UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERÍA EN SISTEMAS, ELECTRÓNICA E INDUSTRIAL

CARRERA DE TELECOMUNICACIONES

Tema:

SISTEMA DE SEGURIDAD PARA LAS OFICINAS DEL GAD MUNICIPAL DEL CANTÓN TISALEO CON ARQUITECTURA IOT

Trabajo de titulación modalidad Proyecto de Investigación, presentado previo a la obtención del título de Ingeniera en Telecomunicaciones

ÁREA: Electrónica

LÍNEA DE INVESTIGACIÓN: Tecnología de la información y Sistemas de control

AUTOR: Marcela Jazmín Carrera Zurita

TUTOR: Ing. Edgar Freddy Robalino Peña Mg.

AMBATO - ECUADOR

Agosto - 2023

APROBACIÓN DEL TUTOR

En calidad de tutor del trabajo de titulación con el tema: SISTEMA DE SEGURIDAD PARA LAS OFICINAS DEL GAD MUNICIPAL DEL CANTÓN TISALEO CON ARQUITECTURA IOT, desarrollado bajo la modalidad Proyecto de Investigación por la señorita Marcela Jazmín Carrera Zurita, estudiante de la Carrera de Telecomunicaciones, de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial, de la Universidad Técnica de Ambato, me permito indicar que la estudiante ha sido tutorada durante todo el desarrollo del trabajo hasta su conclusión, de acuerdo a lo dispuesto en el Artículo 17 del Reglamento para la Titulación de Grado en la Universidad Técnica de Ambato y el numeral 6.3 del instructivo del reglamento referido.

Ambato, agosto 2023

Firmado electrónicamente por:
EDGAR FREDDY
ROBALINO PENA

……..

Ing. Edgar Freddy Robalino Peña, Mg.

TUTOR

AUTORÍA

El presente trabajo de titulación titulado: SISTEMA DE SEGURIDAD PARA LAS OFICINAS DEL GAD MUNICIPAL DEL CANTÓN TISALEO CON ARQUITECTURA IOT es absolutamente original, auténtico y personal y ha observado los preceptos establecidos en la Disposición General Quinta del Reglamento para la Titulación de Grado en la Universidad Técnica de Ambato. En tal virtud, el contenido, efectos legales y académicos que se desprenden del mismo son de exclusiva responsabilidad del autor.

Ambato, agosto 2023

.....

Marcela Jazmín Carrera Zurita

C.C. 1804851135

AUTOR

DERECHOS DE AUTOR

Autorizo a la Universidad Técnica de Ambato para que reproduzca total o parcialmente este trabajo de titulación dentro de las regulaciones legales e institucionales correspondientes. Además, cedo todos mis derechos de autor a favor de la institución con el propósito de su difusión pública, por lo tanto, autorizo su publicación en el repositorio virtual institucional como un documento disponible para la lectura y uso con fines académicos e investigativos de acuerdo con la Disposición General Cuarta del Reglamento para la Titulación de Grado en la Universidad Técnica de Ambato.

Ambato, agosto 2023

.....

Marcela Jazmín Carrera Zurita

C.C. 1804851135

AUTOR

APROBACIÓN TRIBUNAL DE GRADO

En calidad de par calificador del informe final del trabajo de titulación presentado por la señorita Marcela Jazmín Carrera Zurita, estudiante de la Carrera de Telecomunicaciones, de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial, bajo la modalidad Proyecto de Investigación titulado: SISTEMA DE SEGURIDAD PARA LAS OFICINAS DEL GAD MUNICIPAL DEL CANTÓN TISALEO CON ARQUITECTURA IOT, nos permitimos informar que el trabajo ha sido revisado y calificado de acuerdo al Artículo 19 del Reglamento para la Titulación de Grado en la Universidad Técnica de Ambato y el numeral 6.4 del instructivo del reglamento referido. Para cuya constancia suscribimos, conjuntamente con la señora Presidente del Tribunal.

Ambato, agosto 2023.

Firmado electrónicamente por:
ELSA PILAR URRUTIA URRUTIA

Ing. Pilar Urrutia, Mg.

PRESIDENTE DEL TRIBUNAL

Firmado electrónicamente por:
GEOVANNI DANILO BRITO MONCAYO

Ing. Mg. Geovanni Brito Moncayo

PROFESOR CALIFICADOR

Firmado electrónicamente por:
SANTIAGO MAURICIO ALTAMIRANO MELENDEZ

Ing. Mg. Santiago Altamirano Meléndez

PROFESOR CALIFICADOR

DEDICATORIA

A mi amor eterno mi madre Carmita, quien dedicó su vida a guiarme por el mejor camino, mamita gracias por todos tus consejos, tus enseñanzas, por hacerme una mujer de bien, por inculcarme los mejores valores, por estar siempre en cada etapa de mi vida, por ser mi guía y apoyo durante mi carrera universitaria. Hoy con lágrimas en los ojos te digo que todo el esfuerzo ha valido la pena, aunque no estes físicamente mamita este logro es para ti, que difícil es la vida sin ti mamá, pero cada sueño y meta que vaya cumpliendo en mi vida será para ti, te amaré ínfimamente.

A mi padre Olger quien ha sido mi apoyo durante toda esta etapa gracias papito por no dejarme sola, gracias por tu amor y enseñanzas. Por ser quien me ha dado la fortaleza necesaria para culminar mi carrera profesional, por ser ese apoyo incondicional para continuar con mi vida, aunque mi mundo se haya caído en pedazos, gracias por permitirme culminar esta meta y estar en cada paso que doy.

A mi hermana Mayté quien ha sido mi pilar fundamental, el motor de mi vida, quien ha luchado cada día a mi lado a partir del día de que mamá ya no está en casa y a pesar de no tener fuerzas para seguir su sonrisa, sus ocurrencias, a pesar de no tener el valor de seguir cada día he luchado por y para ella, mi princesa gracias por siempre estar para mí, que la vida me permita estar contigo y verte cumplir cada una de tus metas, te amo ñañita todo esto para ti.

A Dios porque en esta etapa universitaria me guio por el mejor camino, cuidó de mi en cada paso que daba, por brindarme un nuevo despertar cada día. A mi madre la Virgen Dolorosa quien ha cuidado de mí y me ha guiado en esta larga etapa, gracias virgencita porque durante esta etapa pusiste en mi vida a las mejores personas, gracias por darme la fortaleza para seguir adelante a pesar de las difíciles pruebas que la vida me puso, mamá me dejó la mejor herencia al enseñarme a encomendarme a ti todos los días.

A mi prima Maricruz, a mi pequeña Sarita, a Juan, no tengo palabras para agradecerles todo lo que han hecho por mí, por ser quienes han estado cada día pendientes, gracias, Maricruz y Juan por sus consejos, por su cariño, por abrirme las puertas de su casa, por esos abrazos que cuando no podía más y me estaba dando por vencida eran los que me ayudaban a seguir adelante. Gracias Sarita porque cuando mi vida se derrumbó fuiste tú quien alegró mis días y has sido mi apoyo para seguir adelante y no rendirme, tus ocurrencias, tu inocencia, tu sonrisa han sido la mejor terapia, te quiero mucho pequeña.

Dedico todo este esfuerzo a todas las personas y docentes que estuvieron en mi largo caminar en esta etapa universitaria siendo ellos quienes me formaron y compartieron sus conocimientos conmigo, a mi docente tutor quien siempre ha estado pendiente de mí, del trabajo de titulación y siendo un gran docente dentro de un aula.

Jazmín

AGRADECIMIENTO

Agradezco en primer lugar a mi mamita quien a pesar de que ya no está físicamente todos los días la recuerdo por todo lo que hizo por mí, gracias por las noches de desvelo, por los días de madrugada, por ser quien tenía lista todo para mí, gracias por todo lo que en vida hiciste por mí, hoy no tengo palabras para expresarte toda la gratitud que te tengo, pero Dios le pague por toda mamá.

A mi hermana y a mi padre por ser quienes hoy son mi pilar fundamental, mi apoyo, gracias por todo su amor y enseñanzas, les agradezco de todo corazón por todo lo que hacen a diario por mí, los amo.

Agradezco a mi tutor el Ing. Freddy Robalino que durante toda la carrera ha sido mi guía y apoyo, quien antes de ser docente me brindo su apoyo y amistad durante este largo camino, en donde él me ha guiado a tomar las mejores decisiones, gracias inge por todos sus conocimientos y enseñanzas impartidas en el aula de clases, y sus consejos que día a día me han formado como persona y como profesional.

Agradezco al GAD Municipal Tisaleo siendo la institución que por medio del señor Alcalde electo el Ing. Milton Ramírez no dudo en abrirme las puertas de la institución de la cual está al frente para el desarrollo de mi tesis, Dios le pague de todo corazón ingeniero por permitirme realizar mi proyecto de investigación en esta prestigiada institución.

A mis abuelitos Melita, Néstor, Rosa, por ser mi ejemplo para seguir, gracias por todo lo que han hecho por mí. A mi abuelito Lucho quien a pesar de ya no estar físicamente conmigo siempre fue mi ejemplo a seguir, gracias por hacerme una persona de bien por dejarme grandes enseñanzas y excelentes valores.

A todos mis tíos Dios le pague por todo su apoyo incondicional, por su amor, por su paciencia, por no dejarme sola en esta etapa que para mí es la difícil de culminar, gracias por sus consejos, sus enseñanzas sus valores inculcados, gracias porque por medio de un mensaje o una llamada siempre han estado pendientes de mi persona.

A mis primos Pauly, Kathy, Jorge, Lenin, Andy, Mary, Cristóbal, Lizz, Rosita, Roberto, Kathy, Geovys, Dome, Dennis, Lucy Z, Lucy C, Vale, Susa, gracias por tanto la vida me puso la prueba más difícil y ustedes jamás me han dejado sola, Dios le pague de todo corazón por no dejarme en esta etapa, este logro es por y para ustedes, los quiero mucho.

A mis amigos Ángeles, Julio, Ponce, Orlandito, lo mejor que la vida universitaria me pudo regalar, personas excelentes que la vida puso en mi camino, quienes han estado en cada paso que he dado, quienes han sido mi compañía en mis días buenos, días malos, días en donde no podía sostenerme de pie y ustedes me extendieron una mano, secaron mis lágrimas y me ayudaron a seguir adelante, gracias por todo mis chiquitos los quiero mucho.

A Dennis quien sin esperar nada a cambio ha sido un gran apoyo en momentos donde simplemente quería rendirme, gracias por llegar durante esta etapa, por ser quien siempre estás en las buenas y en las malas situaciones, de verdad gracias.

Jazmín

ÍNDICE GENERAL DE CONTENIDOS

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN EJECUTIVO

El desarrollo acelerado de la tecnología de Internet de las cosas (IoT) ofrece una oportunidad única para mejorar la gestión de la seguridad en entidades gubernamentales. Al combinar la conectividad de dispositivos y sensores con la potencia del análisis de datos en tiempo real, se logra un sistema de monitoreo avanzado que permite identificar posibles amenazas y prevenir incidentes de seguridad de manera proactiva. De acuerdo a ello, la presente investigación tuvo como finalidad implementar un sistema de monitoreo con tecnología IoT para dotar de seguridad a los Departamentos de la Administración General y Financiero del GAD Municipal Tisaleo. Para la implementación del sistema se parte de la selección de los componentes electrónicos que van a conformar el mismo, considerando los requerimientos tanto en tecnología, hardware y compatibilidad de software que faciliten acoplarlos entre cada uno. El sistema de seguridad se compone de cámaras de seguridad, sensores de movimiento, control de acceso y alarma, los cuales están distribuidos estratégicamente en áreas clave de la entidad. El sistema implementado comprende cámaras que detectan el movimiento durante un horario programado, capturando imágenes, almacenándolas en una carpeta del servidor (hosting) a través de FTP, y enviando correos electrónicos con notificaciones de movimiento. La aplicación diseñada ejecuta tareas en paralelo y verifica correos electrónicos para actualizar el estado de la alarma en la base de datos. Además, se incorpora un sistema de control de acceso mediante sensor dactilar que permite la autorización de acceso a las oficinas de Tesorería y Alcaldía. Finalmente se determinó que la implementación de dispositivos IoT en el diseño del sistema de seguridad mejora la capacidad de respuesta y la integración del sistema, asegurando una mayor protección para el personal y los recursos del GAD.

Palabras clave: IOT, seguridad, monitoreo, incidentes.

ABSTRACT

The rapid development of Internet of Things (IoT) technology offers a unique opportunity to improve security management in government entities. By combining the connectivity of devices and sensors with the power of real-time data analysis, an advanced monitoring system is achieved that makes it possible to identify potential threats and proactively prevent security incidents. Accordingly, the purpose of this investigation was to implement a monitoring system with IoT technology to provide security to the General Administration and Financial Departments of the Tisaleo Municipal GAD. For the implementation of the system, it starts from the selection of the electronic components that will make it up, considering the requirements both in technology, hardware and software compatibility that facilitate coupling between each one. The security system is made up of security cameras, motion sensors, access control and alarm, which are strategically distributed in key areas of the entity. The implemented system includes cameras that detect movement during a scheduled time, capturing images, storing them in a server folder (hosting) via FTP, and sending emails with movement notifications. The designed application runs tasks in parallel and checks emails to update the alarm status in the database. In addition, an access control system is incorporated using a fingerprint sensor that allows access authorization to the Treasury and Mayor's offices. Finally, it will be concluded that the implementation of IoT devices in the design of the security system improves the response capacity and the integration of the system, ensuring greater protection for the personnel and the resources of the GAD.

Keywords: IoT, security, monitoring, incidents.

CAPÍTULO I

MARCO TEÓRICO

1.1. Tema de investigación

Sistema de Seguridad para las oficinas del GAD Municipal del cantón Tisaleo con arquitectura IOT.

1.1.1. Planteamiento del problema

Según la Fiscalía General del Estado en su informe de estadísticas de robos se puede evidenciar la inseguridad que se sufre en el Ecuador, pues hasta agosto de 2022, se registraron 51,041 robos en el país, lo que representa un aumento significativo en comparación con los datos hasta junio, que eran de más de 30,000 robos. El robo a domicilios y viviendas, así como el robo de bienes, son los delitos más comunes registrados durante el año con 5496 y 5420 respectivamente. De esta manera se corrobora que el nivel de seguridad en el país es deficiente, por lo que los robos se dan a toda hora y en cualquier lugar [1].

De acuerdo a los medios de comunicación locales, Tungurahua ha presentado altos índices de violencia e inseguridad en todos sus cantones, siendo uno de ellos el cantón Tisaleo que ha sido vulnerado muchas veces por delincuentes ya sea en las calles del cantón, en domicilios e incluso en las instituciones públicas y financieras del mismo. Dentro de las instituciones que ha sido vulnerada la seguridad se encuentra el GAD Municipal Tisaleo que en varias ocasiones ha sido víctima de malhechores siendo blanco para el robo de objetos personales y de alto valor económico dentro de las oficinas de este.

En la actualidad los departamentos de Administración General y Financiero del GAD Municipal de Tisaleo, cuentan con un sistema de monitoreo obsoleto, debido a la falta de mantenimiento por lo que ha empezado a deteriorarse y desgastarse, ocasionando que la seguridad dentro del mismo sea vulnerada en varias ocasiones, permitiendo el hurto de objetos personales de los empleados, documentos importantes y bienes de la municipalidad, y de esta manera poniendo en riesgo la pérdida o hurto de documentos

físicos de elevada importancia para las autoridades, además del robo de los equipos de cómputo de la institución. El sistema monitoreo actual cuenta con 4 cámaras en el edificio principal del GAD Municipal Tisaleo estas no cubren en su totalidad la seguridad de este debido a que no están ubicadas en puntos estratégicos y que por falta de mantenimiento de la administración anterior algunas ya no se encuentran funcionando en perfectas condiciones.

Realizadas la entrevista con la persona principal de la institución siendo esta el señor Alcalde Dr. Víctor Hugo Zumba, manifestó que la municipalidad requiere un sistema de monitoreo que permita mejorar el nivel de seguridad del edificio ya que la municipalidad maneja información física de suma importancia y alta confidencialidad, altos valores económicos ya que en el departamento financiero se realiza el cobro de los servicios básicos de todo el cantón ingresando un alto valor económico a las instalaciones del GAD Municipal, además de bienes computacionales de la institución de alto valor económico y objetos personales de los empleados, que en varias ocasiones ya se ha producido el robo de dinero, teléfonos celulares e incluso perdida de bienes de la municipalidad.

Después de dar a conocer la situación actual del nivel de seguridad de las instalaciones, indicando que el mismo es obsoleto, el alcalde del GAD Municipal Tisaleo manifestó que para los departamentos de Administración General y Financiero se requiere con suma urgencia un sistema de monitoreo que permita mejorar el nivel de seguridad de los mismos, pero que la municipalidad no cuenta con el presupuesto adecuado para cubrir con los gastos que la implementación de este tipo de sistemas requiere.

1.2. Antecedentes investigativos

A través de una detallada revisión a las distintas fuentes bibliográficas a nivel nacional e internacional, se encontraron investigaciones similares referentes al tema en contexto, que sirvieron como guía para el desarrollo del presente proyecto, entre los cuales se mencionan las siguientes:

En la investigación publicada el año 2018, en la Universidad Pedagógica y Tecnológica de Colombia, se realizó una investigación con el tema “Diseño del

sistema de seguridad y de control de iluminación para el conjunto cerrado el portal del bosque en la ciudad de Tunja" en donde se plantea un sistema domótico que basa su funcionamiento en la tecnología inalámbrica WiFi, por medio de la plataforma ESP8266 y está diseñado a partir de módulos con funciones específicas, que satisfacen diferentes procesos o tareas que se realizan dentro de una vivienda común. Para facilidad en el diseño se optó por dividir el sistema domótico general en dos sistemas más específicos, sistema de seguridad y sistema de luminosidad. Para el sistema de seguridad se propuso el diseño de dos módulos, un módulo de monitoreo de incendios y uno de control de acceso; el módulo de monitoreo de incendios consta de varios sensores los cuales obtienen información de variables como la temperatura, humedad y la presencia de humo o algunos gases, además de incorporar un sensor de presencia con el cual se detectan intrusos dentro de la vivienda que genera una notificación en una interfaz web. El módulo de control de acceso bloquea la puerta principal por medio de un hardware y les da el paso a los usuarios por medio de una contraseña, además, registra cada ingreso al sistema en una base de datos [4].

En la investigación que se realizó en el año 2020 con el tema: "Diseño de la red Internet de las cosas (IOT) para el edificio de la empresa CONSEL" tuvo como finalidad diseñar la red Internet de las Cosas (IoT) en el edificio de la empresa Consel para que satisfaga las necesidades de seguridad en los departamentos mediante IoT del edificio. La tecnología utilizada para la red IoT es Aruba HPE, y para los dispositivos finales de IoT Wi-Fi, como cámaras, sensores de movimiento, detección de incendios e intercomunicadores de video, se han considerado los dispositivos Dahua para brindar mayor seguridad y cumplir con las necesidades de los residentes, el personal administrativo y los empleados, utilizando el monitoreo y control centralizados de los dispositivos de seguridad IoT-Wi-Fi. La simulación del diseño de la red Wi-Fi IoT permite visualizar los parámetros de tráfico de datos en 2 escenarios, para que el aumento de dispositivos IoT no afecte el rendimiento en los parámetros de retraso, rendimiento, carga y pérdida de paquetes. Se ha realizado un análisis de costos de implementación, operación e ingeniería basado en el análisis del precio unitario, y se estima que la recuperación de la inversión se dará en aproximadamente un año, lo que agregará un valor adicional al costo total de cada departamento del edificio [2].

De igual manera, en la Escuela Politécnica Nacional, en el año 2020, se llevó a cabo la investigación titulada, “Diseño e implementación de un prototipo de seguridad para control domótico basado en IoT bajo ambientes de dispositivos móviles con Android”, en donde se propone una solución al problema de inseguridad en las viviendas de las ciudad de Quito, se ha planteado el diseño e implementación de un prototipo de seguridad de bajo coste para control domótico basado en internet de las cosas (IoT) bajo ambientes de dispositivos móviles con Android. El sistema de seguridad para control domótico fue construido bajo el marco de desarrollo Scrum y está conformado por cuatro componentes esenciales. El primero hace referencia al hardware (Raspberry Pi, sensores y actuadores) que fue instalado en el inmueble prototipo. El segundo se basa en los controladores de hardware desarrollados con Python. El tercero consiste en una aplicación móvil para la plataforma Android, utilizando Kotlin. Finalmente, el cuarto consiste en la base de datos que permite el almacenamiento de toda la información generada por el usuario y los diversos elementos que coexisten en el sistema, utilizando Firebase. Al concluir el diseño e implementación del prototipo de seguridad para control domótico, se obtuvo como resultado un sistema económico, innovador, de grandes prestaciones orientadas al confort y al elevamiento de seguridad física de los miembros del hogar y sus bienes; convirtiéndola así en una solución tecnológica al alcance de la mayor parte de sectores socioeconómicos de la ciudad de Quito [3].

En la investigación desarrollada en el año 2022 con el tema: “Diseño de un sistema de seguridad en el hogar basado en IOT y creación de prototipo” tuvo como objetivo diseñar y crear el prototipo de un sistema de seguridad doméstico basado en Raspberry Pi que utiliza dispositivos Internet of Things (IoT). El sistema de seguridad incorporó una variedad de sensores y actuadores. Entre los sensores se encuentran detectores de presencia basados en infrarrojos pasivos y cámaras. Por otro lado, los actuadores incluyeron una cerradura automática, un pulsador, luces y un altavoz. El sistema tuvo la capacidad de detectar movimientos, grabar imágenes y reproducirlas de manera remota gracias a los sensores instalados. Además, puede notificar el estado del sistema a los usuarios y permite la configuración del modo de funcionamiento mediante una interfaz en Internet. Uno de los aspectos destacados del sistema es la posibilidad de controlar la cerradura de forma remota a través de un bot de Telegram. Además, el

sistema permite simular la presencia de personas en el área para disuadir posibles intentos de robo. Esto se logra mediante la reproducción de audio y el control de la iluminación, actividades que el usuario también puede controlar. De esta manera se concluyó que las tecnologías Internet of Things (IoT) pueden agregar flexibilidad y versatilidad significativas a un sistema de seguridad sencillo cuando se implementa en la práctica [4].

El trabajo de titulación desarrollado en la Escuela Superior Politécnica del Litoral en el año 2023 con el título "Diseño e implementación de un sistema de control de accesos para dispositivos de seguridad basado en tecnología IoT" se enfoca en un sistema de control de dispositivos de seguridad mediante tecnología IoT, utilizando WiFi y Bluetooth. Se trabajó con programas de simulación y modelado en 3D, junto con sensores como lectores biométricos y teclados matriciales. El diseño del dispositivo se dividió en dos partes. La primera parte, el sistema principal, que contó con una App que permite al usuario conectarse por WiFi o Bluetooth. Si se elige WiFi, debe ingresar una dirección IP para activar la cerradura; si elige Bluetooth, se le solicita una clave de 4 dígitos para validar su ingreso. La segunda parte, el sistema secundario, estuvo diseñada para situaciones en las que el usuario pierda su móvil. Requiere una doble validación: una clave de 5 dígitos y la huella dactilar del usuario. Si la huella se encuentra en la base de datos, se activará la cerradura. También se incorporó un sensor de movimiento para permitir al usuario activar la cerradura desde dentro de su casa y un contacto magnético en la entrada para alertar sobre intentos de robo. Este enfoque innovador reemplaza el uso de llaves con comunicaciones inalámbricas, como el teléfono móvil y credenciales personales, para abrir la puerta de manera segura [5].

1.3. Fundamentación teórica

1.3.1. Sistemas de monitoreo de seguridad

Los sistemas de seguridad son una herramienta importante para proteger personas, instalaciones y bienes materiales en hogares y empresas. Estos sistemas están compuestos por elementos tecnológicos interconectados que pueden gestionar diferentes eventos, tales como sirenas, cámaras de video, luces y envío de mensajes a

bomberos y policía. Un sistema de monitoreo de seguridad es una tecnología diseñada para detectar, analizar y responder a eventos que puedan comprometer la seguridad de un sistema, ya sea una red, un edificio o cualquier otro tipo de instalación. Los sistemas de monitoreo de seguridad pueden incluir diversas tecnologías, como cámaras de seguridad, sensores de movimiento, alarmas, sistemas de control de acceso y sistemas de detección de intrusos [6].

Estos sistemas trabajan juntos para proporcionar una cobertura completa y garantizar que cualquier posible amenaza sea detectada de inmediato. Una vez que se detecta una amenaza, el sistema de monitoreo de seguridad puede tomar una serie de acciones para responder a ella. Por ejemplo, puede activar una alarma, enviar una alerta a los operadores de seguridad, grabar evidencia en video, bloquear el acceso a ciertas áreas o enviar una respuesta táctica inmediata.

Además, los sistemas de monitoreo de seguridad pueden integrarse con otras tecnologías, como sistemas de gestión de edificios y sistemas de gestión de crisis, para brindar una respuesta aún más rápida y efectiva. En resumen, los sistemas de monitoreo de seguridad son esenciales para garantizar la seguridad de cualquier tipo de instalación. Proporcionan una protección completa y una respuesta rápida y efectiva ante cualquier amenaza potencial [7].

Dentro de los sistemas de monitoreo de seguridad se encuentran los siguientes:

1.3.1.1. Sistema anti- intrusión

Ayudan a detectar la presencia de personas no autorizadas y pueden alertar sobre situaciones de robo en proceso. Estos sistemas cuentan con diferentes componentes que se comunican entre sí para brindar mayor efectividad y precisión. Al conectar una alarma de intrusión a una central, es posible informar sobre situaciones extrañas desde cualquier parte del mundo y evitar hurtos. Los detectores activan señales como sirenas, luces, notificaciones a una central de monitoreo o alertas vía correo electrónico, mensajes de texto o radio VHF-UHF. La elección de los medios de señalización depende de las necesidades y preferencias del usuario [8].

1.3.1.2. Sistema de control de accesos

Es un conjunto de dispositivos y programas que se utilizan para controlar el acceso de personas o vehículos a un área o edificio específico. Estos sistemas suelen utilizar diferentes tecnologías para autenticar la identidad de los usuarios, como tarjetas de acceso, lectores de huellas digitales, reconocimiento facial, entre otros. Además, permiten establecer diferentes niveles de acceso para diferentes usuarios y pueden registrar la información de ingreso y salida de cada persona o vehículo, lo que facilita la gestión y el monitoreo de la seguridad del lugar. Se los utiliza generalmente para el control de puertas en el interior o exterior de un establecimiento ya sea público o privado [9].

1.3.1.3. Sistema de detección de incendios

El sistema de detección de incendios tiene como objetivo detectar un incendio en el menor tiempo posible y enviar señales de alarma y ubicación adecuadas para tomar medidas preventivas. Las señales pueden ser enviadas a dispositivos de alarma visual o audiovisual, al servicio de bomberos mediante un dispositivo de transmisión de alarma de incendio o a un equipo automático de control o lucha contra incendios. Este sistema es esencial para prevenir y controlar incendios y proteger vidas y propiedades [10].

Existen varios tipos de sistemas electrónicos de detección de incendios, los más comunes son los sistemas de detección de humo, sistemas de detección de calor y sistemas de detección de llamas. Cada uno de estos sistemas funciona de manera diferente, pero todos tienen el mismo objetivo final de detectar un incendio en su etapa inicial y alertar a las personas para que puedan tomar medidas preventivas [11].

- **Sistemas de detección de humo:** Utilizan sensores que detectan la presencia de partículas de humo en el aire. Estos sensores pueden ser fotoeléctricos o ionización y son muy efectivos para detectar incendios en su etapa inicial. Sin embargo, estos sistemas pueden ser menos efectivos en áreas con altas concentraciones de humo, como en instalaciones industriales [12].
- **Sistemas de detección de calor**: Detectan la presencia de calor en un área determinada. Estos sistemas utilizan sensores que miden la temperatura en una

habitación y alertan a las personas cuando la temperatura supera un umbral preestablecido. Estos sistemas son efectivos para detectar incendios en su etapa inicial, pero pueden ser menos efectivos en áreas con temperaturas fluctuantes, como en áreas cerca de maquinarias industriales [10].

- **Sistemas de detección de llamas**: Utilizan sensores que detectan la presencia de luz ultravioleta o infrarroja emitida por las llamas. Estos sistemas son muy efectivos para detectar incendios en su etapa inicial, pero pueden ser menos efectivos en áreas con llamas ocultas, como en instalaciones industriales [11].

1.3.1.4. Sistema CCTV

Un circuito cerrado de televisión es un sistema de seguridad que utiliza cámaras de video para capturar imágenes de zonas específicas en tiempo real como se visualiza en la figura 1. El CCTV se utiliza para prevenir robos y actos delictivos, supervisar la seguridad del personal, controlar procesos industriales y mejorar el servicio al cliente. Este sistema es ampliamente utilizado en empresas, edificios gubernamentales, instalaciones militares, tiendas minoristas y hogares [13].

