movimientos detectados por las cámaras, está característica se activó para enviar las imágenes mediante correo electrónico configurando un correo determinado para capturar las imágenes mediante el protocolo SMTP.

Figura 45. Notificación de Motioneye en correo electrónico



Fuente: Autor

Working Schedule: este parámetro permite configurar el horario y días para la detección de movimiento, puede ser los 7 días de la semana, las 24 horas, esto dependerá de las necesidades del usuario, para el sistema se configuró para que capture imágenes los 7 días de la semana en horarios de 11 de la noche a 5 de la mañana, y los videos se guarden todo el día.

File Storage: este apartado es para determinar donde sea van a guardar las imágenes y videos, por lo general esto será enviado a la memoria de la raspberry, en este sistema se

configuró para que sean re direccionados a un disco duro externo conectado a la raspberry de 2 TB.

3.8.8 Instalación de Open CV y Tkinter

Posteriormente se realizó la instalación de Open CV, que sirve para visualizar imágenes, este procedimiento se tarda alrededor de 2 horas, pero si se sigue los pasos necesarios la instalación finalizará correctamente, este paso es necesario ya que se necesita cargar imágenes en la interfaz deseada para el sistema de video vigilancia.
Para la instalación se debe seguir los siguientes pasos:
Primero se debe actualizar e instalar los repositorios de los paquetes con la siguiente línea de comando, abriendo una consola de Raspberry Pi.

- **sudo apt update && sudo apt upgrade**

Con estas líneas se instalará las dependencias necesarias para instalar OpenCV.

- **sudo apt install build-essential cmake pkg-config libjpeg-dev libtiff5-dev libjasper-dev libpng12-dev libavcodec-dev libavformat-dev libswscale-dev libv4l-dev libxvidcore-dev libx264-dev libgtk2.0-dev libatlas-base-dev gfortran**

Se requiere instalar Python y pip, con los siguientes comandos:

- **sudo apt install python3**
  sudo apt install python3-pip

Con la siguiente línea se descarga OpenCV:

- **wget -O opencv.zip https://github.com/opencv/opencv/archive/master.zip**

Como el archivo se descarga en .zip se debe leer con la siguiente línea de comando:

- **unzip opencv.zip**

A continuación, se debe crear un directorio de compilación utilizando el comando:

- **cd opencv-master**
  mkdir build
  cd build

Con el siguiente comando se compila e instala OpenCV:

- **make -j4 # Cambia 4 al número de núcleos de tu Raspberry Pi para acelerar la compilación**
  sudo make install

Ahora ya se tiene instalado y listo para utilizar OpenCV.

3.8.9 Instalación de Firebase en Raspberry Pi

Firebase es una plataforma de desarrollo de aplicaciones de google que proporciona un conjunto de herramientas y servicios, que ayudan a los desarrolladores crear aplicaciones de alta calidad de una forma fácil y rápida.

Para instalar Firebase en Raspberry Pi se requiere tener instalado Python y pip
Entonces primero se verifica si se tiene instalado Python y pip en la Raspberry Pi con los siguientes comandos:

- **python –versión**
- **pip –version**

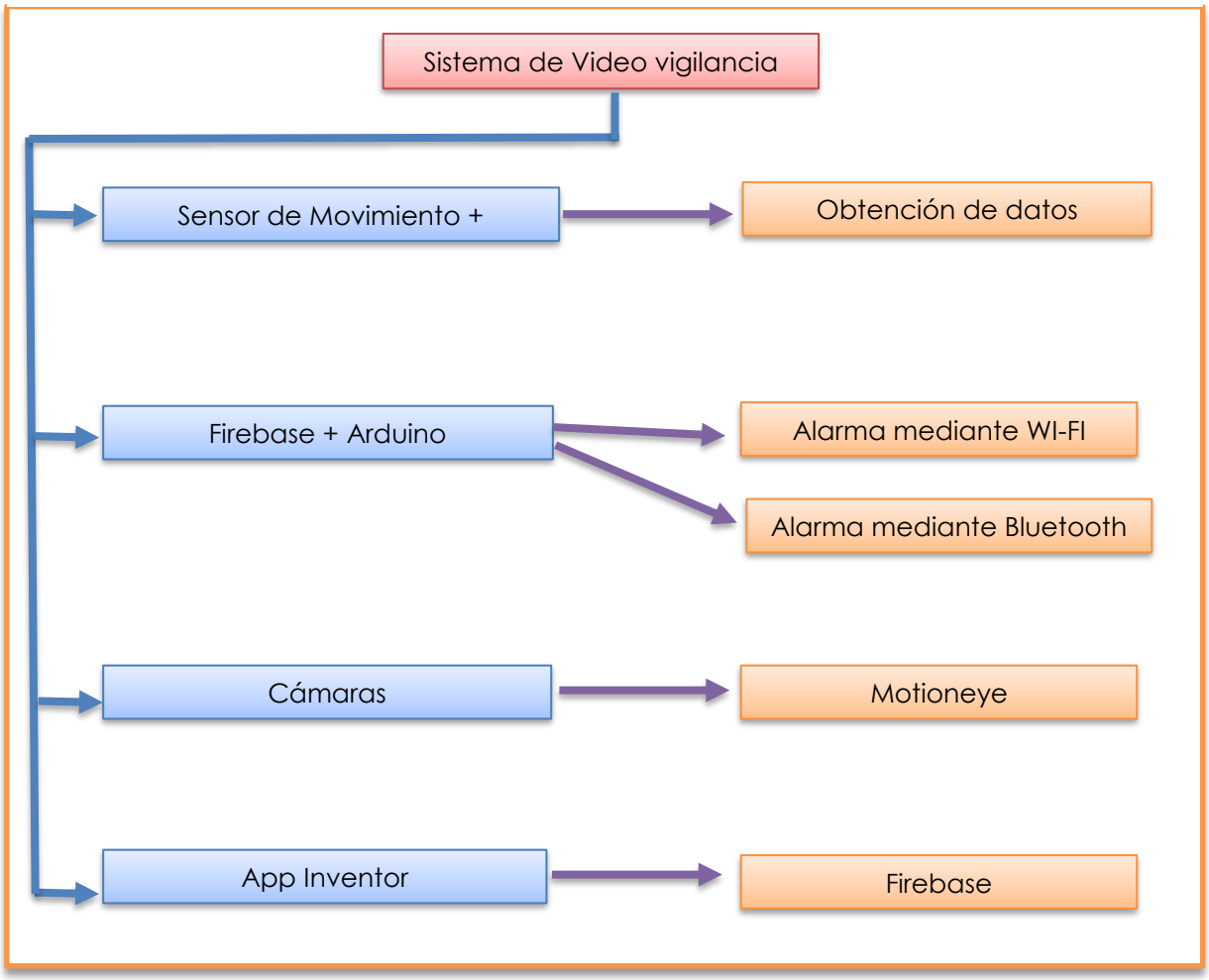
Para OpenCV y Motioneye se requirió la instalación de Python y pip, es por ello que se debe continuar con la instalación utilizando la siguiente línea:

- **pip install firebase-admin**

ahora ya se puede acceder a Firebase a través de la consola de la Raspberry Pi.

3.9 Implementación del Sistema de Video vigilancia

Figura 46. Diagrama de Interfaz Móvil



Fuente: Autor

3.9.1 Sensor de Movimiento + Esp32 con Arduino y Firebase

Como se observa en la figura anterior para la implementación del sistema IOT, se inicia trabajando con 4 sensores de movimiento y Firebase, estos sensores de movimiento fueron programados en arduino en el que se programó el módulo ESP32 conjuntamente con Firebase, es importante iniciar instalando las librerías necesarias para trabajar con Firebase, así como con el módulo ESP32.

