UNIVERSIDAD LAICA "ELOY ALFARO" DE MANABÍ

FACULTAD CIENCIAS DE LA VIDA Y TECNOLOGÍAS

TRABAJO DE TITULACIÓN MODALIDAD PROYECTO INTEGRADOR, PREVIO A LA OBTENCIÓN DEL TÍTULO: INGENIERO EN TECNOLOGÍAS DE LA INFORMACIÓN

TEMA:

"DISEÑO E IMPLEMENTACIÓN DE DISPOSITIVOS DE SEGURIDAD BASADO EN TECNOLOGÍA IOT EN LAS AULAS DE LA CARRERA DE AGROPECUARIA DE LA FACULTAD DE CIENCIAS DE LA VIDA Y TECNOLOGÍAS DE LA ULEAM"

AUTORES:

LOOR MENDOZA KEVIN JOSÉ

OVIEDO INSUASTI DAYANA SAMANTHA

TUTOR:

ING. LUIS MENDOZA CUZME

MANTA - MANABÍ – ECUADOR

CERTIFICACIÓN

En calidad de docente tutor de la Facultad Ciencias de la Vida y Tecnologías de la Universidad Laica "Eloy Alfaro" de Manabí, CERTIFICO:

Haber dirigido, revisado y aprobado preliminarmente el Trabajo de Integración Curricular bajo la autoría de los estudiantes **OVIEDO INSUASTI DAYANA SAMANTHA – LOOR MENDOZA KEVIN JOSE**, legalmente matriculados en la carrera de Ingeniería en Tecnologías de la Información, período académico 2024-2025, cumpliendo el total de 400 horas, cuyo tema del proyecto es **"DISEÑO E IMPLEMENTACIÓN DE DISPOSITIVOS DE SEGURIDAD BASADO EN TECNOLOGÍA IOT EN LAS AULAS DE LA CARRERA DE AGROPECUARIA DE LA FACULTAD DE CIENCIAS DE LA VIDA Y TECNOLOGÍAS DE LA ULEAM".**

La presente investigación ha sido desarrollada en apego al cumplimiento de los requisitos académicos exigidos por el Reglamento de Régimen Académico y en concordancia con los lineamientos internos de la opción de titulación en mención, reuniendo y cumpliendo con los méritos académicos, científicos y formales, y la originalidad del mismo, requisitos suficientes para ser sometida a la evaluación del tribunal de titulación que designe la autoridad competente.

Particular que certifico para los fines consiguientes, salvo disposición de Ley en contrario.

Manta 11 de febrero de 2025

Lo certifico,

Ing. Luis Jacinto Mendoza Cuzme, Mg.
Docente Tutor
Facultad de Ciencias de la Vida y Tecnologías

TRABAJO DE TITULACIÓN MODALIDAD PROYECTO INTEGRADOR, PREVIO A LA OBTENCIÓN DEL TÍTULO: INGENIERO EN TECNOLOGÍAS DE LA INFORMACIÓN

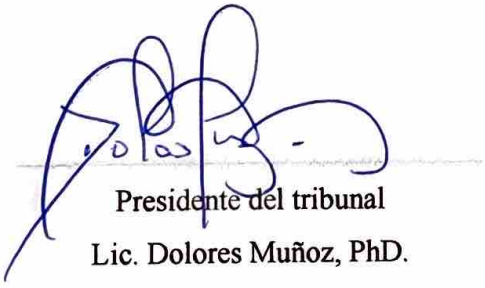
"DISEÑO E IMPLEMENTACIÓN DE DISPOSITIVOS DE SEGURIDAD BASADO EN TECNOLOGÍA IOT EN LAS AULAS DE LA CARRERA DE AGROPECUARIA DE LA FACULTAD DE CIENCIAS DE LA VIDA Y TECNOLOGÍAS DE LA ULEAM"

TRIBUNAL EXAMINADOR QUE DECLARA APROBADO

EL GRADO DE INGENIERO EN TECNOLOGÍAS DE LA INFORMACIÓN DE:

Loor Mendoza Kevin José

Oviedo Insuasti Dayana Samantha

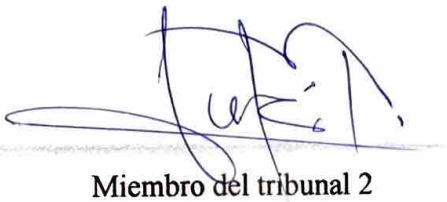


Presidente del tribunal

Lic. Dolores Muñoz, PhD.

Miembro del tribunal 1

Ing. Henry Mero, Mg.



Miembro del tribunal 2

Arq. Luigi Pihuave Calderón, Mg.

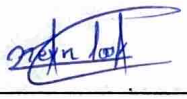
Manta, febrero del 2025

DECLARACIÓN EXPRESA DE AUDITORÍA

Yo, Oviedo Insuasti Dayana Samantha con ciudadanía 1722362108 y Loor Mendoza Kevin José de ciudadanía 1754716940; en calidad de autor del trabajo de titulación "**DISEÑO E IMPLEMENTACIÓN DE DISPOSITIVOS DE SEGURIDAD BASADO EN TECNOLOGÍA IOT EN LAS AULAS DE LA CARRERA DE AGROPECUARIA DE LA FACULTAD DE CIENCIAS DE LA VIDA Y TECNOLOGÍAS DE LA ULEAM**", autorizo a la Universidad Laica "Eloy Alfaro" de Manabí, hacer uso total o parcial de este trabajo de titulación del que soy responsable, con fines estrictamente académicos o investigativos.

Lo certifica,

Oviedo Insuasti Dayana Samantha
Cedula: 1722362108
Correo: e1722362108@live.uleam.edu.ec



Loor Mendoza Kevin José
Cedula: 1754716940
Correo: e1754716940@live.uleam.edu.ec

DEDICATORIA

Dedico este trabajo, en primer lugar, a mis padres, Paulina Insuasti y Christian Oviedo, quienes han sido un pilar fundamental en mi vida, brindándome su amor, apoyo y confianza incondicional a lo largo de mi vida estudiantil.

A mi abuelita, Yolanda Cisneros, por estar siempre a mi lado desde el momento en que nací, siendo mi refugio y fortaleza en cada paso que doy.

A mi tío, Rommel Insuasti, quien ha sido como un segundo padre para mí, dándome siempre su apoyo y guía incondicional, y a mi tía, Ximena Insuasti, quien ha sido como una hermana, acompañándome con cariño y comprensión a lo largo de mi vida.

A mi primo, Miguel Ángel Insuasti, que es como un hermano pequeño y una fuente constante de alegría y compañía en mi vida.

A mi familia paterna, que incluso desde la distancia siempre se preocupan por mi bienestar y felicidad, haciéndome sentir su amor y apoyo inquebrantable.

Y, con especial cariño, dedico este logro a mis abuelitos, Fanny Yangari y Miguel Ángel Insuasti, quienes, aunque ya no están físicamente, siguen siendo luz y guía en mi vida, dejando en mí una huella imborrable de amor y enseñanzas.

A mi tutor, Ing. Luis Mendoza Cuzme, por su orientación, paciencia y sabiduría, que me ayudaron a superar los retos que surgieron durante el desarrollo de esta tesis.

A mis compañeros de estudio, especialmente a Jean Pier Casquete, Kevin Loor y Jostin Bailón, por su colaboración, apoyo moral y por compartir conmigo este viaje lleno de aprendizajes, retos y logros.

Con todo mi amor y gratitud.

Dayana Samantha Oviedo Insuasti

AGRADECIMIENTO

Las palabras no lograrán expresar lo que siento en este momento, pero siempre quiero agradecer a Dios por ayudarme en cada paso que he dado, por guiarme, por estar siempre allí dándome fortaleza para seguir adelante. Sin su presencia en mi vida, este logro no habría sido posible.

A mis padres, por darme un buen ejemplo, por guiarme por el camino correcto y por su esfuerzo constante a lo largo de todos estos años. Gracias por darme las herramientas para convertirme en una profesional, por ser mi fuerza, mi guía y por los consejos que me ayudaron a ser la persona que soy hoy. No me caben las palabras para expresar mi agradecimiento por todo lo que han hecho por mí, por su sacrificio, por estar siempre a mi lado en cada paso de este reto. Sin ustedes, no habría podido lograrlo.

A mis abuelitos, quienes siempre me han tratado con mucho cariño y se han preocupado por mí. Aunque dos de ellos ya no estén físicamente, los recuerdo con mucho amor y gratitud. Recuerdo a mi abuelita, que siempre me aconsejaba y su mayor sueño era verme convertida en una profesional. Lo lograré por ti y por todos los que confiaron en mí. A mis tíos, que siempre me han apoyado en cada paso para que este sueño fuera posible. Gracias por estar ahí, por su amor y apoyo incondicional.

A mi familia, que siempre ha hecho todo lo posible para que yo pueda salir adelante, por estar siempre dispuesta a ofrecerme lo mejor y por querer lo mejor para mí. A mis amistades, que han estado a mi lado, incondicionalmente, brindándome apoyo en cada momento y celebrando conmigo cada logro. Y, por supuesto, agradezco a mi compañero de tesis, porque sin su colaboración, este proyecto no habría sido posible.

A todos ustedes, gracias, de corazón, por su apoyo constante y por ser parte de este logro.

Dayana Samantha Oviedo Insuasti

DEDICATORIA

Este proyecto de titulación va dedicado a mi madre María Mendoza y a mi padre José Loor por el esfuerzo y apoyo incondicional que han hecho en toda mi vida universitaria y de mi vida personal guiándome y acompañándome en cada paso que doy.

También dedico a toda mi familia al que ha estado conmigo desde principio hasta este momento les agradezco que me han dado consejos y apoyado en mis logros gracias por estar ahí.

A mi tutor, Ing. Luis Mendoza Cuzme, por su orientación, paciencia y sabiduría, que me ayudaron a superar los retos que surgieron durante el desarrollo de esta tesis.

A mis compañeros de estudio, especialmente a Ericka Dayana Lorente, Jostin Bailon y Jean Pier Casquete, por su colaboración, apoyo moral y por compartir conmigo este viaje lleno de aprendizajes, retos y logros.

Por otra parte, dedico a la persona que estuvo en este logro y esfuerzo a mi compañera de tesis Dayana Oviedo en la que superamos todos los obstáculos para seguir aquí y no rendirnos gracias por ser mi compañera en todo el trascurso universitario.

Con todo mi amor y de corazón.

Kevin José Loor Mendoza

AGRADECIMIENTO

Quiero expresar mi más profundo agradecimiento a todas aquellas personas que, de una u otra manera, contribuyeron al desarrollo de esta tesis.

En primer lugar, agradezco a Dios, fuente de fortaleza e inspiración, por haberme guiado en cada etapa de este trabajo y darme las fuerzas para seguir día a día adelante.

A mi familia, que ha sido mi pilar fundamental, brindándome siempre su apoyo incondicional. A mis padres, por inculcarme valores como la perseverancia y la responsabilidad, y por ser un ejemplo constante de esfuerzo y dedicación. A mis hermanos, por su aliento y por creer en mí, incluso en los momentos en que las dificultades parecían insuperables.

Extiendo mi gratitud a mis docentes y tutores, quienes con su conocimiento, orientación y paciencia fueron fundamentales para el desarrollo de esta investigación. Su guía fue clave para superar los retos que encontré en el camino.

A mis compañeros de carrera, quienes compartieron experiencias, ideas y apoyo moral durante este proceso. Su compañerismo fue invaluable.

Les agradezco a todos de corazón y siempre los llevare presentes y ser parte de un escalón mas de este logro de mi vida.

Kevin José Loor Mendoza

Contenido

Índice de figuras

Indice de Tablas

RESUMEN

El principal objetivo de este proyecto es el diseño e implementación de dispositivos de seguridad basados en tecnología IoT en las aulas de la carrera agrícola de la Facultad de Ciencias y Tecnologías de la Vida de la Universidad Laica Eloy Alfaro de Manabí (ULEAM). Este proyecto pretende mejorar la seguridad en las aulas a través de un sistema que controle el acceso de forma eficiente y segura. Esto evitará el acceso no autorizado y protegerá los recursos disponibles.

Además de aumentar la seguridad, el objetivo es optimizar el uso de los recursos tecnológicos, integrando soluciones modernas que se adapten a las necesidades específicas de la profesión agrícola. La implementación de dispositivos de seguridad IoT es una medida clave para garantizar la protección de instalaciones y equipos, creando un entorno seguro para estudiantes y profesores.

La propuesta se refiere a la implementación técnica de dispositivos IoT y la promoción de una cultura de seguridad entre los usuarios. Se aplicó una metodología que incluyó entrevistas y encuestas a docentes y estudiantes para identificar sus inquietudes y necesidades en relación a la seguridad en el aula.

Los resultados obtenidos demuestran que el sistema propuesto es factible y puede satisfacer las necesidades de seguridad. Además, revelan un alto nivel de aceptación y disposición para utilizar la tecnología implementada, respaldando la importancia de la propuesta para mejorar la seguridad en el entorno académico.

ABSTRACT

The central objective of this integrative project is the implementation of an automated access control system in the teachers' room of the Agricultural career of the Faculty of Life Sciences and Technology of the Laica Eloy Alfaro University of Manabí. The main purpose is to improve security in said room by introducing a system that guarantees safe and authorized access for teaching staff.

Altogether, this integrative project seeks to contribute to the improvement of security in the teachers' room, providing a specific solution adapted to the needs of the Agricultural career. The implementation of the automated access control system is presented as an effective measure to guarantee authorized and secure access, thus improving the management and protection of valuable resources in the staff room.

The proposal comprehensively addresses security in the teachers' room, considering not only the technical implementation of the automated access control system, but also the awareness and participation of teachers.

The applied methodology involved representative samples, interviews and surveys directed at teachers, allowing a deep understanding of their level of knowledge about the proposed system. The results obtained support the feasibility and relevance of the implementation, revealing valuable information about the specific perceptions and needs of users.

CAPÍTULO 1

1.1 Introducción

La presente tesis, titulada "Diseño e Implementación de Dispositivos de Seguridad Basado en Tecnología IoT en las instalaciones destinadas a la Carrera de Agropecuaria dentro de la "Facultad de Ciencias de la Vida y Tecnologías de la ULEAM", Se plantea como finalidad primordial establecer un sistema de seguridad automatizado para gestionar el acceso. A través de la integración de dispositivos IoT, se busca fortalecer la seguridad, permitiendo un acceso controlado y monitoreado en tiempo real, proporcionando una solución tecnológica innovadora y eficiente.

En el Capítulo I, se aborda la delimitación y análisis del problema, el cual surge de la necesidad de mejorar la seguridad en los espacios académicos de la carrera de Agropecuaria. Este capítulo aborda la ubicación y contextualización del problema, seguido de la formulación del mismo. Se incluye un diagrama causa-efecto que permite identificar los factores que inciden en la falta de seguridad actual. Además, se establecen los objetivos generales y específicos, junto con la justificación del proyecto, que destaca la relevancia del uso de tecnología IoT para incrementar la seguridad en un entorno académico.

El Capítulo II se centra en el marco teórico, donde se exploran los antecedentes históricos relacionados con la implementación de sistemas de seguridad basados en IoT y las definiciones conceptuales pertinentes. Se examinan los beneficios de la tecnología IoT en estos sistemas y se analizan los dispositivos adecuados para satisfacer las necesidades de seguridad en aulas, enfocados únicamente en el control de acceso. Asimismo, se detallan las características indispensables de los dispositivos IoT, la tecnología de conectividad, y aspectos de seguridad y privacidad.

En el Capítulo III, se describe el marco investigativo, los métodos de investigación empleados, y las herramientas de recolección de datos, como encuestas y entrevistas, realizadas a docentes y estudiantes para evaluar sus expectativas y conocimientos sobre los sistemas de control de acceso basados en IoT. Se presentan los resultados obtenidos a partir de estas herramientas y su análisis, que sirvieron para estructurar el diseño e implementación del sistema propuesto.

El Capítulo IV detalla el proceso de diseño y la implementación de los dispositivos IoT en las aulas de la carrera de Agropecuaria. Se describe el esquema del sistema, la selección de componentes y sensores, y la arquitectura de seguridad diseñada. Se incluyen evaluaciones de funcionalidad y efectividad de los dispositivos, un análisis de los gastos de implementación, y sugerencias para futuras optimizaciones del sistema.

En el Capítulo V, se lleva a cabo una evaluación de los resultados obtenidos después de la implementación del sistema. Este capítulo incluye un análisis exhaustivo del desempeño y eficiencia de los dispositivos IoT instalados, validación de los resultados frente a los objetivos específicos, y una comparación de la seguridad de las aulas antes y después de la implementación. Además, se examinan los niveles de satisfacción y retroalimentación de los usuarios, y se realiza un análisis estadístico de los incidentes de seguridad registrados durante el período de prueba, así como de la eficiencia de las alertas y tiempos de respuesta. Finalmente, se discuten las limitaciones encontradas y los hallazgos principales, ofreciendo una evaluación integral del sistema de seguridad implementado.

Por último, el Capítulo VI presenta las conclusiones y recomendaciones derivadas de todo el proceso de investigación y desarrollo del proyecto. En las conclusiones se resaltan los logros alcanzados, los beneficios de la implementación y el cumplimiento de los objetivos planteados. En las recomendaciones, se proponen acciones y mejoras futuras para optimizar el sistema de seguridad, con el fin de garantizar su efectividad a largo plazo y su adaptación a nuevas necesidades o tecnologías emergentes.

Este proyecto no solo busca solucionar la problemática de seguridad actual, sino también abrir paso a la modernización tecnológica dentro de la FCVT, contribuyendo a crear un entorno educativo más seguro y controlado.

1.2 Planteamiento del problema

1.3 Ubicación y contextualización del problema

La "ULEAM" Se trata de una destacada universidad de nivel superior, situada en la intersección de la Av. Circunvalación y la calle 12, en Manta, provincia de Manabí, Ecuador. La institución está compuesta por seis facultades que ofrecen una variada selección de programas académicos, alcanzando un total de 44 carreras. Sobresale por su enfoque en la educación de alta calidad y el impulso a la innovación tecnológica.

En este contexto, surge una problemática particular en las aulas de Agropecuaria, perteneciente a la FCVT. Las aulas están equipadas con diversos recursos educativos clave, como pupitres, sillas, computadoras con acceso a internet, proyectores y otros dispositivos tecnológicos necesarios para llevar a cabo las actividades académicas. Sin embargo, la preocupación por la seguridad en estos espacios ha ido en aumento, debido a la necesidad de resguardar tanto los equipos materiales como la integridad física de los estudiantes y docentes.

La adopción de dispositivos de seguridad basados en tecnología IoT permitirá un monitoreo y control más efectivo en las aulas, ofreciendo soluciones tecnológicas de vanguardia que faciliten el acceso autorizado y garanticen un entorno seguro para el desarrollo de las actividades académicas. Este proyecto tiene como finalidad diseñar e implementar un sistema de seguridad que permita la supervisión remota de estos espacios, proporcionando así una protección continua y una respuesta rápida ante cualquier posible incidente.

***Figura No.** 1. Ubicación y contextualización del problema. Fuente Propia.*

1.4 Problemática

En la actualidad, las aulas de la carrera de Agropecuaria de la FCVT presentan serias deficiencias en cuanto a la seguridad y el control de acceso. Estas aulas albergan valiosos equipos tecnológicos, materiales educativos y recursos especializados que son indispensables para el correcto desarrollo académico. Sin embargo, el acceso no controlado o la falta de un sistema eficiente de monitoreo y seguridad pone en riesgo tanto los recursos físicos como la integridad de los estudiantes y docentes que utilizan estas instalaciones.

El problema principal radica en que no existe un sistema de seguridad adecuado que permita gestionar el acceso al personal autorizado ni prevenir el ingreso de personas no autorizadas, lo cual incrementa la posibilidad de robos o uso indebido de los equipos. Además, las soluciones de seguridad actuales resultan ineficaces ante la creciente necesidad de una protección más avanzada y automatizada, acorde con las tecnologías emergentes.

A medida que la carrera de Agropecuaria crece en términos de infraestructura y número de estudiantes, la complejidad para administrar y controlar el acceso a las aulas aumenta, generando un entorno vulnerable para la comunidad académica.

Por tanto, es imprescindible diseñar e implementar un sistema de seguridad basado en tecnología IoT, que permita monitorear y restringir el acceso a las aulas de manera automática y remota. Este sistema no solo debe garantizar la seguridad de los recursos físicos y tecnológicos, sino también brindar tranquilidad al personal docente y estudiantil, reduciendo el riesgo de incidentes relacionados con la seguridad.

1.4.1. Formulación del problema

¿Cómo puede el diseño e implementación de un sistema de seguridad automatizado basado en tecnología IoT ayudar a mejorar el control de acceso en las aulas, resguardando de manera efectiva los recursos físicos y tecnológicos?