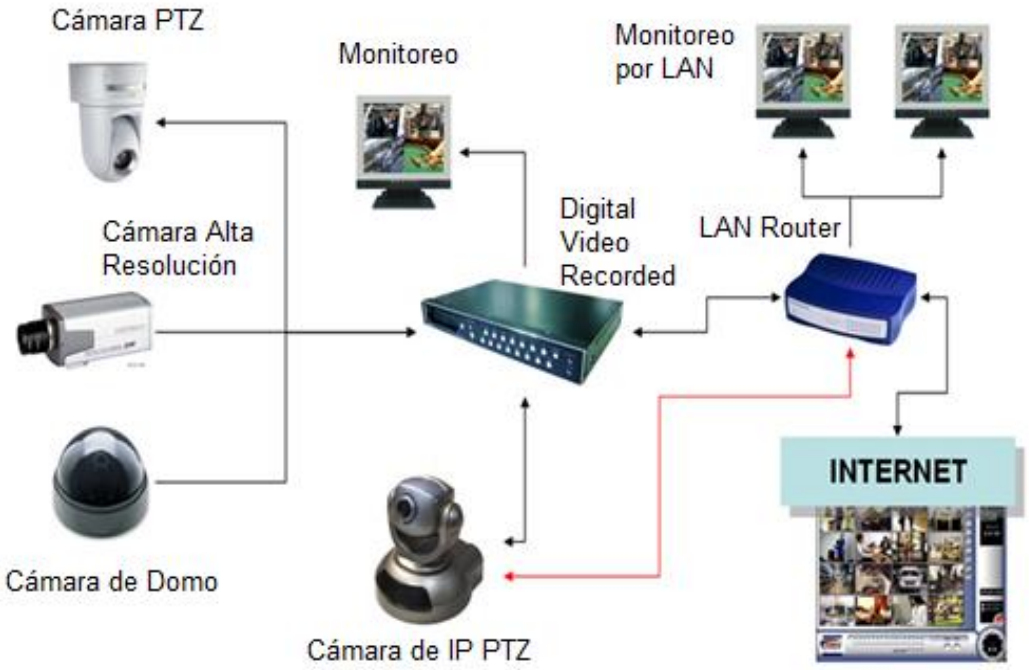


Figura 1. Componentes de un sistema CCTV *[14]*

Este sistema consta de cámaras, monitores y dispositivos de grabación, y puede enviar imágenes de manera remota a través de internet [15].

- Las cámaras pueden ser fijas o móviles y se colocan en lugares estratégicos para capturar imágenes de las áreas que se desean monitorear.
- Los monitores se utilizan para visualizar en tiempo real las imágenes capturadas por las cámaras. A diferencia de un televisor los monitores de video no incluyen sintonizador de televisión ni poseen altavoces.
- Los dispositivos de grabación se utilizan para almacenar las imágenes capturadas por las cámaras y se pueden configurar para grabar continuamente o solo cuando se detecta movimiento.

El CCTV es utilizado por diferentes motivos, como la prevención de robos y actos delictivos, la supervisión de la seguridad del personal, el control de procesos industriales y la mejora del servicio al cliente. Además, los sistemas de CCTV modernos a menudo están equipados con características avanzadas, como reconocimiento facial y detección de objetos, lo que los hace aún más efectivos para la seguridad.

1.3.2. Internet de las cosas (IoT)

La expresión Internet de las cosas se atribuye al británico Kevin Ashton en 1999 quien, mientras trabajo en Procter & Gamble, propuso que los objetos de la vida cotidiana pueden ser capaces de introducir información a la web sin ayuda de las personas [16].

El Internet de las Cosas (IoT, por sus siglas en inglés) busca que todos los objetos con los cuales las personas interactúan tengan una dirección IP (Protocolo de Internet) para que generen información y transfieran datos a través de la red, sin la necesidad de que los seres humanos intervengan o a su vez intervengan las personas-computadoras [17].

Desde otro punto de vista, el internet de las cosas IoT se define como una interconexión de sensores y controladores que proporcionan la capacidad de compartir información mediante plataformas, desarrollando un marco operativo normal para habilitar aplicaciones innovadoras. Dicho de otra manera, la IoT, es una red interconectada altamente a entidades heterogéneas como por ejemplo etiquetas, sensores, dispositivos

embebidos, dispositivos de mano, y servidores, los cuales proveen nuevos servicios y aplicaciones [18].

Cabe destacar que las ventajas del Internet de las Cosas, son las siguientes [17]:

- La automatización de las tareas con mayor transparencia, mejor calidad y uniformidad.
- La eficacia y ahorro de tiempo puesto que la interacción entre los dispositivos permite lograr resultados exactos y con un mínimo margen de error.
- El ahorro económico debido a que se reduce el consumo de energía en espacios privados y públicos, por medio de la programación y la comunicación de alerta en caso de que ocurra algún daño.
- El mejoramiento de la calidad de vida de las personas.
- La gestión de varias actividades de manera más confortable.

Por otro lado, las desventajas que puede presentar la Internet de las Cosas se mencionan a continuación [17]:

- La pérdida de la privacidad y seguridad personal, la conexión de todos los objetos genera una cantidad de información privada y personal.
- La compatibilidad de los dispositivos debido a que son de diferentes fabricantes.
- La complejidad de la red, debido a los fallos del hardware y software, o de un corte de energía eléctrica, causando consecuencias graves.
- La pérdida de trabajo de quienes no poseen conocimientos sobre automatización.
- El control de la tecnología en las personas, convirtiéndolas en dependientes de la misma.

1.3.2.1. Arquitectura IoT

La estructura es elaborada en torno a una arquitectura multicapas en donde objetos inteligentes son enlazados y utilizados para proporcionar varios servicios mediante capas principales. Cabe desatacar que existen algunos modelos de referencia que permiten describir la arquitectura del IoT, en este caso se considera el modelo UTI [19]. En la figura 2 se muestra la arquitectura del sistema IoT.

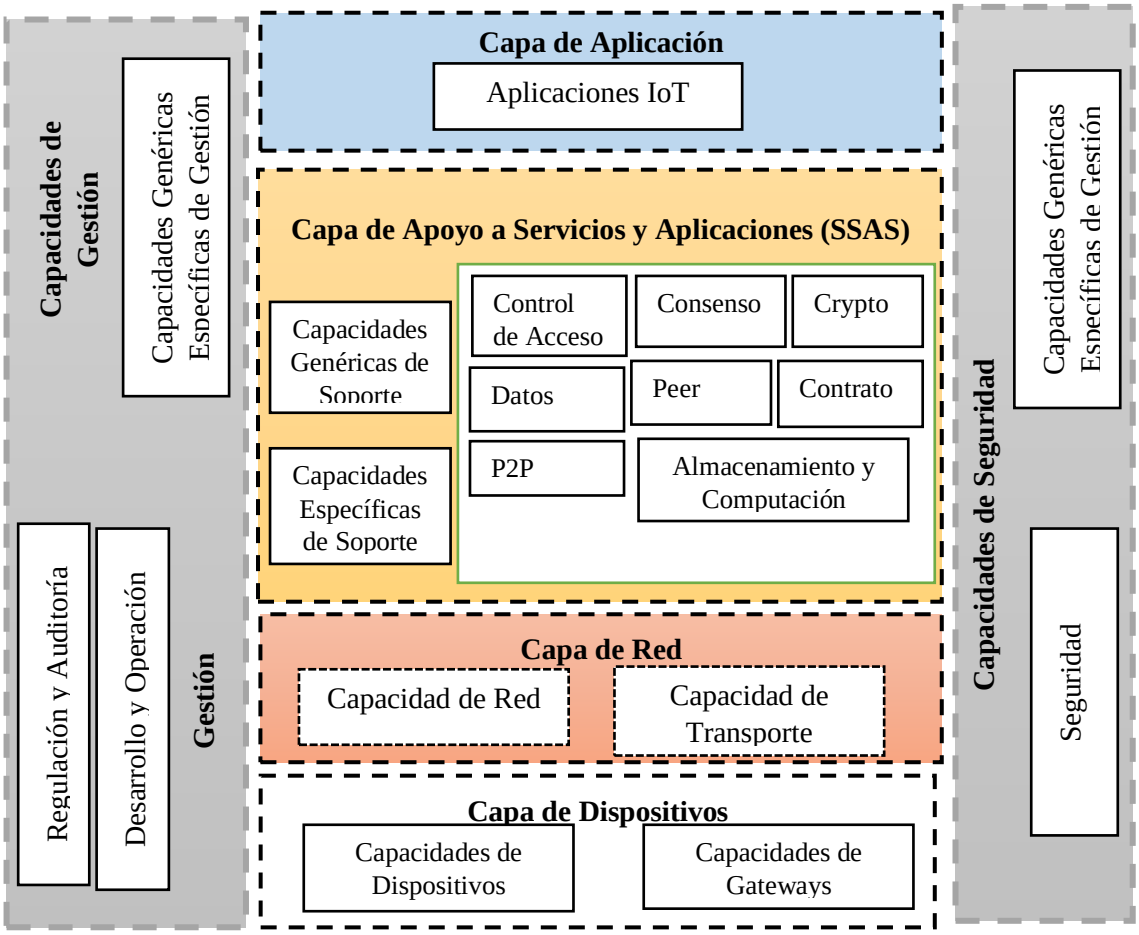


Figura 2. Arquitectura del sistema IoT *[20]*

El modelo UTI fue creado en 2012 con el nombre Y.2060, posteriormente denominado Y.4000; se encuentra compuesto por cuatro capas, de manera adicional el modelo sugiere capacidades para la gestión y la seguridad; cabe señalar que este modelo indica con claridad el objetivo que tiene cada una de las capas.

Las capas del modelo de arquitectura IoT se describe a continuación:

Capa de Aplicación IoT: Es la capa que posee varias aplicaciones para la IoT así como para el control de las mismas, a través de la computación en la nube, reconocimiento difuso entre otras tecnologías de computación inteligente para el análisis y computo de grandes cantidades de información y de control inteligente [19].

Capa de apoyo de servicios y aplicaciones IoT: Esta capa se la conoce como middleware se encarga de almacenar datos que provienen de la capa de transferencia, tambien extrae información que es previamente procesada y analizada; por tanto, esta

capa puede administrar y proporcionar servicios a capas inferiores. Es la responsable de entregar servicios y aplicaciones específicas al usuario final [21].

Capa de dispositivo IoT: Es la que tiene la función de gestionar los dispositivos que conforman el IoT, la cual debe recolectar toda la información del entorno [20].

En esta capa las funciones o capacidades se clasifican en dos grupos que son:

Capacidades de dispositivo: Son las que muestran la probabilidad de interactuar con la red de comunicaciones de forma directa o indirecta [20].

A continuación, se menciona las capacidades de dispositivo:

- Interacción directa con la red de comunicaciones. – ocurre cuando los dispositivos lograr obtener y cargar información de manera directa en la red de comunicación, también cuando reciben información de modo directo de la red de comunicación.
- Interacción indirecta con la red de comunicaciones. – se presenta cuando los dispositivos consiguen y cargan información de manera indirecta en la red de comunicación, por medio de capacidades de pasarela, de la misma manera cuando receptan información de forma indirecta de la red de comunicación.
- Redes ad-hoc. - sucede cuando los dispositivos consiguen construir rede de modo ad-hoc en diferentes situaciones cuando sea importante ampliar la capacidad evolutiva y la velocidad de despliegue.
- Modo reposo y activo. - es cuando las capacidades de dispositivo deben poseer herramientas para pasar a los modos “reposo” y activo con la intención de ahorrar energía [19].

Capacidad de Gateway: Tiene como característica principal el soporte a múltiples interfaces para acceder a una mayor cantidad de tecnologías de comunicación [20].

Las capacidades Gateway o también conocidas como pasarela se clasifica en:

- Soporte de interfaces múltiples. - permite admitir tecnologías de comunicación, ya sean de tipo alámbricas o inalámbricas, como, por ejemplo: CAN, ZigBee, Bluetooth o Wifi.

- Conversión de protocolo. - cuando en las comunicaciones en la capa de dispositivo se utiliza distintos protocolos como: protocolos de tecnología ZigBee y Bluetooth; por otro lado, cuando en la comunicación intervienen la capa de dispositivo y la de red y se recurre al uso de varios protocolos [20].

Capa de Red: Se encarga de determinar la comunicación entre los datos medidos y servidor web de capa posterior. Posee un módulo de conexión que proporciona la transferencia de los datos a la red, un protocolo de comunicaciones y un lenguaje de intercambio que provee la transferencia de datos [22].

Capacidades de Gestión: Según este modelo comprenden: gestión de fallos, configuración, el rendimiento y seguridad; estas capacidades se clasifican en genéricas y específicas, por un lado, las primeras ayudan a manipular los dispositivos, así como tambien gestionar la tipología y el tráfico, por su parte las segundas se encuentran relacionadas a las exigencias específicas de las diferentes aplicaciones [20].

Capacidades de Seguridad: Se encarga de recopilar la información creada a partir del IoT acerca de las diferentes tareas que se efectuaran de acuerdo a las necesidades del cliente, además es donde se encuentra el mayor potencial [20].

1.3.2.2. Protocolos utilizados en IoT

OPC UA: Este protocolo de comunicación se orienta a los servicios independientes de la plataforma que compone toda la funcionalidad de las especificaciones individuales de OPC Classic en un marco extensible. Por tal razón la arquitectura unificada OPC UA que comunica datos entre aplicaciones SCADA y sensores y además con aplicaciones de una organización por medio de todas las capas existentes en una empresa [23].

HTTP (REST/JSON): Es un protocolo de IoT usado para el intercambio de páginas web y servidores por medio de mensajes de petición/respuesta, el cual es utilizado para otros propósitos, además usa mensajes de cabecera que intercambian información entre cliente y servidor [24].

TCP/IP: Es un protocolo de control de transmisión, el cual está ideado para ser usado como un protocolo de fiabilidad entre los miembros de redes de comunicación de computadoras mediante intercambio de paquetes y en un sistema interconectado de redes. Es considerado un protocolo básico que permite enviar y recibir segmentos de longitud variada de información rodeada en datagramas de internet [25].

MQTT. - Es un protocolo de mensajería tipo publicación/subscripción que cuenta con un flujo de datos optimizado que permite reducir el tráfico de red. Fue diseñado para redes de comunicación poco fiable y tiene un consumo mínimo de energía [26].

CoAP: Es un protocolo diseñado para microcomputadores con poca memoria y capacidad de procesamiento [26].

DDS: Es un protocolo para sistemas en tiempo-real, utiliza middleware, utiliza el modelo publicar/suscribir para el envío, recepción de datos, registro de eventos y comandos entre los nodos en la transmisión M2M. Es un estándar abierto y descentralizado. Los nodos de DDS se comunican directamente punto a punto a través de UDP/multidifusión (multicast). DDS es una buena solución para aplicaciones que requieren intercambio de datos en tiempo real como el control del tráfico aéreo, gestión de redes inteligentes, vehículos autónomos, robótica, sistemas de transporte, generación de electricidad, entre otros. Ofrece seguridad, portabilidad, escalabilidad y efectividad del rendimiento [27].

AMQP: Este protocolo da prioridad a garantizar la recepción de todos mensajes, trabaja sobre TCP y proporciona una conexión punto a punto fiable [26].

UDP Y TCP: Son protocolos de la capa de transporte del TCP/IP, estos permiten la transmisión de datos entre el trasmisor u el receptor con una confiabilidad segura y evitando perdida a la hora de la transmisión. Otro punto a favor de estos protocolos es que ofrece flujo de bytes ordenado haciendo que el receptor al momento de recibir los datos sea capaz de ordenarlos correctamente [28]

LoRawan: Permite la comunicación a un gran alcance de cobertura y de baja potencia entre los sensores remotos y puertas de enlace que se encuentran conectadas a la red, y también es el encargado de sistematizar las frecuencias de comunicación, también potencia los dispositivos y velocidad de los datos [27].

Sigfox: Usa una tecnología patentada de estaciones bases que se encuentran desplegadas en varios países en las bandas de radio industriales, científicas y médicas (ISM) de sub-GHz sin licencia; los dispositivos finales se conectan a estaciones base, utilizando la modulación BPSK en una banda ultra estrecha de 100 Hz, a una velocidad máxima de datos de 100 bps, con muy bajos niveles de frecuencia de ruido, consumo de energía bajo, alta sensibilidad del receptor y diseño de antena y hardware de bajo costo [29].

RFID: Se utiliza en varios desarrollos y aplicaciones de identificación, donde se incluyen una cadena de suministros para localizar objetos, automatizar hogares, sistema de seguridad y entrega de productos entre otros [30].

Bluethoot: Es una tecnología inalámbrica de corto alcance, el mismo que va de 10 a 100m con un ancho de banda moderado de 1 Mbpss basado en el estándar IEE 802.15.1. Es utilizado para intercambiar datos entre notebooks, tablets, cámaras e impresoras [31].

WiFi (Estándar IEEE 802.11n): Es un patrón que usa múltiples antenas para apresurar la transmisión de los datos. El propósito que tiene este estándar es ampliar la capacidad de la red con relación a los otros estándares anteriores. Del mismo modo acrecienta enormemente en la transferencia de datos de 54 Mbs a 600 Mbs y se puede utilizar en dos anchos de bandas de frecuencias de 2.4 GHz o 5 GHz. Este estándar utiliza diferentes avances en las capas físicas y MAC para mejorar el rendimiento, al mismo tiempo que incluye la técnica de modulación OFDMA y la tecnología MIMO que favorecen el aumento de velocidad en las tasas de datos [32].

ZigBee (Estándar IEEE 802.15.4): Es considerada una tecnología de red inalámbrica que tiene un alcance corto de alrededor de 100 m, un consumo bajo baja complejidad,

fiabilidad y seguridad que permite la configuración de redes en topologías estrella, árbol de clusters y malla. Se utiliza de manera extensiva para la automatización de sistemas de energía, salud, seguridad entre otros [31].

1.3.2.3. Modelos de comunicación IoT

El Internet de las cosas consta de muchos dispositivos inteligentes que se comunican entre sí. Estos dispositivos permiten el intercambio y la recopilación de datos. Los dispositivos inteligentes pueden tener una conexión por cable o inalámbrica. Por lo general, los dispositivos IoT se conectan a Internet a través de la pila de Protocolo de Internet (IP). Esta combinación es muy compleja y requiere una gran cantidad de energía y memoria de los dispositivos conectados. Estos dispositivos también se pueden conectar localmente a través de redes NO IP que consumen menos energía y se conectan a Internet a través de una puerta de enlace inteligente [33]. Los modelos de comunicación que se emplean en IoT son los que se describen a continuación:

Dispositivo a dispositivo

Este modelo implica que dos o más dispositivos se conectan y comunican directamente sin necesidad de un servidor intermediario, tal y como se muestra en la figura 3. Este modelo se utiliza en muchas redes, incluyendo la Internet, pero a menudo se emplean protocolos como Bluetooth, Z-Wave o ZigBee para establecer conexiones directas Estas redes son comúnmente utilizadas en aplicaciones de automatización del hogar, donde los dispositivos de IoT se comunican entre sí a través de pequeños paquetes de datos con requisitos relativamente bajos en términos de la tasa de transmisión. Por ejemplo, las bombillas, interruptores, termostatos y cerraduras residenciales se comunican entre sí para realizar funciones específicas, como encender una luz o indicar el estado de bloqueo de una puerta [34].

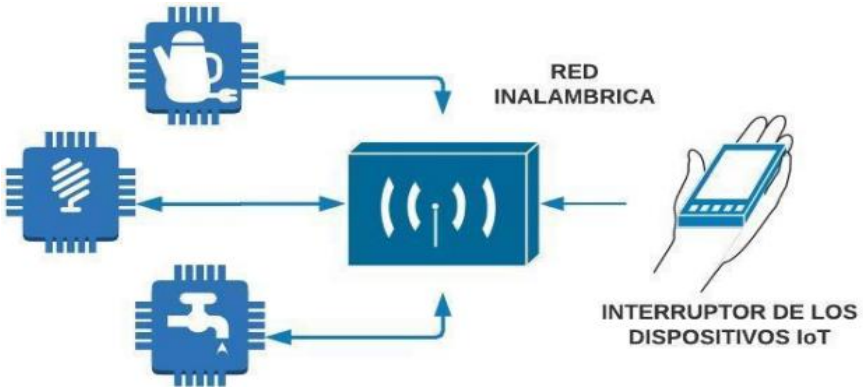


Figura 3. Modelo de comunicación dispositivo a dispositivo [35]

Dispositivo a Nube

Presenta una interconexión direccional entre dispositivos IoT y proveedores de servicios en la nube para transferir información y recursos con mensajes de control y sensores utilizando tecnologías de comunicación existentes, como tecnología de sensores, tecnología basada en la nube, tecnología de mensajería, tecnología IP y tecnología inalámbrica [36].

En el modelo de comunicación de dispositivo a nube, los dispositivos se conectan directamente a un servicio de Internet en la nube con conexiones Wi-Fi existentes y la red IP para intercambiar datos y controlar el tráfico de mensajes, como se puede observar en la figura 4. La nube permite al usuario obtener acceso remoto a sus dispositivos, por ejemplo, a través de un teléfono inteligente o una interfaz web. Para el modelo de dispositivo a nube, el dispositivo IoT se conecta a la nube a través de un dispositivo de puerta de enlace local, que puede proporcionar seguridad y otras funciones.

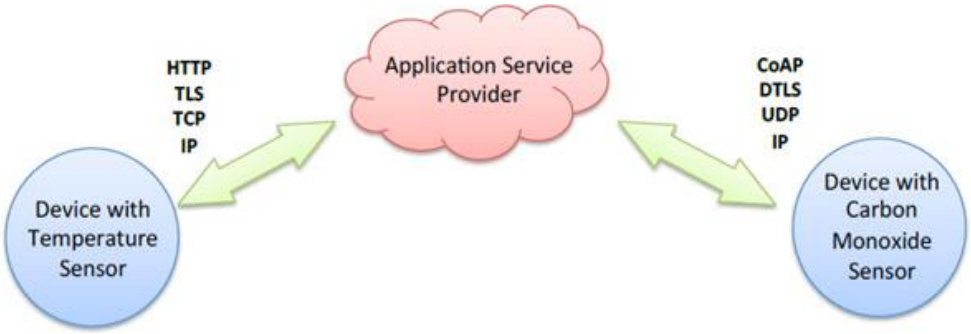


Figura 4. Modelo de comunicación de dispositivo a nube *[37]*

Dispositivo a Puerta de enlace

Como se muestra en la figura 5, en el modelo de dispositivo a puerta de enlace, la puerta de enlace de la capa de dispositivo a la aplicación (ALG). El dispositivo IoT se comunica a través de un ALG que sirve como canal para acceder a los servicios en la nube. Simplemente, esto significa que hay un programa de aplicación ejecutándose en un dispositivo de puerta de enlace local que actúa como intermediario entre el dispositivo y el servicio en la nube y proporciona seguridad y traducción de datos. En la mayoría de los casos, un teléfono inteligente con una aplicación para comunicarse con un dispositivo [33].

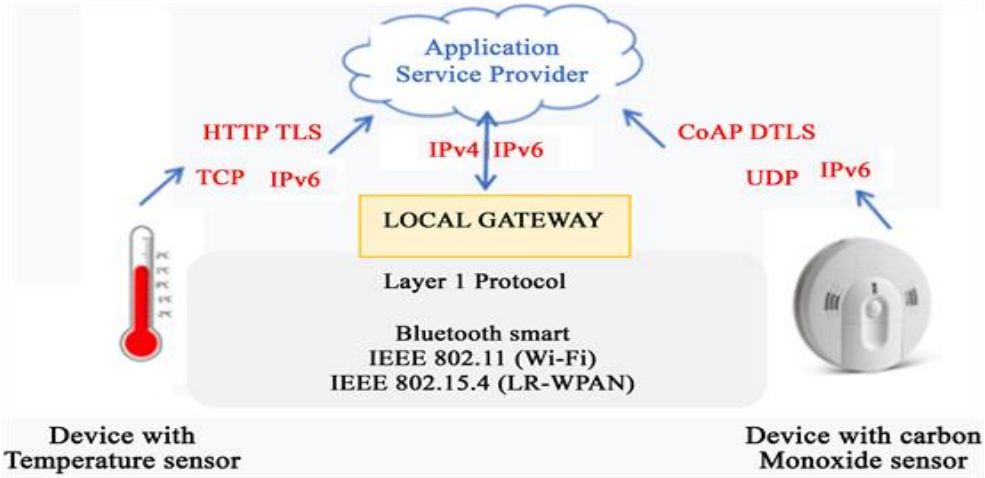


Figura 5. Modelo de comunicación dispositivo a puerta de enlace *[33]*.

Back End Data Sharing

El modelo de intercambio de datos de back-end se refiere a una arquitectura de comunicación que permite a los usuarios exportar y analizar datos de objetos inteligentes desde un servicio en la nube en combinación con datos de otras fuentes. Esta arquitectura admite "el deseo [del usuario] de otorgar acceso a los datos del sensor cargados a terceros". Este enfoque es una extensión del modelo de comunicación de un solo dispositivo a la nube, que puede conducir a silos de datos en los que los dispositivos IoT cargan datos solo a un único proveedor de servicios de aplicaciones. Una arquitectura de uso compartido de back-end permite que los datos recopilados de flujos de datos de dispositivos IoT únicos se agreguen y analicen (Ver figura 6) [38].

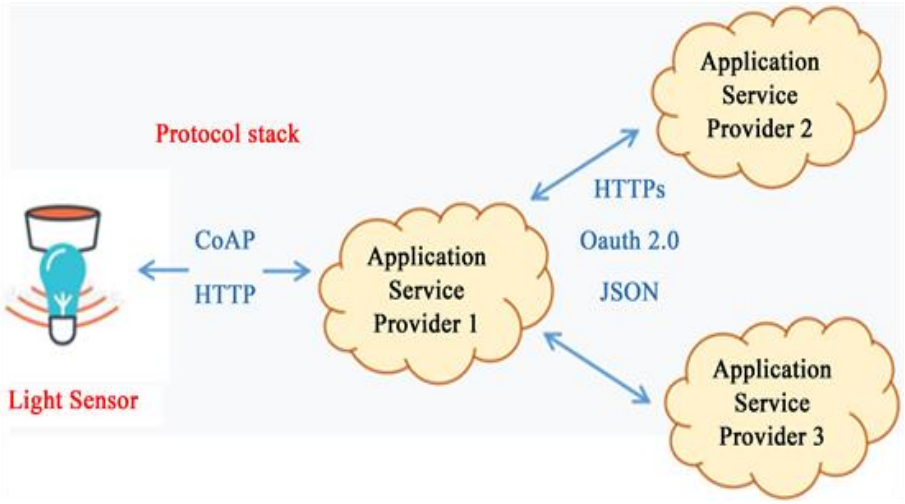


Figura 6. Modelo de comunicación Back End Data Sharing [33].

Este tipo de arquitectura facilita las necesidades de portabilidad de datos. Las arquitecturas efectivas de intercambio de datos de back-end permiten a los usuarios mover sus datos cuando cambian entre los servicios de IoT, rompiendo las barreras tradicionales de los silos de datos. El modelo de intercambio de datos de back-end sugiere que se necesita un enfoque de servicios en la nube federados o interfaces de programador de aplicaciones en la nube (API) para lograr la interoperabilidad de los datos de dispositivos inteligentes alojados en la nube.

1.3.2.4. Dispositivos utilizados en IoT

Sensores

El texto habla sobre los sensores, que son dispositivos que miden una magnitud física del entorno y entregan una magnitud eléctrica proporcional para informar sobre el estado de una variable. Los sensores pueden ser analógicos o digitales y se utilizan en diferentes aplicaciones, como la domótica. Los sensores analógicos miden la magnitud a través de un rango continuo de valores, mientras que los sensores digitales sólo pueden tomar dos valores, uno o cero. Se da el ejemplo de los sensores de detección de presencia como un ejemplo de los sensores digitales. Los sensores siempre están en contacto con la magnitud o variable que miden [39].

Los sensores también se pueden clasificar dependiendo de su aplicación final, por ejemplo, en sistemas de vigilancia, se utilizan 4 tipos de sensores: de contacto, infrarrojos, vibración y microondas, aunque existen otros para aplicaciones especiales. En tareas como el accionamiento de persianas es utilizado comúnmente un sensor de luminosidad, el cual mide la intensidad lumínica del ambiente. La medición de la temperatura, la humedad, la presencia de algún gas, movimiento, entre otros, son algunos ejemplos de las aplicaciones en las cuales los sensores se utilizan [40].

Actuadores

Actuador es un dispositivo que puede generar un ajuste en el suelo cambiando la energía eléctrica conectada a un cierto tipo de energía valiosa. Algunos modelos son componentes de refrigeración o calefacción, luces, altavoces, espectáculos y motores. Los actuadores, que provocan el movimiento, se pueden organizar en tres clases, para ser actuadores específicos, eléctricos, accionados por presión y neumáticos, dependiendo de su actividad. Los actuadores impulsados por presión fomentan el movimiento mecánico utilizando la fuerza impulsada por líquido o agua. Los actuadores neumáticos utilizan el peso del aire comprimido y los eléctricos utilizan energía eléctrica [41].

Dentro de los actuadores, los más comunes son los siguientes [42]:

- **Motores:** Generalmente los motores se controlan utilizando modulación por ancho de pulso (PWM). Se envían pulsos de ancho variable para que el motor gire de manera proporcional a la anchura del pulso.
- **Servomotores:** Este tipo de actuadores permite el control de la posición dentro de un rango y mantener fija esta posición. El control se realiza de igual manera mediante señales PWM, siendo la duración de los pulsos la que indica la posición o el ángulo de rotación. Se no se envía ninguna señal. El servomotor queda libre.
- **Motores paso a paso:** Son motores que pueden avanzar un determinado número de grados o pasos (steps) respecto de su eje. Para lograr esto se requiere un circuito y generar señales que se envían al motor, logrando pasos de pocos grados.

- **Electroválvulas:** son válvulas que se controlan electromecánicamente, las cuales permiten o impiden el paso de líquidos o gases. Estos elementos disponen de posiciones. Abierto o cerrado, por lo que su control es sencillo.