3.9.1.1 Creación de base datos en Firebase

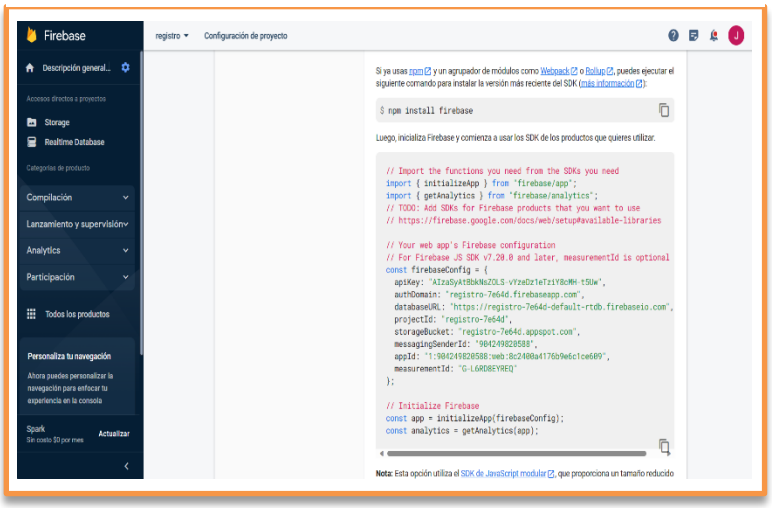
Para trabajar con Firebase se inicia creando un nuevo proyecto y a este se añade una base de datos como se observa en la siguiente imagen:

Figura 47. Creación de base de datos en Firebase

Fuente: Autor

En el código creado en arduino se utiliza Firebase para la obtención de los datos del sensor, mediante los datos del script que fueron generados cuando se creó esta base de datos.

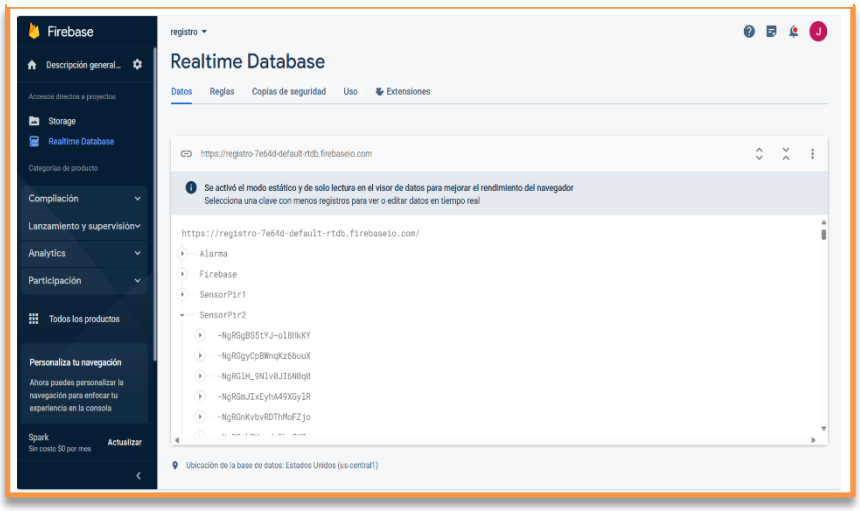
Figura 48. Obtención de datos requeridos en Arduino



Fuente: Autor

Estos datos serán utilizados para un análisis y así determinar con qué frecuencia suelen transcurrir personas por estos espacios donde se colocaron las 4 cámaras.

Figura 49. Firebase conectado con Arduino

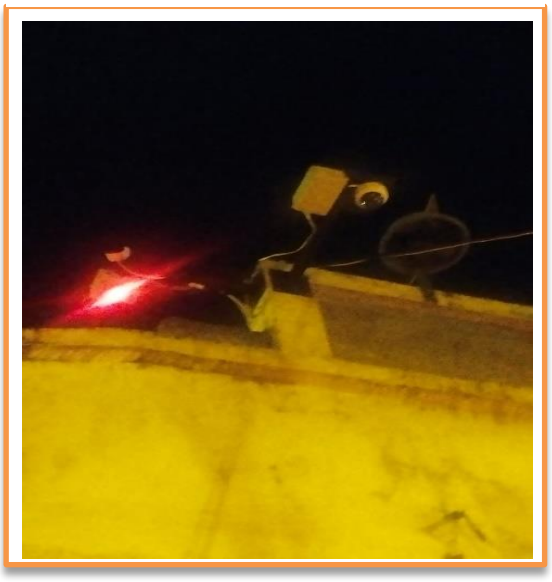


Fuente: Autor

En esta imagen se observa como Firebase ha sido enlazada hacia los módulos ESP32 en arduino y se está recopilando datos de cada sensor, con fecha y hora del movimiento.

3.9.1.2 Firebase y Arduino para Alarma

Figura 50. Alarma integrada a sistema de seguridad



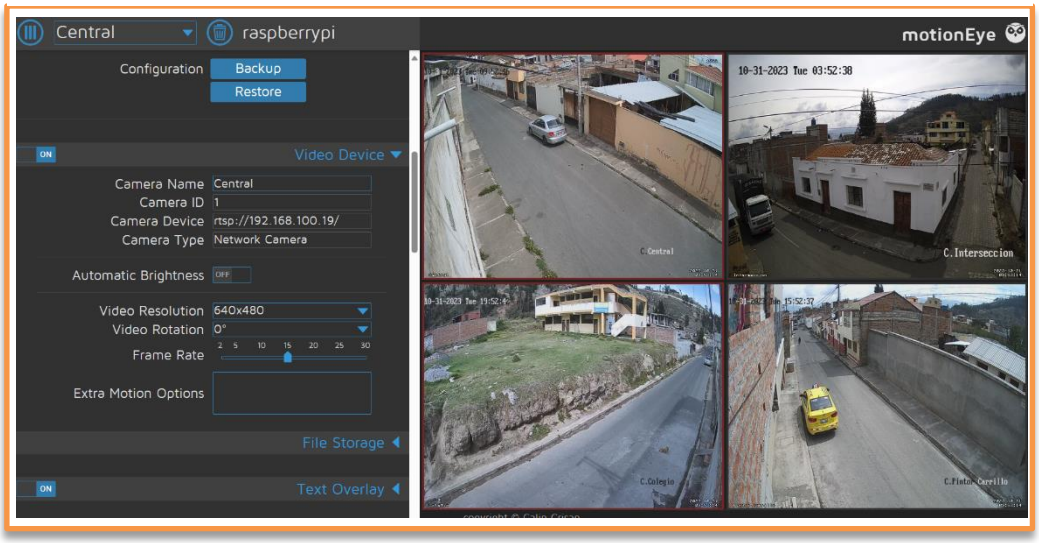
Fuente: Autor

En cuanto a la alarma integrada al sistema de cámaras se trabajó con un módulo ESP32 programado en arduino y enlazado hacia Firebase para visualizar el estado de la alarma cuando este encendida con un valor de 1 y cuando este apagada con un valor de cero.
La alarma fue programada en arduino para encender mediante Wi-Fi, con la utilización de un extensor en la caja donde está colocado este módulo y así conectarse a esta red, mediante Firebase se obtendrá los datos de encendido y apagado de la alarma.
La alarma fue colocada y probada mediante este sistema.
Además, se decidió agregar un sistema para encender y apagar la alarma mediante bluethoot en el caso de no contar con señal de internet, este sistema se puede encender conectándose mediante este sistema conectándose al módulo ESP32 a una distancia máxima de 8 metros.
Con ello se tiene una opción adicional en el caso de no contar con señal de internet.

3.9.1.3 Cámaras y Motioneye

Para integrar las cámaras con la alarma comunitaria se decidió trabajar con Motioneye, plataforma en la cual se integró las cuatro cámaras y se configuró de acuerdo a las necesidades requeridas por el sistema.