1.5 Diagrama Causa-Efecto de la problemática

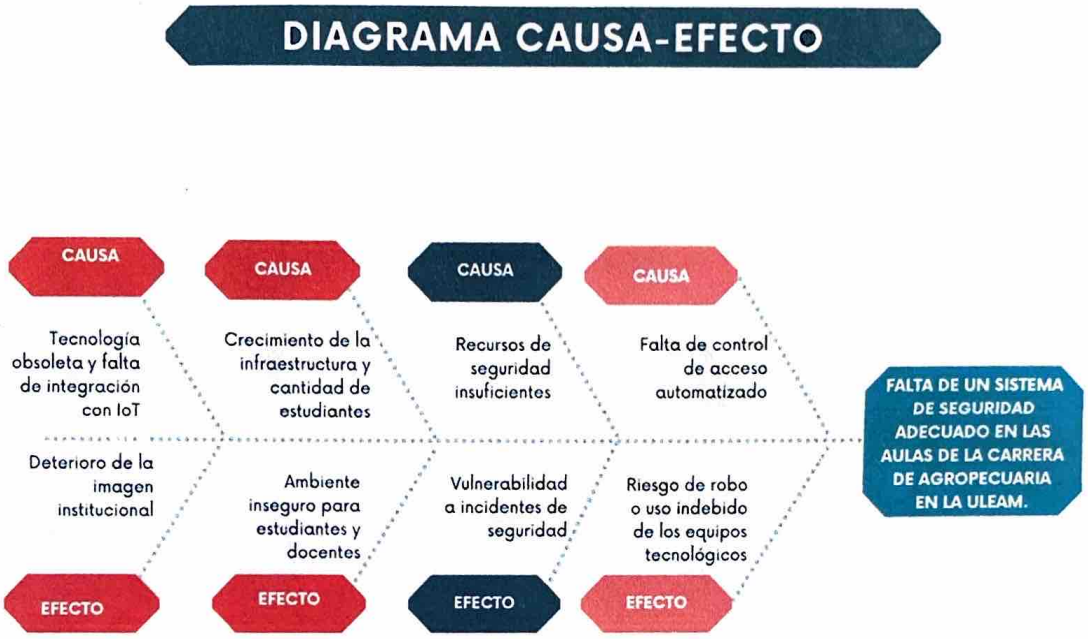


Figura No. 2. Diagrama Causa-Efecto de la problemática. Fuente propia.

1.6 Objetivos

1.6.1 Objetivo General

Implementar dispositivos de seguridad basados en tecnología IoT, diseñados específicamente para las aulas de la carrera de Agropecuaria de la FCVT.

1.6.2 Objetivos Específicos

- Elaborar un cuestionario para recabar información sobre las expectativas y requerimientos de los usuarios de las aulas de la carrera de Agropecuaria.
- Diseñar un diagrama esquemático del dispositivo de seguridad basado en *tecnología* IoT

- Implementar los dispositivos de seguridad IoT en las aulas de la carrera de Agropecuaria, garantizando su funcionalidad y efectividad en la protección del entorno educativo.

1.7 Justificación

La implementación de un sistema de seguridad IoT en las aulas de la carrera de Agropecuaria de la Universidad Laica Eloy Alfaro de Manabí surge de la necesidad de mejorar la seguridad en los espacios educativos, protegiendo tanto a las personas como los recursos que allí se encuentran. Este proyecto se enfoca en la instalación de dispositivos IoT de control de acceso, vigilancia y monitoreo, diseñados para limitar el acceso no autorizado, salvaguardar la privacidad y la integridad de los materiales y equipos, y brindar una respuesta rápida ante situaciones de emergencia.

Uno de los propósitos principales de este proyecto es crear un ambiente seguro que favorezca las actividades educativas, promoviendo un entorno de confianza y tranquilidad para los estudiantes y profesores. Al controlar el acceso de manera digital y eficaz, se asegura que solo las personas autorizadas puedan ingresar a las aulas, lo cual previene el uso indebido o el acceso a equipos y materiales específicos que pueden ser críticos para el desarrollo académico de los estudiantes de Agropecuaria.

Además, la implementación de dispositivos IoT modernos representa una oportunidad para reducir la brecha digital en el ámbito educativo. Al integrar tecnologías avanzadas, la universidad no solo mejora su infraestructura de seguridad, sino que también brinda a sus estudiantes y profesores un entorno con recursos tecnológicos contemporáneos. Esto contribuye a la adopción de herramientas digitales y a la familiarización de la comunidad académica con tecnologías emergentes, incrementando las competencias digitales de los usuarios.

Desde una perspectiva institucional, este proyecto eleva el perfil tecnológico de la Universidad Laica Eloy Alfaro de Manabí, posicionándola como una entidad educativa innovadora y comprometida con el avance de la tecnología en su gestión y en la protección de sus recursos. Al implementar un sistema de seguridad IoT, la universidad reafirma su compromiso con el desarrollo tecnológico y la creación de entornos seguros y modernos para el aprendizaje.

CAPITULO II

2.1 Marco teórico de la investigación

2.2 Antecedentes históricos de investigaciones relacionadas al tema presentado

En esta investigación se tomaron como referencias los estudios realizados por los autores que se detallan a continuación:

Benny García, Leopoldo Mancheno (2023) Creación e instalación de un sistema de control de acceso para dispositivos de seguridad basado en tecnología IoT. Este proyecto busca aplicar un sistema de gestión de acceso con el fin de optimizar la seguridad en los hogares mediante el uso de tecnología IoT.. Se propone un sistema de acceso que emplea un microcontrolador ESP32 para conectar dispositivos móviles y controlar una cerradura eléctrica mediante conexión WiFi o Bluetooth. El sistema incluye validación por huella dactilar y un código de acceso, proporcionando así un método de autenticación doble que incrementa la seguridad del hogar. El diseño incluye también una aplicación móvil, desarrollada con MIT App Inventor, que permite al usuario interactuar con el sistema y controlar el acceso de forma remota.

Además, el sistema ha sido diseñado para adaptarse a distintos desafíos de conectividad y facilidad de uso, incluyendo la creación de una base de datos para almacenar las huellas dactilares y los datos de acceso. Este proyecto destaca por su propuesta de seguridad de bajo costo y accesible, ideal para ser implementada en hogares ecuatorianos donde el índice de robos ha ido en aumento en los últimos años (García & Mancheno, 2023).

Eduardo Fúnez Fernández (2022) Diseño de un sistema de seguridad en el hogar basado en IoT y creación de prototipo. Este trabajo de fin de grado aborda el diseño e implementación de un sistema de seguridad para el hogar utilizando tecnología IoT, con una Raspberry Pi como controlador central. El sistema integra sensores de movimiento PIR, cámaras de seguridad, una cerradura de solenoide, y un bot de Telegram para notificar y permitir el control remoto de sus funciones. Entre las características destacadas, el sistema realiza detección de movimiento, simulación de presencia, y reconocimiento facial, activando automáticamente ciertos dispositivos en respuesta a la detección de intrusos. Además, el sistema está configurado para operar con el protocolo

HTTP y permite al usuario ajustar sus funciones mediante comandos a través de un Bot de Telegram.

El objetivo principal es proporcionar una solución de seguridad asequible y eficiente que los usuarios puedan controlar fácilmente a distancia. Esto permite que, mediante IoT, el sistema se ajuste a las necesidades de los hogares modernos que buscan incrementar su seguridad en un entorno de uso doméstico y cotidiano (Fúnez, 2022).

Cristian Noé Sáez Sáez (2023) Desarrollo e implementación de un sistema IoT para la gestión de pagos y control de acceso vehicular utilizando tecnología NFC para mejorar el tránsito en la EP-EMMPA.

Este proyecto técnico desarrolla un sistema IoT basado en la tecnología NFC para mejorar el control de acceso vehicular y la gestión de pagos en el Mercado de Productores Agrícolas San Pedro de Riobamba (EP-EMMPA). El sistema propuesto está diseñado para optimizar el flujo de tránsito vehicular, evitando la congestión en los accesos al establecimiento. La implementación se centra en una infraestructura IoT combinada con comunicación NFC para facilitar el registro, pago, y control de acceso de manera autónoma y eficiente.

La metodología empleada es de carácter experimental, con un enfoque en la investigación bibliográfica y el método deductivo para identificar los requisitos de la arquitectura y funcionalidad del sistema. En el diseño se integraron protocolos de comunicación como HTTP y MQTT, además de una aplicación móvil conectada a una base de datos en la nube para el manejo remoto de los datos. Para el reconocimiento de placas vehiculares, se desarrolló un script en Python que emplea la API de Google Vision, mejorando la autenticación y la seguridad del sistema. Asimismo, se implementaron medidas de seguridad en varias capas, incluyendo el uso de SSL para la comunicación segura y autenticación mediante PIN para los pagos.

Los resultados muestran que el prototipo redujo los tiempos de espera en un 80% comparado con el sistema anterior, logrando una alta eficiencia en el control de acceso. El análisis de latencia del sistema indicó tiempos de respuesta aceptables de 3693 ms a la entrada y 1640 ms a la salida. El proyecto concluye que la implementación de este sistema IoT proporciona una solución económica y segura que puede ser escalada para un control

de acceso vehicular más amplio en otros entornos. Se recomienda optimizar la capacidad del servicio de hosting para soportar un mayor tráfico de datos (Sáez, 2023).

Cristian Camilo Layton Díaz, Cristian Camilo Hernández Mendoza (2021) Diseño e implementación de un sistema basado en IoT y paneles solares para ayudar a personas con deterioro cognitivo en actividades diarias. En resumen: Este trabajo presenta una solución innovadora basada en el diseño e implementación de un sistema IoT alimentado por energía solar, con el propósito de facilitar la organización diaria y mejorar la calidad de vida de personas con deterioro cognitivo. El dispositivo diseñado recuerda a los usuarios sobre objetos importantes que deben llevar en sus equipajes, especialmente para estudiantes en entornos escolares, optimizando así la preparación para sus actividades y minimizando el impacto de sus dificultades cognitivas.

La investigación utiliza una metodología descriptiva, que se sustenta en una revisión exhaustiva de tecnologías IoT aplicadas al contexto de apoyo cognitivo, así como en la evaluación de energías renovables, específicamente la energía solar, como fuente sostenible de alimentación. El proceso metodológico incluyó la recopilación de información relevante en torno a la identificación de necesidades de la población objetivo, la selección de componentes tecnológicos adecuados y el diseño de prototipos. Se realizaron pruebas de validación que evaluaron la funcionalidad, autonomía energética, y efectividad del sistema en la notificación de recordatorios mediante alertas intuitivas al usuario.

Como parte de los resultados, el sistema demostró ser una solución portable y accesible, capaz de operar en diversos entornos y condiciones, gracias a la autonomía que le confieren los paneles solares. Esta tecnología no solo facilita la organización y el manejo de tareas diarias, sino que también propone un modelo sostenible y de bajo costo que responde a las necesidades de personas en riesgo de deterioro cognitivo.

Este proyecto desarrolla una herramienta práctica que combina IoT y energía solar, proporcionando una alternativa innovadora y eficiente para el cuidado y la asistencia en actividades diarias de personas con deterioro cognitivo, especialmente en entornos educativos, promoviendo una mejora significativa en su calidad de vida (Layton & Hernández, 2021).

Soberón Hernández y Landaeta Arcentales (2021) Desarrollo e implementación de un sistema inteligente de control de accesos basado en IoT para optimizar la seguridad física en el datacenter del Departamento de Informática de la Municipalidad.

Distrital de las Amazonas. En resumen: Este estudio aborda la problemática de la falta de seguridad física en el datacenter del Departamento de Informática, donde existe un riesgo de acceso no autorizado debido a la falta de un control de seguridad adecuado. Como solución, se propone la implementación de un sistema de registro de accesos basado en IoT, que permita un control efectivo y seguro en el ingreso de personas al datacenter.

El objetivo principal de la investigación es mejorar la seguridad física en el datacenter de la Municipalidad Distrital de las Amazonas en la ciudad de Iquitos mediante un sistema IoT. Este sistema utiliza sensores de movimiento y cámaras, enviando alertas y registrando los accesos de personas no autorizadas. La investigación emplea un enfoque descriptivo y aplicado. Utiliza un diseño pre-experimental con pre-test y post-test para analizar la efectividad del sistema implementado. Se trabajó con una población de 10 empleados del departamento, aplicando una encuesta de 12 preguntas mediante la escala de Likert para analizar y contrastar los datos recolectados.

Los resultados muestran que el Desarrollo e implementación de un sistema inteligente de control de accesos basado en tecnología IoT mejoró significativamente la seguridad del datacenter, reduciendo riesgos de acceso no autorizado y contribuyendo a la protección de los activos tecnológicos de la institución. En conclusión, esta solución proporciona un control de acceso más seguro y eficiente para el datacenter, reforzando así la seguridad general del área (Soberon Hernandez y Landaeta Arcentales, 2021)

2.3 Definiciones conceptuales

A continuación, se presentará la información fundamental que es imprescindible conocer para iniciar la investigación. Esta información servirá como base para comprender mejor el tema y guiará el desarrollo de un análisis más profundo en las etapas posteriores del estudio.

2.4 Dispositivos de seguridad basados en IoT

Los dispositivos de seguridad basados en IoT son herramientas electrónicas interconectadas que permiten el monitoreo y control de entornos mediante la recopilación y análisis de datos en tiempo real. Estos dispositivos, que incluyen cámaras de seguridad, cerraduras inteligentes y sensores de movimiento, utilizan tecnologías de conectividad para comunicarse entre sí y con plataformas de gestión, mejorando así la protección de espacios físicos. Al integrarse en un sistema, proporcionan alertas instantáneas y acceso controlado, lo que los convierte en componentes esenciales para la seguridad moderna (Tariq et al., 2023).

2.5 Beneficios del uso de tecnología IoT en sistemas de seguridad

El uso de la tecnología IoT en sistemas de seguridad ha traído múltiples beneficios, principalmente en la mejora de la protección tanto en hogares como en empresas. Dispositivos como cámaras de seguridad y sensores de movimiento, conectados a la red, son capaces de detectar intrusiones y notificar a los propietarios, lo que resulta en una respuesta más rápida ante posibles robos o incidentes. Además, IoT facilita el control del acceso a edificios y vehículos, la detección de intrusiones y la notificación inmediata a las autoridades en caso de emergencias, lo que aumenta la eficiencia y la capacidad de reacción frente a situaciones críticas (Lucena, 2024). En el caso de la implementación de esta tecnología en las aulas de la carrera de Agropecuaria de FCVT, el uso de dispositivos IoT podría mejorar significativamente la seguridad, al integrar sistemas de control de acceso y monitoreo en tiempo real, asegurando un entorno más protegido para estudiantes y docentes, y contribuyendo a la protección de los recursos dentro de las instalaciones académicas.

2.6 Dispositivos IoT según las necesidades de seguridad en aulas

2.6.1 Control de acceso a las aulas

La implementación de sistemas IoT en el control de acceso a aulas ofrece múltiples beneficios, incluyendo la mejora en la seguridad, el monitoreo en tiempo real del acceso y la personalización del entorno de aprendizaje. Esta tecnología no solo optimiza la gestión de seguridad en instituciones educativas, sino que también facilita un control más efectivo sobre quién tiene acceso a las instalaciones. Según González y Pérez (2023), la integración de tecnologías IoT permite adaptar el ambiente educativo a las necesidades específicas de los estudiantes y el personal, promoviendo así un uso más eficiente de los recursos disponibles. Esto se traduce en un entorno más seguro y dinámico que puede responder mejor a las demandas del contexto académico.

2.6.2 Sistemas de vigilancia y monitoreo

Sequea Oliveros (2022) destaca que los sistemas de vigilancia y monitoreo basados en IoT han revolucionado la gestión de la seguridad en diversas instituciones, como en entornos educativos y corporativos. Estos sistemas ofrecen múltiples ventajas, entre ellas la integración de sensores avanzados, cámaras con visión nocturna y alertas en tiempo real, lo que optimiza la capacidad de respuesta ante incidentes de seguridad. Además, Sequea Oliveros menciona que la tecnología IoT facilita una instalación accesible y económica, permitiendo su implementación no solo en grandes corporaciones, sino también en hogares y pequeñas empresas.

2.6.3 Cerraduras electrónicas en dispositivos Iot

Las cerraduras electrónicas inteligentes son dispositivos avanzados de domótica que se instalan fácilmente en todo tipo de puertas, ya sean interiores o exteriores. Su característica más destacada es la capacidad de controlar el acceso de manera remota, autorizando o denegando la apertura de la puerta según la identidad de la persona que intenta ingresar. Este tipo de sistemas de seguridad ofrece una ventaja significativa sobre

las cerraduras tradicionales al permitir un control a distancia más eficiente y flexible. Además, existen diversos modelos de cerrojos inteligentes que varían en sus modos de utilización, permitiendo opciones como el acceso mediante huellas dactilares, códigos numéricos, tarjetas RFID o incluso a través de aplicaciones móviles, lo que aumenta aún más la seguridad y conveniencia para el usuario (Juanes, 2022).

2.7 Características indispensables de los dispositivos IoT

Según José María Escalante Fernández (2021), el Internet de las Cosas (IoT) y los dispositivos IoT se destacan por su capacidad para transformar diversos sectores, principalmente gracias a dos características esenciales: la inteligencia y la versatilidad. Estas características provienen de tres elementos clave que permiten el funcionamiento de los sistemas IoT y sus dispositivos asociados:

Tecnología embebida: los dispositivos IoT están equipados con sensores, microprocesadores, puertos de entrada y salida, memoria, entre otros componentes. Los avances tecnológicos en la miniaturización y el abaratamiento de la producción han permitido que estos sistemas embebidos sean más accesibles, favoreciendo su implementación masiva.

Conectividad: los dispositivos IoT se conectan entre sí mediante redes y protocolos de comunicación avanzados. Innovaciones como antenas más eficientes, el aprovechamiento del espectro electromagnético y el desarrollo de protocolos optimizados han sido determinantes para garantizar una conectividad fluida entre dispositivos de diferentes naturalezas.

Datos: los dispositivos IoT generan y comparten grandes cantidades de información, cuyo valor depende de una gestión adecuada. Tecnologías como el cloud computing y herramientas de big data facilitan el almacenamiento, análisis y aprovechamiento de estos datos, lo que incrementa su utilidad en diversos sectores, desde la salud hasta la agricultura o la industria (Escalante Fernández, 2021).

2.8 Tecnología de conectividad y su integración con IoT

2.9 Seguridad y privacidad en dispositivos IoT

De acuerdo con Kaspersky (2024), la tecnología IoT va más allá de los dispositivos tradicionales como computadoras o teléfonos inteligentes. Cualquier aparato con un interruptor de encendido y apagado tiene el potencial de conectarse a Internet y formar parte de la red IoT. Sin embargo, esta interconectividad genera un volumen considerable de datos de usuario, lo que incrementa las posibilidades de vulnerabilidad frente a ciberataques. Cuantos más dispositivos estén conectados, mayor es el riesgo de que los cibercriminales aprovechen brechas de seguridad para comprometer información sensible.

Las implicaciones de estas vulnerabilidades pueden ser devastadoras, especialmente porque la IoT afecta tanto sistemas virtuales como físicos. Por ejemplo, en los vehículos inteligentes, un ataque cibernético podría desactivar funciones clave de seguridad, poniendo en peligro la vida de sus ocupantes. En el ámbito industrial, conocido como la Internet Industrial de las Cosas (IIoT), un ciberataque puede paralizar procesos productivos o dañar físicamente maquinaria esencial.

En el sector salud, la integración de IoT, también denominada Internet de las Cosas Médicas (IoMT), podría exponer datos sensibles de los pacientes e incluso comprometer su bienestar físico. Por otro lado, en los hogares inteligentes, dispositivos vulnerables pueden ser explotados para vigilar o controlar remotamente entornos domésticos. Estos riesgos subrayan la necesidad de adoptar tecnologías de conectividad seguras que permitan la integración de IoT de manera confiable y eficiente, protegiendo tanto a los usuarios como a los sistemas en los que se implementa.

2.10 METODOLOGÍA PPIDIO aplicada a sistemas de seguridad IoT

Según Diego Fabricio Aguilar Peña (2021), la metodología PPDIOO ofrece un enfoque estructurado para la implementación y gestión de proyectos tecnológicos, dividiéndolos en fases específicas: preparación, planificación, diseño, implementación, operación y optimización. En el contexto de los sistemas de seguridad IoT, su aplicación no solo

facilita un desarrollo eficiente, sino que también asegura la adaptabilidad y sostenibilidad del sistema. Además, permite identificar posibles problemas desde etapas tempranas y establecer mejoras continuas, lo que contribuye a una mejor gestión de los recursos tecnológicos y humanos involucrados.