Teléfonos móviles (smartphones)

Los teléfonos móviles pueden ser sensores y actuadores, además de permitir realizar y recibir llamadas, entre otras funcionalidades. Estos dispositivos disponen de múltiples sensores y actuadores [42]:

- Acelerómetro: Que permite medir movimientos y conocer la posición del móvil.
- Giróscopo: Permite medir el movimiento, el ángulo y la velocidad de giro en las tres coordenadas espaciales.
- Sensores de iluminación: ayuda a registrar la cantidad de luz ambiental.
- Sensores de acústicos: se encuentran equipados con micrófonos que permitan el registro de sonido.
- Barómetro: permite medir la presión atmosférica.
- Sensor táctil: Recibe entradas múltiples de manera simultánea.
- GPS: Proporciona la posición en coordenadas espaciales y la velocidad a la que un dispositivo se mueve, con precisiones de metros y Km/h.

1.3.2.5. Aplicaciones de IoT

El internet de las cosas (IoT) consiste en que diferentes cosas u objetos tengan la capacidad de conectarse a internet en cualquier momento y en cualquier lugar. En un sentido más técnico, consiste en la integración de sensores y dispositivos en objetos cotidianos que estén conectados a internet a través de redes fijas e inalámbricas. De esta manera, cualquier objeto es susceptible de ser conectado y manifestarse en la red. Además, el IoT implica que todo objeto puede ser una fuente de información [43].

IoT es un esquema bien definido de tácticas informáticas interconectadas, dispositivos digitales y mecánicos que poseen la capacidad de transmisión de datos a través de la red definida sin intervención humana en ningún nivel [44]. IoT utiliza dispositivos

inteligentes e Internet para brindar soluciones innovadoras a diversos desafíos y problemas relacionados con diversas industrias comerciales, gubernamentales y públicas/privadas en todo el mundo [45].

En conjunto, IoT es una innovación que reúne una amplia variedad de sistemas inteligentes, marcos y dispositivos y sensores inteligentes. Además, aprovecha la tecnología cuántica y la nanotecnología en términos de almacenamiento, detección y velocidad de procesamiento que antes no eran concebibles [46].

1.3.3. Redes inalámbricas

Las redes inalámbricas pueden trasmitir datos por el aire, utilizan ondas de radio para comunicarse, estas ondas electromagnéticas tienen longitudes de ondas más largas que las infrarrojas [47]. Las redes inalámbricas permiten el uso de dispositivos con redes en cualquier parte, en una oficina, en una casa e, incluso, al aire libre. Entre las ventajas que tienen las redes inalámbricas, se mencionan las siguientes:

- Libertad del movimiento del usuario, como en el caso de los computadores portátiles, tablets, Smartphone, otros.
- Los cambios en las instalaciones son muy fáciles de efectuar, ya que añadir nuevos equipos solo implica tener cobertura en aquellos lugares donde se vayan a colocar esos equipos [48].

1.3.3.1. Clases de redes inalámbricas

- **WPAN (Wireless Personal Area Network)**

Se define por sus siglas en inglés como Wireless Personal Área Network; este tipo de redes permiten la interconexión entre dispositivos de carácter portátil dentro de una zona determinada por el radio de cobertura; entre los dispositivos que comúnmente ocupan este tipo de redes tenemos: teléfonos inteligentes, laptops, tablets, impresoras, cámaras de fotos como se aprecia en la figura 7 [49].

Figura 7. Wireless Personal Area Network *[49]*

Es una red inalámbrica de área personal que tiene un rango máximo de 10 metros. Las WPAN se definen mediante el estándar 802.15, el cual incluye la comunicación de dispositivos a través de Blutooth. La ventaja de esta tecnología es que puede trasmitir simultáneamente voz y datos, consume mucha menos energía que una conexión wifi. En tanto que su mayor desventaja es que la velocidad de trasmisión es muy baja [50].

- **WLAN (Wireless Local Área Network)**

Por sus siglas en inglés se define como Red de Área Local Inalámbrica (WLAN); este tipo de redes permite la interconexión de diversos dispositivos como estaciones de trabajo, PCs, impresoras, servidores, entre otros; estos dispositivos son capaces de comunicarse entre sí, por medio de una dirección IP asignada a cada uno de ellos, ya sea fija o dinámica. Al ser inalámbricas no requieren ningún tipo de cableado [49].

Proporciona comunicación de red inalámbrica en distancias cortas utilizando señales de radio o infrarrojos en lugar del cableado de red tradicional. Es una en la que un usuario móvil puede conectarse a una red de área local (LAN) a través de una conexión inalámbrica (radio) [51].

- **WMAN (Wireless Metropolitan Area Network)**

Este tipo de redes se basa en el estándar IEEE 802.16, y su principal característica es que permiten dar cobertura a un área extensa; mediante el uso de esta tecnología, se

puede por ejemplo realizar una interconexión entre redes que se encuentren lejanas; la principal ventaja es que su costo es reducido, ya que al ser inalámbrica no se necesita ningún cableado [49].

- **WWAN (Wireless Wide Área Network)**

Se definen como redes inalámbricas de área extendida por sus siglas en inglés (WWAN), estas son utilizadas para comunicación en un área geográfica extensa; la comunicación se establece mediante la utilización de antenas satelitales o antenas de microondas, permiten acceder a la red desde lugares remotos, por lo general muy lejanos. Su radio de cobertura es de miles de kilómetros, y sus velocidades de transmisión están en el rango de 56-170 kbps [49].

También llamado Red celular, las redes de área local inalámbricas a menudo confíe en Ethernet y enrutadores inalámbricos de corto alcance, inalámbricos WAN puede usar sistemas de redes celulares para enviar señales a una distancia más larga y conducen a cubrir una gran área geográfica [52].

La conectividad de las redes WWAN es muy superior a las otras redes en cuanto el usuario puede moverse por distintas zonas e incluso cambiar de un punto de acceso a otro sin interrupciones en la conexión [53].

1.3.4. Lenguajes y entornos de programación

1.3.4.1. C Sharp

Este es un lenguaje de programación dirigido a objetos, fue elaborado por Microsoft con la idea de incorporarlo a su plataforma.NET y que después fue utilizado también la ECMA e ISO. Estas ampliaciones en su uso hicieron que fuera obligada su estandarización que fue dirigida también por Microsoft. Está basada en la sintaxis de C/C++, por ello sus sintaxis básicas son muy parecidas. Su modelo de objetos es el de la plataforma.NET que funciona de forma cercana a Java. Sin embargo, C# ha incorporado mejoras que provienen de otros lenguajes [54].

Cabe mencionar que, entre las características de la C Sharp se mencionan las siguientes:

a) Simplicidad: Los proyectistas de C# afirman que es un lenguaje tan poderoso como C++ y tan simple como Visual Basic.
b) Completamente orientado a objetos: en C#, cualquier variable tiene que formar parte de una clase.
c) Fuertemente tipado: ayuda a evitar errores por la manipulación impropia de los tipos y atribuciones incorrectas.
d) Genera código gestionado: así como el entorno .NET, C# también es gestionado.
e) Todo es un objeto: System.Object es la clase base de todo sistema de tipos C#.
f) Control de versiones: cada assembly generado (EXE O DLL) tiene información sobre la versión del código, permitiendo la coexistencia de dos assemblies homónimos, pero de versiones diferentes en el mismo entorno.
g) Soporte de código heredado: C# puede interactuar con código heredado de objetos COM y DLLs escritas en un lenguaje no gestionado.
h) Flexibilidad: cuando el programador necesita usar punteros, C# lo permite, pero al coste de desarrollar código no-gestionado, llamado Unsafe.
i) Lenguaje gestionado: se ejecutan en un entorno gestionado, en efecto, toda la gestión de memoria es realizada por el runtime mediante el Garbage Collector (GC) [55].

1.3.4.2. Arduino

La plataforma Arduino comprende una serie de elementos, tanto hardware, como software, que permite a los estudiantes la creación de proyectos tecnológicos mientras se van desarrollando los conocimientos y habilidades relacionadas con la programación, la electrónica y la robótica. En cuanto al hardware, Arduino cuenta con placas electrónicas, controladoras programables, placas electrónicas de ampliación que se acoplan fácilmente a las primeras para incrementar su funcionalidad, soportes y otros accesorios. Además, es posible comprar kits que incluyen conjuntamente, tanto

la placa controladora, como un conjunto de sensores y actuadores. Entre todo el hardware disponible, la placa programable Arduino UNO es posiblemente la más utilizada en el ámbito educativo. La figura 8 muestra una imagen de esta placa [56].

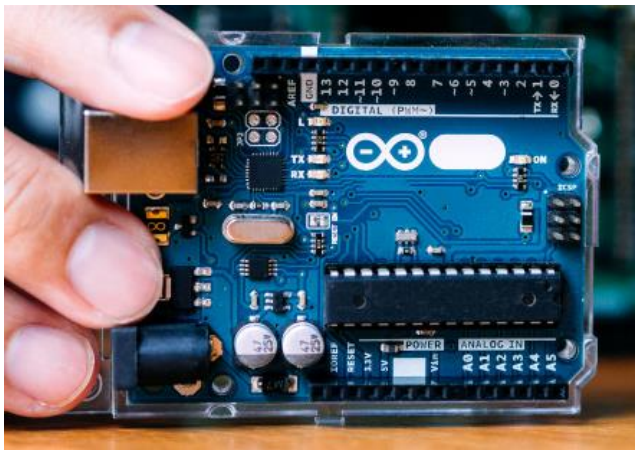


Figura 8. Arduino UNO [56]

Desde otra perspectiva, el Arduino es una tarjeta programable en lenguajes de alto nivel que contiene un micro controlador ARM que en esencia es prácticamente una computadora. Los creadores de Arduino han tenido mucho éxito con su sistema y probablemente una de las razones es que tanto el hardware como el software son abiertos, es decir, los desarrolladores han creado una plataforma que cualquiera puede copiar y en algún caso mejorar, sin tener que pagarles regalías. Tal vez el truco esté en que Arduino hace una serie de tarjetas -como la popular Arduino UNO- que resulta más práctico y barato, que armar de cero la propia. El hecho de poner todo en un entorno abierto da la posibilidad que mucha gente se involucre y los productos mejores significativamente [57].

Con el software de Arduino se programa mediante el uso de un leguaje basados en una programación de alto nivel, el entorno de programación de Arduino es un código abierto, libre en la cual hace fácil escribirlo y cargarlo a la placa, funciona con los sistemas operativos Windows, Mac OS y Linux. También es posible utilizar otros lenguajes de programación y aplicaciones populares de Arduino, algunos de ellos son Java, Python, Matlab, Adobe director, VBScript, la programación de Arduino está basado en C y soporta todas las funciones del estándar de C y algunas de C++ [58].

1.3.4.3. Framework Flutter

Flutter es el framework por excelencia diseñado para la interacción con Dart, optimizando la sintaxis utilizada por su lenguaje raíz. Posee el mejor tiempo de ejecución dentro de los frameworks ofertados en el mercado además de integrar múltiples herramientas gratuitas fáciles y livianas de utilizar para depurar y debuggear el código. Flutter transforma el proceso de desarrollo de aplicaciones desde una perspectiva cómoda y eficiente para los desarrolladores ya que posee librerías fáciles y cómodas de usar e instalar desde un repositorio virtual, con el soporte de cientos de desarrolladores a nivel mundial que realizan constantes contribuciones a la comunidad [59]

En Flutter, todas las aplicaciones están escritas con Dart. El cual es un lenguaje de programación desarrollado y mantenido por Google. Es ampliamente utilizado dentro de Google y se ha demostrado que tiene la capacidad de desarrollar aplicaciones web masivas, como AdWords [60].

1.4. Objetivos

1.4.1. Objetivo General

Implementar un sistema de monitoreo con tecnología IoT para dotar de seguridad a los Departamentos de la Administración General y Financiero del GAD Municipal Tisaleo.

1.4.2. Objetivos Específicos

- Establecer los criterios y estado actual del sistema de seguridad y monitoreo del GAD Municipal Tisaleo.
- Diseñar un sistema de monitoreo para los departamentos de Administración General y Financiero con tecnología IoT.
- Planificar el Sistemas de monitoreo y seguridad para las oficinas del edificio principal del GAD Municipal Tisaleo.

CAPÍTULO II

METODOLOGÍA

2.1. Materiales

Para el desarrollo del Sistema de monitoreo con tecnología IoT para las oficinas del GAD Municipal Tisaleo se seleccionaron diferentes elementos electrónicos, de acuerdo a investigaciones previas realizadas.

- **Arduino Mega:** Para controlar y monitorear diferentes componentes electrónicos, como sensores, cámaras, alarmas, puertas, entre otros.
- **Cámaras IP:** Permite capturar las imágenes y videos claros. Este dispositivo está compuesto por un lente, un sensor de imágenes, un procesador de imagen, un SoC (Sistema en Chip) de comprensión de video y un chip Ethernet para permitir la conectividad de red para la transmisión de los datos.
- **Sensor de Movimiento PIR:** Encargado de detectar la presencia de personas o animales. Este dispositivo detecta el cambio en la radiación infrarroja emitida por los objetos en movimiento dentro de su alcance.
- **Sensor de huellas digitales:** Se utiliza para escanear la huella dactilar de una persona y convertirla en una imagen digital. La función principal de un sensor de huellas digitales es la de identificación y autenticación de personas.
- **Servo motor:** Este dispositivo electromecánico se utiliza en una amplia variedad de aplicaciones para controlar la posición, velocidad y aceleración de un objeto.
- **Display con i2c:** Este dispositivo proporciona una interfaz visual para presentar información de una manera fácilmente comprensible para los seres humanos.
- **Bocina de sirena:** Sirve para producir un sonido fuerte y audible que se utiliza como señal de alarma o advertencia.

2.2. Métodos

2.2.1. Modalidad de la investigación

Investigación aplicada

El presente proyecto se enmarcó dentro de la investigación aplicada, porque se empleó los conocimientos adquiridos durante la formación académica para dar solución a los problemas que se presentan dentro del GAD Municipal Tisaleo en donde se desarrolla este proyecto, planteando una solución acorde a los objetivos planteados inicialmente.

Investigación Bibliográfica

La investigación fue bibliográfica, porque el proyecto de investigación se sustentó mediante la recopilación de información de revistas técnicas, libros, artículos científicos, publicaciones en internet y tesis, relacionados a los sistemas de seguridad, domótica y arquitectura IoT, personalización de la aplicación móvil, las cuales sirvieron para entender de mejor manera la temática y así plantear una solución que se encuentre acorde con las necesidades de las autoridades del GAD Municipal Tisaleo.

Investigación de campo

El presente proyecto se realizó dentro de la investigación de campo, debido a que se recopiló información y se implementó el sistema donde se origina el problema, con el fin de cumplir los requerimientos de las autoridades del GAD Municipal Tisaleo, con el afán de brindar un sistema de seguridad funcional.

2.2.2. Población y Muestra

En la presente investigación se considera como población al señor alcalde del cantón Tisaleo, al cual se le aplicó una entrevista para establecer el estado actual de la seguridad dentro de las oficinas del GAD Municipal.

2.2.3. Recolección de Información

Para el desarrollo de este proyecto de investigación se utilizó la información obtenida de manera directa al señor alcalde del cantón, así como datos recopilados de libros, artículos científicos, y revistas científicas, así como guías prácticas y manuales de construcción por lo que se tomó en cuenta bases de datos confiables que permitan el desarrollo del proyecto.

2.2.4. Procesamiento y Análisis de Datos

Para el procesamiento y Análisis de datos se siguieron los siguientes pasos:

- Revisión de la información recopilada.
- Estudio de las propuestas de solución planteadas para aumentar la seguridad de las oficinas del GAD Municipal de Tisaleo de acuerdo con las necesidades de la institución antes mencionada.
- Interpretación de la información relevante que contribuya al desarrollo del proyecto de investigación que lleve a la solución de la propuesta.
- Planteamiento de la propuesta de solución.
- Control y verificación que el dispositivo implementado este completamente funcional y transmita la información correctamente mediante el desarrollo de pruebas.

2.2.5. Desarrollo del Proyecto

El proceso para la implementación de un sistema de control de calidad utilizando redes neuronales, tuvo las siguientes actividades:

1. Recolección de información acerca del nivel de inseguridad dentro de las oficinas del GAD Municipal Tisaleo.
2. Determinación de los problemas que se generan al no utilizar ninguna medida de seguridad.
3. Análisis las variables que intervienen en monitoreo y control de un sistema de seguridad en las oficinas del GAD Municipal de Tisaleo.

4. Selección de los dispositivos y componentes hardware para el sistema de seguridad con IoT.
5. Selección del software a utilizar para el control del sistema.
6. Diseño la interfaz para el control del sistema de seguridad mediante aplicación móvil.
7. Comunicación entre el hardware y software.
8. Implementación del sistema de seguridad con arquitectura IoT.
9. Desarrollo pruebas de funcionamiento del sistema.
10. Corrección los errores del sistema de seguridad.
11. Evaluación de la eficiencia del sistema diseñado para el control de seguridad del GAD Municipal Tisaleo.
12. Elaboración el informe final del proyecto y posterior revisión con el docente tutor.

CAPÍTULO III

RESULTADOS Y DISCUSIÓN

3.1. Análisis y discusión de resultados

La implementación del sistema de seguridad para las oficinas GAD Municipal de Tisaleo con arquitectura IoT permite el monitoreo en tiempo real de eventos de seguridad dentro del lugar. Los datos de los sensores y dispositivos se transmiten y visualizan en tiempo real, lo que facilita la detección y respuesta rápida a situaciones de riesgo debido a que envía alertas automáticas las autoridades en caso de intrusión o actividad inusual. La ventaja de la implementación del sistema de seguridad con arquitectura IoT es que permite la conexión de los dispositivos de seguridad, como cámaras, sensores y cerraduras, a través de Internet. Esto proporciona acceso remoto a la información y control del sistema de seguridad desde cualquier ubicación con conexión a la red.

3.2. Desarrollo de la propuesta

La implementación de un sistema de monitoreo con tecnología IOT para las oficinas del Gad Municipal Tisaleo ayuda de cierta manera a la administración efectiva de la seguridad de las instalaciones, gestionando la información de las áreas que requieren mayor vigilancia en el establecimiento.

Tisaleo es un cantón ubicado en el sector Sur Occidental de la provincia de Tungurahua, a 15 Km al sur de la ciudad de Ambato con una altitud promedio de 3247 m.s.n.m. Se encuentra en la Sierra Central del país, rodeado por montañas y paisajes. Tisaleo es un área mayoritariamente rural y agrícola. La economía local está impulsada principalmente por la agricultura y la ganadería. El cantón Tisaleo se encuentra delimitado de la siguiente manera: Al Norte con el cantón Ambato, al Sur con el cantón Mocha, al Este con el cantón Ambato, Cevallos y Mocha y al Oeste: con una bifurcación entre los cantones Ambato y Mocha.

Actualmente su alcalde es el Ing. Milton Ramírez, elegido por votación popular, de acuerdo con los requisitos y regulaciones previstas en la ley de la materia electoral. Periodo 15/Mayo/2023 al 15/Mayo/2027.

Figura 9. Fotografías del Municipio [61]

3.2.1. Análisis de la situación actual

El Gobierno Autónomo Descentralizado del cantón Tisaleo tiene como finalidad planear, implementar y sostener las acciones del desarrollo del gobierno local. Además de dinamizar los proyectos construcción y servicios, asegurando que se realicen con alta calidad y en el tiempo adecuado para impulsar el desarrollo social y económico de la población. Esto se logrará mediante la participación activa y efectiva de diversos grupos sociales, manteniendo la transparencia y ética en la institución y aprovechando al máximo el talento humano altamente comprometido, capacitado y motivado.

Para lograr este objetivo, el GAD cuenta con los siguientes departamentos:

PLANTA BAJA

- Recaudación
- Tesorería
- Dirección financiera
- Contabilidad

PRIMER PISO:

- Archivo
- Dirección de Obras Públicas

- Planificación
- Avalúos y Catastros
- Jefatura de Agua Potable
- Vicealcaldía

SEGUNDO PISO:

- Alcaldía
- Secretaría General
- Talento Humano
- Asesoría Jurídica

Sistema de seguridad del GAD Municipal de Tisaleo

Respecto al sistema de seguridad de las oficinas del GAD del Municipio de Tisaleo, en la tabla se detallan los elementos con los que cuenta la institución actualmente (cámaras y DVR).

Tabla 1. Elementos de seguridad con los que cuenta actualmente el GAD Municipal de Tisaleo

Elemento	Tipo	Ubicación
Cámara 1	Hikvision Turbo 720P Bullet Camera 28Mm Ir 20M Metal Ip66	Planta Baja (Sala de espera)
Cámara 2	Hikvision Turbo 720P Bullet Camera 28Mm Ir 20M Metal Ip66	Planta Baja (junto al ascensor)
Cámara 3	Hikvision Turbo 720P Bullet Camera 28Mm Ir 20M Metal Ip66	Primer Piso Alto (Sala de espera)
Cámara 4	Hikvision Turbo 720P Bullet Camera 28Mm Ir 20M Metal Ip66	Primer Piso Alto (Junto al ascensor)
Cámara 5	Hikvision Turbo 720P Bullet Camera 28Mm Ir 20M Metal Ip66	Segundo Piso (Sala de espera)
Grabador de video digital (DVR)	HIKVISION 720/1080P	Segundo Piso (Alcaldía)

Elaborado por: La investigadora

Para el desarrollo de la presente investigación se va a considerar exclusivamente a las áreas de la planta baja y del segundo piso, que como menciona el alcalde en la entrevista realizada son las áreas más críticas y que requieren mayor seguridad debido a la información que se maneja en los departamentos.

Planta baja

Como se observa en la figura 10, en la planta baja se ubica una cámara de seguridad tipo bullet montada en la parte superior de la pared, sin embargo, debido a su ubicación solamente cubre el ingreso al GAD, lo que significa que no se tiene una vigilancia adecuada sobre otras áreas críticas, como la Tesorería y Dirección Financiera.

Esta falta de cobertura en el resto de las áreas representa un riesgo potencial para la seguridad y protección de los empleados, así como para los activos y la información confidencial que se encuentran en las oficinas. La falta de cobertura representa un riesgo significativo para la seguridad de los activos financieros y la información confidencial que se maneja en este departamento. Al no contar con una supervisión visual constante, se expone a la posibilidad de robos internos o externos, fraudes o cualquier otra actividad ilícita que pueda poner en peligro la estabilidad financiera y la reputación de la empresa.

Figura 10. Cámara de videovigilancia instalada en la planta baja del edificio del GAD

Elaborado por: La investigadora

Segundo Piso

De igual manera, como se muestra en la figura 11, la ausencia de un control de acceso digital significa que no se cuenta con una forma eficiente y segura de limitar el acceso a información financiera confidencial y a los sistemas que manejan los activos económicos de la compañía. Esto puede conducir a situaciones de riesgo como acceso no autorizado a datos financieros sensibles, robo de información confidencial, manipulación de registros contables o incluso fraude interno.

Estos incidentes pueden ocasionar graves consecuencias, desde la pérdida de datos hasta interrupciones en las operaciones financieras y daño a la reputación de la empresa. De acuerdo a lo expuesto se señala la necesidad de implementar un control de acceso digital adecuado para proteger la información financiera y garantizar la integridad de las operaciones. Este mecanismo permitirá restringir el acceso solo a aquellos empleados y usuarios autorizados, lo que reducirá considerablemente los riesgos de vulnerabilidades internas y ataques externos.

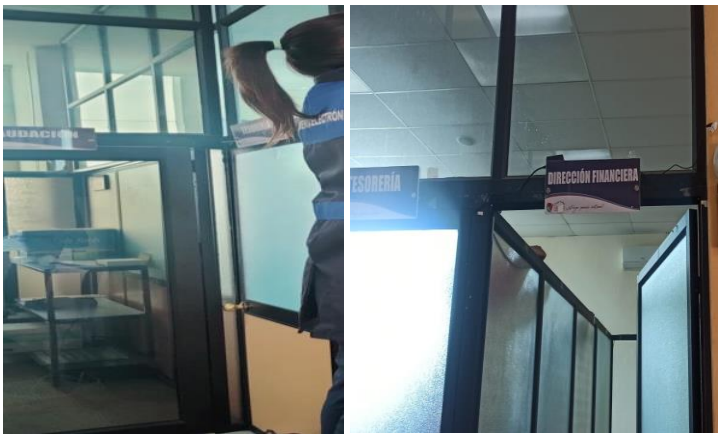


Figura 11. Acceso a Tesorería

Elaborado por: La investigadora

En el segundo piso de la institución se encuentra ubicada una cámara tipo bullet como se aprecia en la figura 12, que si bien es cierto cubre la mayor parte del área administrativa, no alcanza a visualizar el ingreso a la misma, lo cual representa un problema por cuanto no se puede alertar de la llegada de personas que pueden representar una amenaza para la institución.

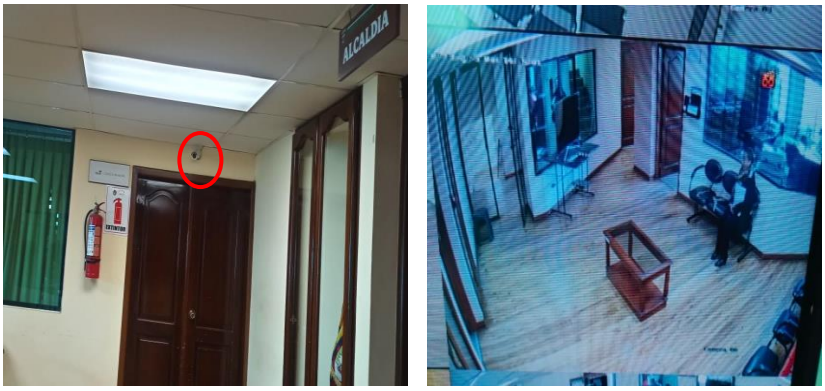


Figura 12. Cámara de videovigilancia instalada en la planta baja del edificio del GAD

Elaborado por: La investigadora

De igual manera este piso no cuenta con un control de acceso adecuado a la oficina de la Alcaldía, lo cual representa un problema en cuanto a seguridad debido a la importancia de documento e información que se maneja en dicho lugar.

Sistema de Cableado

Así también, como se evidencia en la Figura 13, el GAD presenta un sistema de cableado deficiente, desorganizado, lo cual da una mala impresión y afecta negativamente la estética del espacio, especialmente en entornos como oficinas. Además de ello, los cables desorganizados que se encuentran en el suelo o atraviesan pasillos pueden causar accidentes y tropiezos, lo que representa un peligro para las personas y un riesgo de daños a los cables. De acuerdo a lo establecido se verifica la necesidad de utilizar canaletas y abrazaderas para organizar y fijar los cables de manera ordenada.

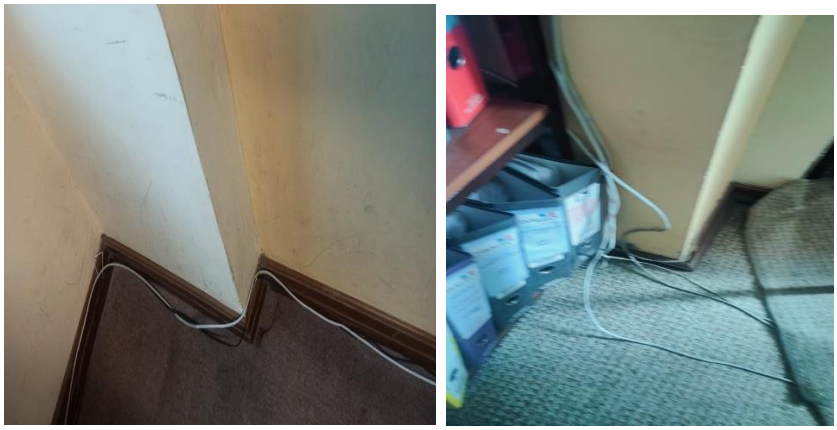


Figura 13. Sistema de Cableado

Elaborado por: La investigadora

Entrevista al alcalde del GAD de Tisaleo

De igual manera para conocer la situación actual en cuanto a seguridad del GAD Municipal del cantón Tisaleo se realizó una entrevista dirigida al alcalde la municipalidad el Ing. Milton Ramírez, para obtener la mayor cantidad de información acerca del proceso de vigilancia de la entidad.

Tabla 2. Entrevista al alcalde del GAD de Tisaleo

Tema de investigación:	**Sistema de seguridad para las oficinas del GAD municipal del cantón Tisaleo con arquitectura IOT**
Datos del investigador	Jazmín Carrera
Lugar:	GAD Tisaleo
Fecha:	30 de junio del 2023
Preguntas	**Resultado**
1. ¿Conoce usted si en las instalaciones del GAD Municipal de Tisaleo ha sido víctima de robo?	En el tiempo de mi administración no se ha tenido ninguna novedad de este tipo, pero en administraciones anteriores si se ha tenido el robo de objetos personales de los trabajadores de la municipalidad.
2. ¿El GAD Municipal de Tisaleo cuenta con algún sistema de seguridad?	El GAD municipal cuenta con cámaras de video vigilancia, pero las mismas están ubicadas en puntos no visibles, en puntos en donde las mismas no son estratégicas, por lo tanto, dificulta la oportuna seguridad.
3. ¿Cómo califica el sistema de seguridad del GAD Municipal de Tisaleo?	Debido a la falta de más dispositivos de seguridad y la deficiencia del sistema actual yo lo califico como malo.
4. ¿Qué áreas necesitan mayor control de seguridad dentro de las instalaciones del GAD Municipal de Tisaleo?	Las áreas en donde se debe tener mayor control de seguridad son los departamentos de Administración General y Tesorería Municipal.