Figura 51. Cámaras de seguridad en Motioneye



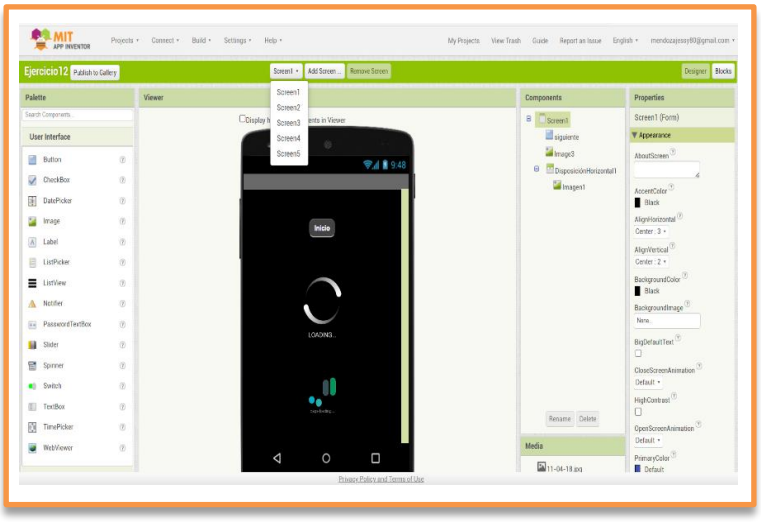
Fuente: Autor

3.9.1.4 APP Inventor

Para la integración de la alarma con las cámaras de seguridad se trabajó mediante APP Inventor, que es una aplicación de código abierto para la creación de aplicaciones móviles para dispositivos que cuenten con sistema Android.

Esta plataforma es fácil de utilizar y tiene componentes que permitieron crear la interfaz de una manera muy eficaz.
Para la creación de esta interfaz se trabajó mediante 5 ventanas, las cuáles e fueron configurando cada una de acuerdo a lo que se deseaba que apareciera en cada una de ellas, como se puede observar en la siguiente figura:

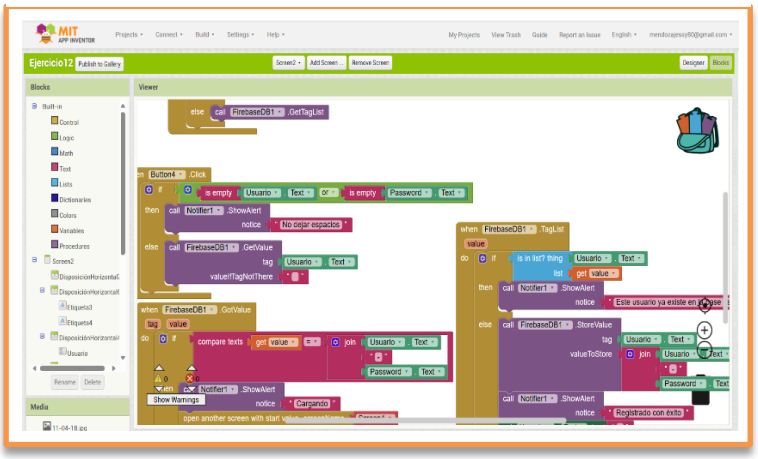
Figura 52. Ventanas creadas en App Inventor



Fuente: Autor

Cada una de estas ventanas se trabajó con botones, etiquetas, cuadro de listas, notificadores, cuadros de contraseñas, imágenes, icono principal de la aplicación, etc.
Para la parte de programación de todos estos componentes se trabajó mediante bloques que se los va enlazando uno por uno con cada componente.

Figura 53. Programación por bloques App Inventor



Fuente: Autor

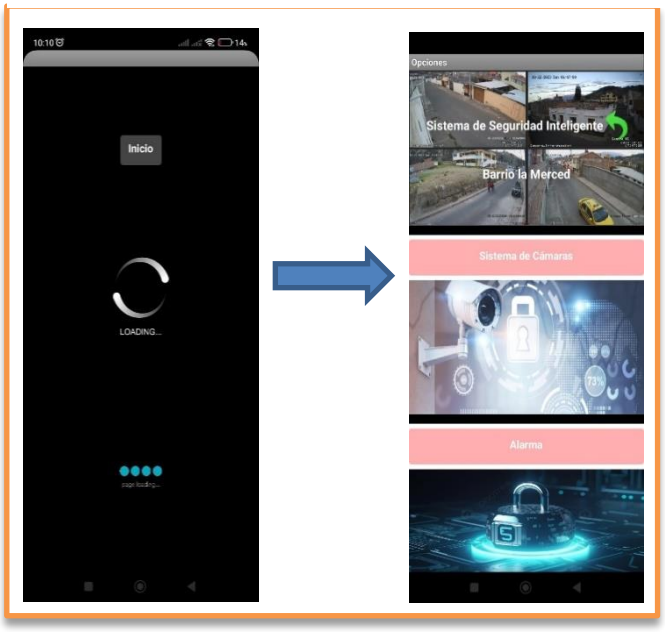
En esta figura se observa la programación de la ventana 3 que esta enlazada a Firebase para la autenticación del usuario.

Una vez terminada la interfaz se procedió a descargarla como archivo apk, desde play store se instaló App Inventor desde donde se escaneó el código QR de la aplicación y así se obtiene la aplicación instalada y lista para ejecutar desde el teléfono móvil.

Figura 54. Aplicación SVIBM IOT

Fuente: Autor

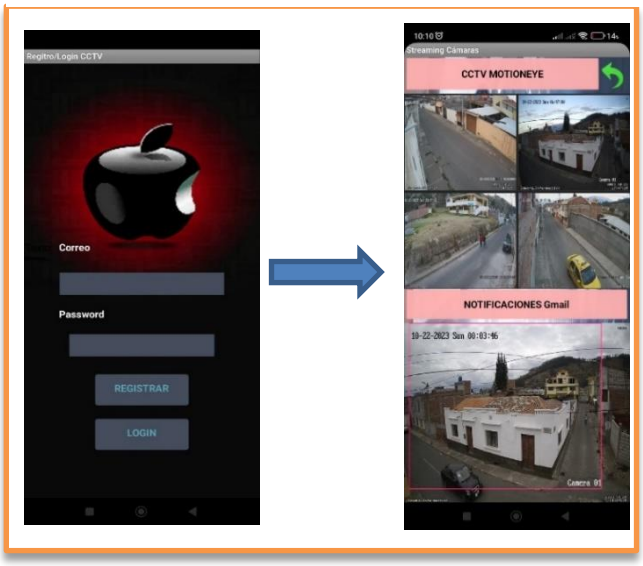
Figura 55. Aplicación SVIBM IOT



Fuente: Autor

En la figura se puede observar la pantalla inicial de la aplicación, donde al dar clic en el botón inicio se abre una nueva pantalla con dos opciones, la una para ingresar a las cámaras de seguridad y la otra para ingresar a la alarma comunitaria del sistema.

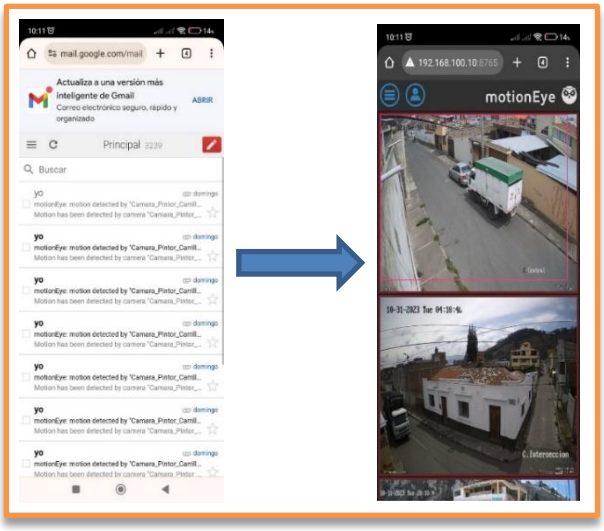
Figura 56. Aplicación SVIBM IOT



Fuente: Autor

Para ingresar a las cámaras de seguridad, se debe ingresar las credenciales que trabaja con la base de datos Firebase en tiempo real, para ello se ingresa creando un nuevo usuario o con un usuario ya creado, cuando el usuario ha sido autenticado, se abrirá una ventana donde se tiene dos opciones, la una es para visualizar las cámaras desde motioneye y la otra permite ver las notificaciones de los movimientos detectados por las cámaras y enviadas a un correo creado específicamente para recibir estas notificaciones.