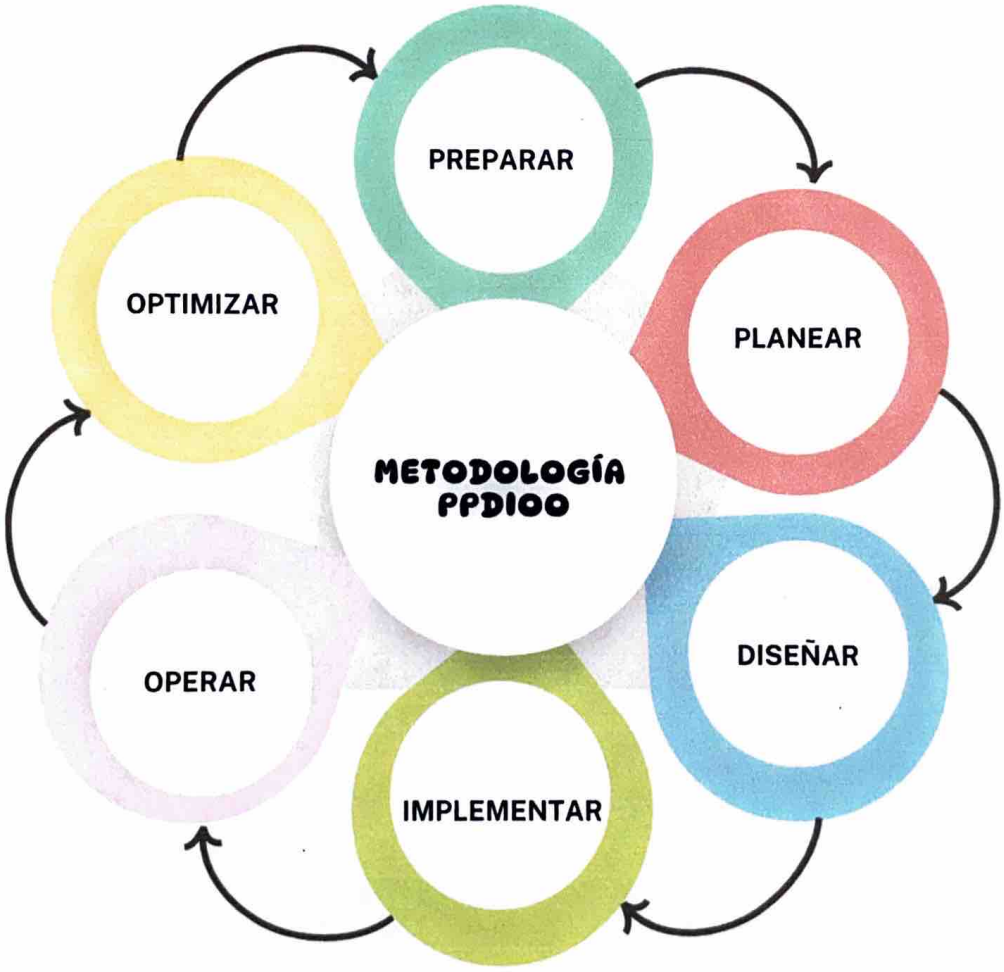


Figura No. 3. *Metodología PPDIO. Fuente propia.*

Este estudio tiene como objetivo establecer un enfoque organizado para las diferentes fases involucradas en la creación e implementación de un sistema de control de acceso, utilizando tecnología IoT, en las aulas de la Carrera de Agropecuaria de la FCVT. Aunque existen otros modelos competitivos, un análisis exhaustivo de las alternativas disponibles concluye que este modelo es el más adecuado para describir de manera efectiva el proyecto en cuestión.

En conclusión, la metodología PPDIOO proporciona una estructura sólida y bien definida para la implementación exitosa del sistema de seguridad. Asegura el cumplimiento de los requisitos del usuario, garantiza la protección del sistema y mejora su rendimiento a largo plazo.

Preparar:

En la fase de Preparar dentro de la metodología PPDIOO, se definirán los objetivos específicos del proyecto y se realizará un análisis detallado de los requisitos del sistema de control de acceso basado en tecnología IoT para las aulas de la Carrera de Agropecuaria de la FCVT. En esta etapa, se identificarán las necesidades de seguridad, funcionalidad y accesibilidad que deberá cumplir el sistema, tanto para los usuarios como para los administradores. Asimismo, se llevará a cabo una evaluación exhaustiva de los recursos disponibles, incluyendo infraestructura, personal y tecnologías, para asegurar que el proyecto pueda ser diseñado e implementado de manera eficiente. Esta fase inicial será crucial, ya que establecerá las bases para la correcta planificación del sistema de control de acceso, garantizando que todos los aspectos del proyecto estén alineados con los objetivos estratégicos y las capacidades de la institución.

Planificar:

En la fase de Planificar, se elaborará un plan detallado que describirá el enfoque para llevar a cabo la implementación del sistema de control de acceso basado en tecnología IoT en las aulas de la Carrera de Agropecuaria de la FCVT. En este plan, se identificarán los requisitos físicos, de hardware y software necesarios para el funcionamiento óptimo del sistema. Asimismo, se determinarán los recursos humanos, materiales y tecnológicos necesarios para su implementación. También se establecerá un cronograma de actividades que especificará las diferentes etapas del proyecto, desde la adquisición de los equipos hasta la instalación y configuración final del sistema, asegurando que todas las tareas se realicen de manera eficiente y dentro de los plazos establecidos.

Diseñar:

En la fase de Diseñar, se elaborará un diseño técnico detallado que guiará la implementación del sistema de seguridad basado en tecnología IoT en las aulas de la Carrera de Agropecuaria de la FCVT. En esta etapa, se planificará de manera meticulosa

cómo se llevarán a cabo las diferentes fases del proyecto, considerando cómo se integrarán de manera eficiente los dispositivos IoT en el entorno físico de las aulas. Se definirán los componentes técnicos necesarios, como los dispositivos de control de acceso y los sistemas de comunicación que permitirán el funcionamiento del sistema. El diseño se basará en los requisitos previamente establecidos, buscando asegurar que el sistema cumpla con las necesidades de seguridad y accesibilidad del personal docente y administrativo. Además, se garantizará la interoperabilidad de los dispositivos dentro del sistema global, asegurando su correcta operación y adaptabilidad a futuros ajustes. Este diseño tendrá como objetivo establecer una solución de seguridad eficaz, optimizando tanto la funcionalidad como la eficiencia del sistema en el contexto académico de la Carrera de Agropecuaria.

Implementar:

En la fase de Implementar, se procederá con la instalación y configuración de los dispositivos de seguridad basados en tecnología IoT, siguiendo el diseño previamente establecido para las aulas de la Carrera de Agropecuaria de la FCVT. En esta etapa, se instalarán los dispositivos de control de acceso y otros componentes necesarios para el sistema de seguridad, asegurando que estén correctamente configurados para su funcionamiento adecuado. Además, se realizarán pruebas exhaustivas para verificar que el sistema cumpla con los requisitos establecidos, evaluando aspectos como la conectividad entre los dispositivos, la interoperabilidad dentro del sistema y su capacidad de respuesta ante diferentes situaciones. Estas pruebas serán fundamentales para garantizar que el sistema de seguridad funcione de manera eficiente y segura antes de su implementación final.

Operar:

En la fase de Operar, se llevará a cabo la gestión y supervisión continua del sistema de seguridad basado en tecnología IoT en las aulas de la Carrera de Agropecuaria de la FCVT, con el objetivo de garantizar su correcto funcionamiento y mantenimiento a lo largo del tiempo. Durante esta etapa, se establecerá un monitoreo constante de todos los dispositivos de control de acceso y demás componentes del sistema, asegurando que operen según los parámetros definidos previamente. Se realizará un seguimiento detallado del rendimiento de cada dispositivo, verificando su disponibilidad y detectando

cualquier anomalía que pueda surgir. Además, se implementarán medidas de mantenimiento preventivo y correctivo para solucionar cualquier inconveniente de manera oportuna, asegurando que el sistema de seguridad continue funcionando de manera eficiente, manteniendo un nivel óptimo de seguridad en las aulas. Este monitoreo constante permitirá identificar áreas de mejora y optimizar el rendimiento del sistema, adaptándose a las necesidades cambiantes de la Carrera de Agropecuaria.

Optimizar:

En esta etapa, se realizará un análisis exhaustivo de los datos recopilados durante las fases de implementación y operación del sistema de control de acceso, con el fin de identificar áreas que requieran ajustes o mejoras. Este proceso incluirá la evaluación del desempeño de los dispositivos de seguridad, la calidad de la conectividad, la efectividad del sistema en cuanto a accesibilidad y su capacidad para mantener un nivel óptimo de seguridad en las aulas. Además, se revisarán los informes de funcionamiento y las experiencias de los usuarios (profesores y administradores) para detectar posibles problemas o limitaciones que puedan estar afectando el rendimiento del sistema. A partir de este análisis, se implementarán cambios y actualizaciones en los dispositivos y software, buscando optimizar la eficiencia, reducir posibles fallos y adaptarse a nuevas necesidades que puedan surgir en el entorno académico. Esta fase será clave para garantizar que el sistema se mantenga actualizado, eficiente y eficaz a lo largo del tiempo, mejorando la experiencia de los usuarios y la seguridad general del entorno educativo.

CAPÍTULO III

3.1 Marco Investigativo

3.2 Introducción

Esta investigación tiene como objetivo desarrollar un sistema automatizado para controlar el Control de entrada a la sala de profesores de la carrera de Agropecuaria en la Facultad de Ciencias de la Vida y Tecnología de la Uleam..

3.3 Tipo de investigación

3.3.1 Investigación bibliográfica

Según Ocampo (2019), en la sociedad actual estamos rodeados de una abundante cantidad de información, impulsada en gran medida por las Tecnologías de la Información y la Comunicación (TIC), que facilitan la transmisión y el acceso inmediato a contenido de todo tipo. Esta constante conexión nos permite estar al tanto de los acontecimientos globales en tiempo real. No obstante, el verdadero reto no reside en encontrar la información, ya que está al alcance de todos, sino en tener la habilidad de filtrar, clasificar y analizar el material de manera crítica, asegurando su veracidad y relevancia. Esta capacidad de discernimiento se ha vuelto esencial para evitar la desinformación y aprovechar efectivamente el conocimiento disponible.

3.3.2 Investigación de campo

Según Rus Arias (2020), la investigación de campo se centra en la recolección de datos directamente desde la realidad, permitiendo así la obtención de información de primera mano sobre un problema específico. Este método es fundamental para desarrollar investigaciones de tipo exploratorio, correlacional o mixto. En el contexto del método hipotético-deductivo, comúnmente empleado en el ámbito de la economía, la investigación de campo se presenta como un paso posterior al establecimiento de las hipótesis. Una vez definimos qué queremos investigar, es necesario realizar una recolección de datos en el terreno, lo cual constituye el trabajo de campo.

3.4 Métodos de investigación

Según Guevara Albán, Verdesoto Argüello y Castro Molina (2020), el método de investigación es un aspecto fundamental que determinará los pasos a seguir en el estudio, proporcionando una guía para el investigador. Este método incluye las técnicas y los enfoques que se utilizarán durante el proceso investigativo. En general, el tipo de investigación seleccionado influye en todos los aspectos del estudio, desde la elección de los instrumentos hasta la forma en que se analizarán los datos recopilados.

3.4.1 Método analítico

El método analítico aplicado en este estudio se enfoca en evaluar detalladamente los elementos clave asociados con la implementación de dispositivos de seguridad basados en tecnología IoT. Este enfoque incluye un análisis de los costos involucrados, tales como la adquisición de hardware, la instalación de los dispositivos, la integración de la tecnología en el entorno educativo y los gastos operativos continuos. Además, se deben considerar los beneficios que se esperan obtener, como la mejora en la seguridad de las aulas, la optimización de la gestión de accesos, la monitorización en tiempo real y la reducción de incidentes no deseados.

3.4.2 Método Histórico-Comparativo

En este enfoque, se analizan los sistemas de seguridad utilizados en el pasado y su efectividad en términos de costos, implementación, características técnicas y desempeño. Posteriormente, se comparan con las soluciones tecnológicas actuales, destacando las mejoras que se han producido en la tecnología IoT, como la conectividad, la integración de dispositivos inteligentes, la facilidad de manejo y la capacidad de automatización. A través de este análisis histórico, se busca identificar las ventajas y limitaciones de los sistemas antiguos y cómo las nuevas tecnologías pueden ofrecer mejores soluciones a los desafíos actuales en el ámbito académico.

También permite evaluar las lecciones aprendidas de implementaciones previas, lo cual es fundamental para elegir la solución más adecuada para la seguridad de las aulas en la Facultad de Ciencias de la Vida y Tecnología de la ULEAM, asegurando que el sistema propuesto no solo sea tecnológicamente avanzado, sino también viable y efectivo según las necesidades específicas de la institución.

3.4.3 Método inductivo-deductivo

Según Palmett Urzola (2020), el método deductivo parte de premisas generales o teorías abstractas, utilizando un proceso lógico y lineal para llegar a conclusiones específicas. En el caso de esta investigación, el enfoque deductivo puede utilizarse para aplicar teorías existentes sobre la seguridad en entornos educativos y la efectividad de las tecnologías

IoT, con el objetivo de validar si estos sistemas son adecuados para el contexto específico de las aulas de Agropecuaria.

Por otro lado, el método inductivo comienza con la recopilación de datos y observaciones empíricas en las aulas y otros espacios educativos similares. A través de la implementación de dispositivos IoT y su análisis en condiciones reales, se pueden generar patrones y conclusiones sobre el comportamiento de los sistemas de seguridad, la eficiencia en la gestión de accesos y la mejora en la seguridad. Los datos recolectados a partir de la experiencia práctica permitirán identificar los beneficios y limitaciones de la tecnología IoT en el entorno académico, generando nuevas teorías o principios generales que podrían aplicarse en el futuro en otros contextos similares.

Al combinar ambos enfoques, el método inductivo-deductivo permite partir de las teorías y conceptos preexistentes sobre seguridad y tecnología IoT, pero también se apoya en datos empíricos y observaciones para adaptar y refinar esas teorías según los resultados obtenidos en el contexto específico de la ULEAM. Este enfoque holístico ayuda a validar la viabilidad y efectividad de los dispositivos de seguridad IoT, además de permitir ajustes continuos en la implementación conforme se recogen nuevos datos y se observan patrones emergentes.

3.5 Herramientas de recolección de datos

3.5.1 Encuestas para recabar expectativas y requerimientos

Según Gómez (2023), una encuesta es un método de investigación que permite recolectar información, datos y opiniones a través de una serie de preguntas específicas, con el fin de hacer inferencias sobre una población o muestra representativa. En el presente estudio, se aplicó una encuesta para evaluar el nivel de conocimiento que poseen los docentes de la carrera de Agropecuaria de la Facultad de Ciencias de la Vida y Tecnología de la Universidad Laica Eloy Alfaro de Manabí sobre los sistemas automatizados de control de acceso. Esta encuesta incluyó un total de 15 preguntas, diseñadas para explorar en profundidad la comprensión y el grado de familiaridad de los docentes con estos sistemas.

3.5.2 Entrevistas

Según Mata Solís (2020), la entrevista se destaca como una herramienta clave en la recolección de datos cualitativos, ya que permite obtener una visión detallada y profunda sobre los temas de estudio. Este método no solo ofrece una amplia gama de información, sino que también captura datos subjetivos y matices interpersonales que exigen análisis interpretativos complejos. Gracias a su enfoque personalizado, las entrevistas logran captar las experiencias y perspectivas de los participantes, brindando así una comprensión integral del contexto investigado.

3.6 Fuentes de información de datos

3.6.1 Fuentes primarias

Como fuentes primarias en esta investigación, se realizaron encuestas dirigidas exclusivamente a los docentes de la carrera de Agropecuaria en la Facultad de Ciencias de la Vida y Tecnología de la ULEAM. El propósito de estas encuestas fue identificar los problemas y limitaciones del sistema de seguridad actual en las aulas, así como recopilar las opiniones y expectativas de los docentes sobre las características deseadas en un nuevo sistema automatizado basado en tecnología IoT.

Las preguntas fueron estructuradas para abordar aspectos clave como las dificultades de seguridad que enfrentan los docentes en el acceso a las aulas, las funciones esenciales que consideran necesarias en un sistema de control de acceso, y las expectativas sobre cómo un sistema automatizado podría mejorar la seguridad, optimizar la gestión de accesos y prevenir incidentes no deseados. Con esta información, se buscó obtener una visión detallada y realista de las necesidades de los docentes, lo que permitirá diseñar e implementar un sistema de seguridad adecuado que responda a las demandas específicas del entorno académico.

3.6.2 Fuentes secundarias

Como fuentes secundarias, se llevó a cabo una revisión exhaustiva de la literatura académica y técnica sobre sistemas de seguridad y control de acceso basados en tecnología IoT en entornos educativos. Este análisis incluyó artículos científicos, libros especializados y estudios previos que abordan el uso de dispositivos inteligentes para mejorar la seguridad en instituciones académicas. La revisión de literatura permitió comprender mejor las soluciones existentes, sus ventajas y limitaciones, así como las mejores prácticas implementadas en contextos similares.

Además, se realizó una investigación de mercado para conocer los productos y tecnologías actuales en el ámbito del control de acceso automatizado. Esta investigación incluyó el análisis de las características de los sistemas disponibles, sus costos de implementación, y las opiniones de usuarios y expertos sobre su efectividad en la mejora de la seguridad. La información obtenida de estas fuentes secundarias proporcionó una base sólida para identificar las tecnologías más adecuadas para el diseño del sistema de seguridad IoT en las aulas de la Facultad de Ciencias de la Vida y Tecnología de la ULEAM.

3.7 Mecanismos para recolección de datos

3.7.1 Segmentación

3.7.1.1 Segmentación de usuarios

La segmentación de usuarios en este proyecto implica identificar y clasificar a los docentes en grupos específicos según sus niveles de acceso y responsabilidades dentro de las aulas de la carrera de Agropecuaria. Este proceso de segmentación facilita que el sistema de control de acceso basado en IoT asigne permisos adecuados a cada grupo de docentes.

3.7.1.2 Segmentación de áreas de acceso

Esto puede aplicarse a la división de las aulas en zonas con distintos niveles de acceso mediante el sistema de control de acceso basado en tecnología IoT. Por ejemplo, algunos docentes tendrían permisos para acceder a áreas básicas del aula, mientras que otros, dependiendo de sus responsabilidades y roles específicos, podrían acceder también a zonas adicionales, como laboratorios, áreas de almacenamiento de materiales o salas con equipo especializado. Este enfoque permite un control más seguro y adecuado de los espacios, asegurando que cada docente acceda solo a las áreas necesarias según su función dentro del proyecto.

3.7.2 Población y tamaño de la muestra

3.7.2.1 Población

La población que se aborda en este estudio incluye a los profesores de la carrera de Agropecuaria de la Facultad de Ciencias de la Vida y Tecnología en la Universidad Laica Eloy Alfaro de Manabí (ULEAM). Este grupo representa a quienes están más directamente involucrados en el uso y supervisión de las aulas en dicha carrera. Según los datos actuales para el año 2024, la carrera cuenta con alrededor de 52 docentes, quienes tienen un rol importante en la gestión de estos espacios y cuyos aportes serán esenciales para evaluar las necesidades y expectativas respecto a la implementación de un sistema de seguridad automatizado basado en tecnología IoT.

3.7.2.2 Muestra

La muestra es una parte representativa de la población, seleccionada de manera que mantenga las mismas características generales de esta. Su propósito es permitir el análisis y obtención de resultados aplicables al total de la población sin necesidad de estudiar a todos sus integrantes. Según Condori-Ojeda (2020), la muestra representa un subconjunto significativo del universo de estudio, asegurando que las conclusiones obtenidas sean válidas y reflejen las condiciones del grupo completo. Esta técnica facilita el estudio de poblaciones extensas de forma práctica y precisa.

3.7.3 Técnica de muestreo

Según Lerma Meza et al. (2020), el muestreo consiste en una serie de pasos diseñados para asegurar la veracidad y precisión de los datos obtenidos en una investigación. Este proceso permite la selección de una muestra representativa de la población total, de modo que los resultados puedan reflejar las características particulares del grupo de estudio. La segmentación dentro del muestreo asegura que los datos recopilados sean adecuados y relevantes, proporcionando una visión detallada y fiel de la realidad que se está investigando.

Formula general

Para este estudio, se seleccionará una muestra de 95 docentes a partir de una población total de 125 docentes, considerando un nivel de confianza del 95% y un margen de error del 5%. El cálculo del tamaño de la muestra se realizó aplicando la fórmula específica para poblaciones finitas, lo que garantiza que los datos obtenidos sean representativos y estadísticamente significativos para el análisis posterior

$$\frac{N * p * q * Z^2}{(N-1) * e^2 + p * q * Z^2}$$

Donde:

- **N** es el tamaño de la población (125 docentes).
- **p** es la proporción esperada (0.5).
- **q** es 1−p1 - p1−p.
- **Z** es el valor correspondiente al nivel de confianza (1.96 para un 95%).
- **e** es el margen de error (0.05).