5.	¿Tienen conocimiento acerca de los sistemas de monitoreo y videovigilancia?	Si tengo conocimiento en dicho tema por lo que dentro de la municipalidad si hace falta un sistema más sofisticado.
6.	¿Conoce usted que por medio de internet se puede realizar la conexión de varios dispositivos para la vigilancia de un lugar determinado?	No tengo conocimiento del tema, pero sería algo innovador.
7.	¿Qué elementos de seguridad considera necesario implementar en el GAD de Tisaleo para llevar un adecuado monitoreo de la seguridad? (cámaras, control de acceso, alarmas)	• Cámaras • Sensores de movimiento • Sirena • Sensores de huella
8.	¿De qué manera considera que sería más efectivo recibir las alertas que brinde un sistema de monitoreo de seguridad?	Sería más efectivo recibir alertas mediante una aplicación móvil ya que se procedería de forma más rápida al aviso a las autoridades competentes.
9.	¿Cree usted que es necesario implementar un sistema de seguridad que permita alertar cualquier acto de inseguridad en las instalaciones del GAD?	Si debido a que el sistema actual no es eficiente, además de que al contar con un sistema de seguridad adecuado se tendría más control en los departamentos antes mencionados.

Conclusión:
De acuerdo a la información proporcionada por el entrevistado se evidencia que el GAD del catón Tisaleo presenta ciertas falencias en cuanto a la seguridad de sus oficinas, específicamente en las áreas en donde se debe tener mayor control de seguridad que son los departamentos de Administración General y Tesorería Municipal. Por tal motivo indica que la implementación de un sistema de seguridad basado en la arquitectura IOT sería de gran ayuda para superar dichas dificultades y mejorar la administración de la seguridad.

Elaborado por: La investigadora

3.2.2. Requerimientos del sistema

Una vez determinado el objetivo del sistema de monitoreo con tecnología Iot para las oficinas del Gad Municipal Tisaleo se procede a establecer los requerimientos técnicos tanto de software como de hardware.

Requerimientos del sistema

Es importante contar con una estación de trabajo, puede ser un computador de escritorio o portátil con acceso a internet o a la red del Gad Municipal de Tisaleo.

Para el desarrollo del sistema se requiere:

- Sistema operativo: mínimo Windows 10
- Visual studio 2019
- Arduino IDE 1.0 en adelante
- Android studio IDE solo como entorno de desarrollo de flutter.

Para instalar la aplicación se requiere:

- RAM: 4GB
- Procesador: Mínimo Core I3

Requerimientos de los usuarios

El sistema de seguridad debe admitir lo siguiente:

- Monitoreo desde la aplicación móvil o sistema de escritorio web
- Activación y desactivación de la detección de movimiento
- Notificación por detección de movimiento
- Almacenamiento de video-imagen de la detección de movimiento
- Fácil registro de los usuarios en el sistema
- Acceso al área restringida únicamente a la persona responsable del departamento.

3.2.3. Diseño del sistema

Dentro del diseño del sistema de vigilancia se realiza en primera instancia la selección de los componentes para posteriormente realizar el diseño electrónico.

3.2.3.1. Selección de componentes Hardware

A continuación, se realiza la selección de los componentes y dispositivos del sistema de acuerdo a los requerimientos establecidos.

Cámara IP

En el mercado es posible encontrar diferentes modelos y marcas de cámaras IP, los más utilizados son los que se detallan en la tabla 3:

Tabla 3. Cuadro comparativo de las Cámaras IP

				
MARCA	HIKVISON	HIKVISON	DLINK	DAHUA
Modelo	DS-2CD1123G0E-I	2CD2020F	DCS-932L	N43AB52
Tipo	Dome	Bullet	Cube	Bullet
Resolución	HD720P, 1Mpx	1920x1080P	640x480 p	2688x1520
Lente	2.8mm	4.0 mm	5.01 mm	2.8mm
Compresión	H.264, H.265 y M-JPEG	H.264/MJPEG	MJPEG	H.265 Plus
Distancia	20m	30m	5 m	50 m
Iluminación	0.1 Lux/F1.2	0,01Lux(F1.2)	1 Lux (F2.8)	Color: 0.005 lux at F1.6
Ángulo de visión	El ángulo máximo alcanzado por su bandeja es 355°. Ángulo vertical: 0 a 70°	85º (datos del fabricante)	Horizontal: 45.3° Vertical: 34.5° Diagonal: 54.9°	Horizontal: 103° Vertical: 55° Diagonal: 122°
Visión Nocturna	SI	SI	SI	SI
Alimentación	12 V DC	12 V DC / 580 mA	5V DC, 1.2ª	12 V DC
Consumo de energía	MAX. 5W	≤7W	2 W	<5.4 W
Estándar	-	TCP/IP	TCP/IP, UDP, ICMP, DHCP, NTP, DNS, entre otros	IPv4, IPv6, HTTP, HTTPS, TCP, UDP, entre otros.
Costo	$72,00	$136	$70	$199
Grado de protección IP	IP67	IP66	-	IP67
S/N Ratio	>62Db	> 50 dB	-	>56dB

Elaborado por: La investigadora a partir de [62] [63] [64]

En base a las características presentadas en la tabla anterior, se ha seleccionado la cámara DS-2CD1123G0E-I debido a cumple con los requerimientos de compresión y resolución para el sistema de monitoreo que se diseña para el Gad de Tisaleo, además de la facilidad de adquisición en el mercado.

Sensor biométrico de huellas

Para la elección del sensor de huellas dactilares se analizan las características de los elementos que se encuentran en el mercado, los mismos que se especifican en la Tabla 4:

Tabla 4. Cuadro comparativo de sensores biométricos

		
MARCA	AS608	DFRobot SEN0348
Tipo	Óptico	Capacitivo
Comunicación	Serial/ UART TTL	Serial/ UART TTL
Tiempo de verificación	<1ms	300-400ms
Resolución de la imagen	508 dpi	508 dpi
Voltaje de operación	3.6 a 6.0VDC	3.3 V
Consumo de funcionamiento	<120 mA	<60 mA
Temperatura	-20°C y 50°C	-20°C y 50°C.
Número de usuarios permitidos	162 huellas dactilares	80 huellas dactilares
Dimensiones	23.3x20.3x48.1 mm	8.0 mmx8.0mm
Precio	$18	$30

Elaborado por: La investigadora a partir de [65] [66]

Después de realizar el análisis comparativo de los sensores de huella dactilares se eligió el lector de huellas AS608 debido a que se puede integrar fácilmente con otros sistemas de seguridad, como control de acceso, sistemas de alarma o sistemas de tiempo y asistencia. Esto permite una mayor versatilidad y adaptabilidad al entorno de seguridad existente.

Tarjetas de desarrollo

La unidad de almacenamiento es de vital importancia para el desarrollo del proyecto, ya que es donde los datos y registros son almacenados. A continuación, se compara las características de los diferentes dispositivos de almacenamiento que se encuentran en el mercado:

Tabla 5. Cuadro comparativo de Unidad de almacenamiento

			
Elemento	Arduino Mega	Raspberry Pi 2	Beaglebone Black
Procesador	ATmega 328P	Quadcore ARM Cortex-A53	Texas Instruments Sitara AM335x ARM Cortex-A8 de 1 GHz
Velocidad de reloj	16 MHz	900 MHz	1 GHz
SRAM	8 KB	1GB	512 MB DDR3
GPU	-	250 MHz VideoCore IV	PowerVR SGX530
Conectividad de Red	Módulos o Shields externos	1X10/100 Ethernet Rj45	10/100 Ethernet RJ45
Puertos USB	54 DI/O, 12 AI, 2 AO	GPIO de 40 pines	69 GPIO, LCD, GPMC, MMC1, MMC2, 7 AIN, 4 temporizadores, 4 puertos serial, CAN0.
Alimentación	3.3 V a 5V	5V	5V
Entorno de desarrollo	Arduino IDE	Linux, IDEL, Eclipse, Embedded, Scratchbox, Java, Python	Python, Scartch, Linux, Eclipse, Android ADK
Costo	De $22 a $80	De $22 a $80	De $22 a $80

Elaborado por: La investigadora a partir de [67] [68] [69]

Se eligió el Arduino Mega para el desarrollo del sistema de monitoreo de seguridad debido a que consume menos energía en comparación con Raspberry Pi 2. Esto es especialmente importante en sistemas de seguridad que requieren un funcionamiento continuo y prolongado, ya que reduce los costos de energía y la necesidad de recargar o reemplazar frecuentemente las baterías. De igual manera Arduino Mega utiliza un lenguaje de programación basado en C/C++, que es ampliamente utilizado y fácil de aprender. Esto facilita la programación y personalización del sistema de seguridad de acuerdo con los requisitos específicos.

3.2.3.2. Selección de software

Para la codificación del sistema implementado se requirió de un software que sea compatible con los componentes a emplear y cuente con las librerías necesarias para

cumplir con los requerimientos del sistema, para lo cual analizó las características del Software Arduino IDE y el ARM mbed como se observa en la tabla 6.

Tabla 6. Selección de entorno de desarrollo

Características	Arduino IDE	ARM mbed
Licencia	Open Source	Open Source
Lenguaje de programación	C/C++	C++
Hardware especifico	Placa Arduino	-
Conectividad	WiFi, Bluetooth o Ethernet	WiFi, Bluetooth o Ethernet
Nivel de simplicidad	Alto	Profesional

Elaborado por: La investigadora, a partir de [70] [71]

La combinación de la facilidad de uso, la amplia compatibilidad de hardware y la capacidad de conectar sensores y actuadores hacen que Arduino sea una opción óptima para la implementación de un sistema de seguridad, especialmente para proyectos de prototipado rápido y aplicaciones de Internet of Things (IoT).

Lenguaje de programación

Tabla 7. Selección Lenguaje de programación

Características	Visual Studio C#	Python
Sistema operativo	Nativo de Window	Windows, macOS y Linux.
Sintaxis	Simple	Simple
Facilidad de manejo	Alto	Alto
Compatibilidad con los componentes	Alta	Medio

Elaborado por: La investigadora [72] [73]

Se selecciona Visual Studio C# para el sistema de seguridad, debido a que con ello se obtendrá un lenguaje orientado a objetos con un IDE completo y una buena integración con el sistema operativo Windows, además de su compatibilidad con las cámaras IP seleccionadas.

Framework

La elección del framework de desarrollo para un sistema de seguridad con arquitectura IoT es de vital importancia, ya que puede tener un impacto significativo en el rendimiento, la eficiencia, la seguridad y la facilidad de mantenimiento del sistema. De esta manera, en la tabla se muestra las características de los Framework y React Native.

Tabla 8. Elección del Framework

Características	Flutter	React Native
Lenguaje de programación	Dart	JavaScript y React
UI Nativa	Widgets	Componentes nativos de la plataforma y JavaScript
Plataformas admitidas	iOS y Android.	iOS y Android
Documentación	Alta	Alta
Esfuerzo de desarrollo	Bajo	Medio
Intuitivo	Alto	Medio

Elaborado por: La investigadora, a partir de [74]

Una vez analizada las características de los dos framework se ha elegido Flutter para la creación del sistema de seguridad con arquitectura IoT, debido a permite un desarrollo más fluido y consistente. De igual manera permite crear una interfaz de usuario nativa y atractiva, lo que es relevante para el sistema de seguridad con IoT que requiere una experiencia de usuario intuitiva y rápida.

3.2.3.3. Arquitectura del sistema

El sistema de seguridad para las oficinas del Gad Municipal de Tisaleo basado en arquitectura IOT está estructurado en cuatro capas en base a la arquitectura IOT: Capa de dispositivos, Capa de conectividad, Capa de servicios, Capa de aplicación.

En la capa dispositivos, a través del uso de diversos sensores articulados a la seguridad, se obtienen los datos asociados a las variables movimiento, imagen y lector de huellas, los cuales son enviados a una placa de captura de hardware libre que es el Arduino Mega 2. Desde la capa conectividad se realiza la comunicación entre los dispositivos

y la plataforma IoT. Aquí es donde se establecen las conexiones físicas o inalámbricas necesarias para transmitir los datos capturados por los dispositivos de seguridad.

En la capa de servicios, una vez obtenido los datos de las variables de interés es almacenado en una base de datos, el cual es útil para realizar procesos de consulta del histórico de los datos. En esta capa se proporcionan los servicios necesarios para el funcionamiento del sistema. Puede incluir servicios de procesamiento de datos, análisis de video, almacenamiento en la nube, autenticación y autorización de usuarios, entre otros. Finalmente, en la capa de visualización es posible presentar de manera gráfica al usuario final la las variables capturadas en el tiempo, así como los resultados asociados a la consulta del histórico de los datos capturados.

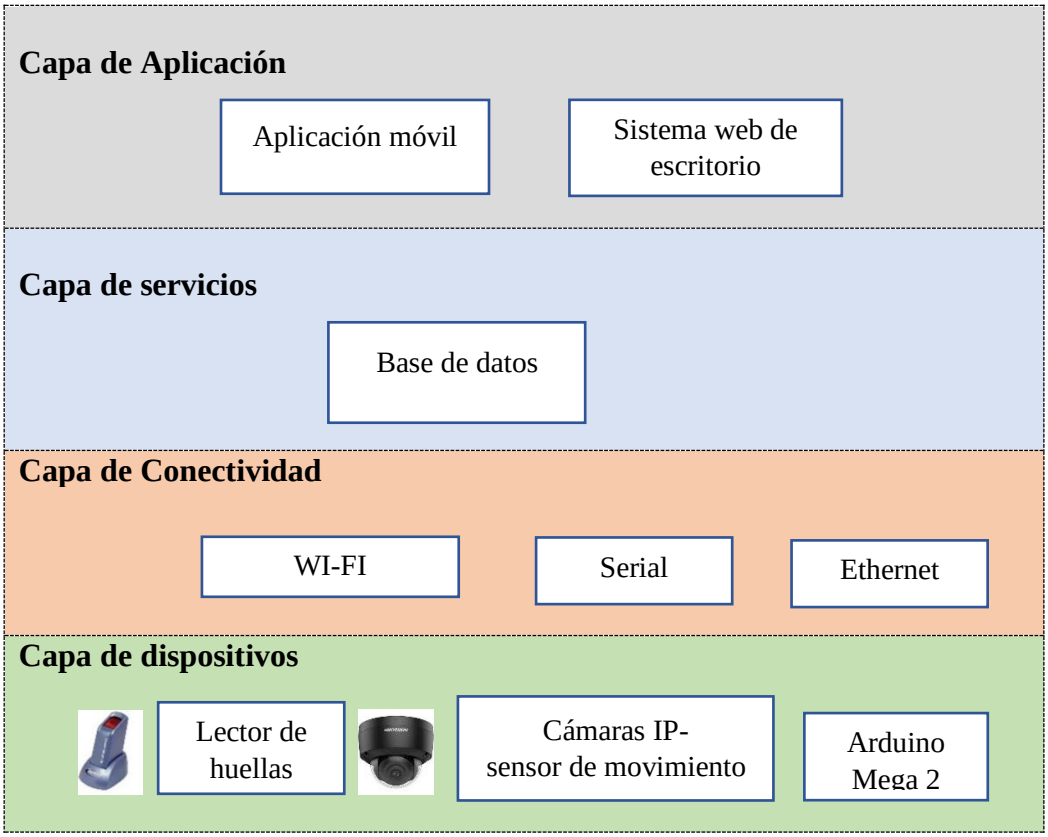


Figura 14. Esquema general del sistema

Elaborado por: La investigadora

De acuerdo a la arquitectura establecida, el sistema de seguridad desarrollado consta de dos partes principales, cada una relacionada con el control de acceso a los departamentos Financiero y Alcaldía, respectivamente, y la vigilancia mediante

cámaras de video. El diagrama para el sistema de seguridad para las oficinas del GAD de Tisaleo basado en Arquitectura IOT es el que se muestra en la Figura 15.

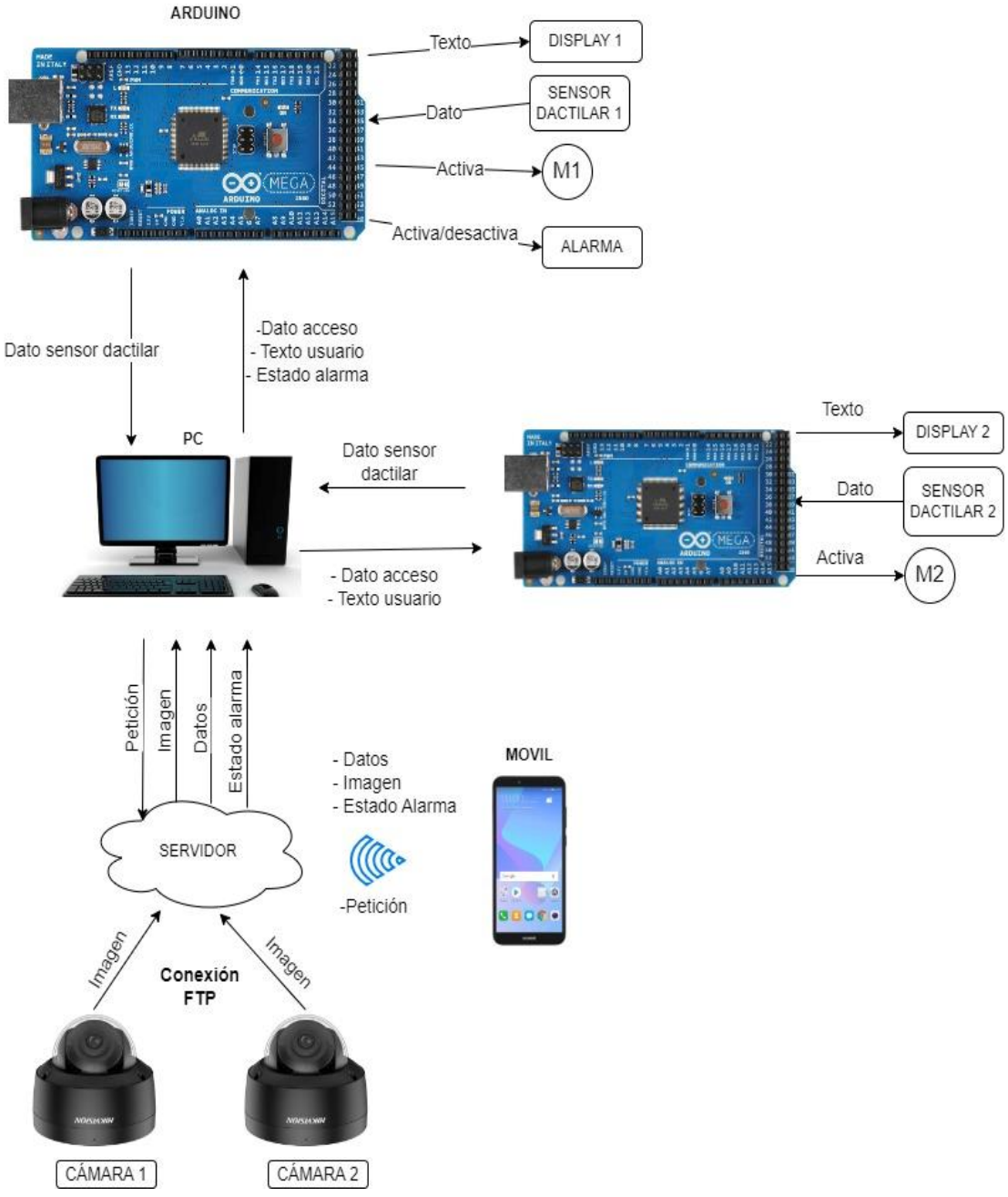


Figura 15. Esquema general del sistema

Elaborado por: La investigadora

Control de acceso

Se utilizan dos dispositivos Arduino Mega, uno para cada departamento. Cada Arduino recibe la señal del sensor dactilar que se utiliza para el control de acceso, cuando una persona coloca su dedo en el sensor dactilar, el Arduino verifica si la huella dactilar coincide con la información almacenada en su base de datos para el acceso autorizado. Si la huella dactilar es correcta, el Arduino activa un motor que permite la apertura del acceso al departamento correspondiente.

Control de cámaras de video vigilancia

Existe dos cámaras de video vigilancia que se encuentran monitoreando en tiempo real, al detectar la presencia de alguna persona u objeto toma 4 capturas de la imagen. Estas imágenes son posteriormente almacenadas en una carpeta específica del servidor a través del protocolo FTP. Además, con el objetivo de proporcionar notificaciones instantáneas, la cámara envía un correo electrónico a una dirección de correo electrónico designada para el sistema, informando sobre la detección de movimiento. Para hacer posible estas operaciones, las cámaras se encuentran conectadas a través de una red cableada, lo que no solo les permite estar integradas en la red local, sino que también les otorga acceso a Internet. De este modo, las cámaras pueden llevar a cabo el proceso de almacenamiento de imágenes y enviar correos electrónicos mediante la conexión a Internet.

3.2.3.4. Diagrama de flujo del sistema

En el diagrama de flujo que se muestra en la Figura 16 se observa el proceso de funcionamiento del sistema de seguridad diseñado para el GAD de Tisaleo. El algoritmo que se diseña refleja la integración y funcionalidad del sistema, que permite una respuesta rápida y efectiva ante situaciones de seguridad. Como se puede observar, dentro de las funcionalidades del sistema se encuentra el otorgar acceso a los departamentos mediante el uso del sensor de huellas dactilares, el cual activa el motor colocado en las puertas para permitir el ingreso únicamente a personas autorizadas. También muestra cómo las cámaras de video vigilancia capturan imágenes en tiempo

real, las almacenan en un servidor y envían la información al PC para su visualización, de igual manera con el sensor de movimiento que se ubican en las mismas permiten la activación de la alarma en caso de detectar eventos no autorizados.

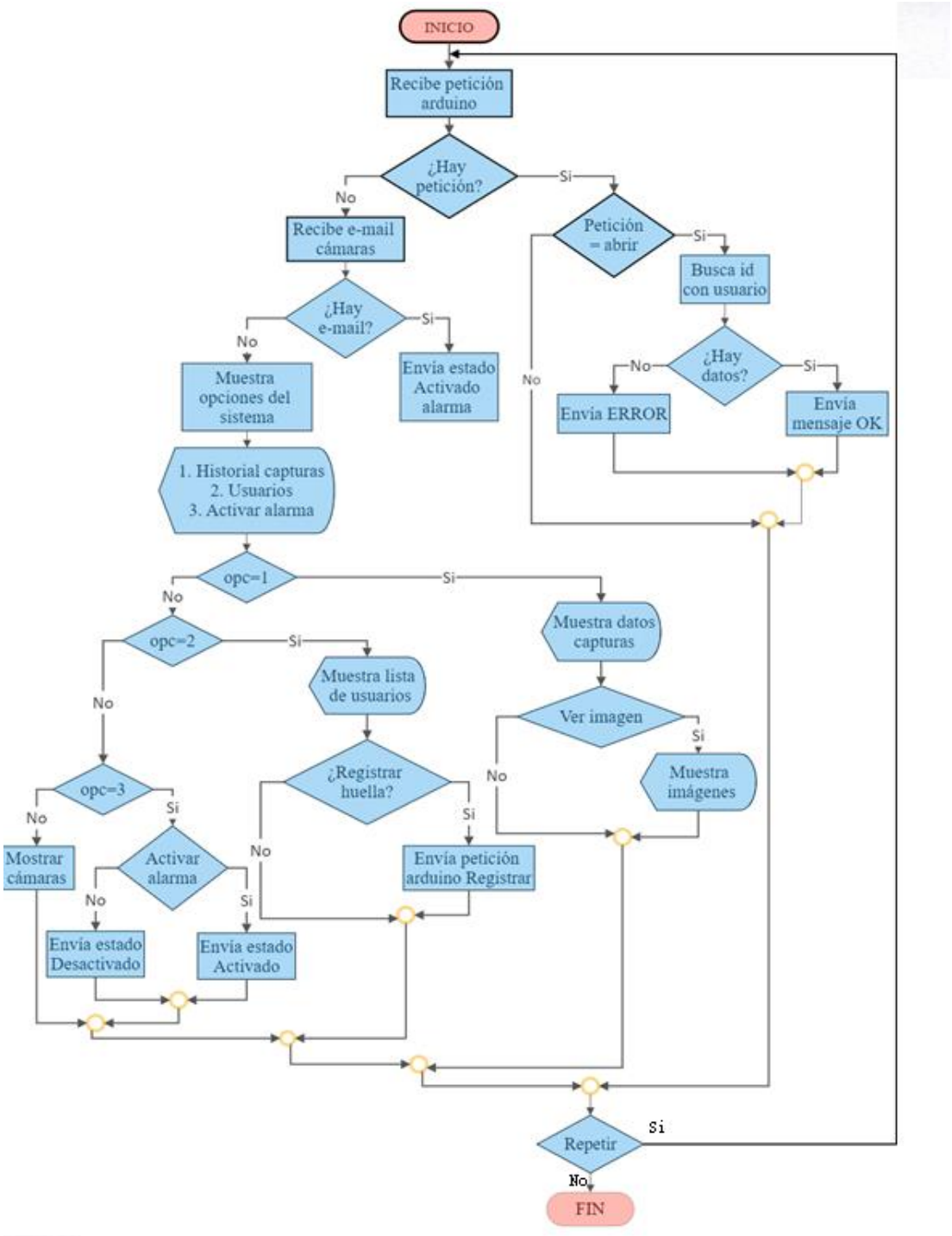


Figura 16. Diagrama de flujo del funcionamiento del sistema de seguridad

Elaborado por: La investigadora

3.2.3.5. Codificación del sistema

Lectura de email: Se registran los datos de configuración del servidor de correos para la entrada de información. Este proceso se realiza en un hilo separado o en otro proceso, asegurando que no afecte el funcionamiento del sistema principal. De esta manera, se garantiza una integración eficiente y sin interferencias con las funciones principales del sistema.

```
string server = "mail.seguridadtisaleo.com";
int port = 143;
bool useSsl = false;
string username = "sensores@seguridadtisaleo.com";
string password = "@@Seguridad.2023";
// Crear el cliente IMAP
client = new ImapClient();
// Conectar y autenticar en un hilo separado
Thread thread = new Thread(() =>
{
    client.Connect(server, port, useSsl);
    client.Authenticate(username, password);
});
thread.Start();
```

Figura 17. Codificación lectura de email

Elaborado por: La investigadora

Este proceso permite esperar peticiones del servidor de correo, detectando así nuevos correos entrantes, los mismos que ha sido enviados desde cada cámara al detectar movimiento.

```
private void timerVerificarMensajes_Tick(object sender, EventArgs e)
{
    // Verificar nuevos mensajes en un hilo separado
    Thread verificarMensajesThread = new Thread(() =>
    {
        if (client.IsConnected && client.IsAuthenticated)
        {
            var inbox = client.Inbox;

            try
            {
                inbox.Open(FolderAccess.ReadOnly);

                int unreadMessages = inbox.Search(SearchQuery.NotSeen).Count;

                if (unreadMessages > 0)
                {
                    MostrarNuevoMensaje();
                }
            }
            catch { }

        }
    });
    verificarMensajesThread.Start();
}
```

Figura 18. Esperar peticiones del servidor de correo

Elaborado por: La investigadora

Función MostrarNuevoMensaje: se activa automáticamente al recibir un nuevo mensaje, lo cual desencadena la activación de la alarma al actualizar su estado a 1. Además, en este proceso, se modifica el estado del mensaje a "leído", asegurando que la notificación se haya recibido y atendido correctamente.

```
private void MostrarNuevoMensaje()
{
    // Mostrar el MessageBox en el hilo de la interfaz gráfica
    Invoke((MethodInvoker)delegate
    {
        //MessageBox.Show("Nuevo mensaje");
        registrarAlarma("1");
    });

    // Marcar el primer mensaje no leído como leído
    if (client.IsConnected && client.IsAuthenticated)
    {
        var inbox = client.Inbox;
        inbox.Open(FolderAccess.ReadWrite);

        lock (imapLock)
        {
            var unreadMessage = inbox.Search(SearchQuery.NotSeen).FirstOrDefault();
            if (unreadMessage != null)
            {
                inbox.AddFlags(unreadMessage, MessageFlags.Seen, true);
            }
        }
    }
}
```

Figura 19. Función Mostrar Nuevo Mensaje

Elaborado por: La investigadora

Se programa el tiempo de ejecución de lectura de los mensajes, se los realiza cada 10 segundos.

```
// Iniciar el temporizador para verificar nuevos mensajes cada 10 segundos
timerVerificarMensajes.Interval = 10000;
timerVerificarMensajes.Start();
```

Figura 20. Tiempo de ejecución de lectura de los mensajes

Elaborado por: La investigadora

Función cargar Usuarios: Esta función permite traer los datos de los usuarios y ubicarlos dentro de la lista de usuarios que se visualiza en la interfaz.

```
private void cargarUsuarios()
{
    try
    {
        dgvUsuarios.Rows.Clear();
        // Crear la solicitud HTTP GET para obtener los datos actualizados
        string url = "https://seguridadtisaleo.com/datos/usuarios/lista.php";
        WebClient client = new WebClient();
        try
        {
            // Obtener la respuesta del servidor
            string response = client.DownloadString(url);
            // Parsear la respuesta como una lista de objetos
            var usuarios = JsonConvert.DeserializeObject<List<UsuarioBDD>>(response);
            // Agregar los usuarios a la lista
            usuariosList.AddRange(usuarios);
            // Agregar las filas al DataGridView
            foreach (var usuario in usuarios)
            {
                // Crear una nueva fila y asignar los valores de cada columna
                DataGridViewRow row = new DataGridViewRow();
                row.CreateCells(dgvUsuarios, usuario.Id, usuario.Cedula, usuario.Nombre, u

                // Agregar la fila al DataGridView
                dgvUsuarios.Rows.Add(row);
            }
        }
        catch (Exception ex)
        {
            MessageBox.Show("Error al obtener los datos: " + ex.Message);
        }
    }
```