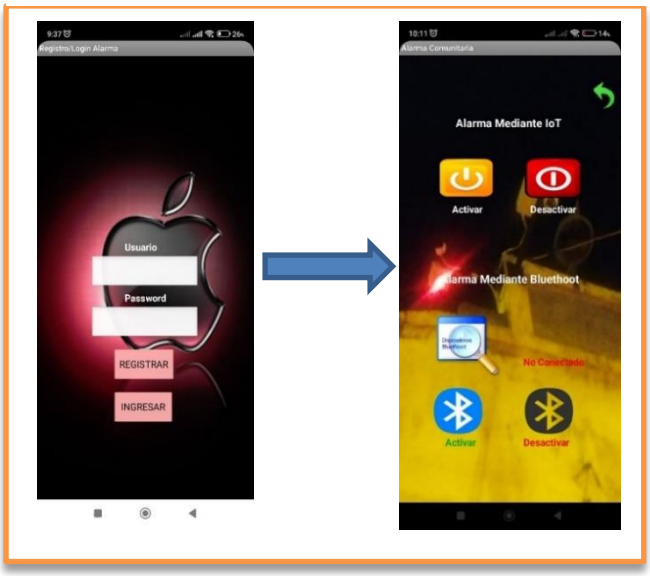
Figura 57. Aplicación SVIBM IOT



Fuente: Autor

En la siguiente figura se puede observar la pantalla para ingresar a la alarma comunitaria, en esta ventana también se creó autenticación para evitar posibles contratiempos con mal uso de la aplicación, entonces al ingresar las credenciales estas se almacenan y trabajan con Firebase en tiempo real, al autenticarse se abre la pantalla de la alarma, donde esta consta de dos opciones para su activación, la una mediante Wi-FI, que el único requerimiento es estar conectado a alguna red de internet y la otra opción es en el caso de no contar con una red Wi-Fi activarla mediante Bluetooth, tan solo estar dentro del área permitida para trabajar con esta tecnología.

Figura 58. Aplicación SVIBM IOT

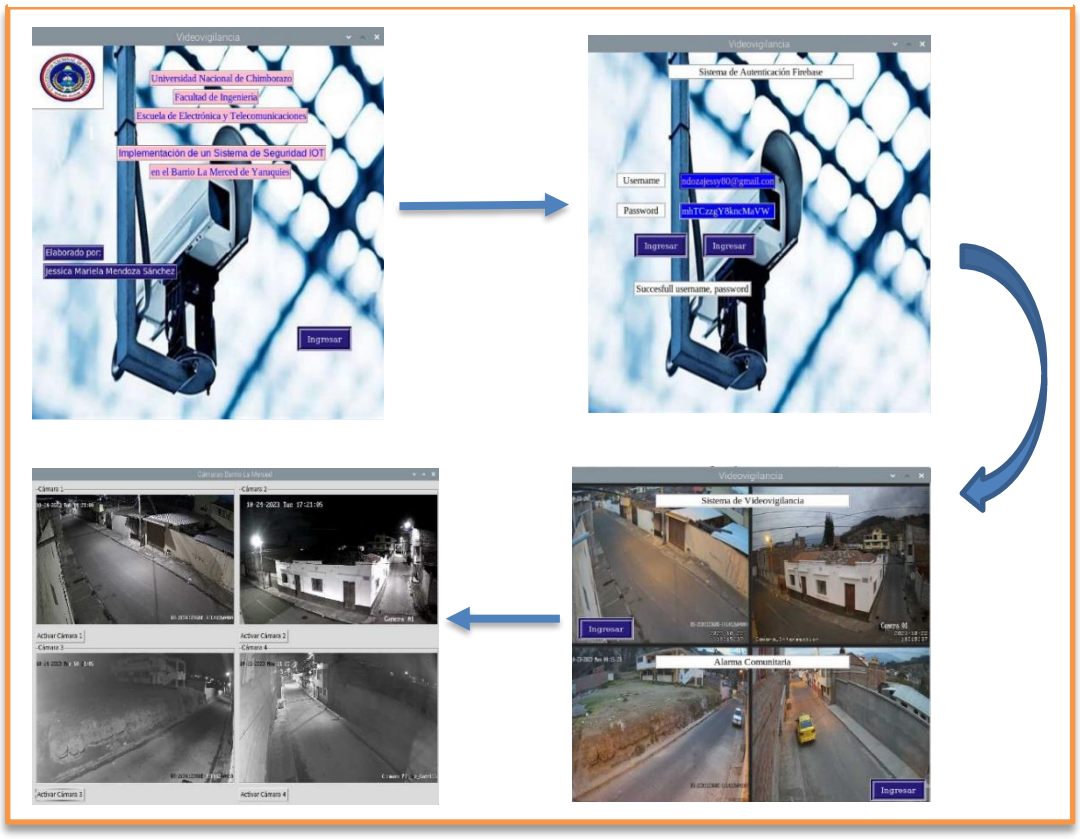


Fuente: Autor

Es así como con un conjunto de 8 ventanas enlazadas y creadas en app inventor se realizó la aplicación IOT para el sistema de seguridad del Barrio La Merced de Yaruquies de la ciudad de Riobamba.

3.9.2 Creación de Interfaz video vigilancia en Tkinter Raspberry Pi

Figura 59. Aplicación en Tkinter Raspberry Pi



Fuente: Autor

Para la creación de la interfaz local dentro de la Raspberry Pi se la realizó mediante cuatro ventanas, donde la primera es la presentación del creador del proyecto, conteniendo un botón inicial para ingresar al sistema.

La segunda ventana es para la autenticación del usuario mediante Firebase, donde para ingresar al sistema se requiere autenticar al usuario, y cuando este ingrese el nombre y clave para el ingreso al sistema se generará un mensaje push al administrador, informando que se está in, al sistema mediante la autenticación con Firebase , se pasa a la tercera ventana donde consta de 4 cuadros, uno por cada cámara colocado en el sistema, y cuatro botones para visualizar el Streaming de cada una de ellas.

Finalmente, en la última ventana se puede acceder a las cámaras llamando a la página de motioneye.

4. CAPÍTULO IV. RESULTADOS Y DISCUSIÓN

Con la obtención de los datos de los 3 sensores colocados en lugares estratégicos se logró obtener una base de datos de los movimientos detectados por estos dispositivos y almacenarlos en Firebase.
Se ha tomado datos durante 30 días de los cuáles se ha determinado realizar el análisis del total de los datos para mayor fiabilidad del sistema.
Los Datos obtenidos en firebase se pasan a Excel, para posteriormente pasarlo al analizador estadístico IBM SPSS, para determinar las lecturas de cada sensor.

Tabla 4. Datos aleatorios de los sensores de movimiento

	Sensor1	Sensor2	Sensor3
Días	**Datos**		
Lunes	593	514	722
Martes	486	356	687
Miércoles	568	616	665
Jueves	386	369	733
Viernes	476	117	987
Sábado	342	249	1360
Domingo	443	165	870

Fuente: Autor

En la tabla N° 4 se obtuvo los datos generados en la primera semana de los tres sensores, posteriormente estos datos analizarlos en IBM SPSS.
Como se puede observar en la tabla en el sensor 3 existen mayor cantidad de movimientos, este sensor está ubicado al frente de un colegio abandonado, además de estar en una calle principal donde hay la parada de bus.

Tabla 5. Estadística Descriptiva IBM SPSS Sensor1

Estadísticos

		Hora	Sensor1
N	Válido	673	672
	Perdidos	0	1
Media			43,00
Mínimo			0
Máximo			100

Fuente: Autor

En la tabla 5 se puede observar que en el sensor 1 durante los 30 días se obtuvo un total de 673 datos, hubo un máximo de 100 movimientos y un valor mínimo de 1 movimiento detectado, dando así un promedio de 43 movimientos en el día.