Sustituyendo los valores

$$n = \frac{125 * 0.5 * 0.5 * (1.96)^2}{(125-1) * (0.05)^2 + 0.5 * 0.5 * (1.96)^2}$$

$$n = \frac{125 * 0.25 * 1.96^2}{124 * 0.0025 + 0.25 * 3.8416}$$

$$n = \frac{125 * 0.25 * 3.8416}{124 * 0.0025 + 0.25 * 3.8416}$$

$$n = \frac{125 * 0.25 * 3.8416}{0.31 + 0.9604}$$

$$n = \frac{120.05}{1.2704}$$

$$n = 94.50$$

El tamaño de muestra calculado es aproximadamente 94.5 docentes. Sin embargo, al redondear este resultado, se trabajará con una muestra de 95 docentes para garantizar la representatividad de los datos y cumplir con los parámetros establecidos.

3.7.4 Análisis de las herramientas de recolección de información

Con base en la información recopilada, se diseñó un banco de preguntas que sirve como una herramienta esencial para estructurar la investigación, lo que facilita el análisis y la interpretación de los resultados obtenidos. Según Cisneros Caicedo, Guevara García, Urdánigo Cedeño y Garcés Bravo (2022), el uso de las TICs ha revolucionado los procesos investigativos, al permitir la recolección de datos más precisa y rápida mediante herramientas digitales. Estas tecnologías también mejoran la colaboración, gestionan grandes volúmenes de datos de manera eficiente y optimizan la calidad y transparencia de las investigaciones. Además, este enfoque promueve una mejor organización de los proyectos, permitiendo un análisis más detallado y accesible.

3.8 Presentación y descripción de los resultados obtenidos

A continuación, se procederá a mostrar el conjunto de preguntas y los resultados obtenidos mediante el proceso de tabulación, tomando como base la muestra seleccionada de docentes de la carrera de Agropecuaria, que forman parte de la Facultad de Ciencias de la Vida y Tecnología en la Universidad Laica Eloy Alfaro de Manabí. Este estudio busca proporcionar un análisis detallado de las opiniones y experiencias de los profesores respecto a los temas evaluados, permitiendo identificar patrones y perspectivas relevantes que puedan contribuir al desarrollo académico y profesional dentro de la facultad. Asimismo, este análisis ofrecerá insumos valiosos para futuras investigaciones y mejoras en el ámbito educativo.

En el análisis e interpretación de esta etapa, se presentan diversos aspectos y preguntas que surgieron, los cuales se detallan y explican en la siguiente tabla.

Tabla 1: Plan de análisis e interpretación de datos

¿Quién?	¿Cómo?	¿Cuándo?	¿Dónde?
Desarrolladores: Loor Mendoza Kevin José Oviedo Insuasti Dayana Samantha	Encuestas realizadas a los docentes de la Facultad de Ciencias de la Vida y Tecnologías de la carrera de Agropecuaria.	Agosto del 2024	Manta-Manabí

Nota. Fuente: Elaboración propia de los autores.

Pregunta 1:

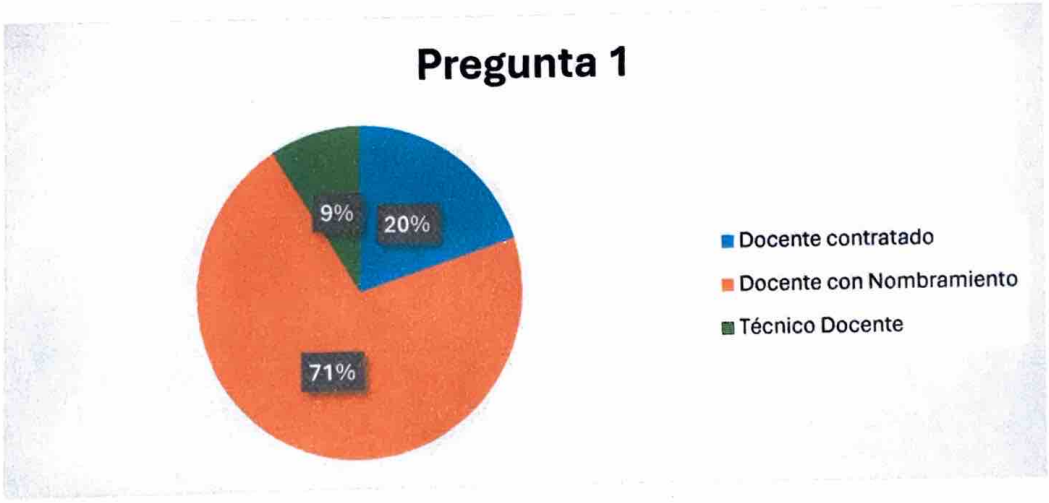
¿Cuál es su condición de docente en la Carrera de Agropecuaria de la FCVT?

- Docente contratado
- Docente con Nombramiento
- Técnico Docente

Tabla 2: **Tabulación de la pregunta 1 – Encuesta aplicada a los docentes de la Facultad de Ciencias de la Vida y Tecnologías de la carrera de Agropecuaria.**

Opciones	Frecuencia	Porcentaje
Docente Contratado	19	20,00%
Docente con Nombramiento	67	71,00%
Técnico Docente	9	9,00%
TOTAL	**95**	**100%**

Nota. Fuente: Encuesta aplicada a los docentes de la Facultad de Ciencias de la Vida y Tecnologías de la carrera de Agropecuaria.



y permanencia en el cuerpo docente. Por otro lado, un porcentaje menor (20%) corresponde a Docentes Contratados, quienes desempeñan un rol complementario en la estructura educativa. Finalmente, un pequeño porcentaje (9%) pertenece a la categoría de Técnico Docente, representando un grupo más específico dentro del sistema académico.

Este análisis proporciona una perspectiva detallada de la distribución del personal docente en relación con su rol en la facultad. Esta información es clave para entender las dinámicas laborales y su relación con la implementación de dispositivos de seguridad

basados en tecnología IoT. Por ejemplo, la predominancia de docentes con nombramiento puede facilitar el uso constante de los dispositivos en las aulas, mientras que los grupos de docentes contratados y técnicos docentes pueden aportar perspectivas específicas o especializadas en este proceso.

La diversidad en las categorías docentes también pone en evidencia la importancia de considerar las necesidades y responsabilidades de cada grupo para maximizar la efectividad de la tecnología IoT en el contexto educativo.

Pregunta 2:

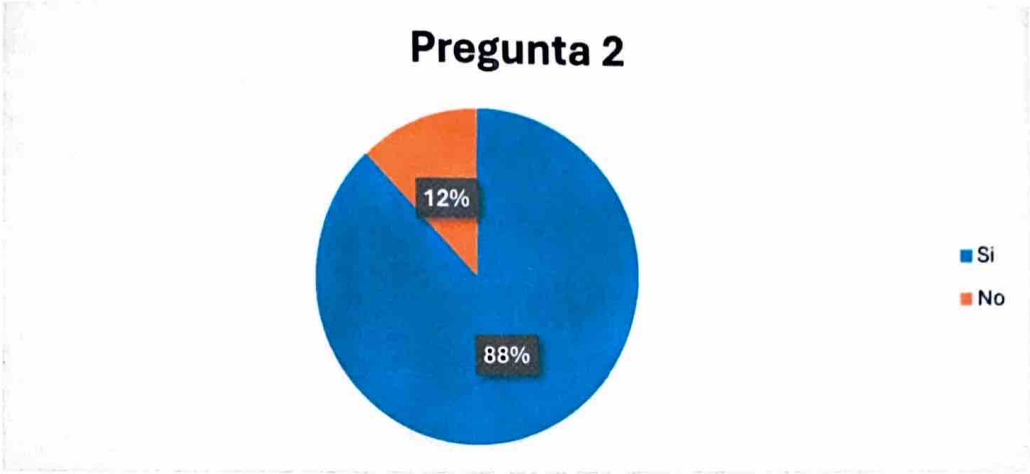
¿Está familiarizado con los dispositivos de seguridad basados en tecnología IoT?

- Sí
- No

Tabla 3: **Tabulación de la pregunta 2 – Encuesta aplicada a los docentes de la Facultad de Ciencias de la Vida y Tecnologías de la carrera de Agropecuaria.**

Opciones	Frecuencia	Porcentaje
Si	84	88,00%
No	11	12,00%
TOTAL	**95**	**100%**

Nota. Fuente: Encuesta aplicada a los docentes de la Facultad de Ciencias de la Vida y Tecnologías de la carrera de Agropecuaria.



Análisis:

Este resultado indica que un alto porcentaje (88%) de los docentes encuestados en la Carrera de Agropecuaria de la Facultad de Ciencias de la Vida y Tecnologías de la ULEAM están familiarizados con los dispositivos de seguridad basados en tecnología IoT. Este nivel de aceptación generalizada refleja que la temática es bien recibida por la mayoría, lo cual puede facilitar la implementación de estas tecnologías en las aulas.

Un porcentaje menor (12%) de los docentes no está familiarizado con esta tecnología. En conjunto, los resultados destacan que la tecnología IoT cuenta con una buena aceptación dentro de la comunidad docente, lo que representa un punto de partida favorable para la ejecución del proyecto propuesto en el diseño e implementación de estos dispositivos en las aulas de la carrera.

Pregunta 3:

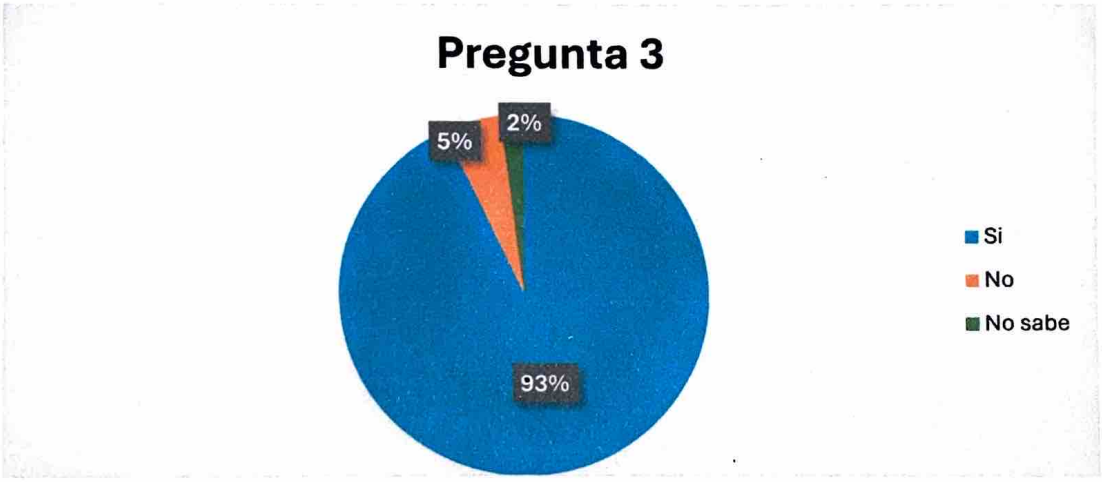
¿Conoce algún sistema de control de acceso biométrico?

- Sí
- No
- No sabe

Tabla 4: **Tabulación de la pregunta 3 – Encuesta aplicada a los docentes de la Facultad de Ciencias de la Vida y Tecnologías de la carrera de Agropecuaria.**

Opciones	Frecuencia	Porcentaje
Si	88	93,00%
No	5	5,00%
No sabe	2	2,00%
TOTAL	**95**	**100%**

Nota. Fuente: Encuesta aplicada a los docentes de la Facultad de Ciencias de la Vida y Tecnologías de la carrera de Agropecuaria.



Análisis:

Los resultados obtenidos en esta pregunta reflejan que un 93% de los docentes encuestados en la Carrera de Agropecuaria de la Facultad de Ciencias de la Vida y Tecnologías de la ULEAM están familiarizados con los sistemas de control de acceso biométrico. Este alto nivel de conocimiento indica que los docentes poseen una buena base en cuanto a tecnologías relacionadas con la seguridad, lo que representa una ventaja para la implementación de dispositivos basados en IoT en las aulas.

Por otro lado, un porcentaje menor, equivalente al 7% de los encuestados, se divide entre quienes no conocen esta tecnología (5%) y quienes no están seguros (2%). Este pequeño grupo refleja que, si bien la mayoría está familiarizada con la temática.

Los resultados destacan una gran apertura y aceptación hacia las tecnologías de seguridad, lo que constituye un entorno favorable para el desarrollo del proyecto

propuesto, permitiendo proyectar una implementación exitosa de los dispositivos IoT en las aulas de la carrera.

Pregunta 4:

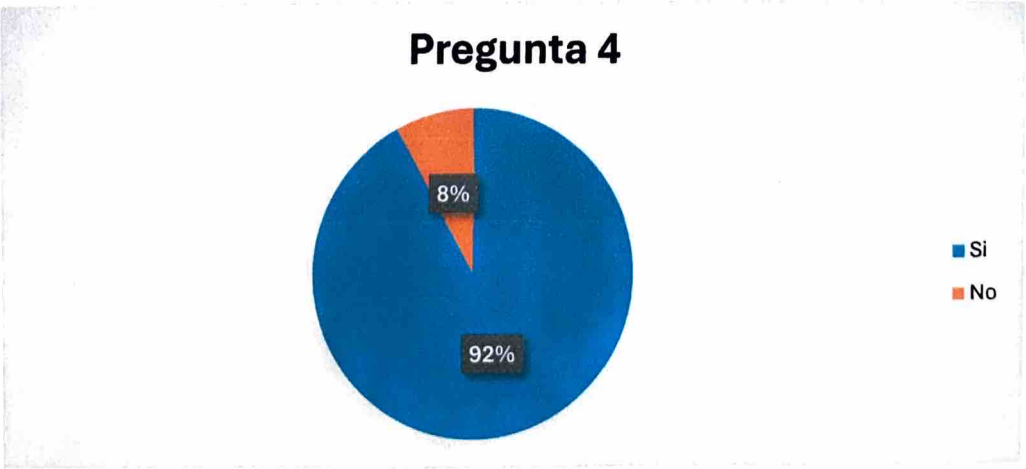
¿Ha utilizado alguna vez un sistema de control de acceso biométrico?

- Sí
- No

Tabla 5: **Tabulación de la pregunta 4 – Encuesta aplicada a los docentes de la Facultad de Ciencias de la Vida y Tecnologías de la carrera de Agropecuaria.**

Opciones	Frecuencia	Porcentaje
Si	87	92,00%
No	8	8,00%
TOTAL	**95**	**100%**

Nota. Fuente: Encuesta aplicada a los docentes de la Facultad de Ciencias de la Vida y Tecnologías de la carrera de Agropecuaria.



Análisis

El análisis de esta pregunta muestra que un 92% de los docentes encuestados en la Carrera de Agropecuaria de la Facultad de Ciencias de la Vida y Tecnologías de la ULEAM ha tenido experiencia previa en el uso de sistemas de control de acceso biométrico. Esto indica un nivel significativo de interacción práctica con esta tecnología dentro de la comunidad docente, lo que representa un punto favorable para la implementación de dispositivos IoT orientados a la seguridad.

Por otro lado, un 8% de los encuestados mencionó no haber utilizado nunca esta tecnología. Esto señala que, aunque la mayoría cuenta con experiencia, existe una pequeña parte que no ha interactuado directamente con este tipo de sistemas.

En general, estos resultados reflejan que la familiaridad de los docentes con tecnologías biométricas constituye un apoyo significativo para llevar a cabo la implementación del proyecto planteado.

Pregunta 5:

En caso afirmativo, ¿qué tecnología de verificación de identidad le parece más fácil de utilizar?

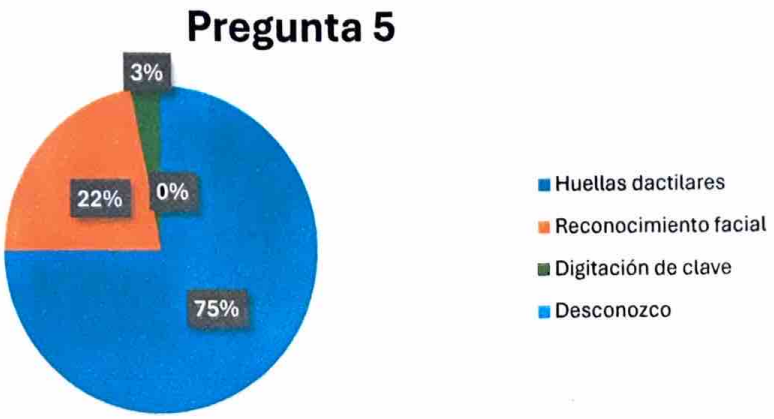
- Huellas dactilares
- Reconocimiento facial
- Digitación de clave
- Desconozco

Tabla 6: **Tabulación de la pregunta 5 – Encuesta aplicada a los docentes de la Facultad de Ciencias de la Vida y Tecnologías de la carrera de Agropecuaria.**

Opciones	Frecuencia	Porcentaje
Huellas dactilares	65	75,00%
Reconocimiento facial	19	22,00%
Digitación de clave	3	3,00%

Desconozco	0	0,00%
TOTAL	**95**	**100%**

Nota. Fuente: Encuesta aplicada a los docentes de la Facultad de Ciencias de la Vida y Tecnologías de la carrera de Agropecuaria.



Análisis

Los resultados muestran que la mayoría de los docentes encuestados en la Carrera de Agropecuaria de la Facultad de Ciencias de la Vida y Tecnologías de la ULEAM considera que el reconocimiento por huellas dactilares es la tecnología más fácil de utilizar, con un 75% de las respuestas. Este resultado destaca que esta tecnología es ampliamente percibida como práctica y accesible, lo que probablemente se deba a su simplicidad y familiaridad.

El reconocimiento facial ocupa el segundo lugar, con un 22% de las preferencias. Aunque menos mencionado, este método también es valorado por su facilidad, especialmente al no requerir contacto físico. Por otro lado, la digitación de claves fue seleccionada únicamente por un 3% de los encuestados, lo que podría indicar que este sistema es considerado menos intuitivo o más propenso a errores en comparación con las opciones biométricas.

Es importante resaltar que ningún docente indicó desconocer estas tecnologías, lo que sugiere que existe un conocimiento generalizado sobre los métodos de verificación de identidad. Estos resultados son alentadores para la implementación de sistemas de

seguridad IoT, ya que las tecnologías más aceptadas, como las huellas dactilares y el reconocimiento facial, pueden integrarse de manera efectiva en el proyecto propuesto.

Pregunta 6:

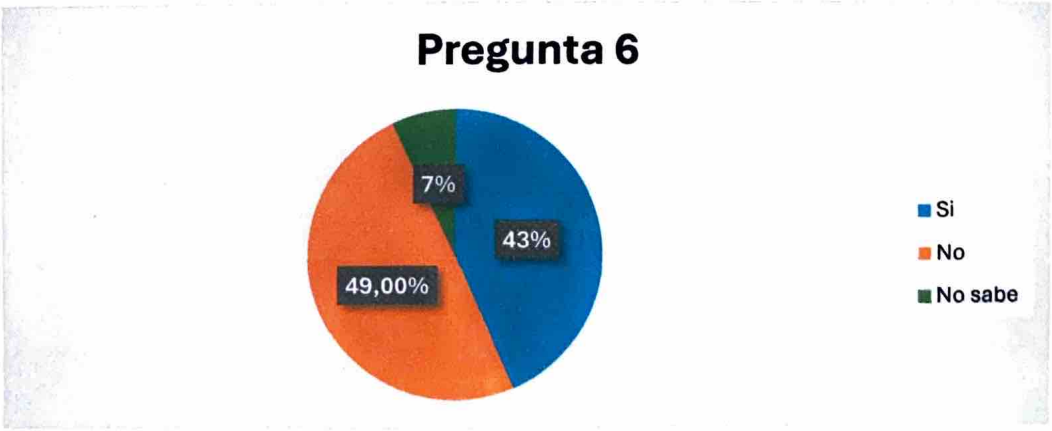
¿Considera que las actuales medidas de seguridad en la sala de docentes de la Carrera de Agropecuaria son eficaces?

- Sí
- No
- No sabe

***Tabla* 7: Tabulación de la pregunta 6 – Encuesta aplicada a los docentes de la Facultad de Ciencias de la Vida y Tecnologías de la carrera de Agropecuaria.**

Opciones	Frecuencia	Porcentaje
Si	41	43,00%
No	47	49,00%
No sabe	7	7,00%
TOTAL	**95**	**100%**

Nota. Fuente: Encuesta aplicada a los docentes de la Facultad de Ciencias de la Vida y Tecnologías de la carrera de Agropecuaria.



Análisis

Los resultados indican que solo el 43% de los docentes encuestados considera que las medidas de seguridad actuales en la sala de docentes son eficaces. Este porcentaje, aunque significativo, demuestra que menos de la mitad de los encuestados percibe las medidas existentes como suficientes para garantizar la seguridad.

Por otro lado, el 49% de los docentes considera que las medidas actuales no son eficaces, reflejando una preocupación predominante sobre la capacidad de las medidas vigentes para proteger adecuadamente el espacio. Además, un 7% de los encuestados manifestó no tener una opinión formada al respecto.