Figura 21. Función cargar Usuarios

Elaborado por: La investigadora

Función detectar estado de alarma: Se configura el tiempo de repetición para buscar el estado de la alarma.

```
// Iniciar el temporizador para verificar nuevos mensajes cada 5 segundos
timerVerificarAlarma.Interval = 5000;
timerVerificarAlarma.Start();
```

Figura 22. Función detectar estado de alarma

Elaborado por: La investigadora

Función cargarAlarma: tiene la finalidad de obtener el estado actual de la alarma. Si el estado es igual a 1, entonces se activará la alarma; de lo contrario, la alarma permanecerá desactivada. Este proceso garantiza un control adecuado del estado de la alarma según su valor actual.

```
private void cargarAlarma()
{
    try
    {
        // dgvIngreso.Rows.Clear();
        // Crear la solicitud HTTP GET para obtener los datos actualizados
        string url = "https://seguridadtisaleo.com/datos/alarma/lista.php";
        WebClient client = new WebClient();

        try
        {
            // Obtener la respuesta del servidor
            string response = client.DownloadString(url);

            // Parsear la respuesta como una lista de objetos
            var ingresos = JsonConvert.DeserializeObject<List<AlarmaBDD>>(response);

            foreach (var ingreso in ingresos)
            {
                int valorAlarma = Convert.ToInt32(ingreso.Estado);
                if (valorAlarma != globalAlarma)
                {
                    if (valorAlarma == 1)
                    {
                        Invoke((MethodInvoker)delegate
                        {
                            button1.Text = "Desactivar";
                            button1.BackColor = Color.DarkRed;
                            pictureBox1.Image = Properties.Resources.warning;
                            label5.Text = "Activado";
                            alarmaCount = 0;
                            globalAlarma = 1;
                        });


                    }
                    else
                    {
                        Invoke((MethodInvoker)delegate
                        {
                            button1.Text = "Activar";
                            button1.BackColor = Color.DarkGreen;
                            pictureBox1.Image = Properties.Resources.police_light;
                            label5.Text = "Desactivado";
                            globalAlarma = 0;
                        });


                    }
                }

            }

        }
        catch (Exception ex)
        {
            MessageBox.Show("Error al obtener los datos: " + ex.Message);
        }
```

Figura 23. Función cargarAlarma

Elaborado por: La investigadora

Seleccionar usuario dentro de la lista obtenida: Al hacer clic en una fila de la lista de usuarios, se recupera la información correspondiente a ese usuario y se visualiza en los respectivos componentes. Esto permite llevar a cabo los procesos de actualización o registro de huellas de manera eficiente y precisa.

```
private void dgvUsuarios_SelectionChanged(object sender, EventArgs e)
{
    try
    {
        int rowIndex = dgvUsuarios.CurrentRow.Index;
        if (rowIndex >= 0)
        {
            txtId.Text = dgvUsuarios.Rows[rowIndex].Cells[0].Value.ToString();
            txtCedula.Text = dgvUsuarios.Rows[rowIndex].Cells[1].Value.ToString();
            txtNombre.Text = dgvUsuarios.Rows[rowIndex].Cells[2].Value.ToString();
            txtApellido.Text = dgvUsuarios.Rows[rowIndex].Cells[3].Value.ToString();
            comboBox2.SelectedIndex = Convert.ToInt32(dgvUsuarios.Rows[rowIndex].Cells[4].Value.ToString());
            comboBox1.SelectedIndex = Convert.ToInt32(dgvUsuarios.Rows[rowIndex].Cells[5].Value.ToString());
            proceso = 2;
            if (dgvUsuarios.Rows[rowIndex].Cells[6].Value.ToString() == "0")
            {
                lblRegistrandoHuella.Text = "No registrado";
                button6.Enabled = true;
            }
            else
            {
                lblRegistrandoHuella.Text = "Registrado";
                button6.Enabled = false;
            }
            if (dgvUsuarios.Rows[rowIndex].Cells[7].Value.ToString() == "0")
            {
                lblRegistrandoHuellaE.Text = "No registrado";
                button7.Enabled = true;
            }
            else
            {
                lblRegistrandoHuellaE.Text = "Registrado";
                button7.Enabled = false;
            }
```

Figura 24. Selección de usuario dentro de la lista obtenida

Elaborado por: La investigadora

Proceso para visualizar cámara en tiempo real desde pc y red local

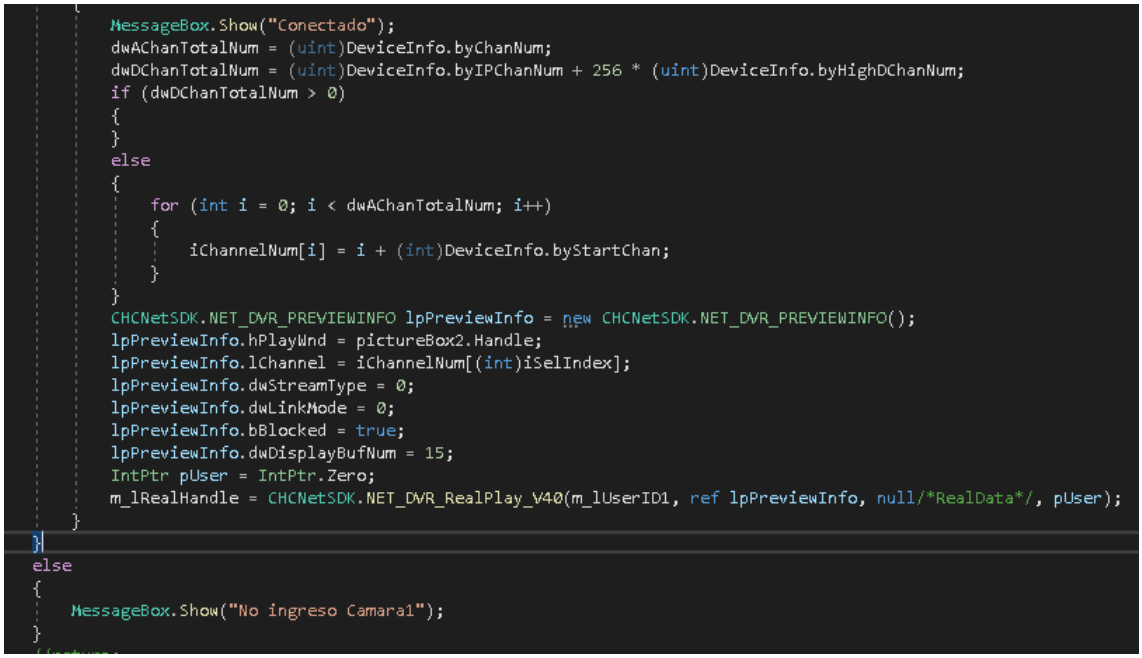
Para comenzar, es necesario inicializar las librerías de HKVision. Una vez detectada la presencia de una cámara, se procede a establecer la conexión con ella utilizando la dirección IP de la cámara, el puerto de conexión, así como el nombre de usuario y contraseña correspondientes.

```
private void activarCamara1()
{
    m_bInitSDK = CHCNetSDK.NET_DVR_Init();
    if (m_bInitSDK == false)
    {
        MessageBox.Show("NET_DVR_Init error!");
        return;
    }
    else
    {
        CHCNetSDK.NET_DVR_SetLogToFile(3, "C:\\SdkLog\\", true);
        for (int i = 0; i < 64; i++)
        {
            iIPDevID[i] = -1;
            iChannelNum[i] = -1;
        }
    }
    if (m_lUserID1 < 0)
    {
        string DVRIPAddress = ip1;
        Int16 DVRPortNumber = Int16.Parse(puertoConf.ToString());
        string DVRUserName = usuarioConf;
        string DVRPassword = contrasenaConf;
        m_lUserID1 = CHCNetSDK.NET_DVR_Login_V30(DVRIPAddress, DVRPortNumber, DVRUserName, DVRPassword, ref DeviceInfo);
        if (m_lUserID1 < 0)
        {
            iLastErr = CHCNetSDK.NET_DVR_GetLastError();
            string str = "NET_DVR_Login_V30 failed, error code= " + iLastErr;
            MessageBox.Show("No Conectado " + str);
            return;
        }
        else
        {
```

Figura 25. Proceso para visualizar cámara en tiempo real desde pc y red local

Elaborado por: La investigadora

Una vez que se haya realizado la conexión con éxito, se procede a obtener la imagen en tiempo real y ubicarla en los componentes visuales del sistema, si la conexión es incorrecta o no hay cámaras conectadas se emite un error de conexión.

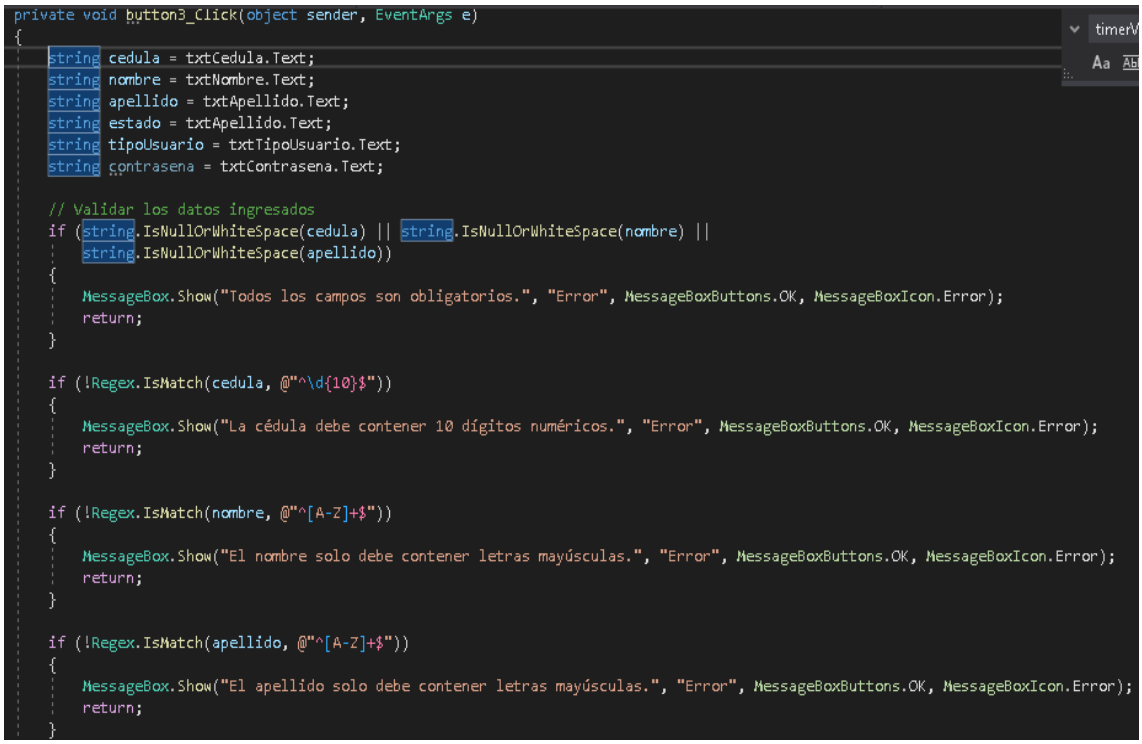


```
        MessageBox.Show("Conectado");
        dwAChanTotalNum = (uint)DeviceInfo.byChanNum;
        dwDChanTotalNum = (uint)DeviceInfo.byIPChanNum + 256 * (uint)DeviceInfo.byHighDChanNum;
        if (dwDChanTotalNum > 0)
        {
        }
        else
        {
            for (int i = 0; i < dwAChanTotalNum; i++)
            {
                iChannelNum[i] = i + (int)DeviceInfo.byStartChan;
            }
        }
        CHCNetSDK.NET_DVR_PREVIEWINFO lpPreviewInfo = new CHCNetSDK.NET_DVR_PREVIEWINFO();
        lpPreviewInfo.hPlayWnd = pictureBox2.Handle;
        lpPreviewInfo.lChannel = iChannelNum[(int)iSelIndex];
        lpPreviewInfo.dwStreamType = 0;
        lpPreviewInfo.dwLinkMode = 0;
        lpPreviewInfo.bBlocked = true;
        lpPreviewInfo.dwDisplayBufNum = 15;
        IntPtr pUser = IntPtr.Zero;
        m_lRealHandle = CHCNetSDK.NET_DVR_RealPlay_V40(m_lUserID1, ref lpPreviewInfo, null/*RealData*/, pUser);
    }
}
else
{
    MessageBox.Show("No ingreso Camara1");
}
```

Figura 26. Obtener la imagen en tiempo real

Elaborado por: La investigadora

Guardar usuario: Función que permite guardar nuevo usuario o actualizar sus datos, primero se obtiene los datos ingresados y se valida si los datos son correctos.



```
private void button3_Click(object sender, EventArgs e)
{
    string cedula = txtCedula.Text;
    string nombre = txtNombre.Text;
    string apellido = txtApellido.Text;
    string estado = txtApellido.Text;
    string tipoUsuario = txtTipoUsuario.Text;
    string contrasena = txtContrasena.Text;

    // Validar los datos ingresados
    if (string.IsNullOrWhiteSpace(cedula) || string.IsNullOrWhiteSpace(nombre) ||
        string.IsNullOrWhiteSpace(apellido))
    {
        MessageBox.Show("Todos los campos son obligatorios.", "Error", MessageBoxButtons.OK, MessageBoxIcon.Error);
        return;
    }

    if (!Regex.IsMatch(cedula, @"^\d{10}$"))
    {
        MessageBox.Show("La cédula debe contener 10 dígitos numéricos.", "Error", MessageBoxButtons.OK, MessageBoxIcon.Error);
        return;
    }

    if (!Regex.IsMatch(nombre, @"^[A-Z]+$"))
    {
        MessageBox.Show("El nombre solo debe contener letras mayúsculas.", "Error", MessageBoxButtons.OK, MessageBoxIcon.Error);
        return;
    }

    if (!Regex.IsMatch(apellido, @"^[A-Z]+$"))
    {
        MessageBox.Show("El apellido solo debe contener letras mayúsculas.", "Error", MessageBoxButtons.OK, MessageBoxIcon.Error);
        return;
    }
```

Figura 27. Guardar usuario

Elaborado por: La investigadora

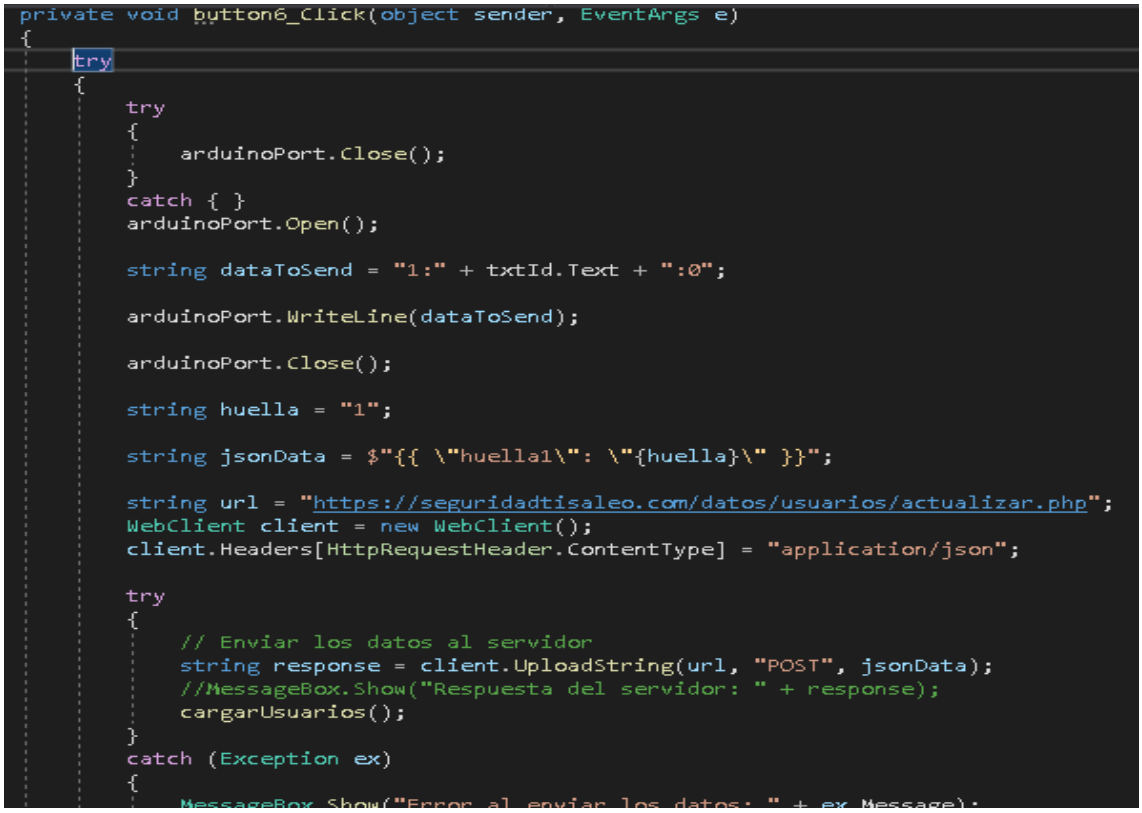
Si se va a crear nuevo usuario el estado del proceso se ubica en 1. Si el proceso es para ingresar un nuevo usuario, se ejecuta el archivo "crear.php". En caso de que se trate de una actualización de usuario existente, se llama al archivo "actualizar2.php".

```
if (proceso == 1)
{
    jsonData = $"{{ \"cedula\": \"{cedula}\", \"nombre\": \"{nombre}\", \"apellido\": \"{apellido}\"

    // Crear la solicitud HTTP POST
    string url = "https://seguridadtisaleo.com/datos/usuarios/crear.php";
    WebClient client = new WebClient();
    client.Headers[HttpRequestHeader.ContentType] = "application/json";

    try
    {
        // Enviar los datos al servidor
        string response = client.UploadString(url, "POST", jsonData);
        //MessageBox.Show("Respuesta del servidor: " + response);
        cargarUsuarios();
    }
    catch (Exception ex)
    {
        MessageBox.Show("Error al enviar los datos: " + ex.Message);
    }


}
else
{

    jsonData = $"{{ \"cedula\": \"{cedula}\", \"nombre\": \"{nombre}\", \"apellido\": \"{apellido}\"

    string url = "https://seguridadtisaleo.com/datos/usuarios/actualizar1.php";
    WebClient client = new WebClient();
    client.Headers[HttpRequestHeader.ContentType] = "application/json";

    try
```

Figura 28. Creación y actualización de usuario

Elaborado por: La investigadora

En este proceso se realizar la apertura del puerto correspondiente a la huella activada para enviar la petición de creación de huella en el Arduino correspondiente, conectando por puerto serial. Además de actualizar el estado del usuario indicando que la huella ha sido creada.



```
private void button6_Click(object sender, EventArgs e)
{
    try
    {
        try
        {
            arduinoPort.Close();
        }
        catch { }
        arduinoPort.Open();

        string dataToSend = "1:" + txtId.Text + ":0";

        arduinoPort.WriteLine(dataToSend);

        arduinoPort.Close();

        string huella = "1";

        string jsonData = $"{{ \"huella1\": \"{huella}\" }}";

        string url = "https://seguridadtisaleo.com/datos/usuarios/actualizar.php";
        WebClient client = new WebClient();
        client.Headers[HttpRequestHeader.ContentType] = "application/json";

        try
        {
            // Enviar los datos al servidor
            string response = client.UploadString(url, "POST", jsonData);
            //MessageBox.Show("Respuesta del servidor: " + response);
            cargarUsuarios();
        }
        catch (Exception ex)
        {
            MessageBox.Show("Error al enviar los datos: " + ex.Message);
```

Figura 29. Petición de creación de huella en el Arduino

Elaborado por: La investigadora

Proceso para recibir datos desde Arduino

En este proceso se realiza la conexión a Arduino esperando recibir un dato.

```
//puerto serial
Thread thread1 = new Thread(() =>
{
    // Realizar el proceso en segundo plano aquí
    while (true)
    {
        try
        {
            arduinoPort.DataReceived += SerialPortDataReceived; // Suscribirse al evento de recepción de datos
            try
            {
                arduinoPort.Open();
            }
            catch { }
        }
        catch (Exception ee)
        {
            MessageBox.Show("Error: " + ee);
        }

        // Esperar el intervalo de tiempo antes de repetir el proceso
        Thread.Sleep(4000); // 10 segundos
    }
});

// Iniciar el hilo en segundo plano
thread1.IsBackground = true;
thread1.Start();
```

Figura 30. Proceso para recibir datos desde Arduino

Elaborado por: La investigadora

Función SerialPortDataReceived2: Se encarga de recibir los datos desde el puerto serial. Luego, realiza una búsqueda en la lista de usuarios registrados con huella para comprobar si el usuario existe. Si el usuario se encuentra registrado correctamente, la función devolverá el nombre del usuario correspondiente. En caso contrario, mostrará un mensaje de error indicando que el usuario no fue encontrado.

```
public void SerialPortDataReceived2(object sender, SerialDataReceivedEventArgs e)
{
    try
    {
        arduinoPort2.Open();
    }
    catch { }
    SerialPort sp = (SerialPort)sender;
    string data = sp.ReadLine(); // Leer la línea de datos recibida
                                 // MessageBox.Show("Dato recibido: " + data);

    if (Convert.ToInt32(data) > 0)
    {

        UsuarioBDD usuarioEncontrado = BuscarUsuarioPorId(data);

        if (usuarioEncontrado != null)
        {
            string usu = usuarioEncontrado.Nombre + ":" + usuarioEncontrado.Apellido;
            //MessageBox.Show("Bienvenido " + usu);
            try
            {

                try
                {
                    arduinoPort2.Close();
                }
                catch { }
                arduinoPort2.Open();

                string dataToSend = "2:" + usu;

                arduinoPort2.WriteLine(dataToSend);
```

Figura 31. Función SerialPortDataReceived2

Elaborado por: La investigadora

Programación en Arduino

Para programar el sistema de seguridad basado en Arduino Mega, se toma en cuenta los diferentes componentes y sensores que se utilizan en el proyecto. En el contexto del sistema mencionado, se utilizaron displays, sensores dactilares y motores para el control de acceso, además de una interfaz USB para la comunicación con el servidor o PC central.

Para la programación en Arduino es importante incluir una serie de librerías para la adecuada comunicación. A continuación, se indica el funcionamiento de las librerías incluidas:

- **<Wire.h>:** Esta librería permite la comunicación I2C entre dispositivos en Arduino. I2C es un protocolo de comunicación serial que permite la transferencia de datos entre diferentes componentes conectados al bus I2C.
- **<Adafruit_Fingerprint.h>**: Esta librería es utilizada para trabajar con módulos de huellas dactilares. Permite la captura, almacenamiento y verificación de huellas dactilares.
- **<LiquidCrystal_I2C.h>:** Esta librería se utiliza para controlar pantallas LCD basadas en el controlador I2C PCF8574. Permite mostrar texto en una pantalla LCD de forma sencilla y eficiente.
- **<Servo.h>:** Esta librería permite controlar servomotores en Arduino. Los servomotores son actuadores que pueden girar a una posición específica según la señal que se les envíe.

```
#include <Wire.h>
#include <Adafruit_Fingerprint.h>
#include <LiquidCrystal_I2C.h>
#include <Servo.h>
```

Figura 32. Librerías de Arduino

Elaborado por: La investigadora

El código presenta la declaración de varias variables y constantes, así como la inicialización de diferentes módulos y dispositivos. Se declara un objeto "myservo" para controlar un servo motor, y se definen variables "pos", "state" y "flag" para su posterior uso. También se establecen las constantes para configurar un display LCD mediante I2C, definiendo el número de columnas y filas, y la dirección de comunicación. Se define el pin "rele" como 7 y se inicializa una comunicación serial "mySerial" utilizando los pines 10 y 11. Además, se crea un objeto "finger" para utilizar el módulo de huella dactilar Adafruit_Fingerprint a través de la comunicación serial. Por último, se inicializa un objeto "lcd" para controlar el display LCD con la dirección y configuraciones previamente definidas.

```
Servo myservo;
int pos = 0;
int state; int flag=0;

// Constantes para la configuración del display I2C
const int DISPLAY_COLUMNS = 16;  // Número de columnas del display
const int DISPLAY_ROWS = 2;     // Número de filas del display
const int DISPLAY_ADDRESS = 0x23;  // Dirección I2C del display

#define rele 7
SoftwareSerial mySerial(10, 11);
Adafruit_Fingerprint finger = Adafruit_Fingerprint(&mySerial);
LiquidCrystal_I2C lcd(DISPLAY_ADDRESS, DISPLAY_COLUMNS, DISPLAY_ROWS);
```

Figura 33. Declaración de varias variables y constantes

Elaborado por: La investigadora

Función setup(): En esta función se lleva a cabo varias configuraciones y acciones iniciales del programa. Primero, se inicializa y se enciende la retroiluminación del display LCD. Luego, se adjunta el servomotor al pin 9 y se establece la comunicación serial a una velocidad de 9600 baudios. Se escribe una posición inicial al servomotor y se espera hasta que haya una conexión serial disponible.

A continuación, se inicializa el módulo de huella dactilar y se configura el display LCD con el número de columnas y filas especificados. Se muestra un mensaje de bienvenida en el display durante 4 segundos, se borra el contenido del display y se muestra un mensaje de "Conectando..." durante otros 4 segundos. A continuación, se verifica la contraseña del módulo de huella dactilar y se muestra en el display si el sensor está listo o si hay un error. Finalmente, se espera otros 4 segundos y se borra el contenido del display.

```
void setup() {
  lcd.init();
  lcd.backlight();
  myservo.attach(9);
  Serial.begin(9600);
  myservo.write(60);
  while (!Serial) {}
  finger.begin(57600);
  lcd.begin(DISPLAY_COLUMNS, DISPLAY_ROWS);
  lcd.setCursor(0, 0);
  lcd.print("Bienvenido");
  lcd.setCursor(0, 1);
  lcd.print("Sis de Seguridad");
  delay(4000);
  lcd.clear();
  lcd.setCursor(0, 0);
  lcd.print("Conectando . . .");
  delay(4000);
  lcd.clear();
  if (finger.verifyPassword()) {
    lcd.setCursor(0, 0);
    lcd.print("Sensor 2. OK");
  } else {
    lcd.setCursor(0, 0);
    lcd.print("Sensor 2. ERROR");
    while (1) { delay(1); }
  }
  delay(4000);
  lcd.clear();
```

Figura 34. Función setup()

Elaborado por: La investigadora

Función "loop": Se espera recibir datos a través del puerto serial (Serial) y se almacenan en una variable "dataReceived". Luego, se divide el string recibido en tres partes separadas por el delimitador ":". Cada parte se almacena en una variable ("value1", "value2" y "value3") para su posterior uso en el programa.

```
void loop() {
  if (Serial.available() > 0) {
    String dataReceived  = Serial.readStringUntil('\n');

    // Dividir el string en las dos partes utilizando el delimitador ":"
    int firstSeparatorIndex = dataReceived.indexOf(":");
    int secondSeparatorIndex = dataReceived.indexOf(":", firstSeparatorIndex + 1);

    String value1 = dataReceived.substring(0, firstSeparatorIndex);
    String value2 = dataReceived.substring(firstSeparatorIndex + 1, secondSeparatorIndex);
    String value3 = dataReceived.substring(secondSeparatorIndex + 1);
```

Figura 35. Función "loop"

Elaborado por: La investigadora

El programa está interactuando con el sensor de huellas dactilares, tomando y convirtiendo imágenes de huellas y almacenándolas en el sensor. Además, muestra mensajes en la pantalla LCD indicando el estado de las operaciones.

```
if (value1 == "1") {
  lcd.clear();
  lcd.setCursor(0, 0);
  lcd.print("Acerque su dedo");
  delay(4000);
  int p = -1;

  while(p != FINGERPRINT_OK){

  p = finger.getImage();
  switch(p){
    case FINGERPRINT_OK:
      lcd.clear();
      lcd.setCursor(0, 0);
      lcd.print("Huella tomada");
      delay(4000);
      //Serial.println("Imagen tomada.");
      break;
    case FINGERPRINT_NOFINGER:
      lcd.clear();
      lcd.setCursor(0, 0);
      lcd.print(".");
      delay(4000);
      //Serial.println(".");
      break;
```

Figura 36. Interacción con el sensor de huellas dactilares

Elaborado por: La investigadora

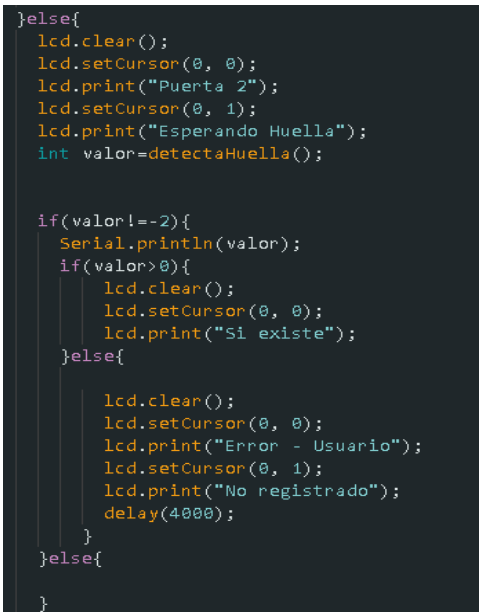
```
p = finger.storeModel(value2.toInt());
switch(p){
  case FINGERPRINT_OK:
      lcd.clear();
      lcd.setCursor(0, 0);
      lcd.print("Huella");
      lcd.setCursor(0, 1);
      lcd.print("almacenada");
      delay(4000);
    //Serial.println("Huella almacenada.");
    break;
  case FINGERPRINT_PACKETRECIEVEERR:
      lcd.clear();
      lcd.setCursor(0, 0);
      lcd.print("Error");
      lcd.setCursor(0, 1);
      lcd.print("Comunicacion");
      delay(4000);
    //Serial.println("Error de comunicación.");
    return p;
  case FINGERPRINT_BADLOCATION:
      lcd.clear();
      lcd.setCursor(0, 0);
      lcd.print("No se pudo");
      lcd.setCursor(0, 1);
      lcd.print("almacenar");
      delay(4000);
```

Figura 37. Interacción con el sensor de huellas dactilares

Elaborado por: La investigadora

Proceso que espera que reconozca una huella para activar el servo

En este fragmento de código, primero se limpia la pantalla del display LCD y se muestra un mensaje "Puerta 2" y "Esperando Huella". Luego, se llama a una función llamada "detectaHuella()" que está diseñada para detectar y verificar una huella dactilar en un sensor. El resultado de esta función se almacena en la variable "valor". Si el valor es diferente de -2, se verifica si es mayor a 0, lo que indicaría que se ha detectado una huella correspondiente a un usuario registrado y se muestra un mensaje "Si existe". Si el valor es menor o igual a 0, se muestra un mensaje de error indicando que el usuario no está registrado. Si el valor es igual a -2, no se realiza ninguna acción.



```
}else{
  lcd.clear();
  lcd.setCursor(0, 0);
  lcd.print("Puerta 2");
  lcd.setCursor(0, 1);
  lcd.print("Esperando Huella");
  int valor=detectaHuella();


  if(valor!=-2){
    Serial.println(valor);
    if(valor>0){
        lcd.clear();
        lcd.setCursor(0, 0);
        lcd.print("Si existe");
    }else{

        lcd.clear();
        lcd.setCursor(0, 0);
        lcd.print("Error - Usuario");
        lcd.setCursor(0, 1);
        lcd.print("No registrado");
        delay(4000);
      }
  }else{

  }
```

Figura 38. Proceso que espera que coloque un dedo y se reconozca una huella

Elaborado por: La investigadora

Codificación de la aplicación móvil con Flutter

Flutter es un framework de código abierto desarrollado por Google que se utiliza para crear aplicaciones móviles de alta calidad y rendimiento. Flutter utiliza el lenguaje de programación Dart, que también fue desarrollado por Google, y es conocido por su enfoque en la creación de interfaces de usuario atractivas y rápidas.