Tabla 6. Estadística Descriptiva IBM SPSS Sensor2

Estadísticos

		Hora	Sensor2
N	Válido	673	672
	Perdidos	0	1
Media			30,49
Mínimo			0
Máximo			65

Fuente: Autor

En la tabla 6 se puede observar que en el sensor 2 durante los 30 días se obtuvo un total de 673 datos, hubo un máximo de 65 movimientos y un valor mínimo de 0 movimientos detectados, dándonos un promedio de 30 movimientos en el día.

Tabla 7. Estadística Descriptiva IBM SPSS Sensor3

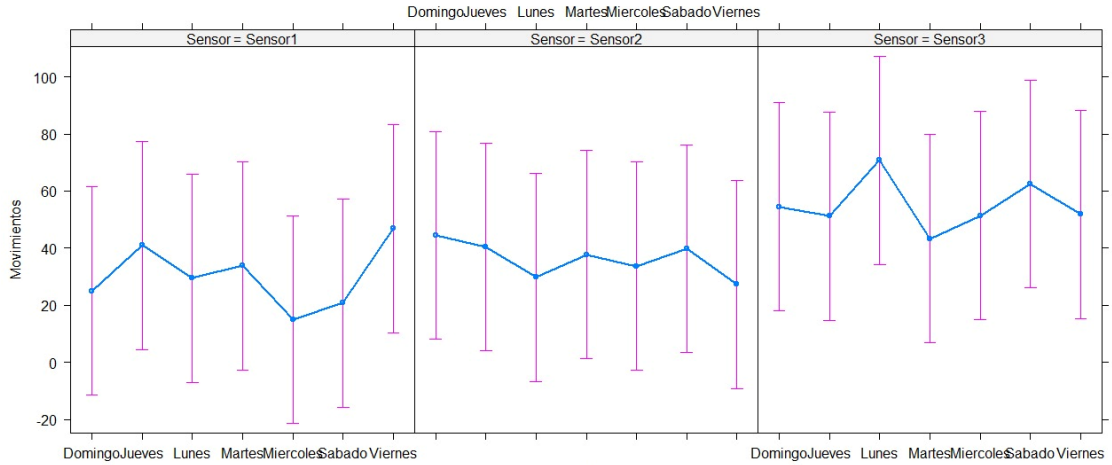
Estadísticos

		Hora	Sensor3
N	Válido	673	672
	Perdidos	0	1
Media			77,93
Mínimo			0
Máximo			249

Fuente: Autor

En la tabla 7 se puede observar que en el sensor 3 durante los 30 días se obtuvo un total de 673 datos, hubo un máximo de 249 movimientos y un valor mínimo de 1 movimiento detectado, dándonos un promedio de 77 movimientos en el día.

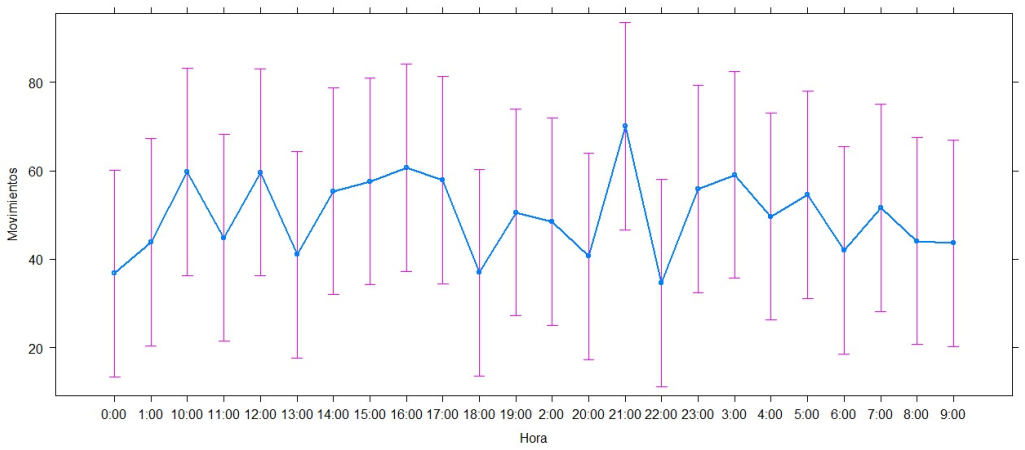
Figura 60. Gráfica de sensores respecto a los movimientos vs días



Fuente: Autor

En la figura 60 se puede observar la gráfica generada de los movimientos detectados de los 3 sensores respecto a los 7 días de cada semana durante los 30 días en el programa estadístico R, de lo cual se determina que en el sensor 3 hay mayor cantidad de movimientos, siendo el día lunes donde se prevalece la mayor cantidad de datos generados, en el sensor 2 se observa que los días domingos se generó mayor cantidad de movimientos y en el sensor 1 los días viernes se observa que existe mayor flujo de movimientos detectados.

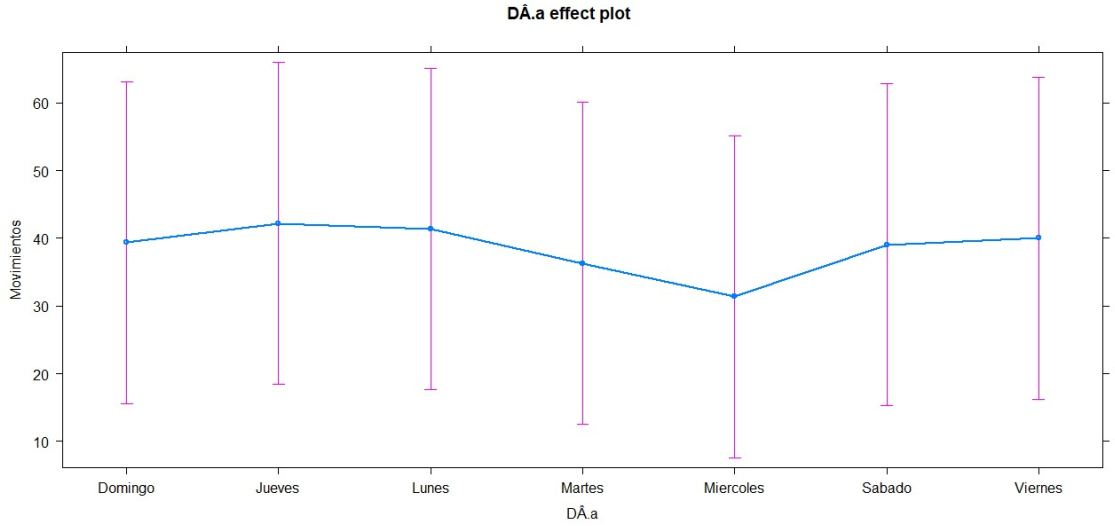
Figura 61. Gráfica de sensores respecto a los movimientos vs las horas



Fuente: Autor

En la figura 61 se puede observar la gráfica generada de los movimientos detectados de los 3 sensores respecto a las 24 horas que se recolectan los datos de estos dispositivos, este análisis se lo realiza en el programa estadístico R, de lo cual se determinar que de acuerdo a los movimientos generados entre las 21:00 se generan mayor cantidad de datos.

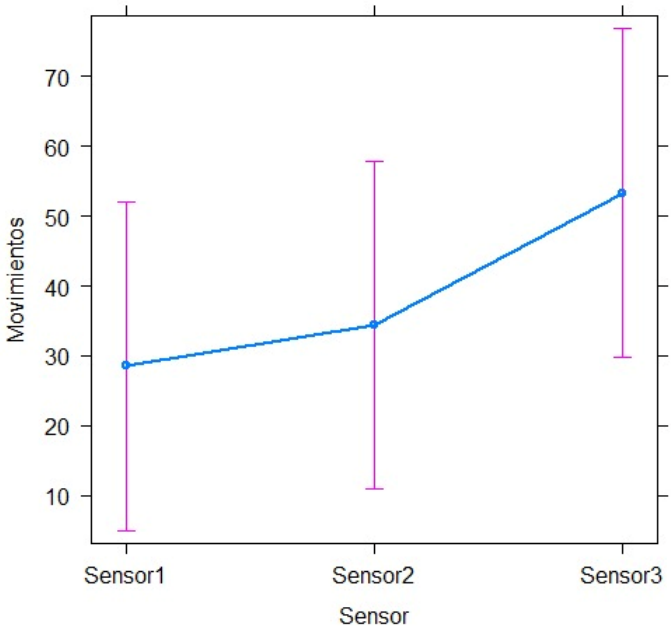
Figura 62. Gráfica de los movimientos de los sensores respecto a los días



Fuente: Autor

En la figura 62 se observa la gráfica de los tres sensores respecto a los días donde se generaron los movimeintos.