En conjunto, estos resultados resaltan la necesidad de mejorar las medidas de seguridad en la sala de docentes, dado que la percepción generalizada es que las actuales no cumplen con las expectativas. Esto refuerza la relevancia y pertinencia del proyecto de diseño e implementación de dispositivos de seguridad basados en tecnología IoT, ya que su desarrollo podría responder directamente a las preocupaciones identificadas por los docentes.

Pregunta 7:

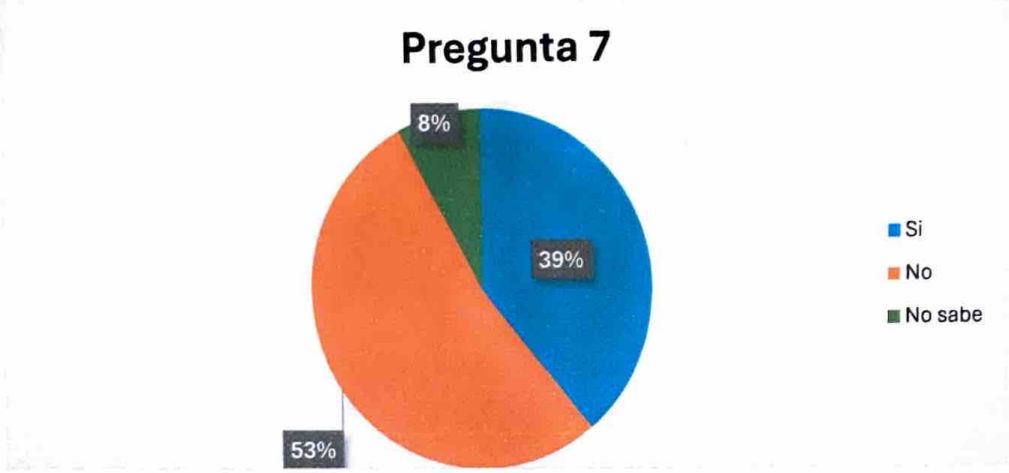
¿Conoce si existe algún dispositivo de control de acceso biométrico en la sala de docentes de la Carrera de Agropecuaria?

- Sí
- No
- No sabe

***Tabla* 8: Tabulación de la pregunta 7 – Encuesta aplicada a los docentes de la Facultad de Ciencias de la Vida y Tecnologías de la carrera de Agropecuaria.**

Opciones	Frecuencia	Porcentaje
Si	37	39,00%
No	50	53,00%
No sabe	8	8,00%
TOTAL	**95**	**100%**

Nota. Fuente: Encuesta aplicada a los docentes de la Facultad de Ciencias de la Vida y Tecnologías de la carrera de Agropecuaria.



Análisis

Los resultados muestran que solo el 39% de los docentes encuestados tiene conocimiento de la existencia de un dispositivo de control de acceso biométrico en la sala de docentes de la Carrera de Agropecuaria. Este porcentaje indica que, aunque algunos docentes están al tanto de su presencia, no representa a la mayoría.

El 53% de los encuestados señaló que no existe un dispositivo de este tipo, mientras que un 8% indicó no estar seguro. Esto evidencia una falta de claridad o desconocimiento generalizado respecto a la implementación de estas tecnologías en el espacio mencionado.

Estos resultados ponen de manifiesto una oportunidad para fortalecer y visibilizar las medidas de seguridad tecnológica en la institución. Además, refuerzan la pertinencia del proyecto de diseño e implementación de dispositivos de seguridad basados en tecnología IoT, ya que podría satisfacer esta necesidad y generar mayor confianza y conocimiento entre los docentes respecto a las medidas de seguridad implementadas.

Pregunta 8:

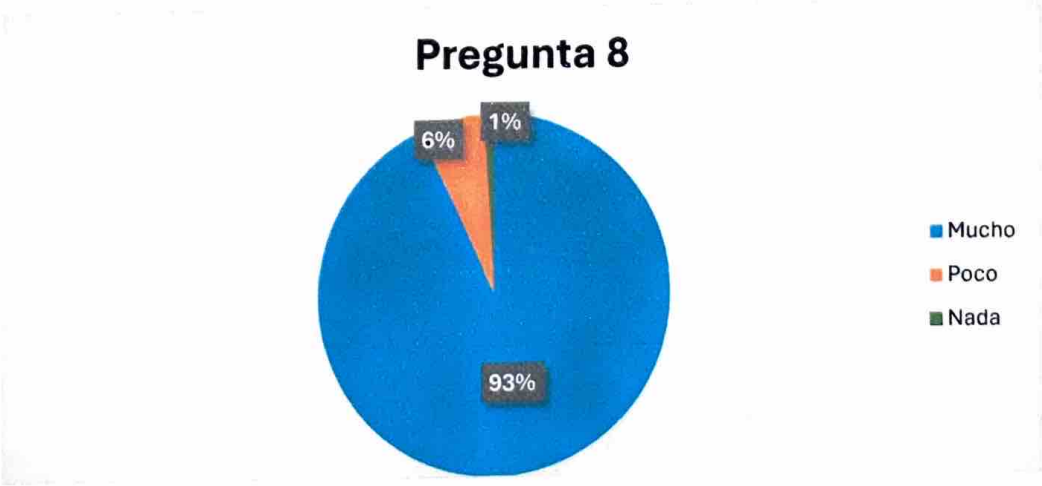
¿Cree que la implementación de un sistema de control de acceso biométrico en la sala de docentes brindaría un entorno seguro para los docentes?

- Mucho
- Poco
- Nada

***Tabla* 9: Tabulación de la pregunta 8 – Encuesta aplicada a los docentes de la Facultad de Ciencias de la Vida y Tecnologías de la carrera de Agropecuaria.**

Opciones	Frecuencia	Porcentaje
Mucho	88	93,00%
Poco	6	6,00%
Nada	1	1,00%
TOTAL	**95**	**100%**

Nota. Fuente: Encuesta aplicada a los docentes de la Facultad de Ciencias de la Vida y Tecnologías de la carrera de Agropecuaria.



Análisis

Los resultados muestran que un abrumador 93% de los docentes encuestados considera que la implementación de un sistema de control de acceso biométrico en la sala de docentes brindaría un entorno seguro. Este alto porcentaje refleja una percepción positiva generalizada sobre la efectividad de este tipo de tecnología para mejorar la seguridad en el área.

Solo el 6% de los encuestados considera que el sistema lo haría poco seguro, mientras que solo un 1% cree que no aportaría ninguna mejora en cuanto a seguridad. Este bajo porcentaje de respuestas negativas sugiere que la mayoría de los docentes tiene confianza en la capacidad de los sistemas biométricos para garantizar un entorno más protegido.

Dado el fuerte respaldo que obtiene esta propuesta, se puede concluir que existe una alta disposición para adoptar tecnologías innovadoras que refuercen la seguridad en el espacio docente. Esto convierte la implementación de un sistema de control de acceso biométrico en una opción bien valorada por la comunidad docente.

Pregunta 9:

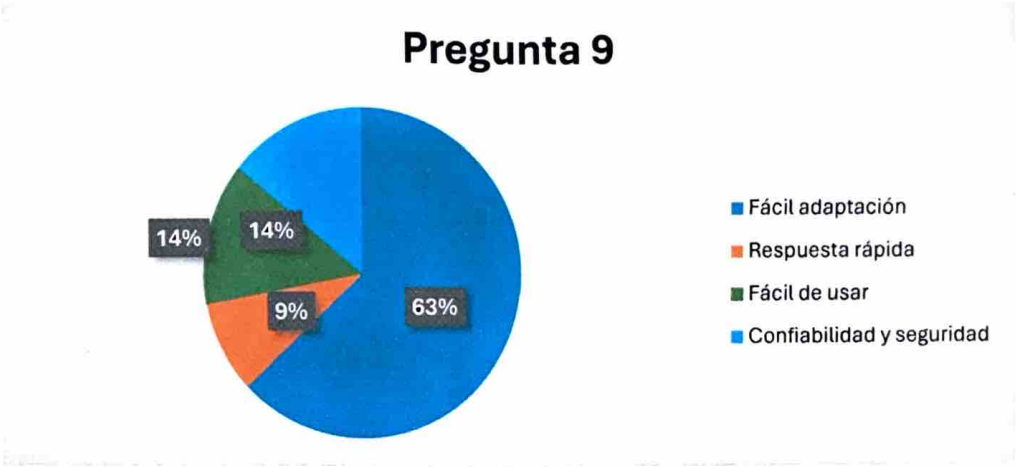
¿Qué características considera importantes en un sistema de control de acceso biométrico?

- Fácil adaptación
- Respuesta rápida
- Fácil de usar
- Confiabilidad y seguridad

Tabla 10: **Tabulación de la pregunta 9 – Encuesta aplicada a los docentes de la Facultad de Ciencias de la Vida y Tecnologías de la carrera de Agropecuaria.**

Opciones	Frecuencia	Porcentaje
Fácil adaptación	60	63,00%
Respuesta rápida	9	9,00%
Fácil de usar	13	14,00%
Confiabilidad y seguridad	13	14,00%
TOTAL	**95**	**100%**

Nota. Fuente: Encuesta aplicada a los docentes de la Facultad de Ciencias de la Vida y Tecnologías de la carrera de Agropecuaria.



Análisis

Los resultados muestran que la facilidad de adaptación es la característica más valorada por los docentes, con un 63% de los encuestados indicando que esta es la cualidad más importante en un sistema de control de acceso biométrico. Este alto porcentaje sugiere que la mayoría de los docentes prefiere un sistema que se integre fácilmente al entorno existente sin generar complicaciones.

En segundo lugar, tanto la facilidad de uso como la confiabilidad y seguridad fueron mencionadas por 14% de los encuestados cada una. Esto refleja que los docentes también consideran esenciales que el sistema sea intuitivo y seguro, garantizando tanto su operatividad como la protección de los usuarios.

Por último, la respuesta rápida fue seleccionada por un 9% de los encuestados, lo que indica que, aunque es un factor importante, no tiene la misma prioridad que las características mencionadas anteriormente. los resultados indican que los docentes consideran como características primordiales la facilidad de adaptación del sistema, seguida de su facilidad de uso y fiabilidad. Estos factores son esenciales para garantizar que el sistema sea aceptado y funcione de manera eficiente dentro del entorno académico, facilitando su implementación y uso por parte de los docentes.

Pregunta 10:

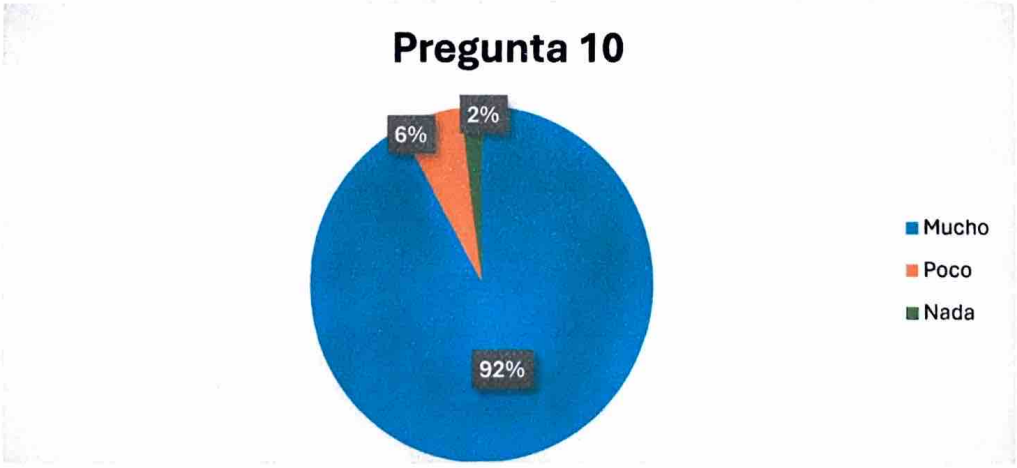
¿Considera que la implementación de un sistema de control de acceso biométrico mejoraría la seguridad y la productividad en el entorno de trabajo?

- Mucho
- Poco
- Nada

Tabla 11: **Tabulación de la pregunta 10 – Encuesta aplicada a los docentes de la Facultad de Ciencias de la Vida y Tecnologías de la carrera de Agropecuaria.**

Opciones	Frecuencia	Porcentaje
Mucho	87	92,00%
Poco	6	6,00%
Nada	2	2,00%
TOTAL	**95**	**100%**

Nota. Fuente: Encuesta aplicada a los docentes de la Facultad de Ciencias de la Vida y Tecnologías de la carrera de Agropecuaria.



Análisis

Los resultados muestran que un 92% de los docentes encuestados considera que la implementación de un sistema de control de acceso biométrico basado en tecnología IoT mejoraría considerablemente tanto la seguridad como la productividad en el entorno de

trabajo. Este alto porcentaje refleja una percepción positiva generalizada sobre cómo la tecnología de control biométrico puede fortalecer la seguridad de los espacios docentes y, a su vez, mejorar la eficiencia en el acceso a las aulas y áreas restringidas.

Un 6% de los encuestados opina que la mejora sería poca, lo que podría señalar dudas sobre el impacto directo de la tecnología en la productividad diaria, o una posible falta de conocimiento sobre cómo la biometría podría optimizar estos aspectos. Solo un 2% de los encuestados cree que la implementación no tendría ningún efecto sobre la seguridad ni la productividad, lo que representa una mínima discrepancia frente al consenso general.

Estos resultados son especialmente relevantes para el diseño e implementación de dispositivos de seguridad IoT en las aulas de la Carrera de Agropecuaria, ya que subrayan la alta aceptación y disposición de los docentes hacia la mejora de la seguridad y la optimización del entorno laboral mediante la adopción de tecnologías avanzadas.

Pregunta 11:

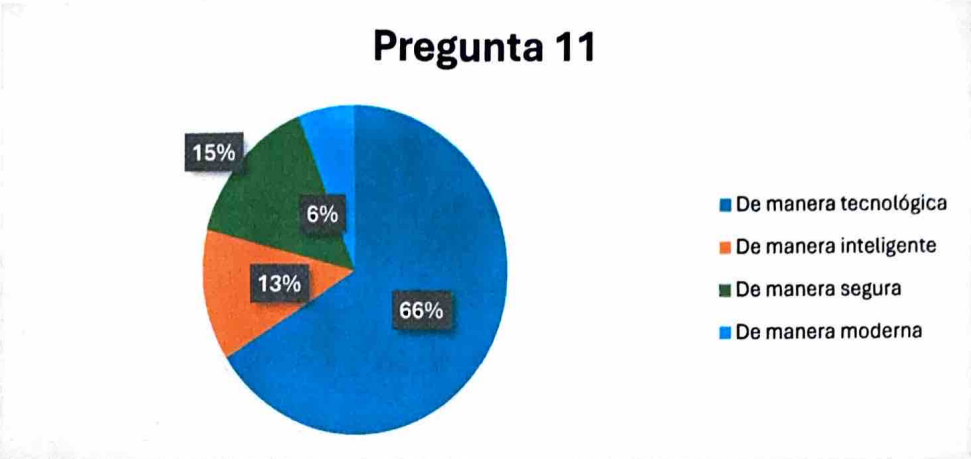
¿Piensa que el uso de nuevas tecnologías, como un sistema de control de acceso biométrico, sería una innovación en la sala de docentes?

- De manera tecnológica
- De manera inteligente
- De manera segura
- De manera moderna

Tabla 12: **Tabulación de la pregunta 11 – Encuesta aplicada a los docentes de la Facultad de Ciencias de la Vida y Tecnologías de la carrera de Agropecuaria.**

Opciones	Frecuencia	Porcentaje
De manera tecnológica	63	66,00%
De manera inteligente	12	13,00%
De manera segura	14	15,00%
De manera moderna	6	6,00%
TOTAL	**95**	**100%**

Nota. Fuente: Encuesta aplicada a los docentes de la Facultad de Ciencias de la Vida y Tecnologías de la carrera de Agropecuaria.



Análisis

Los resultados muestran que un 66% de los docentes considera que la implementación de un sistema de control de acceso biométrico basado en tecnología IoT en la sala de docentes representaría una innovación tecnológica. Este alto porcentaje resalta la percepción de que la adopción de nuevas tecnologías sería un avance significativo en cuanto a la modernización y optimización de los espacios académicos, lo que subraya el interés por la integración de soluciones tecnológicas avanzadas en el ámbito educativo.

Un 15% de los encuestados cree que la innovación sería de manera segura, lo que refleja que una parte de los docentes valora principalmente la seguridad que estos sistemas pueden ofrecer, entendiendo que la tecnología biométrica podría garantizar un control más efectivo y confiable en el acceso a la sala de docentes.

Por otro lado, un 13% optó por la opción de manera inteligente, sugiriendo que algunos docentes perciben que este tipo de tecnología puede traer mejoras inteligentes en la gestión de acceso, con sistemas más eficientes y menos propensos a errores humanos.

Finalmente, solo un 6% considera que la implementación sería de manera moderna, lo que podría reflejar una visión enfocada más en la actualización estética o funcional de los sistemas, pero con una menor prioridad en cuanto a sus aplicaciones tecnológicas o de seguridad.

los resultados subrayan que la mayoría de los docentes ve la innovación tecnológica como el aspecto más relevante de la implementación de un sistema de control de acceso biométrico, lo cual respalda el diseño e implementación de dispositivos IoT en las aulas como un paso importante hacia la modernización de los métodos de seguridad y gestión en el entorno académico.

Pregunta 12:

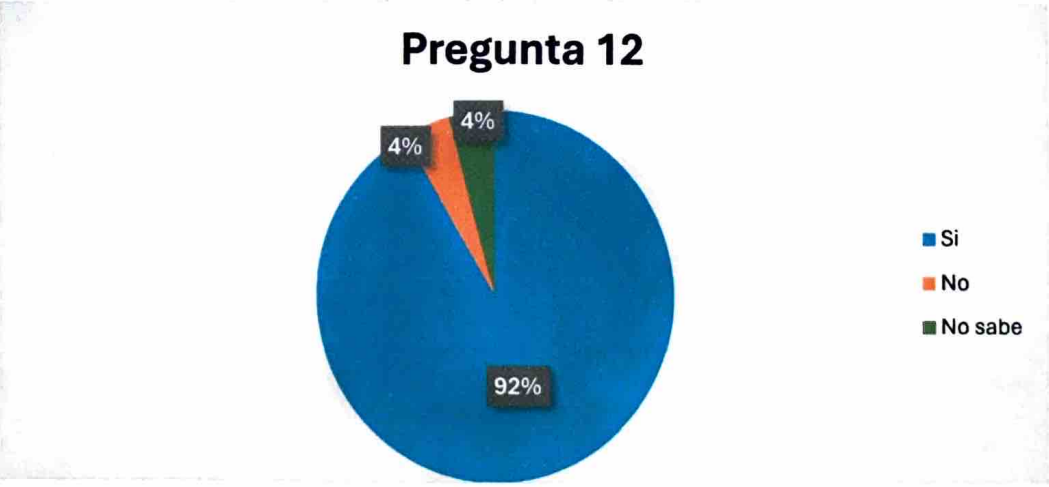
¿Cree que el uso de dispositivos IoT puede mejorar la seguridad en las aulas de la Carrera de Agropecuaria?

- Sí
- No
- No sabe

Tabla 13: **Tabulación de la pregunta 12 – Encuesta aplicada a los docentes de la Facultad de Ciencias de la Vida y Tecnologías de la carrera de Agropecuaria.**

Opciones	Frecuencia	Porcentaje
Si	87	92,00%
No	4	4,00%
No sabe	4	4,00%
TOTAL	**95**	**100%**

Nota. Fuente: Encuesta aplicada a los docentes de la Facultad de Ciencias de la Vida y Tecnologías de la carrera de Agropecuaria.



Análisis

Los resultados indican una respuesta mayoritariamente positiva por parte de los docentes, ya que un 92% considera que el uso de dispositivos IoT puede mejorar significativamente la seguridad en las aulas. Este alto porcentaje refleja la confianza que la comunidad académica deposita en estas tecnologías como una solución eficaz para optimizar las condiciones de seguridad en el entorno educativo.

Por otro lado, tanto el 4% de los encuestados que respondió "No" como el 4% que indicó "No sabe" constituyen una minoría significativa. Estas respuestas podrían estar relacionadas con dudas sobre el funcionamiento práctico de los dispositivos IoT o con una falta de información acerca de sus capacidades y beneficios. Estas percepciones destacan la necesidad de una mayor sensibilización y orientación sobre el tema, para abordar las inquietudes y aumentar la aceptación general de la tecnología.