Para la codificación de la aplicación móvil es importante en primera instancia importar las librerías necesarias para el funcionamiento de la app, además de usar la página principal.dart.

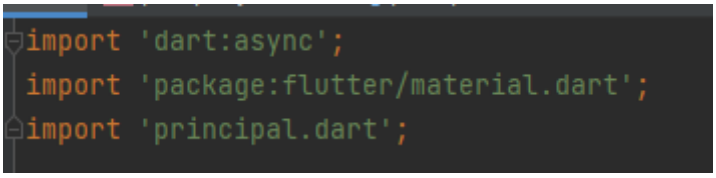


Figura 39. Página main.dart

Elaborado por: La investigadora

El código inicia la ejecución de la aplicación Flutter llamando a la función main(). Dentro de esta función, se ejecuta runApp(MyApp()), que inicia la aplicación y muestra la interfaz de usuario definida en la clase MyApp. Es el punto de entrada de la aplicación donde todo comienza a funcionar y se construye la interfaz gráfica.

Figura 40. Función main en Flutter

Elaborado por: La investigadora

La clase MyApp es un componente principal de la aplicación Flutter que hereda de StatelessWidget, lo que significa que no cambia su estado. En el método build(), se devuelve una instancia de MaterialApp con SplashScreen como la pantalla de inicio de la aplicación. MaterialApp es un widget que proporciona funcionalidades básicas de Material Design, y SplashScreen es otro widget que representa la primera pantalla que se muestra al iniciar la aplicación.

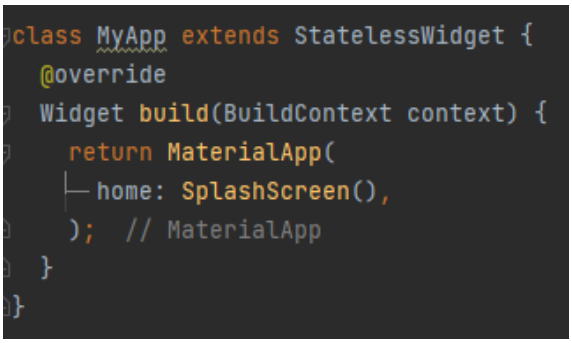


Figura 41. Clase MyApp en Flutter

Elaborado por: La investigadora

Se crea una instancia de esta clase, se llama al método createState(), que devuelve una instancia de la clase _SplashScreenState.

```
class SplashScreen extends StatefulWidget {
  @override
  _SplashScreenState createState() => _SplashScreenState();
}
```

Figura 42. Método createState()

Elaborado por: La investigadora

Función initState: Evento que se ejecuta automáticamente al iniciar la app, y espera 5 segundos para seguir a la siguiente ventana (Principal.dart)

```
@override
void initState() {
  super.initState();
  Timer(Duration(seconds: 5), () {
    // Navegar a la siguiente pantalla después de 5 segundos
    Navigator.pushReplacement(
      context,
      MaterialPageRoute(builder: (context) => PrincipalScreen()),
    );
  });  // Timer
}
```

Figura 43. Función initState

Elaborado por: La investigadora

Código que permite ubicar dos imágenes en una misma fila, para este caso se ubica la imagen de la UTA y la FISEI.

```
Row(
  mainAxisAlignment: MainAxisAlignment.center,
  children: [
    Expanded(
      child: Padding(
        padding: EdgeInsets.symmetric(horizontal: 8.0), // Margen izquierdo y derecho
        child: Image.asset(
          'assets/logoUTA.png',
          fit: BoxFit.contain,
        ),  // Image.asset
      ),  // Padding
    ),  // Expanded
    SizedBox(width: 10.0), // Espacio entre las imágenes
    Expanded(
      child: Padding(
        padding: EdgeInsets.symmetric(horizontal: 8.0), // Margen izquierdo y derecho
        child: Image.asset(
          'assets/logoFISEI.png',
          fit: BoxFit.contain,
        ),  // Image.asset
      ),  // Padding
    ),  // Expanded
  ],
),  // Row
```

Figura 44. Código para ubicar el sello de la universidad y facultad

Elaborado por: La investigadora

El código que se muestra en la figura 45 permite mostrar los datos principales y personales de la investigadora.

```
SizedBox(height: 16),
Text(
  'Universidad Técnica de Ambato',
  style: TextStyle(
    fontSize: 20,
    fontWeight: FontWeight.bold,
  ),  // TextStyle
  textAlign: TextAlign.center,
),  // Text
SizedBox(height: 8),
Text(
  'Facultad de Ingeniería en Sistemas Electrónica e Industrial',
  style: TextStyle(fontSize: 16),
  textAlign: TextAlign.center,
),  // Text
SizedBox(height: 8),
Text(
  'Ingeniería en Telecomunicaciones',
  style: TextStyle(fontSize: 16),
),  // Text
SizedBox(height: 8),
Text(
  'Jazmín Carrera',
  style: TextStyle(fontSize: 16),
),  // Text
SizedBox(height: 8),
```

Figura 45. Código que permite mostrar los datos principales y personales

Elaborado por: La investigadora

Principal.dart: Este código permite obtener la lista de capturas de imágenes creadas por las cámaras, y almacenarlas en una lista y mostrarlas al usuario.

```
Future<void> fetchFileList() async {
  final response =
  await http.get(Uri.parse('https://seguridadtisaleo.com/datos/lista/archivos.php'));
  if (response.statusCode == 200) {
    final jsonList = json.decode(response.body);
    List<String> files = List<String>.from(jsonList);

    setState(() {
      fileList = files;
    });
  } else {
    // Manejar el caso de error de la solicitud HTTP
  }
}
```

Figura 46. Código para obtener la lista de capturas de imágenes creadas por las cámaras

Elaborado por: La investigadora

Con la función checkAlarmStatus se permite realizar la consulta del estado de la alarma para mostrar dicho estado por interfaz.

```
Future<void> checkAlarmStatus() async {
  while (true) {
    final response =
    await http.get(Uri.parse('https://seguridadtisaleo.com/datos/alarma/lista.php'));
    if (response.statusCode == 200) {
      print("ok al ingresar");
      final jsonResponse = json.decode(response.body);
      print(jsonResponse);
      int alarmStatus = int.parse(jsonResponse[0]['estado']);

      setState(() {
        isAlarmActive = alarmStatus == 1;
      });
    } else {
      // Manejar el caso de error de la solicitud HTTP
      print("error al ingresar");
    }

    await Future.delayed(Duration(seconds: 5));
  }
}
```

Figura 47. Función checkAlarmStatus

Elaborado por: La investigadora

Además, dentro de codificación se emplea la función updateAlarmStatus, la cual permite enviar al servidor una actualización al estado de la alarma.

```
void updateAlarmStatus(int value) async {
  print("valor a enviar " + value.toString());
  final url =
  Uri.parse('https://seguridadtisaleo.com/datos/alarma/actualizar1.php?estado=${value.toString()}');
  final response = await http.get(url);

  if (response.statusCode == 200) {
    // Éxito en la solicitud HTTP
    print("Correcto: " + response.body);
  } else {
    // Manejar el caso de error de la solicitud HTTP
    print("Incorrecto");
  }
}
```

Figura 48. Código para la actualización al estado de la alarma

Elaborado por: La investigadora

En la figura 49 se muestra el código que permite mostrar la lista de capturas, con la respectiva fecha que se almacenó la imagen y la ubicación o número de cámara.

```
Row(
  mainAxisAlignment: MainAxisAlignment.spaceBetween,
  children: [
    Expanded(
      flex: 2,
      child: Padding(
        padding: EdgeInsets.symmetric(horizontal: 10),
        child: Text(
          'Fecha',
          textAlign: TextAlign.center,
          style: TextStyle(fontSize: 16, fontWeight: FontWeight.bold),
        ),  // Text
      ),  // Padding
    ),  // Expanded
    Expanded(
      flex: 2,
      child: Padding(
        padding: EdgeInsets.symmetric(horizontal: 10),
        child: Text(
          'Ubicación',
          textAlign: TextAlign.center,
          style: TextStyle(fontSize: 16, fontWeight: FontWeight.bold),
        ),  // Text
      ),  // Padding
    ),  // Expanded
  ],
),  // Row
```

Figura 49. Código para mostrar la lista de capturas

Elaborado por: La investigadora

En la figura 50 se muestra el código que permite abrir una ventana modal y observar la imagen seleccionada dentro de la aplicación de monitoreo de seguridad de Gad de Tisaleo.

```
Expanded(
  child: ListView.builder(
    itemCount: fileList.length,
    itemBuilder: (BuildContext context, int index) {
      String fileName = fileList[index];
      DateTime dateTime = extractDateTime(fileName);
      String formattedDate = DateFormat('yyyy/MM/dd HH:mm:ss').format(dateTime);

      String location = fileName.split('_')[0];
      String url = 'https://seguridadtisaleo.com/imagenes/$fileName';

      Color backgroundColor = index % 2 == 0 ? Colors.white : Colors.grey[200]!;

      return Container(
        color: backgroundColor,
        child: ListTile(
          title: Row(
            mainAxisAlignment: MainAxisAlignment.spaceBetween,
            children: [
              Expanded(
                flex: 2,
                child: Padding(
                  padding: EdgeInsets.symmetric(horizontal: 10),
                  child: Text(
                    formattedDate,
                    textAlign: TextAlign.center,
                    style: TextStyle(fontSize: 16),
```

Figura 50. Código para visualizar la imagen seleccionada dentro de la aplicación

Elaborado por: La investigadora

En la figura 51 se visualiza el código para crear un botón flotante el mismo que muestra y administra el estado de la alarma, si el botón está en gris el estado de la alarma es desactivada, si es de color rojo el estado de la alarma es activada.

```
floatingActionButton: FloatingActionButton(
  onPressed: () {
    int value = isAlarmActive ? 0 : 1;
    print(value);
    updateAlarmStatus(value);
  },
  backgroundColor: isAlarmActive ? Colors.red : Colors.grey,
  child: Icon(Icons.error, color: Colors.white),
),  // FloatingActionButton
```

Figura 51. Código para crear un botón que administra el estado de la alarma

Elaborado por: La investigadora

Administración de la base de datos en PHP dentro del servidor

PHP es un lenguaje de programación ampliamente utilizado para el desarrollo web, y una de sus aplicaciones más comunes es la interacción con bases de datos.

Dentro de la carpeta principal de PHP, se encuentra la carpeta imágenes, en la cual se almacenan todas las fotos creadas por las cámaras al detectar movimiento.

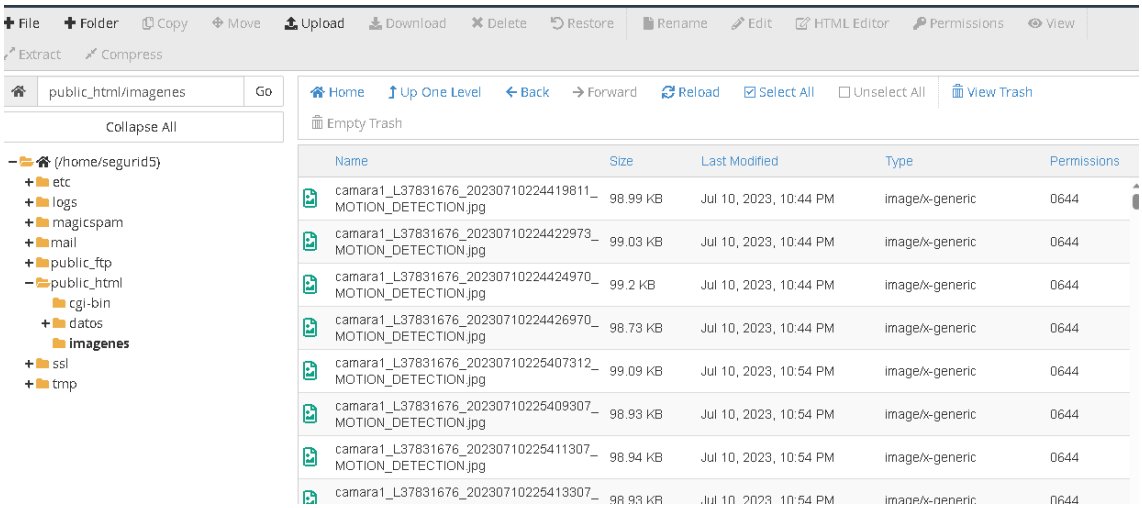


Figura 52. Almacenamiento de las imágenes creadas por las cámaras al detectar movimiento

Elaborado por: La investigadora

De igual manera se encuentra la carpeta **datos**, en donde se hallan los archivos php necesarios para realizar la conexión, consulta, creación y actualización a las bases de datos.

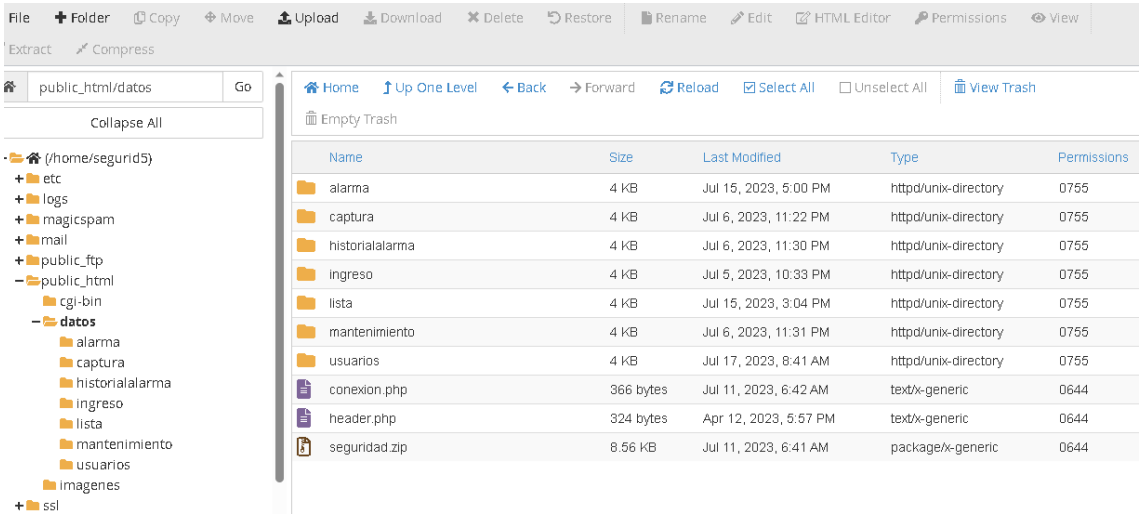


Figura 53. Carpeta datos en php

Elaborado por: La investigadora

En el Archivo conexión.php, contiene los datos de administración y conexión a la base de datos.

```php
<?php

$servername = "localhost";
$dbname = "segu_segur";
$username = "segu_sens";
$password = "seguridad";

$conn = mysqli_connect($servername,$username,$password,$dbname);
$mysqli = new mysqli($servername,$username,$password,$dbname);
$mysqli->set_charset("utf8");
if(!$mysqli){

  die("Error ".mysqli_connect_error());
}
?>
```

Figura 54. Archivo conexión.php

Elaborado por: La investigadora

Nota: los datos enviados en la imagen anterior no son los correctos, ya que por seguridad de la institución se ocultó la información real.

Codificación estado de la alarma

Como se muestra en la Figura 55 también se realiza la codificación que permita visualizar el estado de la alarma.

```php
<?php
include '../header.php';
include '../conexion.php';
$myArray=[];
$sql = "SELECT * FROM alarma";
if ($result = $mysqli->query($sql)){
  while($row = $result->fetch_assoc()) {
    $myArray[] = $row;
  }
  echo json_encode($myArray);
}
else{
  echo json_encode(array('mens'=>'No hay datos'));
}
$mysqli->close();
?>
```

Figura 55. Codificación que permite visualizar el estado de la alarma

Elaborado por: La investigadora

En la Figura 56 se visualiza el código para la actualización del estado de la alarma.

```php
<?php
include '../header.php';
include '../conexion.php';

$estado = $_GET['estado'];

$myArray=[];
$sql = "UPDATE alarma SET estado='$estado'";
try {
    if($mysqli->multi_query($sql) === TRUE){
          echo json_encode(array('ok' => true, 'mensaje' => "Proceso Correcto")) ;
      }else{
        echo json_encode(array('ok'=> false, 'errorMsg' => "Los datos son incorrectos")) ;
      }
  } catch (\Throwable $th) {
    echo json_encode(array('ok' => false, 'errorMsg' => $th->getMessage()));
  }
$mysqli->close();
?>
```

Figura 56. Código para actualizar el estado de la alarma

Elaborado por: La investigadora

De igual manera se puede listar la información de los usuarios registrados, para lo cual se emplea el código que se encuentra en la figura 57.

```php
<?php
include '../header.php';
include '../conexion.php';
$myArray=[];
$sql = "SELECT * FROM usuario WHERE nombre<>'Desconocido'";
if ($result = $mysqli->query($sql)){
  while($row = $result->fetch_assoc()) {
    $myArray[] = $row;
  }
  echo json_encode($myArray);
}
else{
  echo json_encode(array('mens'=>'No hay datos'));
}
$mysqli->close();
?>
```

Figura 57. Código para listar usuarios

Elaborado por: La investigadora

En la Figura 58 se visualiza el código para crear usuarios dentro de la base de datos, para lo cual se declara las variables correspondientes como cédula, nombre, apellido, estado y tipo de usuario.

```php
<?php
include '../header.php';
include '../conexion.php';
$param = json_decode(file_get_contents("php://input"));
$cedula=$param->cedula;
$nombre=$param->nombre;
$apellido=$param->apellido;
$estado=$param->estado;
$tipousuario=$param->tipousuario;


    $myArray=[];
    $sql = "INSERT INTO usuario(cedula,nombre,apellido,estado,tipousuario,huella) VALUES ('$cedula','$
    try {
        if($mysqli->multi_query($sql) === TRUE){
            echo json_encode(array('ok' => true, 'mensaje' => "Proceso Correcto")) ;
        }else{
            echo json_encode(array('ok'=> false, 'errorMsg' => "Los datos son incorrectos",'sql'=>$sql
            echo json_encode("Los datos son incorrectos") ;
        }
    } catch (\Throwable $th) {
        echo json_encode("Error") ;
    }
    $mysqli->close();
```

Figura 58. Código para crear usuarios

Elaborado por: La investigadora

En la Figura 59 se visualiza el código para actualizar usuario, para lo cual se emplea el comando UPDATE usuario SET, donde se ingresa los datos correspondientes para la ejecución exitosa de la acción.

```
<?php
include '../header.php';
include '../conexion.php';
$param = json_decode(file_get_contents("php://input"));
$id=$param->id;
$cedula=$param->cedula;
$nombre=$param->nombre;
$apellido=$param->apellido;
$estado=$param->estado;
$tipousuario=$param->tipousuario;

$myArray=[];
$sql = "UPDATE usuario SET cedula='$cedula', nombre='$nombre',apellido='$apellido',estado='$estad
try {
    if($mysqli->multi_query($sql) === TRUE){
          echo json_encode(array('ok' => true, 'mensaje' => "Proceso Correcto")) ;
      }else{
        echo json_encode(array('ok'=> false, 'errorMsg' => "Los datos son incorrectos")) ;
        echo json_encode("Los datos son incorrectos") ;
      }
  } catch (\Throwable $th) {
    echo json_encode("Error") ;
  }
$mysqli->close();
?>
```

Figura 59. Código para actualizar usuario

Elaborado por: La investigadora

3.2.4. Implementación del sistema de seguridad

En la figura 60 se muestra el diagrama de conexiones del sistema de seguridad diseñado, en donde se configura el pin 7 del Arduino como una salida digital, además, se inicializa una comunicación serial utilizando los pines 10 (RX) y 11 (TX) para permitir la comunicación con otros dispositivos. De igual manera se conecta físicamente el servo motor al pin 9 del Arduino. Además, se configura la comunicación serial a una velocidad de 9600 baudios, lo que establece la tasa de transmisión de datos para la comunicación serial.

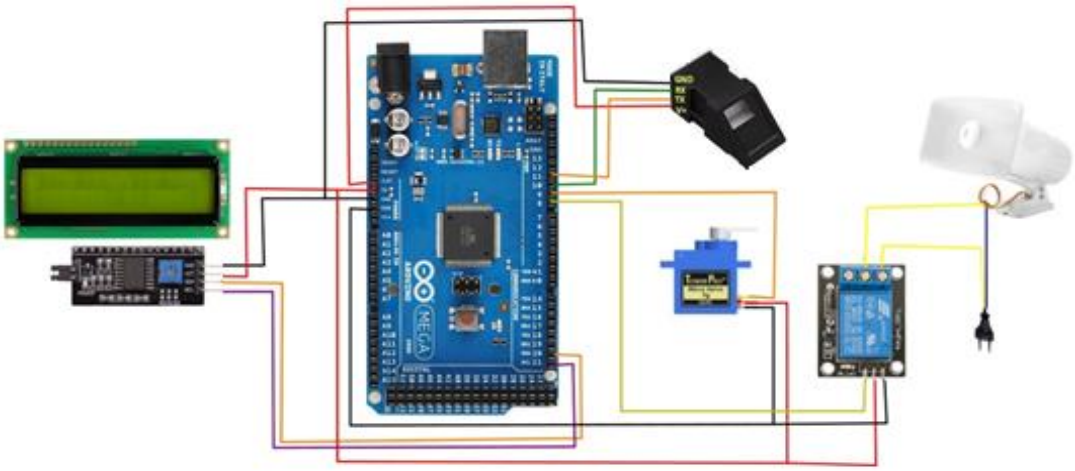


Figura 60. Diagrama de conexiones del sistema de seguridad

Elaborado por: La investigadora

Como se muestra en la figura 61, la conexión entre las cámaras de seguridad IP, el router y el centro de monitoreo se establece a través de una red local o incluso una conexión a internet, lo que permite la transmisión de datos de video y control para la supervisión y gestión de la seguridad. Las cámaras de seguridad IP se conectan físicamente al router a través de cables Ethernet o de manera inalámbrica mediante Wi-Fi. Si se utiliza cableado Ethernet, cada cámara se conecta a un puerto libre del router. Si es una conexión inalámbrica, se configura cada cámara para conectarse a la red Wi-Fi del router.

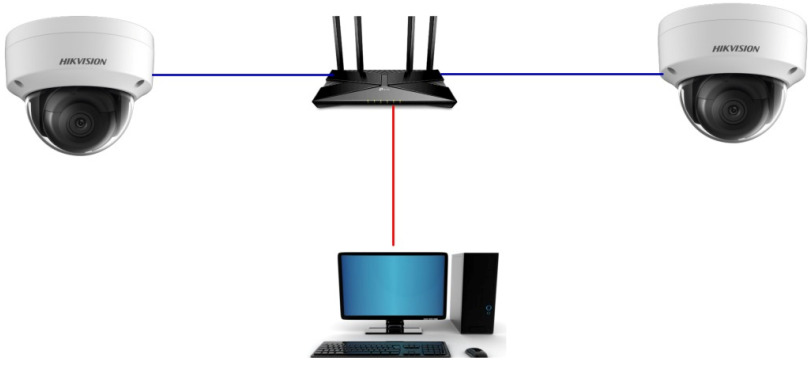


Figura 61. Conexión de las cámaras al Router

Elaborado por: La investigadora

El cableado interno y externo del sistema de seguridad

El cableado interno y externo del sistema de seguridad se refiere a la red de cables y conexiones que permiten la transmisión de información y energía entre los diferentes componentes del sistema de seguridad, como cámaras de vigilancia, sensores, paneles de control y dispositivos de alarma, como se observa en la Figura 62.

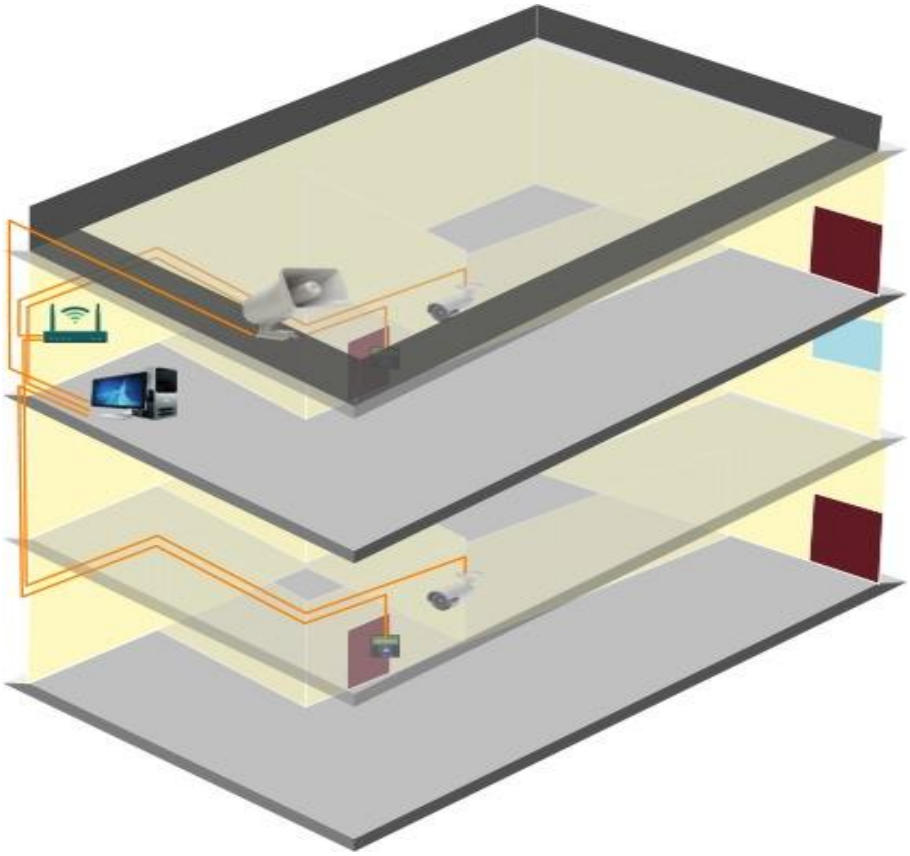


Figura 62. Cableado interno y externo del sistema de seguridad

Elaborado por: La investigadora

Referente al cableado del sistema de seguridad diseñado, las cámaras de vigilancia que incluyen los sensores de movimiento se conectan mediante cables a una fuente de energía, y como son cámaras IP (cámaras de red), se requirió un cable Ethernet para transmitir los datos de video desde las cámaras hasta el sistema de monitoreo.

Al igual que con las cámaras, los dispositivos de control de acceso necesitan alimentación. Se requirió un cableado para conectar los dispositivos a una fuente de energía, al igual que deben estar conectados al panel de control central. Esto implica el uso de cables para transmitir datos de autenticación y control entre los lectores y el panel.

Los dispositivos de alarma como sirenas, se colocaron en áreas externas, es decir en la fachada de un edificio, por lo cual fue necesario un cableado que conecte las sirenas a la red eléctrica y al sistema de seguridad en el interior.

La calidad de la instalación del cableado es fundamental para garantizar un funcionamiento confiable y seguro del sistema de seguridad en su conjunto.

Instalación de los dispositivos

Colocación de cámaras: Antes de comenzar la instalación, fue importante realizar una evaluación detallada del lugar donde se colocarán las cámaras. Identificando las áreas críticas que requieren vigilancia, como la entrada, salidas, áreas de almacenamiento y puntos estratégicos. Se colocó las cámaras en sus posiciones designadas, utilizando soportes de pared y asegurándose de que las cámaras estén firmemente sujetas y niveladas para una visión clara y estable.