Figura 63. Gráfica de Movimientos de los 3 sensores

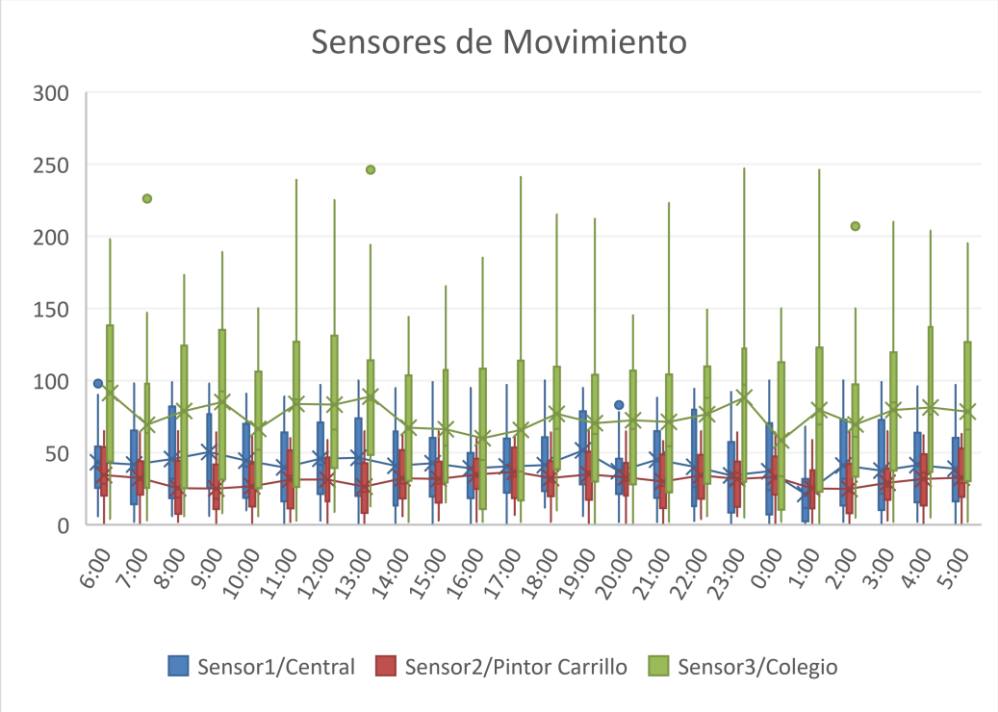


Fuente: Autor

En la figura 63 se puede observar el comportamiento de los tres sensores obtenidos en el programa estadístico R, donde se puede verificar que en el sensor 3 hay mayor cantidad de movimientos, como ya se observó en las anteriores figuras, en este sensor existe mayor tráfico de personas, de acuerdo a esto se puede tener en cuenta que el sistema debe estar monitoreado mayormente en esta zona y así predecir posibles contratiempos con antisociales.

De los datos totales obtenidos de cada sensor se generó una gráfica con los tres sensores y ver cómo actúa cada uno de ellos durante los 30 días que se recolectaron estos datos.

Figura 64. Gráfica de sensores vs tiempo



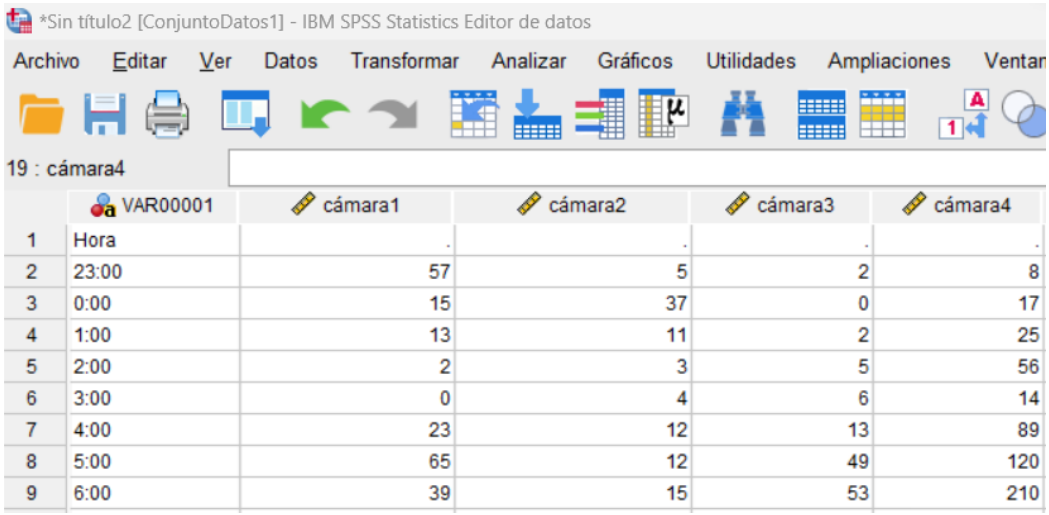
Fuente: Autor

De lo que se puede observar que de acuerdo a la gráfica el sensor3 tiene mayor cantidad de movimientos, esto debido a que este dispositivo se encuentra ubicado en la calle 24 de mayo y Pintor Carrillo, frente a un colegio abandonado, este lugar es concurrido debido a que es una calle principal, donde la parada de bus es a una cuadra de este punto, y como se mencionó a este colegio abandonado concurren un grupo de niños a jugar en las tardes y en la noche se reunían grupo de jóvenes a consumir bebidas alcohólicas y sustancias ilícitas.

La cantidad de datos obtenidos en los sensores 1 y 2 no varían en un porcentaje mayor, los movimientos recolectados tienen muchas similitudes.

En la siguiente tabla se generó los datos obtenidos por las cuatro cámaras durante una semana, estas notificaciones fueron captadas en el correo electrónico generado para almacenar estos datos, las cámaras de seguridad están programadas para capturar los datos en el horario de 23:00 hasta las 06:00 de la mañana.

Tabla 8. Base de Datos ingresada en IBM SPSS Cámaras de Seguridad



	VAR00001	cámara1	cámara2	cámara3	cámara4
1	Hora	.	.	.	.
2	23:00	57	5	2	8
3	0:00	15	37	0	17
4	1:00	13	11	2	25
5	2:00	2	3	5	56
6	3:00	0	4	6	14
7	4:00	23	12	13	89
8	5:00	65	12	49	120
9	6:00	39	15	53	210

Fuente: Autor

En la tabla 10 se puede observar que en la cámara1 durante una semana hubo un máximo de 65 movimientos y un valor mínimo de 0 movimientos detectados, dándonos un promedio de 32 movimientos en el día.

Tabla 9. Estadística Descriptiva IBM SPSS Cámara1

Estadísticos

		Hora	Cámara1
N	Válido	32	32
	Perdidos	0	0
Media			27,3125
Mínimo			,00
Máximo			65,00

Fuente: Autor

En la tabla 10 se puede observar que en la cámara2 durante una semana hubo un máximo de 37 movimientos y un valor mínimo de 0 movimientos detectados, dándonos un promedio de 13 movimientos en el día.

Tabla 10. Estadística Descrptiva IBM SPSS Cámara2

Estadísticos

		Hora	Cámara2
N	Válido	32	32
	Perdidos	0	0
Media			13,8438
Mínimo			,00
Máximo			37,00

Fuente: Autor

En la tabla 11 se puede observar que en la cámara3 durante los 30 días hubo un máximo de 53 movimientos y un valor mínimo de 0 movimientos detectados, dándonos un promedio de 20 movimientos en el día.