Pregunta 13:

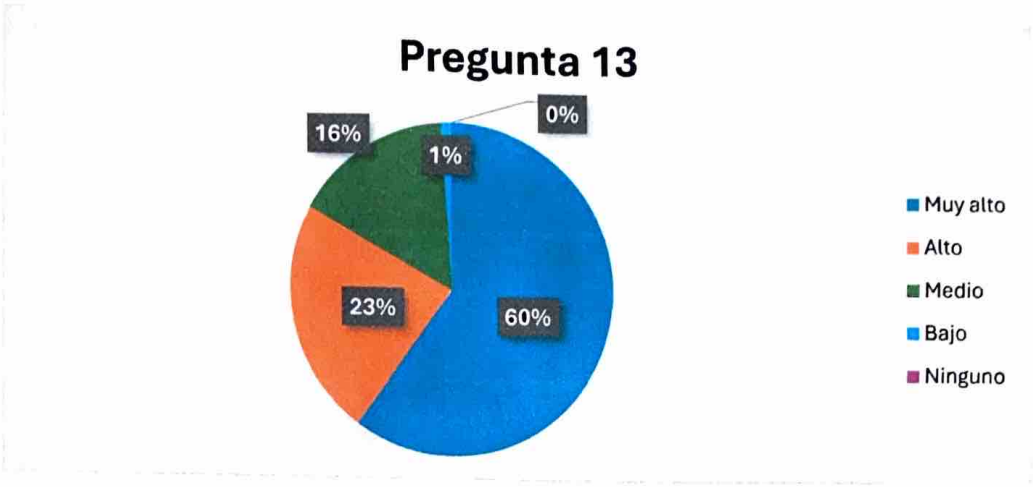
¿Qué nivel de seguridad considera que se obtendría con la implementación de dispositivos IoT en las aulas?

- Muy alto
- Alto
- Medio
- Bajo
- Ninguno

Tabla 14: **Tabulación de la pregunta 13 – Encuesta aplicada a los docentes de la Facultad de Ciencias de la Vida y Tecnologías de la carrera de Agropecuaria.**

Opciones	Frecuencia	Porcentaje
Muy alto	57	60,00%
Alto	22	23,00%
Medio	15	16,00%
Bajo	1	1,00%
Ninguno	0	0,00%
TOTAL	**95**	**100%**

Nota. Fuente: Encuesta aplicada a los docentes de la Facultad de Ciencias de la Vida y Tecnologías de la carrera de Agropecuaria.



Análisis

Los resultados muestran que un 60% de los docentes considera que el nivel de interés por la implementación de un sistema de control de acceso biométrico es muy alto. Este porcentaje indica que la mayoría de los docentes está altamente motivada por la posibilidad de integrar esta tecnología en la sala de docentes, lo que resalta el gran potencial de aceptación del proyecto propuesto.

Un 23% de los encuestados califica su interés como alto, lo que sugiere que una parte significativa también ve con buenos ojos la idea de implementar un sistema de control biométrico, aunque con algo menos de entusiasmo que el grupo anterior.

El 16% restante considera que su interés es medio, lo que refleja una actitud algo más neutral, con docentes que podrían necesitar más información o garantías sobre los beneficios de la tecnología para comprometerse completamente.

Solo un 1% de los encuestados considera que su interés es bajo, lo cual indica que, en general, el proyecto cuenta con una alta predisposición por parte de los docentes. Además, el hecho de que ninguno de los encuestados haya calificado el interés como ninguno refuerza la idea de que, a pesar de algunas diferencias de grado, existe una gran disposición hacia la implementación de tecnología de control de acceso en el ámbito académico.

Pregunta 14:

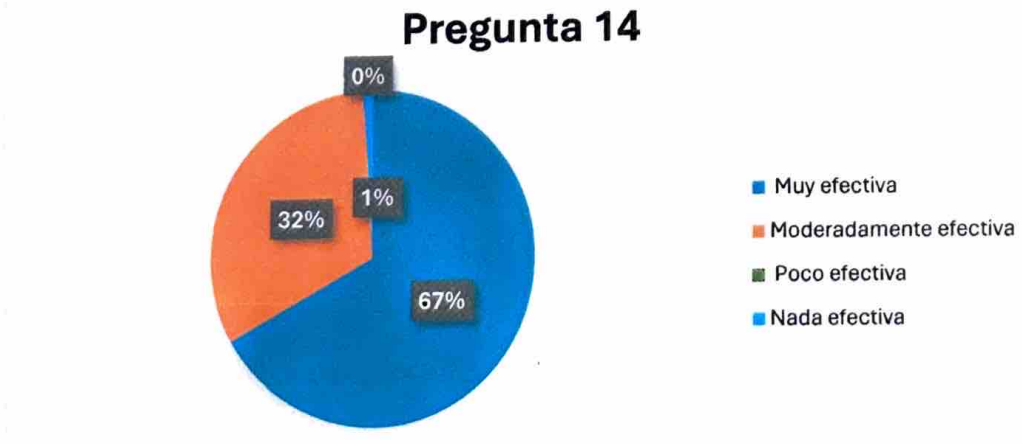
¿Qué tan efectiva considera que sería la implementación de dispositivos de seguridad basados en tecnología IoT para mejorar la seguridad en las aulas de la Carrera de Agropecuaria?

- Muy efectiva
- Moderadamente efectiva
- Poco efectiva
- Nada efectiva

Tabla 13: **Tabulación de la pregunta 14 – Encuesta aplicada a los docentes de la Facultad de Ciencias de la Vida y Tecnologías de la carrera de Agropecuaria.**

Opciones	Frecuencia	Porcentaje
Muy efectiva	64	67,00%
Moderadamente efectiva	30	32,00%
Poco efectiva	0	0,00%
Nada efectiva	1	6,00%
TOTAL	**95**	**100%**

Nota. Fuente: Encuesta aplicada a los docentes de la "acceso a la sala de profesores de la carrera de Agropecuaria, en la Facultad de Ciencias de la Vida y Tecnología de la Uleam FCVT" de la carrera de Agropecuaria.



Análisis

Los resultados revelan que una gran mayoría de los docentes, un 67%, considera que la implementación de dispositivos de seguridad basados en tecnología IoT sería muy

efectiva para mejorar la seguridad en las aulas de la Carrera de Agropecuaria. Este alto porcentaje refleja una percepción positiva sobre la capacidad de la tecnología IoT para optimizar la seguridad en los espacios académicos, sugiriendo que los docentes confían en que este sistema podría ser una herramienta eficaz para controlar el acceso y proteger los recursos de las aulas.

Un 32% de los encuestados opina que la implementación sería moderadamente efectiva, lo que muestra que, aunque estos docentes reconocen los beneficios de la tecnología, pueden tener algunas reservas o dudas sobre su efectividad total, posiblemente debido a factores como la experiencia previa con tecnologías similares o la falta de información detallada sobre su funcionamiento.

Un 6% considera que la implementación sería nada efectiva, lo que representa una pequeña minoría que no ve viabilidad en el uso de tecnologías IoT en este contexto específico. Es interesante notar que ningún docente consideró que la tecnología sería poco efectiva, lo que refuerza la tendencia general de aceptación positiva hacia la solución propuesta.

Pregunta 15:

¿Cuáles considera que serían los beneficios más importantes de implementar dispositivos de seguridad basados en tecnología IoT en las aulas de la Carrera de Agropecuaria?

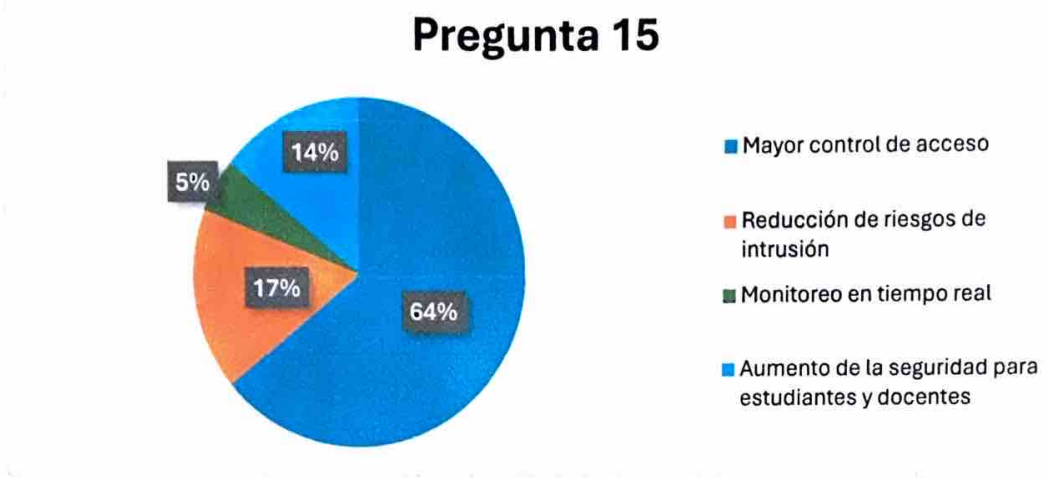
- Mayor control de acceso
- Reducción de riesgos de intrusión
- Monitoreo en tiempo real
- Aumento de la seguridad para estudiantes y docentes

Tabla 14: **Tabulación de la pregunta 15 – Encuesta aplicada a los docentes de la Facultad de Ciencias de la Vida y Tecnologías de la carrera de Agropecuaria.**

Opciones	Frecuencia	Porcentaje
Mayor control de acceso	61	64,00%
Reducción de riesgos de intrusión	16	17,00%
Monitoreo en tiempo real	5	5,00%

Aumento de la seguridad para estudiantes y docentes	13	13,00%
TOTAL	**95**	**100%**

Nota. Fuente: Encuesta aplicada a los docentes de la "FCVT".



Análisis

Los resultados muestran que la mayoría de los docentes considera que el principal beneficio de la implementación de dispositivos IoT es un mayor control de acceso, con un 64% de las respuestas en esta dirección. Esto subraya la importancia que los encuestados le dan a gestionar de manera eficiente quién entra a las aulas, un factor clave para asegurar que solo las personas autorizadas accedan a estos espacios, lo cual contribuiría a un entorno más seguro para todos.

En segundo lugar, un 17% de los docentes ve en la reducción de riesgos de intrusión un beneficio primordial. Este resultado indica que, además de controlar el acceso, los docentes reconocen la necesidad de implementar medidas que prevengan cualquier intento no autorizado de ingresar a las aulas, protegiendo así el ambiente académico.

El monitoreo en tiempo real es considerado un beneficio por el 5% de los encuestados. Esto resalta el valor que algunos docentes le dan a la capacidad de supervisar continuamente la seguridad en las aulas, permitiendo una intervención rápida ante cualquier anomalía que se pueda detectar en el momento.

Un 13% de los docentes destaca el incremento de la seguridad tanto para los estudiantes como para los docentes como uno de los principales beneficios. Este dato refleja el deseo

de contar con un ambiente más seguro y protegido para todos los miembros de la comunidad educativa, promoviendo un clima de confianza y tranquilidad en el aula.

La gestión del acceso es vista como el beneficio más relevante de los dispositivos IoT, lo cual destaca el interés de los docentes en fortalecer la seguridad física dentro de las aulas. La implementación de esta tecnología es percibida como una estrategia efectiva para prevenir intrusiones y mejorar el entorno educativo.

CAPÍTULO IV

4.1 Introducción

El presente capitulo enmarca la descripción del prototipo del dispositivo IoT. Tendrá un enfoque de la construcción del prototipo de seguridad para el control domótico que eleva a la seguridad física tanto a estudiantes, docentes y bienes materiales de la facultad Agropecuaria.

Los dispositivos de IoT al estar interconectados pueden enviar alertas inmediatas al personal de seguridad o al docente responsable ante cualquier situación de riesgo, permitiendo una respuesta rápida y efectiva. La tecnología domótica también brinda la posibilidad de registrar y analizar datos en el tiempo lo cual facilita la implementación de mejoras de seguridad.

4.2 Descripción del diseño esquemático del dispositivo IoT

En la figura No.4. podemos observar el diagrama de caso de uso y las interacciones que tiene el usuario y el usuario administrador con el sistema de la cerradura inteligente.

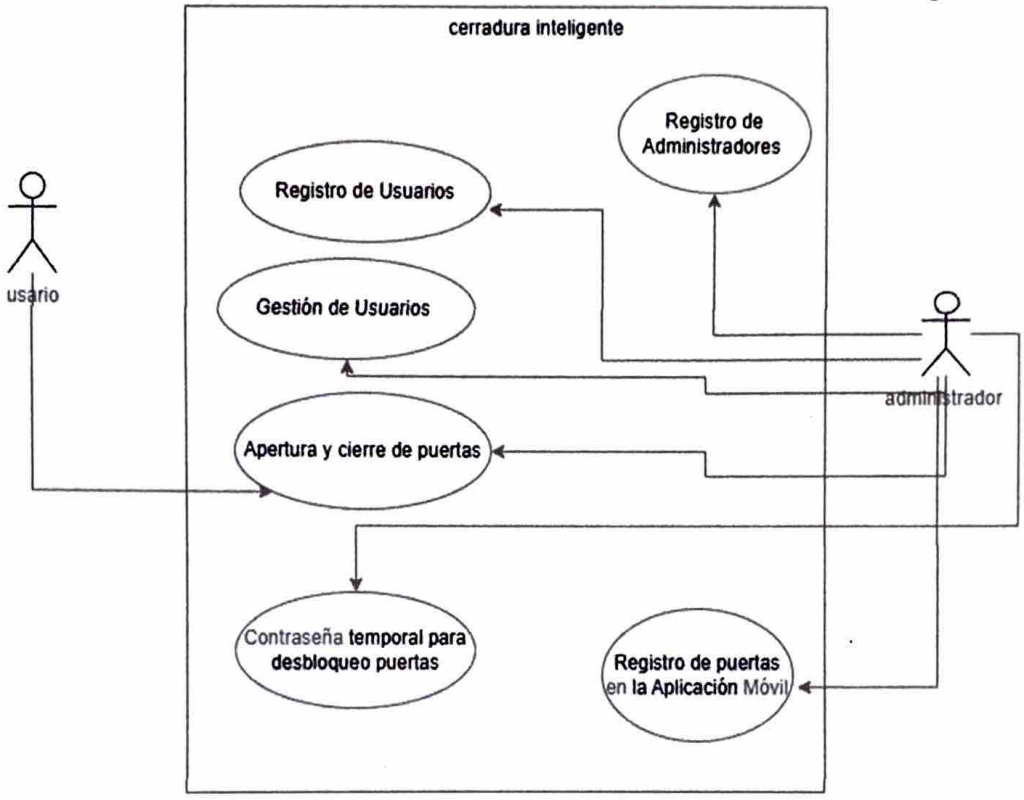


Figura No. 4. Diagrama Caso de Uso de usuarios de la cerradura inteligente.

En la figura No.5. podremos observar el diagrama de flujo del dispositivo IoT de la cerradura inteligente que describe la funcionalidad de la seguridad de la cerradura. Esta muestra los pasos que realiza al comenzar a utilizar el dispositivo. Al interactuar con el dispositivo IoT la funcionalidad interna que está programada va a primero a la autenticación de usuario si no está autenticado se emitirá una alarma y se enviara a la aplicación móvil el mensaje de alerta si no, es asi, el sistema ara una autenticación mediante Huella, PIN O RFID el controlador verifica y manda una señal para ver si es Usuario Externo o Administrador, si es Usuario Administrador tendrá una condición de agregar nuevos usuarios si no pasa directamente a abrir la cerradura inteligente y poder ingresar a la aula al contrario si es Usuario Externo solo se apertura abrir la cerradura

inteligente y ingresar a la aula. Tras un período de tiempo definido, la cerradura se cierra automáticamente.

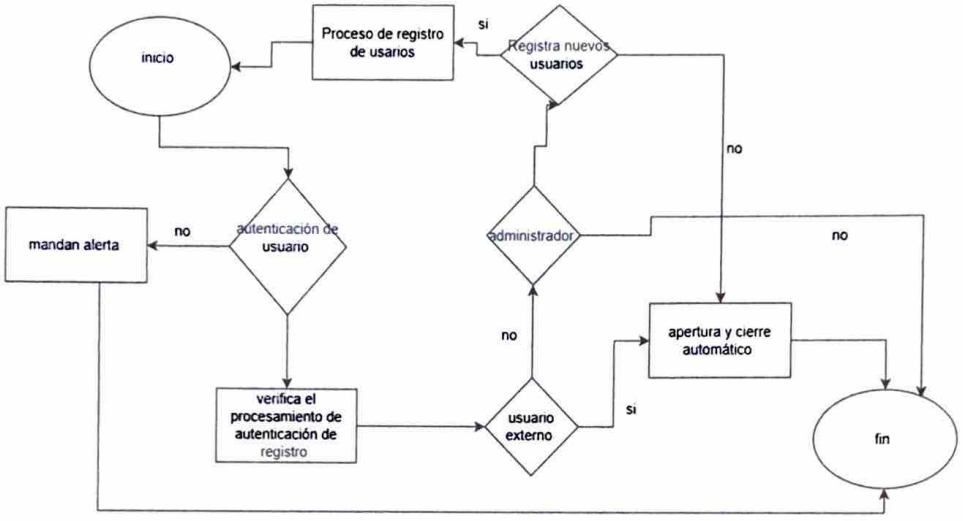


***Figura No. 5. Diagrama** de flujo de la cerradura inteligente.*

A continuación, se muestra la estructura y función de la cerradura inteligente en la figura N_o.6. se verá cómo está determinado cada componente.

- **1.Tornillo de la tapa de la batería:** Asegura la tapa de la batería en su posición, evitando que se mueva o suelte.
- **2.Tornillo de la columna de conexión:** Mantiene la columna de conexión fija en el cuerpo de la cerradura, contribuyendo a la estabilidad de la estructura.
- **3.Tapa de la batería:** Cubierta que protege el compartimento de la batería, permitiendo un acceso rápido para cambiar la batería cuando sea necesario.
- **4.Botón de reinicio:** Permite reiniciar el sistema del dispositivo en caso de fallos o para restablecer ajustes.
- **5.Manija trasera:** Manija en la parte posterior del dispositivo, diseñada para facilitar el agarre y manipulación desde el lado interior.
- **6.Panel trasero:** Parte posterior que cubre y protege los componentes internos del dispositivo.

- **7.Botón de bloqueo interno:** Controla el mecanismo de bloqueo desde el interior, permitiendo asegurar la puerta sin necesidad de llave externa.
- **8.Tornillos del cuerpo de cerradura:** Aseguran el cuerpo de la cerradura a la puerta, garantizando la integridad del dispositivo en su lugar.
- **9.Pestillo:** Mecanismo que mantiene la puerta cerrada al encajar en la ranura de la estructura de la puerta.
- **10.Cerrojo:** Elemento de seguridad que asegura la puerta cuando el mecanismo de bloqueo está activado.
- **11.Cuerpo de la cerradura:** La estructura principal de la cerradura, que alberga todos los componentes mecánicos y electrónicos.
- **12.Cuadrillo de acero:** Pieza de conexión entre la manija y el mecanismo de la cerradura, asegurando la transmisión de movimiento.
- **13.Cable de conexión:** Cable que facilita la transmisión de energía o datos entre diferentes partes del dispositivo.
- **14.Columna de conexión:** Estructura que organiza y soporta los cables y conexiones dentro de la cerradura.
- **15.Panel frontal:** Parte frontal de la cerradura, que incluye los elementos de control y acceso al dispositivo.
- **16.Teclado numérico:** Dispositivo de entrada que permite introducir un código de acceso para desbloquear la cerradura.
- **17.Lector de tarjeta de acceso (NFC):** Permite la autenticación mediante el uso de una tarjeta de acceso compatible.
- **18.Manija frontal:** Manija situada en la parte exterior del dispositivo, que facilita la apertura desde el exterior.
- **19.Sensor de huella digital:** Mecanismo de seguridad que permite el acceso al dispositivo mediante reconocimiento de huellas dactilares.
- **20.Alimentación de emergencia:** Entrada que permite conectar una fuente de energía auxiliar en caso de que la batería interna esté descargada.
- **21.Entrada de la llave física:** Permite el acceso manual mediante una llave física, proporcionando un método de apertura alternativo.

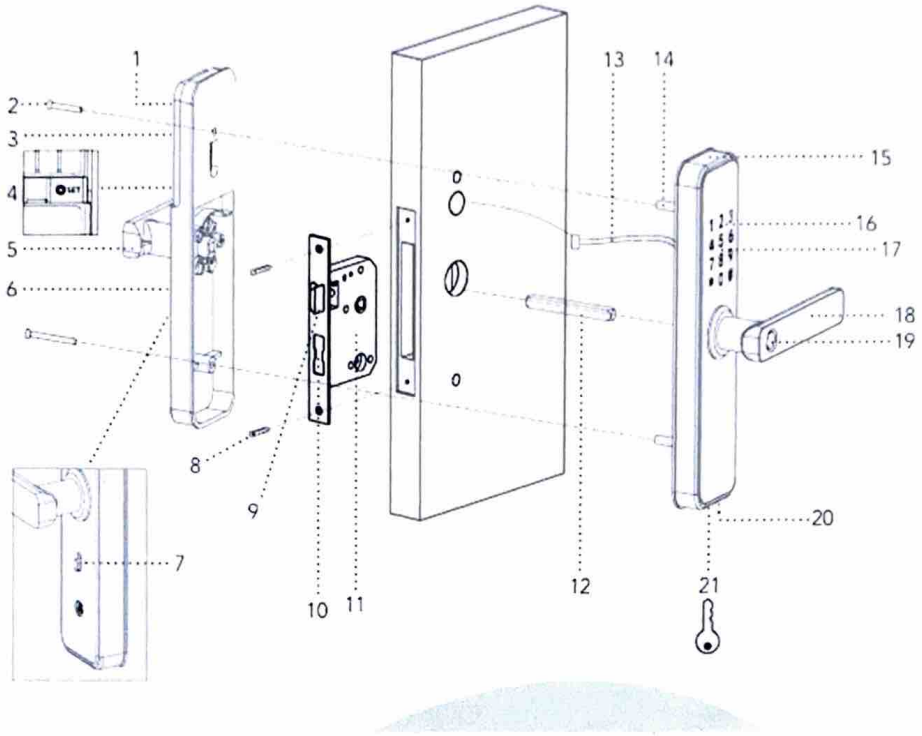


Figura No. 6. *Esquema de la cerradura inteligente* ***(Home, 2022)***.