Figura 63. Colocación de cámaras

Elaborado por: La investigadora

Armado del sistema de control de acceso: El proceso de armado del sistema de control de acceso con el sensor de huella y el display implica la interconexión de los componentes y la configuración adecuada para permitir el control de acceso a un lugar específico.

Figura 64. Armado del sistema de control de acceso

Elaborado por: La investigadora

Colocación del sistema de control de acceso: Lo primero es identificar las puertas o puntos de acceso que requieren control de acceso para de esa forma determinar cuáles serán los puntos de entrada principal que necesitan dispositivos de control de acceso. Luego de ello se montó en la pared asegurándose de que se encuentre a una altura adecuada para que el usuario pueda acceder fácilmente.

Figura 65. Colocación del sistema de control de acceso

Elaborado por: La investigadora

Instalación de la alarma: En primer lugar, se buscó un lugar estratégico que proporcione una cobertura efectiva, en este caso fue la terraza de la institución. Luego de ello se conectan todos los componentes de la alarma a la unidad de control utilizando los cables adecuados.

Figura 66. Instalación de la alarma

Elaborado por: La investigadora

Colocación de la placa Arduino en el case diseñado: Antes de comenzar la colocación, fue necesario asegurarse de que el diseño del case en 3D sea compatible con la placa Arduino y que tenga los orificios o espacios necesarios para los puertos, conectores y elementos adicionales de la placa (Ver anexo 4). Una vez fijada la placa se debe asegurar el cierre del case de acuerdo con el diseño para que la placa Arduino esté protegida de elementos externos como polvo, humedad u otros factores ambientales.

Figura 67. Colocación de la placa Arduino en el case diseñado

Elaborado por: La investigadora

Tendido de cables: Antes de comenzar el tendido de cables, se realizó una planificación y diseño detallado. Esto implicó determinar la cantidad de cables necesarios, el tipo de cableado a utilizar (cables de energía eléctrica, cables de datos o cables de comunicación), la ruta del cableado y la ubicación de los puntos de conexión.

Los cables se extienden desde su punto de origen hasta su destino final siguiendo la ruta planificada. Los cables se fijaron al suelo, paredes y techo utilizando canaletas.

Figura 68. Tendido de cables

Elaborado por: La investigadora

Colocación de abrazaderas: Las abrazaderas se utilizan para mantener el cableado y otros elementos de forma ordenada y segura, evitando que se desplacen o cuelguen libremente. Se ajustó las abrazaderas para que se adapten adecuadamente al diámetro de los cables instalados.

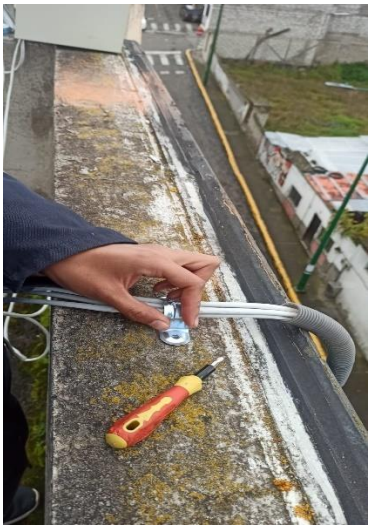


Figura 69. Colocación de abrazaderas

Elaborado por: La investigadora

Instalación de canaletas: El proceso de instalación de canaletas para los cables dentro del edificio del Gobierno Autónomo Descentralizado del cantón Tisaleo fue una tarea crucial para asegurar una distribución ordenada y segura de los cables eléctricos y de datos en las instalaciones. Una vez que las canaletas se encontraban fijadas, se procedió a instalar los cables en su interior de acuerdo con la planificación previa.

Figura 70. Instalación de canaletas

Elaborado por: La investigadora

En el Anexo 2 y 3 se puede apreciar el plano de instalación de los equipos en la planta baja y segundo piso.

3.2.5. Interfaz gráfica

El sistema de seguridad basado en la arquitectura IOT cuenta de dos formas de visualización y manejo de datos, un sistema de escritorio y la aplicación móvil. A continuación, se describe el sistema PC Servidor.

Sistema Pc Servidor

Este sistema cuenta con la opción de controlar el registro de usuario, huellas, envío de señal de alarma al detectar movimiento

Debido a las particularidades de las computadoras de la institución donde se instaló la aplicación, se ha decidido realizar cambios en la arquitectura de la aplicación, pasando de x64 a x86. Esto se debe a que dichas máquinas cuentan con un sistema operativo Windows 8 de 32 bits.

Para el ingreso al sistema se requiere ejecutar la aplicación SeguridadApp.exe que corresponde al ícono que se visualiza en la Figura 71.

Figura 71. Ícono de acceso al sistema

Elaborado por: La investigadora

Pantalla Principal

En la Figura 72, se puede apreciar la pantalla principal del sistema que presenta de manera intuitiva las opciones principales disponibles.

Figura 72. Pantalla Principal

Elaborado por: La investigadora

Como se observa en la Figura 73, dentro del menú de opciones, se encuentra dos pestañas: "Principal" y "Usuarios".

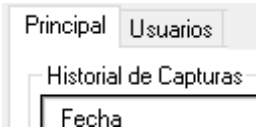


Figura 73. Menú de opciones

Elaborado por: La investigadora

Principal: Permite visualizar el historial de capturas realizadas por la cámara en el preciso momento en que se activa la alarma, como se visualiza en la figura 74. Para acceder a los datos de capturas de imágenes, simplemente haz clic en el botón "Actualizar", ubicado en la pestaña principal.

Al hacer clic en "Actualizar", se puede visualizar la lista de capturas, donde se encuentra la fecha en la que se tomó cada imagen, la ubicación o cámara responsable de la captura, y el nombre del archivo generado dentro del hosting.

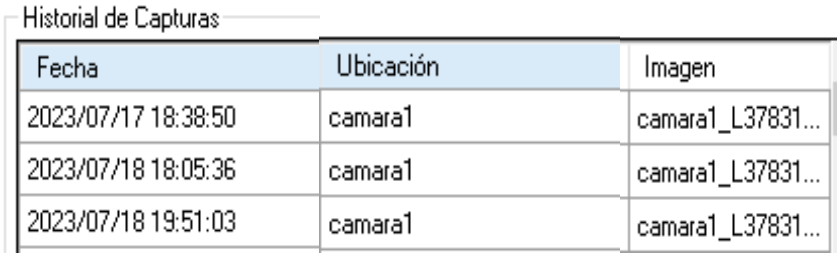


Figura 74. Historial de capturas

Elaborado por: La investigadora

Después de cargar la lista de capturas, se puede visualizar una de estas específica, haciendo doble clic en la imagen correspondiente de la lista. Esto abrirá una nueva ventana que te permitirá ver la imagen seleccionada en detalle.

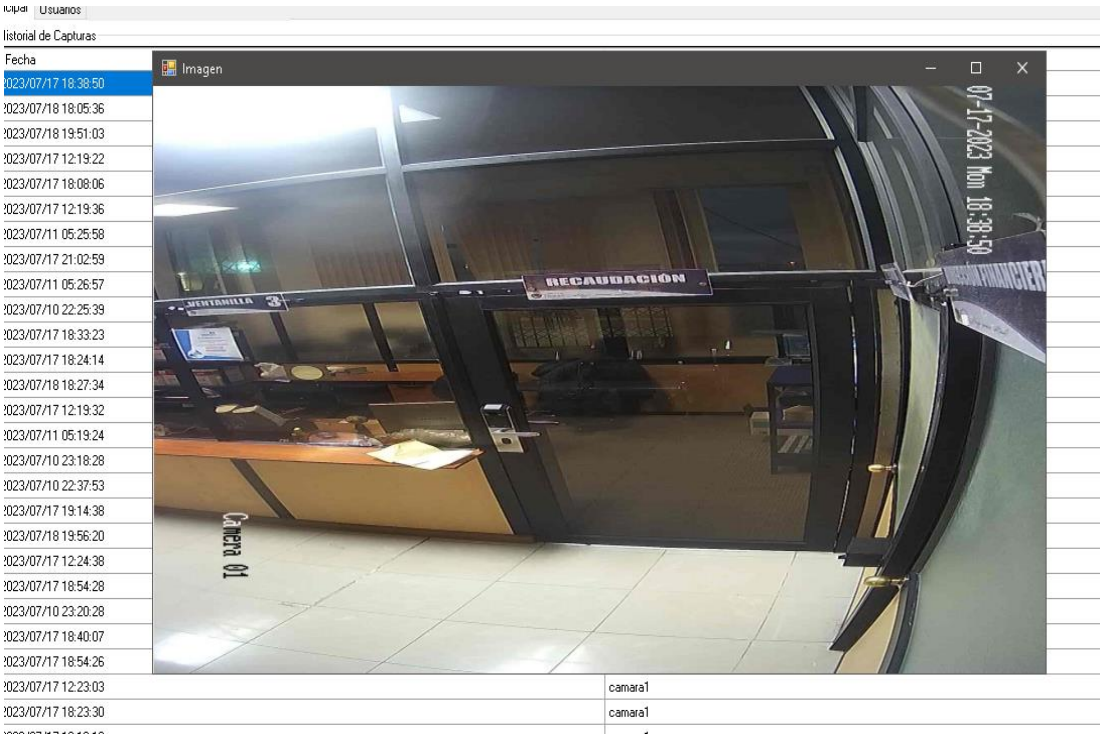


Figura 75. Imagen cuando la luz esta encendida

Elaborado por: La investigadora

Figura 76. Imagen al estar la luz apagada

Elaborado por: La investigadora

Usuarios: Permite administrar a los usuarios, así como su registro de huellas para activar la seguridad.

Configuración: En esta sección, se puede visualizar los datos personales del usuario, y también se encuentra dos botones que permiten registrar su huella tanto para la puerta 1, como para la puerta 2.

Figura 77. Sección de configuración

Elaborado por: La investigadora

De igual manera se puede visualizar la lista de usuarios registrados en el sistema de control de acceso.

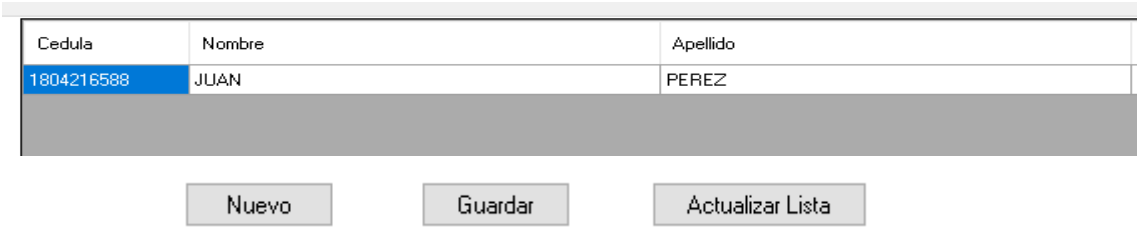


Figura 78. Lista de usuarios registrados

Elaborado por: La investigadora

Dentro de esta sección se tiene las opciones para crear nuevo usuario y guardar las modificaciones, además de actualizar la lista de usuarios.

Sección de Alarma

Como se observa en la figura 79, en la parte inferior derecha de la pantalla principal se encuentra la sección de alarma, que muestra el estado actual de la misma. La información es visual y muy intuitiva, es decir, si la imagen está en color rojo, significa que la alarma está activa, mientras que, si está en color negro, la alarma está apagada. Además, esta sección cuenta con un botón que permite activar la alarma en caso de emergencia.

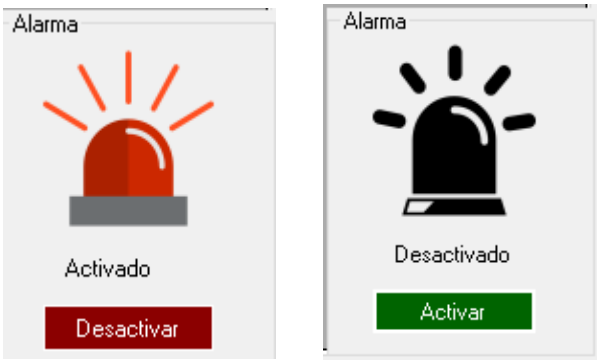


Figura 79. Estado de la alarma

Elaborado por: La investigadora

Sistema Pc Alcalde

Este sistema posee las mismas características de alarma que la PC servidor, pero sin las opciones de conexión con Arduino, ni la recepción de emails al detectar huellas. Las funcionalidades disponibles son las siguientes:

- **Sección de Alarma:** Permite activar o desactivar la alarma y muestra de manera intuitiva su estado actual, representado en rojo cuando está activa y en negro cuando está desactivada.
- **Visualizar Historial de Capturas:** Ofrece la posibilidad de ver el registro histórico de capturas realizadas por las cámaras al activarse la alarma.
- **Visualizar Cámaras:** Permite acceder a las imágenes en tiempo real de las cámaras instaladas en el sistema.

Estas funciones proporcionan una gestión completa de la alarma y el acceso a información importante para mantener la seguridad y el control del sistema.

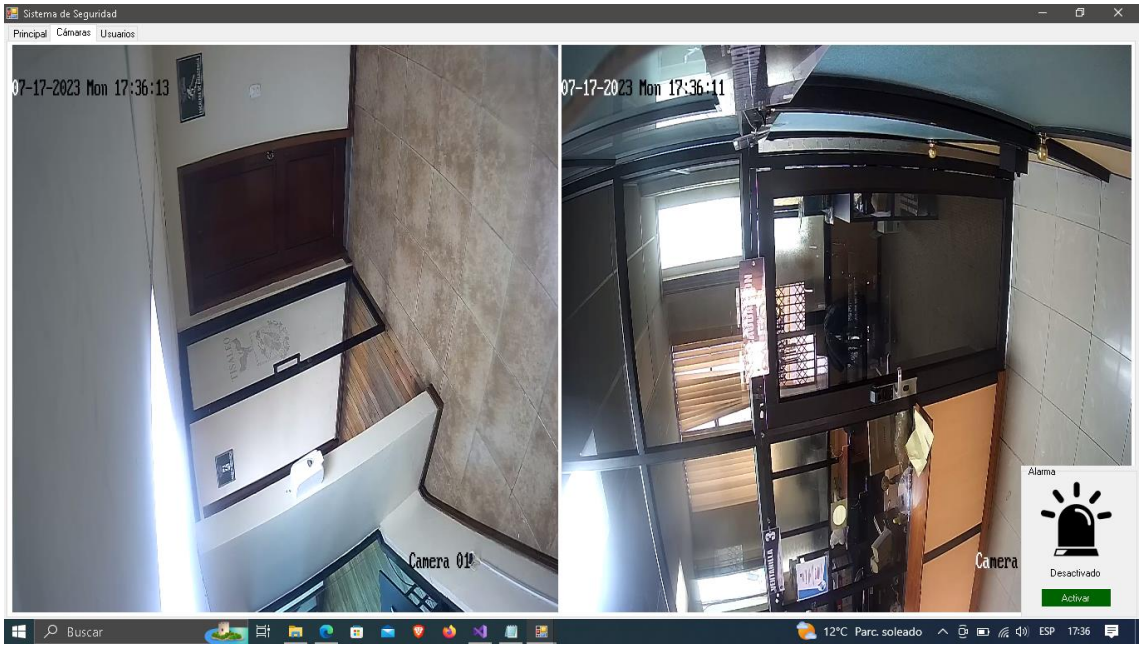


Figura 80. Visualización de las imágenes de las cámaras

Elaborado por: La investigadora

Aplicación móvil

La pantalla de inicio de la aplicación móvil para el sistema de seguridad está diseñada con el sello y logo de la Universidad Técnica de Ambato, y los respectivos datos personales de la investigadora.

Figura 81. Pantalla principal de la aplicación móvil

Elaborado por: La investigadora

En la ventana principal de la aplicación móvil de igual manera se visualiza la lista de capturas tomadas tanto por la cámara 1, como la cámara 2, las cuales toman 4 fotos cada que detecte el movimiento, y en ese mismo instante la cámara envía un email indicando que se detectó movimiento.

Figura 82. Lista de imágenes

Elaborado por: La investigadora

Al dar clic en las imágenes, muestra la captura tomada por la cámara con la respectiva hora y fecha, como se visualiza en la figura 83.

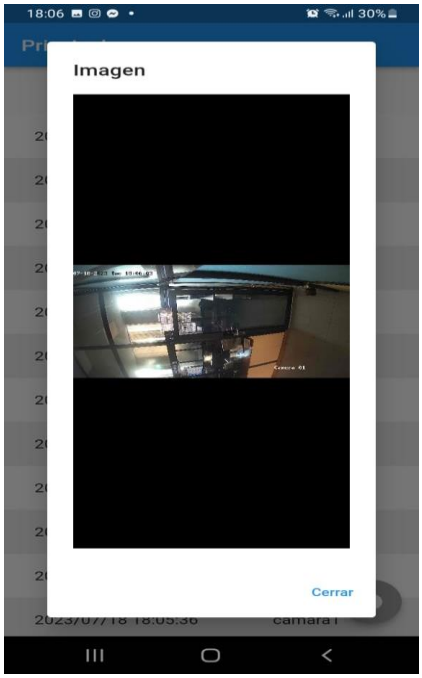


Figura 83. Visualización de imágenes

Elaborado por: La investigadora

En la esquina inferior derecha de la aplicación se visualizar un ícono de color rojo en el caso de que la alarma se active al detectar movimiento, la cual puede ser desactivada por el usuario dando clic en la misma. De igual manera al estar el icono de color gris representa que la alarma se encuentra en estado desactivado.

Figura 84. Alarma en estado activado

Elaborado por: La investigadora

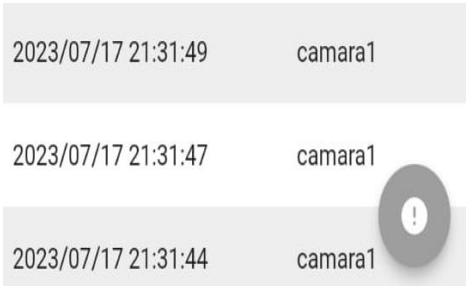


Figura 85. Alarma en estado desactivado

Elaborado por: La investigadora

3.2.6. Pruebas de funcionamiento

Las pruebas realizadas para verificar el funcionamiento del sistema instalado son las siguientes:

3.2.6.1. Pruebas de detección de movimiento de cámaras

Como se indicó anteriormente la alarma de detección de intrusos fue programada para su funcionamiento desde las 18:00 pm hasta las 6:00am. En la figura 86 se visualiza la presencia de una persona fuera de ese horario establecido, por lo cual la alarma se mantiene en estado desactivado.

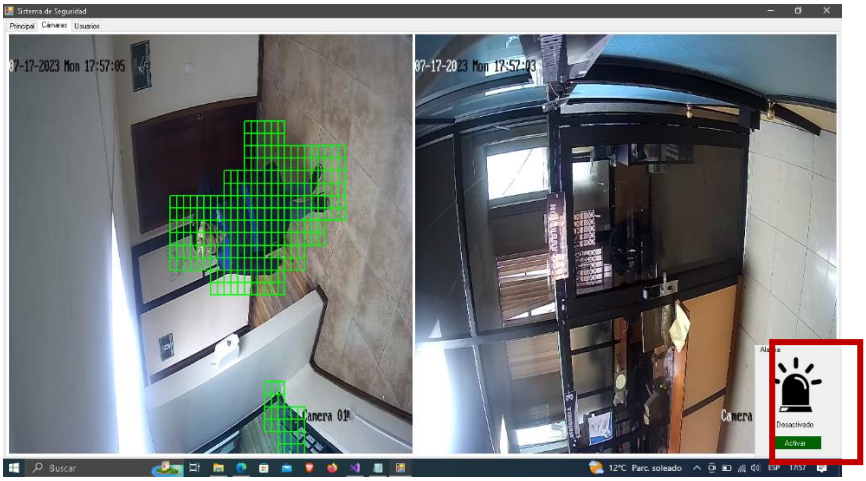


Figura 86. Pruebas de detección de movimiento de cámaras

Elaborado por: La investigadora

Pruebas de activación de alarma

Como se visualiza en la figura 87, la cámara detecta la presencia de una persona dentro del horario programado en el sistema, motivo por lo cual la cámara pasa al estado activado.

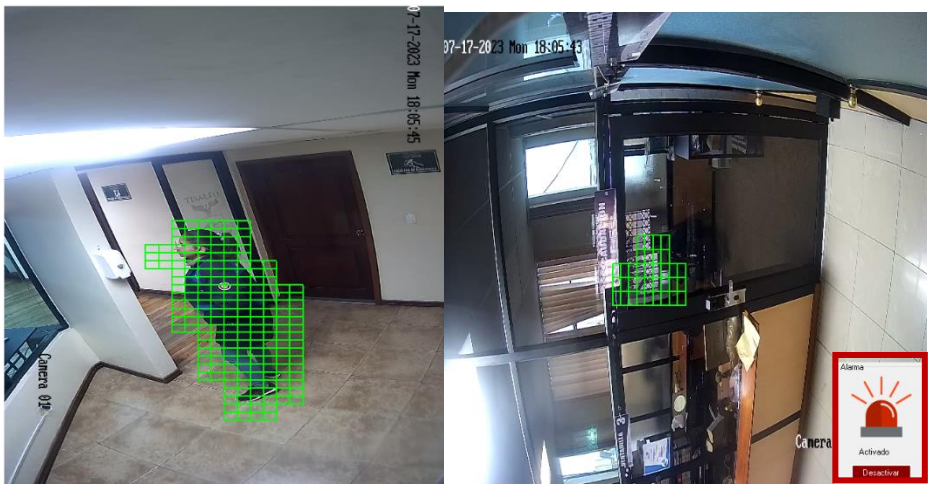


Figura 87. Pruebas de activación de alarma

Elaborado por: La investigadora

3.2.6.2. Pruebas de funcionamiento del control de acceso

Para verificar el adecuado funcionamiento del sistema de control de acceso se realizaron las siguientes pruebas**:**

Activación del sistema de control de acceso

Como se observa en la Figura 88, una vez que se conecta el sistema de control de acceso al Arduino y se inicializar, aparece el mensaje de confirmación de funcionamiento para posteriormente desplazar la leyenda “Esperando huella”, lo cual indica que se ha realizado una conexión exitosa.

Figura 88. Activación del sistema de control de acceso

Elaborado por: La investigadora

En la Figura 89, se visualiza que el usuario registrado coloca su huella digital en el sensor, por lo cual aparece el mensaje de existencia del usuario.

Figura 89. Colocación de la huella de usuario registrado

Elaborado por: La investigadora

Debido a que el usuario que solicita el ingreso si se encuentra registrado, aparece un mensaje de Bienvenida con el nombre respectivo, como se puede visualizar en la figura 90.

Figura 90. Mensaje de Bienvenida al usuario

Elaborado por: La investigadora

Una vez que se confirma la existencia del usuario en la base de datos del sistema, se activa el servomotor para abrir la puerta de acceso a la oficina correspondiente.

Figura 91. Activación de servomotor para abrir la puerta

Elaborado por: La investigadora

Caso contrario, si el usuario que coloca su huella dactilar no se encuentra registrado en la base de datos del sistema aparece el mensaje de usuario no registrado, como se puede visualizar en la Figura 92.

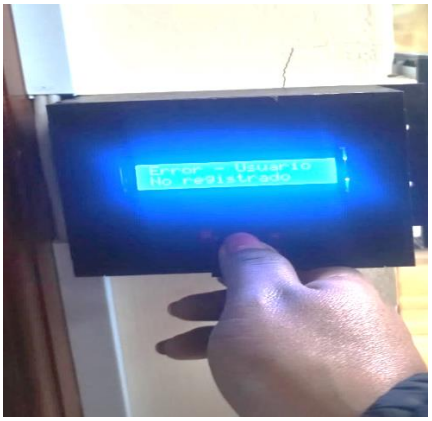


Figura 92. Mensaje de error

Elaborado por: La investigadora

Finalmente se debe considerar que un sistema de seguridad eficiente debe actuar rápidamente ante situaciones de riesgo. De esta manera, una vez implementado el sistema de seguridad en las oficinas de Gad Municipal de Tisaleo se determina que presenta un adecuado tiempo de respuesta, que es el tiempo que le lleva al sistema detectar una amenaza y responder a ella, ya que es de aproximadamente 5 segundos después de haber detectado el movimiento, debido a que es el tiempo que tiene en comprobar nuevos eventos.

3.2.7. Presupuesto

Precio de Hardware

Para el desarrollo del sistema de seguridad de GAD Municipal de Tisaleo se emplearon diferentes componentes eléctricos y electrónicos, los cuales se detallan en la tabla 9:

Tabla 9. Precio de Hardware del sistema

Detalle	Cantidad	Precio Unitario	Total
Cámaras IP HIKVISION	2	$55	$110,00
Arduino Mega	2	$22	$44,00
Sensor de huella	2	$25,75	$51,50
Servomotor chico	2	$4,50	$9,00
Cable UTP CAT5	200	$0,35	$70,00
Cable 2x18 gemelo	30	$0,35	$10,5
Adaptadores 12 V	2	$5,00	$10,00
Tomacorriente	3	$2,50	$7,50
Enchufe lateral	3	$1,15	$3,45
Cable USB impresora	2	$5,50	$11,00
Conectores RJ45	10	$0,15	$1,50
Canaleta	10	$1,90	$19,00

Impresión 3D case para dispositivos	4	-	$21,00
		SUBTOTAL	$368,45
		IVA 12%	$39,47
		TOTAL	$407,92

Elaborado por: La investigadora

Precio del software

Los programas empleados para el desarrollo del sistema son los que se describen en la tabla 10:

Tabla 10. Precio del software

Software	**Costo**
Visual studio 2019	$0,00
Flutter	$0,00
Hosting Express PHP	$47,97
SUBTOTAL	$47,97
IVA 12%	$5,76
TOTAL	**$55,73**

Elaborado por: La investigadora

Precio mano de obra

Para la determinación de la mano de obra se considera el sueldo de un Ingeniero en Telecomunicaciones que, de acuerdo al Ministerio de Trabajo, el salario anual de un Ingeniero Electrónico en Ecuador es de $14,840, dividido para los 12 meses sería un sueldo estimado de $1236,66 al mes y se puede incrementar de acuerdo al rango en que se desempeñe. El tiempo aproximado de ejecución de proyecto fue de 1 mes, por lo tanto, se tiene un costo de mano de obra de $1236,66

Con los valores antes calculados se obtiene el presupuesto total, en donde se suma el presupuesto de hardware, de software y el de mano de obra.

$$Presupuesto\ total = \$407{,}92 + \ \$55{,}73 + \$1236{,}66$$

$$Presupuesto\ total = 1700{,}31$$

CAPÍTULO IV

CONCLUSIONES Y RECOMENDACIONES

4.1. Conclusiones

- En base al análisis de la situación actual en cuanto a seguridad en el Gobierno Autónomo Descentralizado (GAD) del cantón Tisaleo revela la existencia de áreas críticas y vulnerables que requieren urgentemente una mejora en su sistema de seguridad. Se identificó la falta de cobertura de la cámara de seguridad existente, lo que representa un riesgo potencial para la seguridad del personal, activos y la información confidencial que se maneja en los departamentos de Tesorería, Dirección Financiera, Alcaldía, entre otras. Además, se destacó la carencia de un control de acceso digital, lo que implica un peligro significativo para la protección de datos financieros sensibles y la posibilidad de manipulación de registros contables, con ello se evidenció la necesidad de implementar dispositivos de seguridad adicionales, como cámaras, sensores de movimiento, alarmas y sensores de huella, para mejorar la seguridad en las instalaciones del GAD Municipal.

- El diseño propuesto para el sistema seguridad de los departamentos de Administración General y Financiero con tecnología IoT representa una solución innovadora y eficiente. La incorporación de dispositivos IoT permite recopilar datos en tiempo real, mejorar la precisión y agilidad del monitoreo, y brindar una mayor integración entre los diferentes elementos del sistema de seguridad. De esta manera se ha considerado cada aspecto relevante, incluyendo la ubicación estratégica de cámaras, sensores y dispositivos IoT, así como la infraestructura necesaria para su funcionamiento.

- El sistema implementado comprende de dos cámaras instaladas se encargan de detectar el movimiento durante el horario programado, que es desde las 18:00 hasta las 06:00. Cuando se detecta movimiento dentro de este período, la cámara captura 4 imágenes y las guarda en una carpeta del servidor (hosting) a través de FTP. Además, la cámara envía un correo electrónico al correo

específico creado para el sistema, notificando que se ha detectado movimiento. Para lograr esta funcionalidad, las cámaras están conectadas mediante una red cableada, lo que permite que no solo estén conectadas en la red local, sino que también tengan acceso a Internet. De esta manera, pueden llevar a cabo el proceso de almacenamiento de imágenes y enviar correos electrónicos a través de la conexión a Internet.

- Al iniciar la aplicación diseñada, se desarrolla un sistema que ejecuta una tarea en paralelo o hilo, permitiendo que se realice este proceso cada 5 segundos. El sistema se conecta al correo electrónico indicado previamente para verificar si hay nuevos mensajes. Si se detecta un nuevo mensaje, se envía una actualización a la base de datos en la tabla "alarma", cambiando el estado a "activado". Una vez realizada esta actualización, el correo detectado se marca como leído para evitar que se siga procesando el mismo mensaje. Además, se crea otro hilo que realiza peticiones a la base de datos en la tabla "alarma" para verificar el estado de la alarma. El resultado de esta verificación permite que la interfaz cambie el icono de la alarma. Si el estado es "inactivo", el icono se muestra de color gris, y si el estado es "activo", el icono se muestra de color rojo. Además, dependiendo del estado de la alarma, se envía un texto a través de una conexión serial a Arduino para activar el pulso hacia la alarma.