Tabla 11. Estadística Descriptiva IBM SPSS Cámara3

Estadísticos

		Hora	Cámara3
N	Válido	32	32
	Perdidos	0	0
Media			20,8750
Mínimo			,00
Máximo			53,00

Fuente: Autor

En la tabla 12 se puede observar que en la cámara4 durante una semana hubo un máximo de 210 movimientos y un valor mínimo de 8 movimientos detectados, dándonos un promedio de 101 movimientos en el día.

Tabla 12. Estadística Descriptiva IBM SPSS Cámara4

Estadísticos

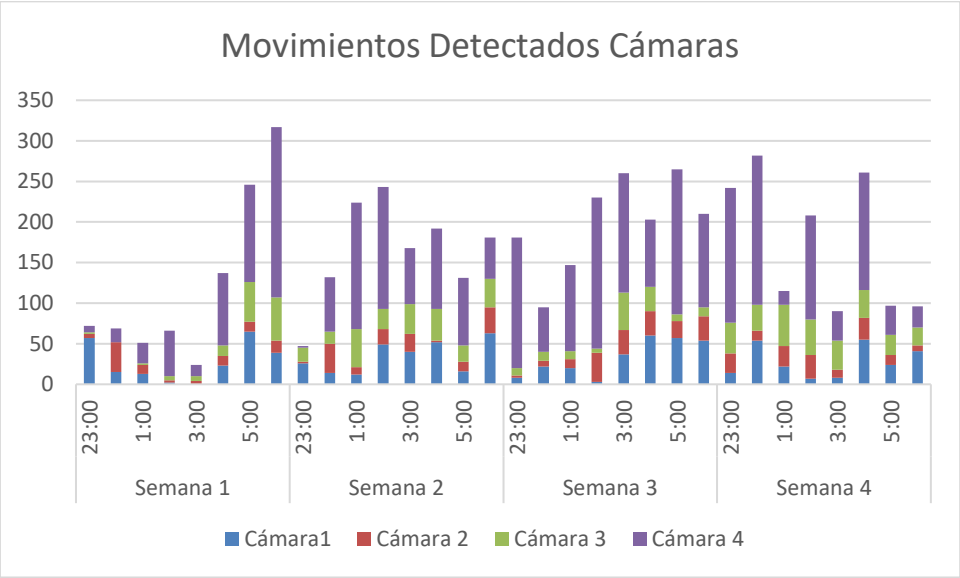
		Hora	Cámara4
N	Válido	32	32
	Perdidos	0	0
Media			101,7500
Mínimo			8,00
Máximo			210,00

Fuente: Autor

En el siguiente gráfico se puede observar los movimientos detectados por las cuatro cámaras de seguridad, mediante la gráfica se puede analizar que durante los 30 días que

en la cámara cuatro que está ubicada en la calle 24 de mayo y Pintor Carrillo, que está enfocada hacia el colegio, existen la mayor cantidad de movimientos detectados entre las 6 de la mañana, debido a que a esa hora se dirigen a las instituciones educativas y a los trabajos.

Figura 65. Gráfica de datos cámaras vs tiempo



Fuente: Autor

Mediante los resultados obtenidos en los 3 sensores, se realizó la programación de la detección de movimientos en las cuatro cámaras de seguridad, debido al análisis se concluyó que de 6 a 7 de la mañana se generan un número considerado de movimientos, así como a las 12 del día y durante la noche a las 20:00, es por ello que mediante esto se puede determinar que las cámaras deben capturar imágenes a partir de las 23:00 hasta las 06:00 de la mañana.

Tabla 13. Cálculo de Fiabilidad del sistema de cámaras

Dispositivos	**Movimientos Detectados**	**Movimientos Erróneos**	**% Error Movimientos**
Cámara 1	1026	8	0,007779
Cámara 2	543	13	0,02394
Cámara 3	746	6	0,008042
Cámara 4	2331	19	0,008151
Total Movimientos	4646	46	0,047912

0,047912% Grado de error del sistema
Entonces el sistema tiene una fiabilidad del 99,95%

5. CAPÍTULO V. CONCLUSIONES Y RECOMENDACIONES

5.1.1 Conclusiones

Una vez finalizado el trabajo se concluye que:
En la actualidad en el mercado existen sistemas como el propuesto y realizado, pero los costos son excesivos para ser adquiridos por una comunidad que vive del día a día, además que estos sistemas no siempre cumplen con lo que mencionan antes de adquirir el producto.

En el diseño del proyecto se utilizó plataformas de software libre como arduino que se utilizó para automatizar la alarma comunitaria, un software fácil y práctico para trabajar con módulos que sirven de soluciones a sistemas IOT.

Otra de las plataformas utilizadas es App Inventor, que es de fácil uso y se lo único que se requirió es bastante investigación para acoplar cada una de las funciones que se deseaba contar en la aplicación.

Se logró implementar el sistema de seguridad IOT en el Barrio La Merced de Yaruquies de la ciudad de Riobamba, a lo largo de la elaboración de la plataforma se encontró varios inconvenientes que con ayuda de investigación se pudo dar solución y concluir con éxito el sistema propuesto y que ahora está activo y funcionando para ser un apoyo para la inseguridad del barrio.
Los puntos estratégicos se tomaron luego de un previo análisis, debido a que en el barrio existen zonas de peligro como un colegio abandonado donde grupos de jóvenes se concentraban a diario para libar y consumir sustancias prohibidas, en el tiempo que lleva implementado el sistema se pudo reducir casos como estos, ya que cuando se tenía la presencia de estas personas se acciona la alarma comunitaria y el grupo de moradores del barrio se ha concentrado haciendo salir del lugar a estos sujetos.

Se comprobó que el sistema es de gran ayuda para el barrio, se dio hace anteriores días un intento de hurto en una casa que está dentro del área vigilada, llegó una notificación de alerta y de inmediato se hizo sonar la alarma comunitaria haciendo que el sospechoso

huyera, y todos los moradores se concentraron al instante, así como miembros de la policía y se realizó una búsqueda del sujeto.

El sistema se compartió con usuarios del barrio y así pudieron verificar que está funcionando correctamente, que puede ser accionado desde cualquier teléfono celular la alarma, en cuestión de las cámaras de seguridad se tiene acceso restringido para dos administradores del barrio, para ello se requiere de autenticación en una base de datos que se trabajó en Firebase.

De los resultados estadísticos se puede determinar que el sistema de seguridad tiene un 99,5% de fiabilidad, este cálculo se determinó mediante la detección de errores obtenidos en las notificaciones de las cámaras de seguridad y el total de las notificaciones obtenidas.

5.2 Recomendaciones

Se recomienda que al trabajar con un microcomputador como es la Raspberry Pi, se tomé todas las debidas precauciones en cuanto a voltaje de trabajo, ya que tiene un alto grado de sensibilidad, y se puede evitar daños en los módulos a futuros por la sobrecarga de voltaje.

Se recomienda trabajar con cámaras de seguridad tipo tubo ya que el área a cubrir es mejor que las cámaras tipo Domo, así como para la instalación de las cámaras se trabajó con un soporte metálico, este debe contar con las medidas necesarias para evitar que haya obstáculos al enfocar las cámaras.

Al trabajar con la Raspberry Pi se recomienda que está tenga una conexión LAN, ya que al trabajar con la red WI-FI se tenía bastantes pérdidas en cuánto a la calidad de imagen.

6. BIBLIOGRAFÍA

[1] Aguilar, T., Brito, G., Altamirano, S., & Sánchez, A. (2019). Monitoreo y Video vigilancia basado en IoT en tiempo real de las Unidades de Transporte Colectivo. Revista Ibérica de Sistemas e Tecnologias de Informação, (E23), 288-301.