4.2.1 Selección de componentes y sensores

Estos dispositivos de cerraduras inteligentes usan tecnologías inalámbricas, y en ciertos casos, se integran asistentes de voz como: Alexa, Google Assistant o Apple HomeKit. Ofreciendo el acceso sin llave mediante: PIN, NFC, RFID o incluso detectando dispositivos móviles o autorizados cercanos (Alarm, 2024).

Un sistema RFID consta de un lector y una etiqueta. Las etiquetas, de tamaño reducido, se pueden integrar en diferentes dispositivos. Están formadas por un microchip que almacena la información y una antena que transmite o recibe señales. Estas etiquetas almacenan los datos de identificación y suelen incluirse en tarjetas, permitiendo que el sistema las lea o actualice según sea necesario (Anónimo, 2022).

El dispositivo IoT ofrecen una conectividad para comunicarse con un dispositivo móvil o Tablet mediante:

Bluetooth

Es cerraduras se conectan al smartphone por Bluetooth, permitiendo abrir automáticamente al detectar la proximidad de un dispositivo autorizado. Aunque su alcance es limitado, son eficaces para el control de distancia cercana.

Wi-Fi

La conectividad Wi-Fi permiten controlar la cerradura de forma remota a través de una aplicación en el celular. ofreciendo al usuario la comodidad de gestionarla desde cualquier lugar con acceso a internet.

Protocolos de Conectividad Domótica

Algunas cerraduras utilizan un sistema de control domótico utilizando protocolos como: Z-Wave, Zigbee o HomeKit, permitiendo facilitar una mayor compatibilidad con otros dispositivos del hogar.

Sistemas Mixtos

Algunas cerraduras inteligentes son compatibles con distintos protocolos, aumentando así su compatibilidad e integración en diversos sistemas de hogar inteligente.

4.2.2 Arquitectura del sistema IoT de seguridad

En la figura No.7. se presenta una arquitectura o diseño del dispositivo de IoT que se va a implementar.

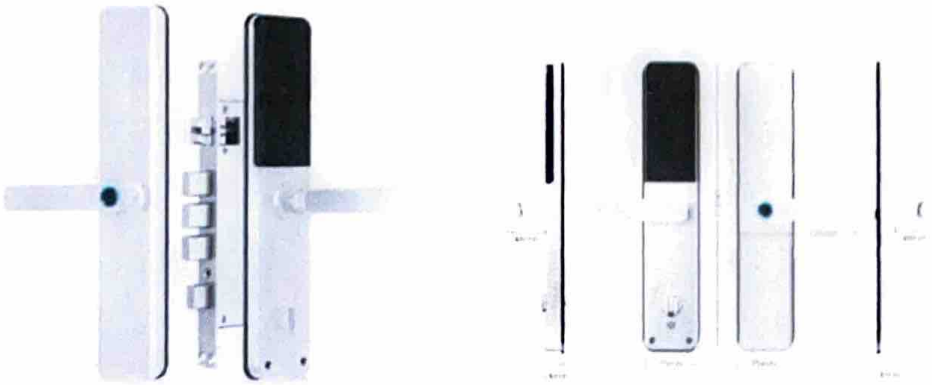


Figura No. 7. Esquema de la cerradura inteligente (McGrathLocks, 2024)

La funcionalidad del sistema consiste en almacenar información de los usuarios y sus huellas digitales en la memoria del lector, garantizando un buen control de acceso y seguridad en el dispositivo IoT, en las distintas aulas de la carrera de Agropecuaria de la FCVT "Facultad de Ciencias de la Vida y Tecnología de la Universidad Laica Eloy Alfaro de Manabí", para esto el sistema consiste en el módulo de acceso, este dispositivo de seguridad IoT conforma una arquitectura del módulo de acceso del sistema Como se muestra la figura No.8. Este dispositivo de seguridad IoT se basa en un módulo de acceso que verifica continuamente la presencia de una tarjeta o huella digital en su alcance. Si detecta una, lee la información para determinar si el usuario tiene autorización para ingresar.

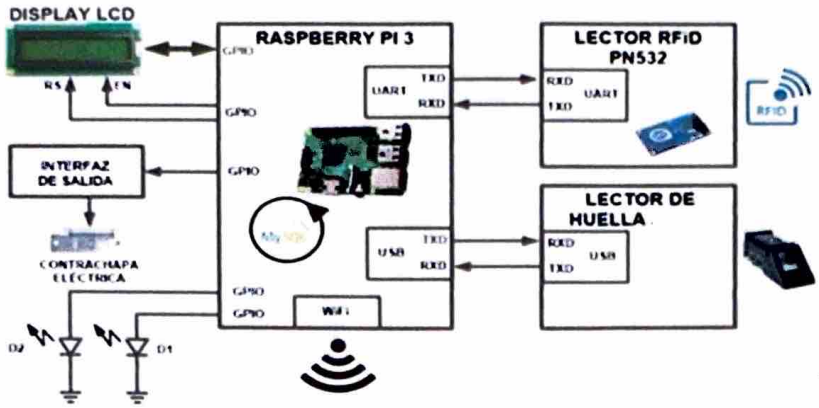


Figura No. 8. Diagrama del sistema de acceso ***(Luna, 2018).***

4.3 Implementación de los dispositivos en las aulas de Agropecuaria

Aquí en esta fase se lleva la instalación de todo lo diseñado y realizado en la etapa anterior. Se procede a identificar los requerimientos específicos del sistema automatizado de control de acceso. Se llevará a cabo una caracterización y evaluación exhaustiva de la infraestructura.

Figura No. 9. Dimensiones del dispositivo de control de acceso ***(Zoominformatica, 2024)***

En la implementación del dispositivo en las aulas de agropecuaria fue necesario realizar nuevos marcos ya que represento un desafío para montar uniformemente las cerraduras inteligentes, la que se optó a colocar nuevas puertas de aluminio para instalar el dispositivo que es la cerradura inteligente como se demuestra en la figura N_o.9.

4.3.1 Preparación del entorno para la instalación

Se planifico y gestionó el entorno para instalar las cerraduras inteligentes en las aulas de la carrera de Agropecuaria evaluando cada puerta y retirándolas figura N_o.10. se muestra las antiguas puertas que se encontraban en las aulas de Agropecuaria, realizando nuevas puertas de aluminio mostrado en la figura N_o.11. ya con sus respectivas dimensiones de la cerradura inteligente en cada puerta y colocadas mostrada en la figura N_o.12.

Figura No. 10. Puerta de la carrera de agropecuaria

Figura No. 11. Puerta realizada con las medidas y dimensiones de la cerradura inteligente

Figura No. 12. Colocado la cerradura inteligente en la puerta

En las instalaciones de la carrera de Agropecuaria, también, Se tomará en cuenta diversos factores identificables, tales como las conexiones de red para la conexión de las cerraduras inteligentes.

4.3.2 Proceso de implementación y configuración de los dispositivos

Una vez realizado la preparación del entorno en la carrera de Agropecuaria se da el proceso de implementación de las puertas en su ubicación designada en las aulas de la carrera figura N_o.13.

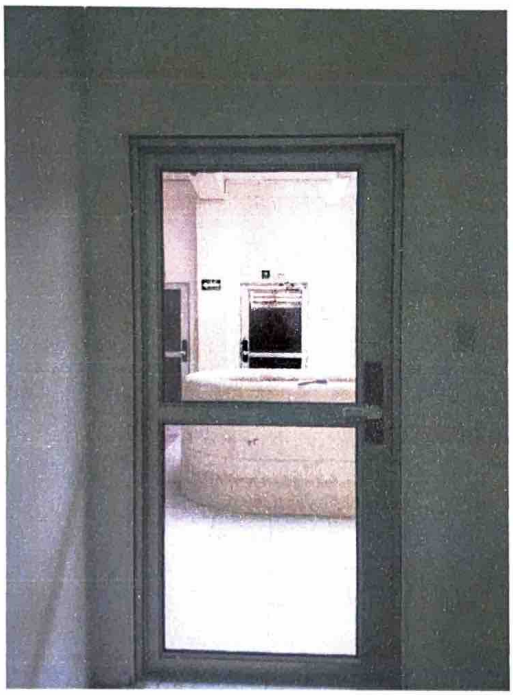


Figura No. 13. Puertas colocadas en la facultad

Para asegurar una buena implementación efectiva, se capacito a los encargados que tendrían el acceso a las aulas de agropecuaria y mediante se realizó a dar las llaves de seguridad aparte del ingreso de su huella en la cerradura inteligente. En caso de fallos en el dispositivo por motivos de carga o perdida de conexión para abrir la puerta mediante código desde el aplicativo móvil, se instruyó como operar manualmente como también el acceso no autorizado o alertas de seguridad al administrador como ver desde el aplicativo y hacer sus respectivos protocolos de seguridad dentro de la facultad.

4.4 Evaluación de la funcionalidad y efectividad de los dispositivos

Se llevo a cabo diversas pruebas para validar el correcto funcionamiento de las cerraduras inteligentes instalas en las aulas de la carrera de Agropecuaria.

Se aprobó la apertura y cierre de las cerraduras mediante la aplicación móvil en condición de red WI-FI optima y de baja intensidad y en pruebas de desconexión de la red, se activó correctamente el modo manual mediante huella digital o clave numérica.

Se simulo un intento de apertura forzada en una de las puertas activando una alerta al dispositivo móvil de administrador en un tiempo de 5.8 segundos desde la detención y emite una alerta el dispositivo de medio minuto. Se probo la resistencia ante intentos de acceso no autorizado mediante huellas no registradas y códigos incorrectos haciendo que el sistema bloque el acceso después de tres intentos fallidos consecutivos y envió de notificación al administrador en tiempo real.

4.5 Gastos de implementación

La fase de gastos de implementación se da a ver en la tabla los gastos realizados para la implementación de las cerraduras inteligentes.

Descripción	**Cantidad**	**Precio Unitario**	**Descuento**	**Extras**	**Envíos**	**Precio Total**
Cerraduras inteligentes	3	$ 110	$ 0	$ 12	$ 1	$ 343
puertas	3	$ 230	$ 0	$ 15	0	$ 705
Brazos	3	$ 30	$ 0	$ 0	0	$ 90
Pilas	6	$ 5.5	$ 0	$ 0	$ 7	$ 40
		$ 375.5	$ 0	$ 27	$ 8	$ 1.178

Tabla 15 gastos de implementación del proyecto

4.6 Optimización del sistema y posibles mejoras futuras

Durante la implementación de las cerraduras inteligentes se identificó algunas limitaciones que podría ser abordadas para optimizar su desempeño y funcionalidad si son necesarios, abordando problemas de rendimiento o ajustando la arquitectura para mejorar la eficiencia y resolver posibles desafíos.

Mejorar la infraestructura y conexión del sistema de control de acceso es crucial para garantizar su eficacia y seguridad. Al optimizar la conexión entre los dispositivos podemos superar los desafíos de independencia de control que actualmente enfrentamos. Esto implica interconectar los dispositivos mediante cableado confiable y eficiente consolidándolos en un único punto de control centralizado. Este enfoque no solo simplificaría la administración del sistema, sino que también aumentaría su capacidad de respuesta y capacidad de monitoreo. Además, al implementar redundancias y protocolos de seguridad adecuados, podemos mitigar los riesgos asociados con posibles fallas de conexión o intrusiones no autorizadas. En última instancia, una infraestructura de conexión mejorada no solo mejora la eficiencia operativa, sino que también fortalece la integridad y confiabilidad del sistema de control de acceso en su conjunto.

Conexión alámbrica

La conexión alámbrica destaca por su estabilidad y confiabilidad al transmitir datos, lo que la hace ideal para sistemas donde la seguridad es primordial, como el control de acceso. No se ve afectada por interferencias externas y reduce riesgos cibernéticos al no depender de señales inalámbricas. Según se muestra en la ilustración, las cerraduras inteligentes se conectan mediante cables a un switch, que distribuye la red hacia un Reuter. Esto permite controlar funciones del sistema desde dispositivos móviles y acceder a la base de datos de manera centralizada, logrando mayor seguridad y eficiencia en el sistema de control.

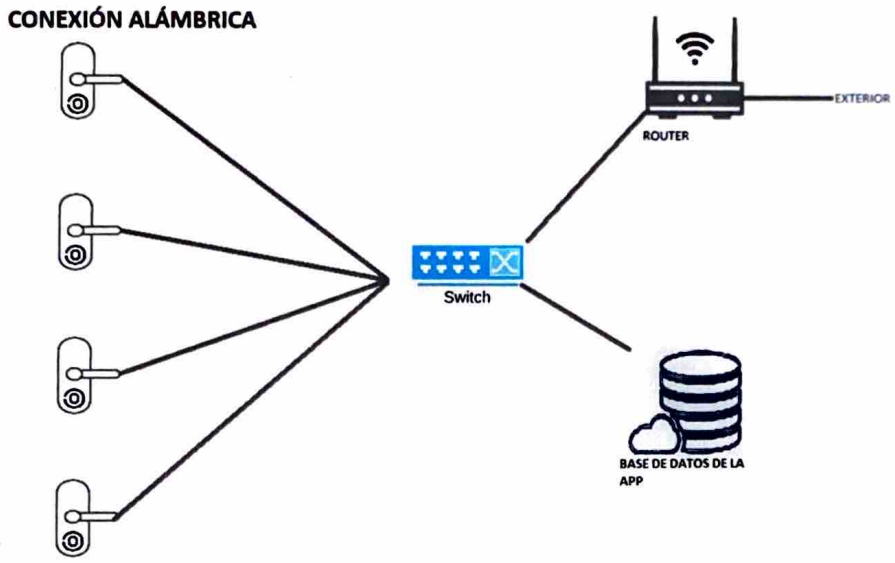


Figura No. 14 Conexión Alámbrica

Conexión inalámbrica

La conexión inalámbrica es una solución práctica cuando no es posible usar cables. Facilita la instalación y expansión, eliminando restricciones físicas y permitiendo que las cerraduras inteligentes se conecten mediante WiFi. Esto resulta conveniente para controlar el sistema de forma remota desde cualquier lugar con internet. Aunque más flexible, requiere medidas de seguridad robustas para proteger la red y evitar accesos no autorizados. Es clave optimizar la infraestructura para garantizar una cobertura estable, incluyendo repetidores o mejoras en la red existente. La ilustración muestra cómo las cerraduras se conectan al WiFi, pasando por un switch y un router, permitiendo el acceso remoto y la integración con la base de datos del sistema.

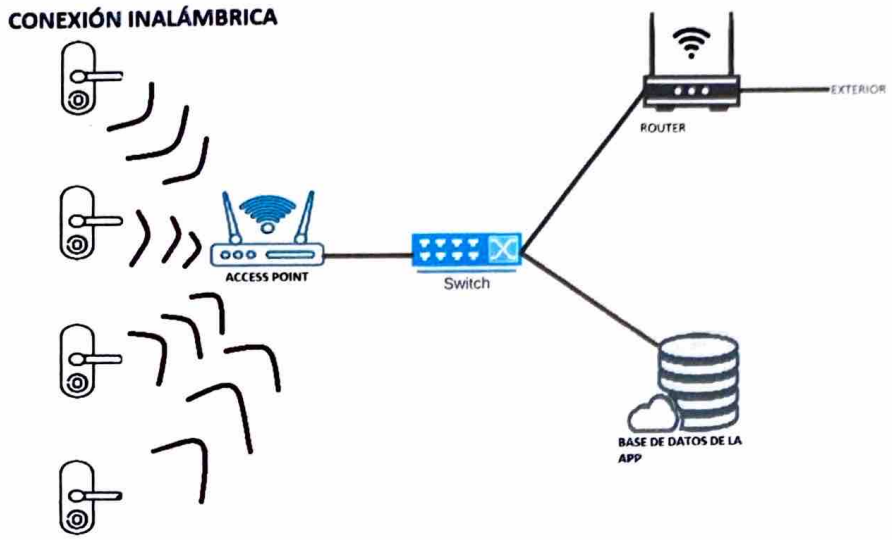


Figura No 15 Conexión Inalámbrica

4.7 Guía de instalación y configuración del dispositivo IoT

Las cerraduras inteligentes fueron configuradas para que sus registros de acceso se integren en el aplicativo móvil controlando el ingreso a cada aula, los niveles de permiso previamente establecidos en el sistema de control de acceso se integraron con la cerradura inteligente, esto permitió asignar permisos de acceso específicos a cada docente como las aulas designadas.

La cerradura inteligente es compatible con todo tipo de puerta y con la aplicación tuya en donde se va a conectar al dispositivo móvil se mostrará cual es el mecanismo interno que este contiene.

4.7.1 Configuración de los sensores y alertas

Configuración de administrador

1) Agregar administrador

Gestión de funciones del bloqueo (paso uno)

➡ Mensaje de voz: presione 1 para configuración de administrador, presione 2 para configuración de usuario.

➡ Presione 1 para agregar administrador: introduzca huella digital o contraseña (debe ingresar la huella digital 4 veces, una contraseña de 4-8 dígitos 2 veces, por ejemplo: 8888 #, o una tarjeta IC una vez).

➡ Después de ingresar correctamente, presione * para regresar al nivel anterior para continuar agregando un administrador o eliminar un administrador.

2) Eliminar información del administrador

Gestión de funciones del bloqueo (paso uno)

➡ Mensaje de voz: presione 1 para configuración de administrador, presione 2 para configuración de usuario.

➡ Presione 2, mensaje de voz: por favor introduzca el número, presione # para confirmar (por ejemplo: 002 #).

➡ Después de ingresar correctamente, presione * para regresar al nivel anterior para continuar.

Configuración de usuario común

1) Agregar información del usuario

Gestión de funciones del bloqueo (paso uno)

➡ Mensaje de voz: presione 1 para configuración de administrador, presione 2 para configuración de usuario.

➡ Presione 2, mensaje de voz: presione 1 para agregar usuario, presione 2 para eliminar usuario.

➡ Presione 1 para agregar usuario: por favor, introduzca la información de desbloqueo, como huella digital o contraseña (debe ingresar la huella digital 3 veces, una contraseña de 4-8 dígitos 2 veces, por ejemplo: 6666 #, o una tarjeta IC).

2) Eliminar información del usuario

Gestión de funciones del bloqueo (paso uno)

➡ **Mensaje de voz:** presione 1 para configuración de administrador, presione 2 para configuración de usuario.

➡ **Presione 2, mensaje de voz:** presione 1 para eliminar un número, presione 2 para eliminar todo.

Por ejemplo, presione 1 e introduzca el número (010#); eliminará al usuario "010".

Configuración del sistema

1) Configuración de voz

Gestión de funciones del bloqueo (paso uno)

➡ Mensaje de voz: presione 1 para abrir la voz, presione 2 para cerrar la voz.

Puede elegir una opción, y luego le indicará que la operación fue exitosa.

➡ Presione 3, mensaje de voz: por favor presione 1 para configuración de voz, 2 para modo de desbloqueo, 3 para selección de idioma, 4 para configuración de hora.

2) Configuración del modo de desbloqueo

Gestión de funciones del bloqueo (paso uno)

➡ **Mensaje de voz:** presione 1 para configuración de administrador, presione 2 para configuración de usuario.

➡ **Presione 2, mensaje de voz:** presione 1 para modo único, presione 2 para modo combinado.

Presione 3 para habilitar el modo de paso.

Presione 4 para cancelar el modo de paso.

Puede elegir una opción, y luego le indicará que la operación fue exitosa.

➡ **Presione 3, mensaje de voz:** por favor presione 1 para configuración de voz, 2 para modo de desbloqueo, 3 para selección de idioma, 4 para configuración de hora.

3) Configuración de idioma

Gestión de funciones del bloqueo (paso uno)

➡ Mensaje de voz: presione 1 para configuración de administrador, presione 2 para configuración de usuario.

➡ Presione 3, mensaje de voz: por favor presione 1 para chino, presione 2 para inglés, puede elegir una opción, y luego le indicará que la operación fue exitosa.

4) Configuración de hora

Gestión de funciones del bloqueo (paso uno)

➡ Mensaje de voz: presione 1 para configuración de administrador, presione 2 para configuración de usuario.