- Respecto al sistema de control de acceso a las oficinas de Tesorería y Alcaldía, el sensor dactilar se encuentra en estado de espera para realizar la lectura. Puede esperar una huella digital o un mensaje enviado desde la PC a través de la conexión serial. Si se detecta una huella, el sensor verifica si corresponde a una huella almacenada previamente en su memoria y obtiene el ID correspondiente. Luego, envía una solicitud a la PC para verificar si el usuario con ese ID existe en la base de datos. Si el usuario existe, el nombre del usuario se muestra en el Display del sistema, indicando una coincidencia positiva. En caso contrario, se muestra un mensaje de error, indicando que la huella no está registrada en el sistema. Si el usuario es identificado correctamente, el sensor envía el valor de posición necesario para activar el servo motor, lo que

permitirá el acceso o autorización correspondiente según las características del sistema de control al que esté conectado.

4.2. Recomendaciones

- Se recomienda realizar una evaluación detallada de los riesgos específicos presentes en cada departamento, y en base a esa evaluación, implementar una solución integral que incluya la instalación de cámaras de seguridad adicionales y la implementación de un control de acceso digital para proteger los datos financieros y mantener un ambiente seguro para el personal y la información confidencial.

- Se deben evaluar factores como el flujo de personas y actividades en cada departamento, los puntos de acceso, las zonas de mayor concentración de bienes valiosos o información confidencial, y cualquier otro aspecto relevante para determinar los puntos clave donde se deben instalar las cámaras y sensores.

- Es necesario seleccionar dispositivos IoT confiables y compatibles que permitan la recopilación de datos en tiempo real. Además de capacitar al personal en el uso y gestión adecuados de esta nueva tecnología para garantizar su efectividad y correcto funcionamiento.

- Es importante realizar un análisis del cableado existente para asegurarse de que sea adecuado para soportar el despliegue de dispositivos IoT. Si es necesario, se deberán realizar mejoras o ampliaciones en la infraestructura de cableado para garantizar la correcta transmisión de datos entre los dispositivos y los puntos de monitoreo centralizados.

Referencias Bibliográficas

[1] El Metro, «Ecuador: con más de 50 000 robos cierra el año el país y la inseguridad sofoca a diario a los ciudadanos,» enero 2023. [En línea]. Available: https://www.metroecuador.com.ec/noticias/2023/01/02/ecuador-con-mas-de-50-000-robos-cierra-el-ano-el-pais-y-la-inseguridad-sofoca-a-diario-a-los-ciudadanos/. [Último acceso: abril 2023].

[2] R. Gahona y A. Gavilema, Diseño de la red Internet de las cosas (IoT) para el edificio de la empresa CONSEL, Quito: Universidad Politécnica Salesiana, 2020.

[3] D. Herrera, «Diseño e implementación de un prototipo de seguridad para control domótico basado en IoT bajo ambientes de dispositivos móviles con Android,» Tesis de pregrado, Escuela Politécnica Nacional, Quito, 2020.

[4] I. Fúnez, Diseño de un sistema de seguridad en el hogar basado en IOT y creación de prototipo, Linares: Universidad de Jaén, 2022.

[5] B. García y L. Msncheno, Diseño e implementación de un sistema de control de accesos para dispositivos de seguridad basado en tecnología IoT, Guayaquil: Escuela Superior Politécnica del Litoral, 2023.

[6] J. Chiluisa, Sistema de seguridad para el control y monitoreo de la unidad educativa Lago San Pablo cantón Pujilí a traves de una plataforma web, Latacunga: Escuela Superior Politécnica del Ejército, 2022.

[7] J. Sánchez, “Desarrollo de un Sistema de Seguridad Electrónica aplicado a la Supervisión y Monitoreo en Oficinas, Lima: Universidad Tecnológica del Perú, 2019.

[8] A. García, Diseño de un sistema remoto de alarma contra intrusiones, Catalunya: Universitat Oberta de Catalunya, 2022.

[9] G. Alcoba, Área de trabajo de seguridad electrónica, España: AES, 2016.

[10] M. Carrasco, Sistemas de detección y alarma, Primera ed., Barcelona: Detnov, 2016.

[11] J. Esplugas, Guía para el diseño, uso y mantenimiento de los sistemas de Detección automática de incendios, ASEPEYO, 2016.

[12] A. Radhi, «Design and Implementation of a Smart Fire Alarm System Based of Wi-Fi over Long Distance (WiLD),» *ResearchGate,* 2016.

[13] J. Rodríguez, Circuito cerrado de televisión y seguridad electrónica, Segunda ed., Madrid: Paraninfo S.A, 2018.

[14] R. Montilla, «Seguridad. Introducción a los Componentes de un Sistema CCTV,» *Revista Librepensadores,* 2021.

[15] W. Quinde, Implementaciòn de un sistema de videovigilancia CCTV para los pasillos Norte de la Escuela de Formación de GTecnólogos (ESFOT), Quito: Escuela Politécnica Nacional, 2018.

[16] R. Rodríguez, «Internet de las cosas: Futuro y desafío para la epidemiología y la salud pública,» *Revista Universidad y Salud,* vol. 21, nº 3, pp. 253-260, 2019.

[17] M. Pineda, «La Internet de las Cosas, el Big Data y los nuevos problemas de la comunicación en el Siglo XXI,» *Revista Mediaciones Sociales,* pp. 11-24, 2018.

[18] M. Sánchez y G. Ramoscelli, «Creación de valor a partir del internet de las cosas: estudio exploratorio en la provincia de Buenos Aires,» *Revista Visión de Futuro,* vol. 22, nº 1, pp. 149-69, 2018.

[19] Y. Chitiva, «Diseño de una red de IoT para el hogar,» Universidad Cooperativa de Colombia, 2020.

[20] C. Tonato y S. Sinche, «Análisis comparativo entre arquitecturas de sistemas IoT,» *RITI Journal,* vol. 10, nº 21, pp. 40-55, 2022.

[21] B. Hernández, M. Barrón y M. Cedillo, «IoTX: Arquitectura tecnológica integrada (Fase 1),» Instituto Mexicano de Transporte, México, 2021.

[22] A. Ochoa, L. Cangrejo y T. Delgado, «Alternativa Open Source en la implementación de un sistema IoT para la medición de la calidad del aire,» *Revista Cubana de Ciencias Informáticas,* vol. 12, nº 1, pp. 189-204, 2018.

[23] N. Aranda, N. Aguirre y N. Balich, «Plataforma Internet Industrial de las Cosas como servicio local,» *Revista INNOVA,* vol. 10, nº 1, pp. ISSN 2618-1894, 2022.

[24] M. Quiñones y H. Pachar, «Desarrollo y evaluación de un gateway móvil IoT para redes 4G LTE,» *Revista Enfoque UTE,* vol. 11, nº 4, pp. 16-26, 2020.

[25] Hernández, «Visualizador de tráfico de red de comunicación basadas en la Arquitectura TCP/IP,» *Revista Universidad y Sociedad,* vol. 11, nº 2, pp. 193-202, 2019.

[26] C. Medina, C. Calvache, G. Mora, J. Salazar, H. Mora y M. Dagoberto, «Propuesta de Arquitectura IoT orientada a la creación de prototipos para su aplicación en plataformas educativas y de investigación,» *Revista Colombiana de Tecnologías de Avanzada,* vol. 1, nº 39, pp. 118-125, 2022.

[27] M. Mora y K. Urrego, «Internet de las cosas: modelos de comunicación, desafíos y aplicaciones,» Universidad de los Llanos, 2018.

[28] E. Barbecho y I. Llivisaca, «Diseño e implementación de un aplataforma basada en IoT para la gestión de promociones de artículos en estableciemientos comerciales,» Universidad Politécnica Salesiana, 2021.

[29] J. Herrera, K. Sámchez y E. López, «Estudio del modelo de capas de IoT para enlaces descendentes en plataforma de interconexión de la red Sifgox,» *Revista Logos Ciencia & Tecnología,* vol. 13, nº 3, pp. 46-56, 2021.

[30] J. Vega, F. Sánchez, G. Guzmán y M. Lagos, «Sistema de acceso usando RFID y verificación de rostro,» *Revista de Ciencia y Tecnología,* vol. 1, nº 20, pp. 108-118, 2018.

[31] L. González, S. Osiris, D. Laguía, E. Gesto y K. Hallar, «Internet del Futuro – Estudio de tecnologías IoT,» *Revista UNPA,* vol. 12, nº 3, pp. 105-137, 2020.

[32] A. Mora, J. Rodríguez, R. Macías y H. Sacón, «Estudio de la tecnología de comunicación inalámbrica en el estándar IEEE 802.11ax orientada al despliegue en Ecuador para el desarrollo del internet de las cosas,» *Revista Dominio de las Ciencias,* vol. 7, nº 4, pp. 729-762, 2021.

[33] R. Mouha, «Internet of Things (IoT),» *ournal of Data Analysis and Information Processing,* vol. 8, pp. 77-101, 2021.

[34] K. Rose, S. Eldridge y L. Chapin, La internet de las cosas: Una breve reseña, Internet Society, 2015.

[35] M. Mora y K. Urrego, Monografía internet de las cosas: Modelos de comunicación, desafíos y aplicaciones, Colombia: Universidad de los Llanos, 2018.

[36] A. Souri, A. Hussien, M. Hoseyninezhad y M. Norouzi, «A Systematic Review of IoT Communication Strategies for an Efficient Smart,» *LJMU Research Online,* pp. 1-35, 2019.

[37] A. Majumdar, Optical Wireless Communications for Broadband Global Internet Connectivity, Elsevier Inc., 2019.

[38] S. Kulkarni y S. Kulkarni, «Communication Models in Internet of Things: A Survey,» *IJSTE - International Journal of Science Technology & Engineering,* vol. 3, nº 11, pp. 87-91, 2017.

[39] M. Gutierrez y S. Iturrialde, Fundamentos básicos de instrumentación y control, Santa Elena, 2017.

[40] W. Cruz, Diseño del sistema de seguridad y de control de iluminación para el conjunto cerrado El Portal del Bosque en la ciudad de Tunja, Tunja: Universidad Pedagógica y Tecnológica de Colombia, 2018.

[41] A. Laghari, K. Wu, R. Laghari y M. Ali, «A Review and State of Art of Internet of Things (IoT),» *Archives of Computational Methods in Engineering,* 2021.

[42] A. González y J. López, IOT: Dispositivos, tecnologías de transporte y aplicaciones, España: UOC: Universitat Oberta de Catalunya, 2017.

[43] J. Ceja, R. Renteróa, R. Ruelas y Ochoa, «Módulo ESP8266 y sus aplicaciones en el internet de las cosas,» *Revista de Ingeniería Eléctrica,* vol. 1, nº 2, pp. 24-36, 2017.

[44] P. Ravi, J. Mohd, H. Abid y S. Rajiv, «Aplicaciones de Internet de las cosas (IoT) para luchar contra la pandemia de COVID-19,» *Diabetes & Metabolic Syndrome: Clinical Research & Reviews,* vol. 14, pp. 521-524, 2020.

[45] A. Sfart, Z. Chtourou y Y. Challal, «A systemic and cognitive vision for IoT security: A case study of military live simulation and security challenges,» *International Conference on Smart, Monitored and Controlled Cities (SM2C),* pp. 101-105, 2017.

[46] K. Sachin, T. Prayag y Z. Mikhail, «Internet of Things is a revolutionary approach for future technology enhancement: a review,» *Journal of Big Data volume,* vol. 6, nº 111, 2019.

[47] D. Gonzalez, El Único Libro de Redes que Necesitas: Curso de Redesde Desde Cero - Perparate para CCNA 200-301 y Mas., New York, 2022.

[48] . Berral, Instalación y mantenimiento de redes para transmisión de datos 2.a edición. , España: Ediciones Paraninfo, S.A., 2020.

[49] C. Valencia, «Evaluación de tecnologías inalámbricas en redes de área doméstica para obtener la curva característica de carga en edificios inteligentes,» Universidad Politécnica Salesiana, Quito, 2019.

[50] C. Pardo y I. Rodil, Operaciones auxiliares con tecnologías de la información y la comunicación, España: Ediciones Paraninfo, S.A, 2022.

[51] R. Gupta, Information and Communication Technology in Physical Education, India: Friends Publications (India), 2021.

[52] H. Zemrane, «Redes de Sensores Inalámbricos como parte de IOT: Estudio de desempeño del protocolo WiMax - Mobil,» *IV Congreso Internacional de Tecnologías y Aplicaciones de Cloud Computing (Cloudtech),* 2019.

[53] C. Muñoz, E. Hernández, J. Madera, H. Hernández y K. Restrepo, Diseño e implementación de una aplicación que permita controlar dispositivos eléctricos a través de un ordenador o un móvil, Ediciones Unisinú, 2018, pp. 255-272.

[54] N. Machuca, «Algoritmos, herramientas de Algoritmos, programación estructurada: C++, C Sharp, estructura de datos, cadenas de caracteres, tipos de datos, procedimientos y funciones, aplicaciones.,» (Tesis de pregrado, Universidad Nacional de Educación Enrique Guzmán y Valle), Lima, 2018.

[55] Á. Arias, «Aprende a Programar ASP .NET y C# - Nueva Edición,» IT Campus Academy, 2022.

[56] J. Carrillo, «Arduino: tecnología y creatividad en tus manos,» *Observatorio de Tecnología Educativa,* nº 95, pp. 1-7, 2023.

[57] S. Pazmiño, «Programación en Arduino vs. circuitos tradicionales,» *Revista Nueva Educación Latinoamericana,* nº 5, pp. 51-55, 2022.

[58] M. Vital, «Programación para principiantes en Arduino,» *Vida Científica Boletín Científico de la Escuela Preparatoria,* vol. 11, nº 21, pp. 35-40, 2023.

[59] K. Malave y J. Beauperthuy, «"Android" el sistema operativo de Google para dispositivos móviles,» *Negotium,* vol. 7, nº 19, pp. 79-96, 2018.

[60] L. Quisaguano, T. Camalle y J. Toca, «Analisis comparativo de entornos de desarrollo móvil,» *Ciencia Latina Revista Científica Multidisciplinar,* vol. 6, nº 4, pp. 4478-4498, 2022.

[61] G. M. d. Tisaleo, «Administración 2023-2027,» 2023. [En línea]. Available: https://tisaleo.gob.ec/.

[62] HIKVISION, DS-2CD2147G2(-SU) 4 MP ColorVu Fixed Dome Network Camera, Hikvision Digital Techonology Co, 2020.

[63] HIKVISION, Cámara IP DS-2CD2020F-I(4MM) C - 1080p Hikvision, DELTA-OPTI, 2023.

[64] D-Link, Wireless N IR home network camera DCS-932_932L_A1_Datasheet, D-LINK, 2010.

[65] ElectroStore, «Lector de huella dactilar biométrico digital Fingerprint AS608,» 2019. [En línea]. Available: https://grupoelectrostore.com/shop/placas-para-programacion/raspberry/accesorios-para-raspberry/lector-de-huella-digital-biometrico-digital-fingerprint-as608/.

[66] DFRobot, «Capacitive Fingerprint Sensor / Scanner (UART, 80 Fingerprints),» 2023. [En línea]. Available: https://www.dfrobot.com/product-2051.html.

[67] RobotShop, Arduino Mega 2560, 2020.

[68] R. Pi, Raspberry Pi 2, Model B V1.2, 2020.

[69] G. Coley, BeagleBone Black System Reference Manual, Beagleboard, 2013.

[70] Junta de Galicia, Básicos Arduino, 2016: MediaLab USAL, España.

[71] Mbed, «Mbed Rapid IoT device development,» Copyright © 2023 Arm Limited, 2023. [En línea]. Available: https://os.mbed.com/.

[72] M. Muñoz, Introducción a C#. Manual de estudiante, Microsoft Most Valuable Professional, 2017.

[73] J. Swacha y K. Muszynska, «Python and C#: a comparative analysis fromsStudents' perspective,» *Annales Universitatis Mariae Curie-Sklodowska sectio AI – Informatica,* vol. 1, nº 1, pp. 89-101, 2011.

[74] E. Gülcüoğlu, A. Ustun y N. Seyhan, «Comparison of Flutter and React Native Platforms,» *Journal of Internet Applications and Management,* vol. 12, nº 2, pp. 129-143, 2021.

ANEXOS

Anexo 1. Entrevista al señor Alcalde de Tisaleo

UNIVERSIDAD TECNICA DE AMBATO

FACULTAD DE INGENIERÍA EN SISTEMAS, ELECTRÓNICA E INDUSTRIAL

Entrevista al señor Alcalde de Tisaleo

Objetivo: Establecer los criterios y estado actual del sistema de seguridad y monitoreo del GAD Municipal Tisaleo.

Cuestionario

1. **¿Conoce usted si el las instalaciones del GAD Municipal de Tisaleo ha sido víctima de robo?**

……
…….

2. **¿El GAD Municipal de Tisaleo cuenta con algún sistema de seguridad?**

……
……

3. **¿Cómo califica el sistema de seguridad del GAD Municipal de Tisaleo**?

……
……

4. **¿Qué áreas necesitan mayor control de seguridad dentro de las instalaciones del GAD Municipal de Tisaleo?**

……
……

5. **¿Tienen conocimiento acerca de los sistemas de monitoreo y videovigilancia?**

……
……

6. **¿Conoce usted que por medio de internet se puede realizar la conexión de varios dispositivos para la vigilancia de un lugar determinado?**

……
……

7. **¿Qué elementos de seguridad considera necesario implementar en el GAD de Tisaleo para llevar un adecuado monitoreo de la seguridad? (cámaras, control de acceso, alarmas)**

……
……

8. **¿De qué manera considera que sería más efectivo recibir las alertas que brinde un sistema de monitoreo de seguridad?**

……
……

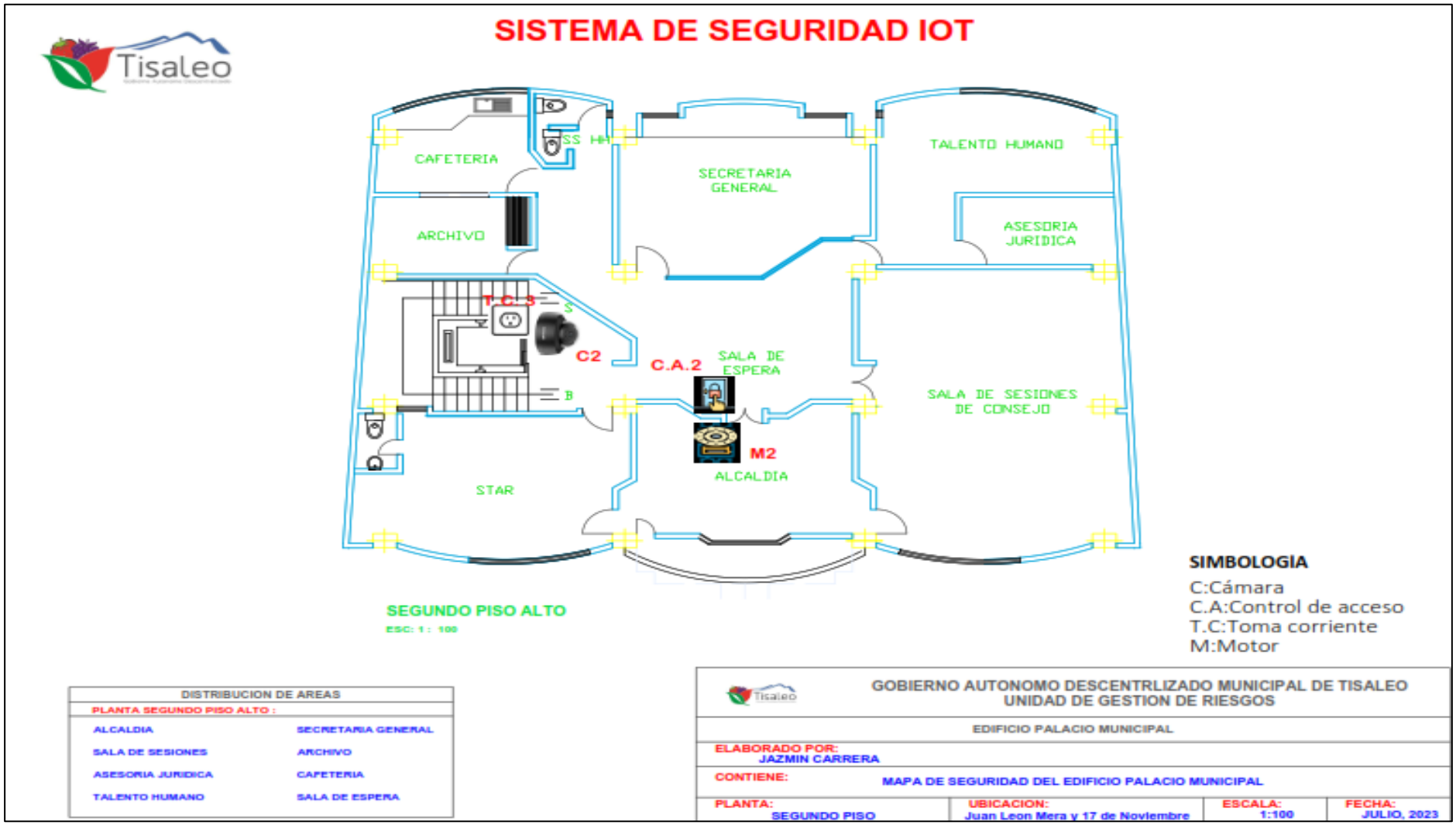
9. **¿Cree usted que es necesario implementar un sistema de seguridad que permita alertar cualquier acto de inseguridad en las instalaciones del GAD?**

……
……

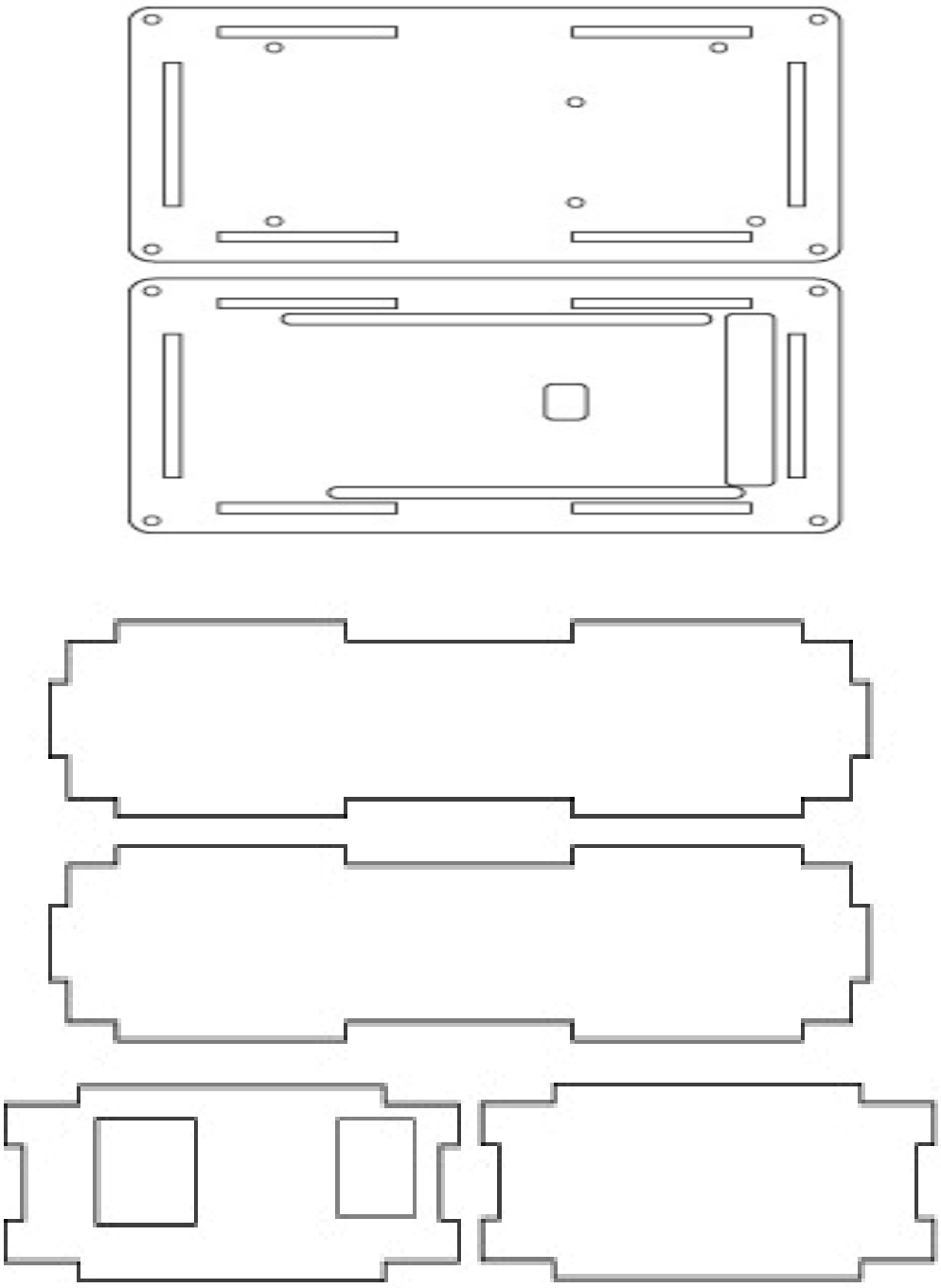
¡MUCHAS GRACIAS POR SU COLABORACIÓN!

Anexo 2. Colocación de los elementos instalados en la planta baja en el plano

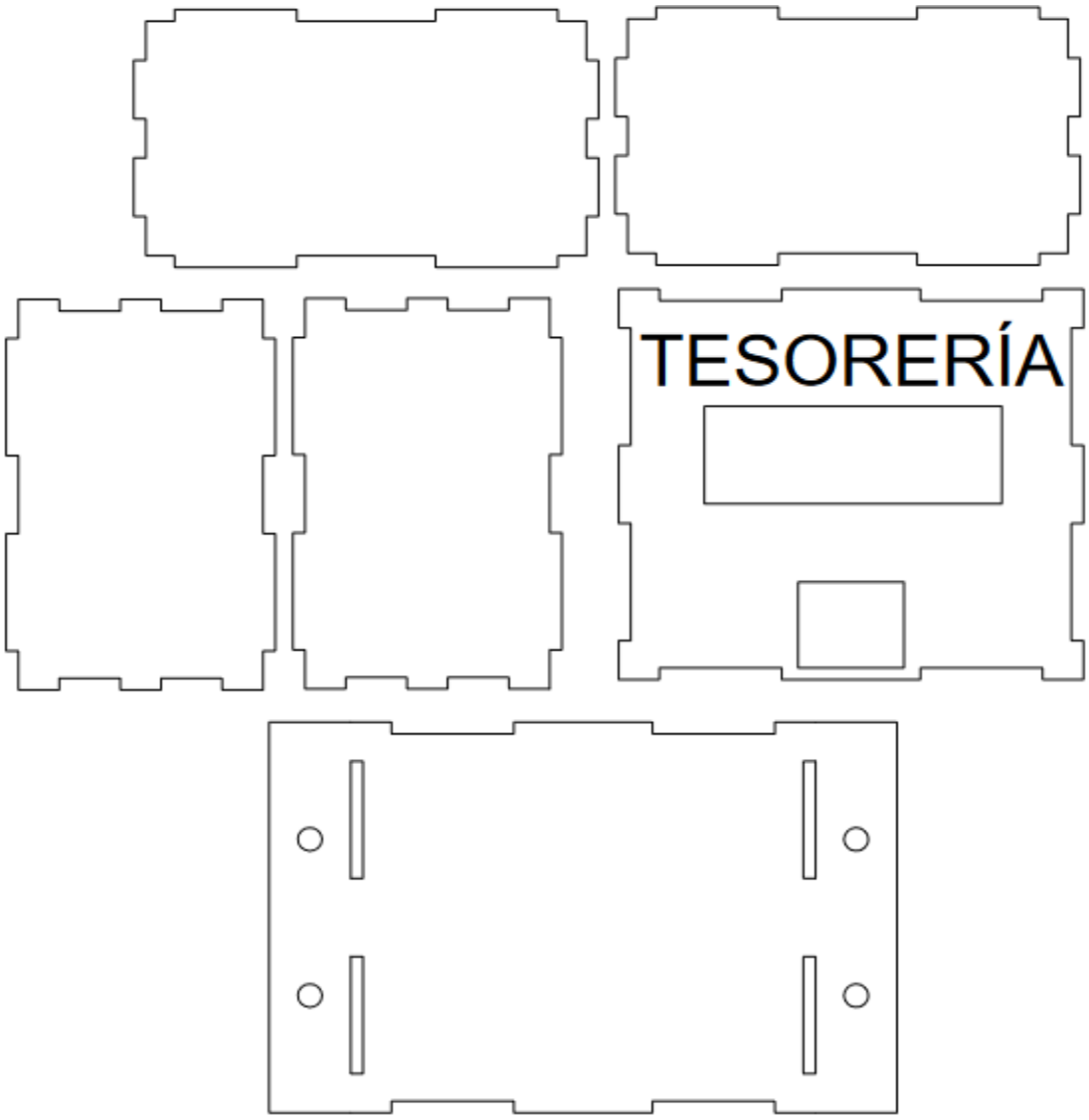
Anexo 3. Colocación de los elementos instalados en la segunda planta en el plano



Anexo 4. Case tarjeta Arduino



Anexo 4. Case control de acceso



Anexo 5. Datasheet Arduino Mega