[2] Tumbaco Peñafiel, L. M. (2022). Diseño y análisis de prototipo de un sistema de seguridad con sensores de movimiento y cámaras IP de video vigilancia aplicando una infraestructura IOT para el envío y recepción de datos entre dispositivos (Doctoral dissertation, Universidad de Guayaquil. Facultad de Ciencias Matemáticas y Físicas. Carrera de Ingeniería en Networking y Telecomunicaciones).

[3] Bulla Rojas, M. J., & Largo Ramirez, B. D. (2020). Prototipo de un sistema de monitoreo y video vigilancia para el hogar con el enfoque de internet de las cosas (iot).

[4] Barboto Ávila, J. D. (2020). Diseño e implementación de un sistema de video vigilancia por medio de radio enlaces para una empresa agrícola (Doctoral dissertation, Universidad de Guayaquil. Facultad de Ingeniería Industrial. Carrera de Ingeniería en Teleinformática.).

[5] Moya Di Mattia, H. A., & Tapia Suarez, B. N. (2018). Diseño e implementación de un sistema de seguridad usando video vigilancia con monitoreo móvil remoto vía internet para las Carreras de Ingeniería en Sistemas Computacionales y Networking de la Facultad de Ciencias Matemáticas y Físicas de la Universidad de Guayaquil (Doctoral dissertation, Universidad de Guayaquil. Facultad de Ciencias Matemáticas y Físicas. Carrera de Ingeniería En Sistemas Computacionales).

[6] Sarabia Buñay, B. W. (2018). Diseño e implementación de un sistema de seguridad mediante video vigilancia inalámbrico usando cámaras IP para la FIE (Bachelor's thesis, Escuela Superior Politécnica de Chimborazo).

[7] Cuenca Maldonado, N. X., & Maza Merchán, C. J. (2021). Diseño e implementación de un sistema inteligente de seguridad con respuesta en tiempo real mediante la integración de cámaras y sensores usando AIoT (Bachelor's thesis).

[8] De La Torre Torres, D. I. (2021). Implementación de un sistema centralizado de video vigilancia (CCTV) para el edificio de la carrera de Ingeniería Eléctrica (CIELE) de la Universidad Técnica del Norte (UTN) (Bachelor's thesis).

[9] GUTIERREZ QUINDE, C. P. (2021). Diseño e implementación de un sistema de seguridad inteligente para el edificio del centro de idiomas de la Universidad Estatal del Sur de Manabí (Bachelor's thesis, jipijapa. Unesum).

[10] MARTÍNEZ MORENO, Francisco José, et al. Diseño e implementación de un sistema de alarma IoT basada en tecnologías Open Source. 2019.

[11] HERRERA CHÁVEZ, Dario Wladimir. Diseño e implementación de un prototipo de seguridad para control domótico basado en IoT bajo ambientes de dispositivos móviles con Android. 2020. Tesis de Licenciatura. Quito, 2020.

[12] Placencia Camacho, F. G. (2021). Alarmas comunitarias basadas en arquitecturas SDN e IOT (Master's thesis, Universidad Técnica de Ambato. Facultad de Ingeniería en Sistemas, Electrónica e Industrial. Maestría en Telecomunicaciones).

[13] Bajaña Molina, H. J., & Molina Sarco, J. C. (2020). Diseño e implementación de un prototipo escalable de detección de gases inflamables, temperatura y alarmas contra incendios basado en tecnología IOT de bajo costo para cocinas en viviendas de Guayaquil (Doctoral dissertation, Universidad de Guayaquil. Facultad de Ciencias Matemáticas y Físicas. Carrera de Ingeniería en Networking y Telecomunicaciones).

[14] Lagua Solís, C. A., & Sánchez González, H. V. (2022). Diseño e implementación de un prototipo de sistema de seguridad para hogares o empresas basado en tecnología Iot de bajo costo que realiza notificaciones en tiempo real mediante mensajería de whatsapp y telegram (Doctoral dissertation, Universidad de Guayaquil. Facultad de Ciencias Matemáticas y Físicas. Carrera de Ingeniería en Networking y Telecomunicaciones).

[15] Tumbaco Peñafiel, L. M. (2022). Diseño y análisis de prototipo de un sistema de seguridad con sensores de movimiento y cámaras IP de videovigilancia aplicando una infraestructura IOT para el envío y recepción de datos entre dispositivos (Doctoral dissertation, Universidad de Guayaquil. Facultad de Ciencias Matemáticas y Físicas. Carrera de Ingeniería en Networking y Telecomunicaciones).

[16] Yanchatipán Moposita, E. G. (2022). Sistema de seguridad integral para la monitorización de alarmas y alerta de emergencia en la parroquia San Andrés del cantón Píllaro de la provincia de Tungurahua (Bachelor's thesis, Universidad

Técnica de Ambato. Facultad de Ingeniería en Sistemas, Electrónica e Industrial. Carrera de Ingeniería en Electrónica y Comunicaciones).

[17] Tapia Bastidas, W. I. (2022). Implementación de un prototipo de alarma comunitaria en el barrio de Chillogallo en el sur de Quito con tecnología Sigfox (Bachelor's thesis, Quito: EPN, 2022).

[18] Toledo, M. R. N., Vélez, W. F. M., & Ortiz, V. Y. (2019). Sistema de monitoreo delicuencial en viviendas basado en internet de las cosas. 3c Tecnología: glosas de innovación aplicadas a la pyme, 8(3), 24-43.

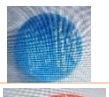
[19] Vélez, M., & Francisco, W. (2018). Dispositivo de monitoreo basado en el internet de las cosas que obtenga evidencias de lo que acontece en el Barrio 20 De Noviembre de la ciudad de Esmeraldas y genere una alarma de alerta en el mismo (Doctoral dissertation, Ecuador-PUCESE-Escuela de Sistemas y Computación).

[20] Tigua Macías, J. A., & Zambrano Bonilla, L. A. (2022). Diseño de sistema de alarma comunitaria basado en tecnología WSN con conexión redundante para la Cooperativa Francisco Jácome de la Ciudad de Guayaquil (Doctoral dissertation, Universidad de Guayaquil. Facultad de Ciencias Matemáticas y Físicas. Carrera de Ingeniería en Networking y Telecomunicaciones).

[21] Chicaiza Guachi, K. G. (2020). Sistema de alarma comunitaria para el mercado San Juan de la Ciudad de Santiago de Píllaro (Bachelor's thesis, Universidad Técnica de Ambato. Facultad de Ingeniería en Sistemas, Electrónica e Industrial. Carrera Ingeniería Electrónica y Comunicaciones).

7. ANEXOS

Tabla 14. Listado de Materiales Implementación del sistema de seguridad

Listado de Materiales		
Imagen	**Materiales**	**Cantidad**
	Tomacorrientes	4
	Cable eléctrico Nº12	50 metros
	Caja Plástica Dexon	4
	Amarras	100
	Tacos Fisher	20
	Tornillos	20
	Llave Nº10	1
	Fuente de alimentación 5V	3
	Protoboard	4
	Conectores macho-macho	30
	Módulo relay	1
	Módulo bidireccional de 3,3 a 5 V	1
	Cautín	1
	RJ45	15
	Pasta de soldar	1
	Estaño para soldar	1 metro

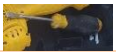
	Taladro	1
	Escalera telescópica	1
	Taype	1
	Cortadora	1
	Ponchadora	1
	Brocas	3
	Destornilladores	2
	Lector Micro Sd + Sd 32 GB	1
	Tensor cable UTP	10
	Grapas	100
	Silicona	20
	Pistola de Silicona	1
	Martillo	1

Tabla 15. Análisis presupuesto Sistema de Video vigilancia IOT

RECURSOS	CANTIDAD	VALOR UNITARIO	VALOR TOTAL
Cámaras	4	60.00	240.00
Materiales Adicionales		100	100
Sensores	4	3	12
Raspberry Pi	1	235	235
Módulos Esp32	5	10	50
PC para el diseño	1	700.00	700.00
Movilidad	1	100,00	100,00
TOTAL	**11**	**1065.00**	**1434.00**

7.1 Implementación del Sistema IOT de Seguridad en el Barrio La Merced