➡ Presione 3, mensaje de voz: por favor presione 1 para modo de desbloqueo, 2 para selección de idioma, 4 para configuración de hora.

➡ Presione 4, mensaje de voz: hora actual 1908080808, luego presione "#". Por favor, modifique según el formato (año-mes-día hora: minuto, por ejemplo: 1903041153), y luego presione # para confirmar.

Restaurar configuración de fábrica

Gestión de funciones del bloqueo (paso uno)

➡ Mensaje de voz: presione 1 para configuración de administrador, presione 2 para configuración de usuario.

➡ Presione 4, mensaje de voz: por favor, introduzca la información del administrador (por ejemplo: 123456), presione # para confirmar.

➡ Inicialización exitosa

4.7.2 Configuración de la red de dispositivos IoT

Configuración de la APP (Tuya Smart)

Búsqueda de la APP: Busca "Tuya Smart" en la App Store o en el mercado de aplicaciones. Descárgala e instálala.

Registro e inicio de sesión: Regístrate con tu número de teléfono y accede a tu cuenta.

Agregar dispositivo: Ve a "Seguridad y Sensor", busca "Cerradura (Wi-Fi)", haz clic y agrega un dispositivo siguiendo las instrucciones antes de usarlo.

Desbloqueo remoto: Despierta la pantalla y presiona "9" + "#". Se escuchará un aviso de voz solicitando el desbloqueo remoto.

Agregar una red

Presiona "*" + "#" para autenticar la identidad del administrador y luego presiona "1" para acceder a la configuración del administrador. Se escuchará un aviso de voz indicando que presiones "3" para la configuración de la red.

Aviso de voz en modo de configuración de red: presiona "1" para la conexión de punto de acceso y "2" para la conexión inteligente.

Cuando la red se agrega correctamente, las luces 1, 2, 3 y 4 del teclado se encenderán en orden con un aviso de voz de "operación completada".

En caso de falla en la adición de la red, las luces 1, 2, 3 y 4 del teclado no se encenderán y se escuchará un aviso de voz de "operación fallida" al cabo del tiempo de espera.

4.7.3 Solución de problemas comunes

Si la alimentación es insuficiente, aparecerá un aviso de alarma y la función de desbloqueo sólo se podrá utilizar aproximadamente 200 veces hasta que se agote la batería, sin embargo, la función Wi Fi podría ser deficiente cuando la batería está baja. Reemplace con 4 baterías nuevas. por eso cada puerta cuenta con unas pilas extras para colocarle mientras las otras están siendo recargadas realizando este método al personal autorizado.

Cuando no pueda desbloquear la cerradura mediante el código numérico, huella digital, tarjeta NFC, RFID o desde la App, use la llave física para hacerlo o llamar al personal ya indicado para abrirla.

CAPÍTULO V

5.1 Introducción

Una vez concluido el proceso de estudio e implementación de la propuesta, se procede a presentar el análisis e interpretación de resultados en la que se analizara el impacto y la efectividad de las cerraduras inteligentes instaladas viendo asi el funcionamiento del dispositivo IoT y el impacto en la seguridad de las aulas en la Facultad Ciencias de la Vida y Tecnología de la Carrera de Agropecuaria.

5.2 Evaluación de los dispositivos IoT instalados

5.2.1 Análisis de desempeño y eficiencia

Las pruebas que se realizaron fueron tiempos de respuestas, evaluando la velocidad con la que las cerraduras responden a comandos de apertura y cierre remoto también de la alarma al ingresar forzosamente, la estimación de la autonomía de las baterías de las cerraduras en condiciones normales de uso y la durabilidad de los materiales realizando observaciones sobre cómo las cerraduras y puertas respondieron al uso diario, en la siguiente tabla N_o. 16. se da un estimado de 1 mes al realizar el análisis.

	Tiempo de apertura	Tiempo de cierre	Tiempo de alarma
Puerta 1	1 segundos	1 segundo	5.8 segundo
Puerta 2	1 segundos	1 segundo	5.8 segundo
Puerta 3	1 segundos	1 segundo	5.8 segundo

Tabla N°. 16. Tiempos de respuesta de la cerradura inteligentes

Este impacto da a conocer los tiempos rápidos que confirman la eficiencia del sistema en situaciones de uso diario y emergencias

	Durabilidad de Batería	Durabilidad de las puertas
Semana 1	100%	100%
Semana 2	80%	100%
Semana 3	50%	100%
Semana 4	10%	100%

Tabla N°. 17. resistencia de durabilidad de las puertas y batería de la cerradura inteligente

Por otro punto las observaciones realizadas durante un mes se indica una disminución progresiva en la capacidad de las baterías mientras las puertas tienen una durabilidad al 100%

5.2.2 Resultados obtenidos de los objetivos específicos

Una vez realizado todos los objetivos específicos se analizaron los puntos adecuados para el análisis de estos resultados en las que se validaron todos los objetivos destacándose la recolección de expectativas de usuarios permitiendo alinear las funciones del sistema con las necesidades específicas. El diseño esquemático con precisión de la instalación y la configuración del sistema y como ultimo la implementación con la que confirmaron que el sistema mejoro significativamente la seguridad y facilito el monitoreo del acceso.

5.3.1 Comparación antes y después de la implementación

Tras la instalación del dispositivo IoT se observó una mejora notable en la seguridad de las aulas.

Antes en la facultad de Ciencias de la Vida y Tecnología en la carrera de Agropecuaria los frecuentes accesos no autorizados eran frecuentes por la falta de registros y un control de entradas a las distintas aulas haciendo que no tenga una seguridad apropiada para los docentes y estudiantes.

Una vez realizado la implementación se puede ver que habido un cambio de monitoreo efectivo realizando un registro automatizado y reducción de incidentes de seguridad en las aulas haciendo que los docentes y estudiantes estén mas protegidos que antes.

5.4.1 Análisis estadístico de incidentes de seguridad

Durante el primer mes, se recopilo información sobre incidentes, realizando un análisis reflejando el impacto positivo directo de la cerradura inteligente en la reducción de vulnerabilidades. Antes de la implementación se reportaron algunos incidentes en promedio mensual sobre la seguridad de estudiantes no autorizados en esas aulas y dejando vulnerable la seguridad de pertenencias de la carrera. Por eso se implementó el dispositivo y los incidentes ya no habían sido reportados en un mes. A continuación, se presenta una tabla estadística comparativa.

Semanas del mes de septiembres	Incidentes de seguridad antes de la implementación	Incidentes de seguridad después de la implementación s
Semana 1	4	N/A
Semana 2	2	N/A
Semana 3	1	N/A
Semana 4	2	N/A

Tabla N°. 18. Análisis de incidentes de seguridad antes y después de la implementación

CAPÍTULO VI

6.1 Conclusiones

El sistema de control de acceso implementado en la carrera de Agropecuaria ha demostrado ser una solución eficiente y segura que responde de manera efectiva a las necesidades específicas del entorno académico. Este dispositivo IoT representado por la cerradura inteligente, ha integrado tecnologías biométricas avanzadas como el reconocimiento de huellas dactilares, junto con tarjetas RFID o NFC. Esta combinación ha permitido superar las limitaciones de los métodos tradicionales como el uso de llaves físicas o contraseñas, ofreciendo una autenticación más precisa, segura y confiable. De esta manera, se han reducido significativamente los riesgos de acceso no autorizado.

La estructura modular y escalable del sistema ha sido un aspecto clave para el éxito del proyecto. Este diseño no solo asegura su funcionalidad inmediata, sino que también permite una fácil adaptación a las necesidades futuras, ya sea integrando nuevas tecnologías o ampliando su capacidad. Este enfoque asegura que el sistema pueda evolucionar junto con las demandas tecnológicas y de seguridad.

La colaboración activa del personal de la carrera de Agropecuaria ha sido fundamental para garantizar el éxito del proyecto. Desde la identificación de necesidades específicas hasta la fase de diseño e implementación, su participación ha permitido establecer objetivos claros y adaptar el sistema a las características particulares del entorno académico. El proceso de investigación y el análisis detallado de los recursos disponibles fueron esenciales para alinear el proyecto con las expectativas de la institución, fortaleciendo la efectividad del sistema y asegurando su correcta implementación.

Además del impacto en la seguridad, el sistema ha optimizado la gestión del acceso. Esta modernización tecnológica también ha fomentado una mayor conciencia sobre la importancia de la seguridad y el uso de tecnologías avanzadas en la facultad.

Sin embargo, es importante destacar que tanto las tecnologías como las amenazas de seguridad evolucionan constantemente. Para mantener la relevancia y efectividad del sistema es necesario adoptar una estrategia activa de actualización tecnológica. Esto incluye la revisión periódica del desempeño del sistema, la incorporación de

recomendaciones de los usuarios y la evaluación constante de las políticas de acceso. Estas acciones no solo garantizan la sostenibilidad del sistema, sino que también aseguran que este siga cumpliendo con los estándares de seguridad y eficiencia requeridos en el largo plazo.

6.2 Recomendaciones

Mejora de las baterías

Para optimizar el rendimiento del sistema de cerraduras inteligentes, es importante considerar la incorporación de baterías con mayor capacidad, las cuales podrían extender la duración del funcionamiento sin necesidad de recargas frecuentes. Esto no solo mejoraría la autonomía de las cerraduras, sino que también reduciría el costo operativo asociado con el reemplazo de baterías. Además, se podría evaluar la posibilidad de integrar sistemas de energía renovable como los paneles solares, que permitirían un sistema de recarga continuo y autónomo, especialmente en zonas donde la energía eléctrica es intermitente o donde se busca una solución más sostenible desde el punto de vista ambiental.

Revisión y Actualización Anual del Sistema

Para mantener la efectividad del sistema de control de acceso, es esencial implementar un plan de mantenimiento preventivo regular. Este plan debe incluir la revisión periódica de las cerraduras inteligentes, las baterías y los dispositivos asociados para garantizar su funcionamiento óptimo. Además, se recomienda establecer rutinas para la actualización y análisis de los datos recolectados, como los registros de acceso y los eventos de seguridad.

Esto incluye revisar tanto el software como el hardware utilizado, evaluando el desempeño de los dispositivos biométricos y RFID. Se debe analizar si existen nuevas tecnologías o mejoras que puedan implementarse para optimizar la seguridad, la eficiencia y la funcionalidad del sistema. Al llevar a cabo este tipo de evaluaciones regulares, se asegura que el sistema siga siendo seguro y relevante a lo largo del tiempo, adaptándose a los avances tecnológicos.

Desarrollo de un Plan de Contingencia Detallado

Para mitigar los efectos de posibles fallos técnicos, es crucial establecer un plan de contingencia que detalle las acciones a seguir en caso de problemas con el sistema. Este plan debe incluir soluciones ante fallos en la red, interrupciones del servicio de los módulos biométricos o cualquier otro inconveniente que afecte el funcionamiento del sistema. Además, debe prever procedimientos alternativos para garantizar que, en situaciones de emergencia, se pueda mantener el control de acceso de forma provisional sin comprometer la seguridad.

Comunicación Continua con los Usuarios

Es importante mantener una comunicación abierta y fluida con los usuarios del sistema para que puedan reportar problemas, sugerencias o cualquier inconveniente que enfrente al utilizarlo, pues permitirá realizar ajuste que optimicen las experiencias del usuario y contribuyen a la eficiencia y efectividad del control de acceso.

Bibliografías

Alarm, S. (07 de 05 de 2024). *Sector Alarm.* Obtenido de Sector Alarm: https://www.sectoralarm.es/consejos-seguridad/cerraduras-inteligentes/#:~:text=Las%20cerraduras%20inteligentes%20se%20integran%20con%20los%20sistemas,y%20aperturas%2C%20para%20alertar%20sobre%20intentos%20de%20intrusi%C3%B3n.

Anónimo. (8 de julio de 2022). *Bambu.* Obtenido de Bambu: https://bambu-mobile.com/tarjetas-rfid-que-son-y-para-que-sirven/

Home, A. (2022). *Advance Home.* Obtenido de Advance Home: https://advancedhome.net/en/cerradura-inteligente-lc-1300/

Luna, j. I. (Noviembre de 2018). Acceso a un crentro de datos utilizando una trajeta rfid y huella digital. *Pistas Educativas*, 17. Obtenido de https://pistaseducativas.celaya.tecnm.mx/index.php/pistas/article/view/1745

McGrathLocks. (10 de Mayo de 2024). *McGrathLocks*. Obtenido de McGrathLocks: https://mcgrathlocks.com.au/mlnx6-digital-lock/

Zoominformatica. (10 de Enero de 2024). *Zoominformatica*. Obtenido de Zoominformatica: https://www.zoominformatica.com/cerradura-para-puerta-huella-compatible-tuya-smart-wifi.html

García Yagual, B. R., & Mancheno Poveda, L. A. (2023). *Diseño e implementación de un sistema de control de acceso para dispositivos de seguridad basado en tecnología IoT* [Proyecto integrador, Escuela Superior Politécnica del Litoral, Facultad de Ingeniería en Electricidad y Computación]. ESPOL. https://www.dspace.espol.edu.ec/handle/123456789/57584

Fúnez Fernández, E. (2022). Diseño de un sistema de seguridad en el hogar basado en IoT y creación de prototipo [Trabajo de Fin de Grado, Universidad de Jaén]. Escuela Politécnica Superior de Linares. https://crea.ujaen.es/bitstream/10953.1/16437/1/Memoria%20TFG%20Eduardo%20Funez%20Fernandez.pdf

Alarm, S. (07 de 05 de 2024). *Sector Alarm.* Obtenido de Sector Alarm: https://www.sectoralarm.es/consejos-seguridad/cerraduras-inteligentes/#:~:text=Las%20cerraduras%20inteligentes%20se%20integran%20con%20los%20sistemas,y%20aperturas%2C%20para%20alertar%20sobre%20intentos%20de%20intrusi%C3%B3n.

Sequea Oliveros, J. (2022, enero 2). La tecnología IoT para el monitoreo y seguridad de los espacios. Mundo Cloud. Recuperado de https://mundo.cloud/noticias/innovacion-noticias/la-tecnologia-iot-para-el-monitoreo-y-seguridad-de-los-espacios

Tariq, U., Ahmed, I., Bashir, A. K., & Shaukat, K. (2023). A critical cybersecurity analysis and future research directions for the Internet of Things: A comprehensive review. Sensors, 23(8), 4117. https://doi.org/10.3390/s23084117

González, J. M., & Pérez, A. (2023). Control de acceso basado en tecnologías IoT en instituciones de educación superior: Prototipo aplicado al control del ingreso a salones y

auditoría en la Universidad Autónoma de Bucaramanga. Universidad Autónoma de Bucaramanga. Recuperado de https://repository.unab.edu.co/handle/20.500.12749/2276

Soberon Hernandez, P. F., & Landaeta Arcentales, C. E. (2021). Diseño e implementación de un sistema de registro de accesos utilizando IoT para mejorar la seguridad física en el datacenter del Departamento de Informática de la Municipalidad Distrital de las Amazonas (Tesis de pregrado). Universidad Científica del Perú, Facultad de Ciencias e Ingeniería. Recuperado de http://repositorio.ucp.edu.pe/bitstream/handle/UCP/2039/PIERO%20FABIAN%20SOBERON%20HERNANDEZ%20Y%20CESAR%20EDU%20LANDAETA%20ARCENTALES%20-%20TESIS.pdf?sequence=1&isAllowed=y

Alarm, S. (07 de 05 de 2024). *Sector Alarm.* Obtenido de Sector Alarm: https://www.sectoralarm.es/consejos-seguridad/cerraduras-inteligentes/#:~:text=Las%20cerraduras%20inteligentes%20se%20integran%20con%20los%20sistemas,y%20aperturas%2C%20para%20alertar%20sobre%20intentos%20de%20intrusi%C3%B3n.

Ocampo, D. S. (2019, diciembre 3). Investigación bibliográfica. Investigalia. https://investigaliacr.com/investigacion/investigacion-bibliografica/

Guevara Albán, G. P., Verdesoto Argüello, A. E., & Castro Molina, N. E. (2020, julio 1). La escogencia del tipo de investigación y su impacto en el estudio. RECIMUNDO. https://www.recimundo.com/index.php/es/article/view/860/1363

Palmett Urzola, A. M. (2020). Métodos inductivo, deductivo y teoría de la pedagogía crítica. Artículo divulgativo. Petroglifos: Revista Crítica, 3(1), 5-19. Recuperado de https://petroglifosrevistacritica.org.ve/wp-content/uploads/2020/08/D-03-01-05.pdf

Anónimo. (8 de julio de 2022). *Bambu.* Obtenido de Bambu: https://bambu-mobile.com/tarjetas-rfid-que-son-y-para-que-sirven/

Home, A. (2022). *Advance Home.* Obtenido de Advance Home: https://advancedhome.net/en/cerradura-inteligente-lc-1300/

Luna, j. I. (Noviembre de 2018). Acceso a un crentro de datos utilizando una trajeta rfid y huella digital. *Pistas Educativas*, 17. Obtenido de https://pistaseducativas.celaya.tecnm.mx/index.php/pistas/article/view/1745

Condori-Ojeda, P. (2020). *Universo, población y muestra. Curso Taller*. Recuperado de https://www.aacademica.org/cporfirio/18.pdf

Lerma Meza, A., Vázquez Araujo, J. G., Martínez Vázquez, M. C., González Cisneros, L. E., Coronado Manqueros, J. M., Barraza Macías, A., Mejía Carrillo, M. J., & Mercado Piedra, J. A. (2020). Un abordaje didáctico. Recuperado de https://centro-investigacion-innovacion-educativa.bravesites.com/files/documents/306aa3ba-3be8-4e59-ab4d-51508f7513c6.pdf#page=82

Gómez, M. C. (2023, August 11). *¿Qué es una encuesta?* HubSpot. Retrieved from https://blog.hubspot.es/service/que-es-una-encuesta

Mata Solís, L. D. (4 de febrero, 2020). *La entrevista en la investigación cualitativa.* Recuperado de https://www.questionpro.com/blog/es/instrumentos-para-recopilar-informacion/

Cisneros Caicedo, A. J., Guevara García, A. F., Urdánigo Cedeño, J. J., & Garcés Bravo, J. E. (2022). *Las TICs en la investigación: Transformación y facilitación en la recolección de datos. Vol. 8, núm. 1, enero-marzo 2022, pp. 1165-1185.* Recuperado de https://dialnet.unirioja.es/descarga/articulo/8383508.pdf

Juanes, G. G. (2022, 27 de marzo). ¿Qué es una cerradura electrónica inteligente y cómo funciona? https://cuadernosdeseguridad.com/2022/03/cerradura-electronica-by-demes/

Lucena, P. (2024). Ventajas y desventajas del Internet de las Cosas (IoT). https://www.cesuma.mx/blog/ventajas-y-desventajas-del-internet-de-las-cosas-iot.html#:~:text=Seguridad%3A%20El%20IoT%20tambi%C3%A9n%20puede,el%20bienestar%20de%20las%20personas.

Escalante Fernández, J. M. (2021, 29 de noviembre). *IoT: Qué es, para qué sirve y cómo funciona*. Laboratorio IoT y desarrollo en Cloud de un dispositivo de sensorización. Recuperado de https://openwebinars.net/blog/iot-que-es-para-que-sirve-y-como-funciona/#caracter%C3%ADsticas-del-iot.

Kaspersky. (2024). *Mejores prácticas de seguridad para IoT*. Recuperado de https://www.kaspersky.es/resource-center/preemptive-safety/best-practices-for-iot-security

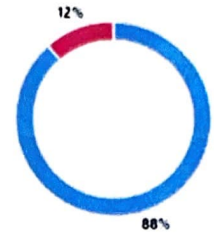
Aguilar Peña, D. F. (2021). Factibilidad de una red Metro Ethernet basada en la metodología PPDIOO aplicada a PYMES. Recuperado de https://repositorio.utmachala.edu.ec/bitstream/48000/16854/1/TTFIC-2021-IS-DE-00001.pdf.

ANEXOS

2. ¿Esta familiarizado con los dispositivos de seguridad basados en tecnología IoT?

Más detalles

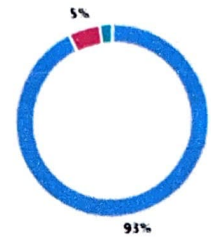
- Sí 84
- No 11



3. ¿Conoce algún sistema de control de acceso biométrico?

Más detalles

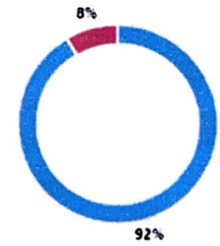
- Sí 88
- No 5
- No sabe 2



4. ¿Ha utilizado alguna vez un sistema de control de acceso biométrico?

Más detalles

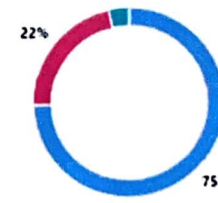
- Sí 87
- No 8



5. En caso afirmativo, ¿qué tecnología de verificación de identidad le parece más fácil de utilizar

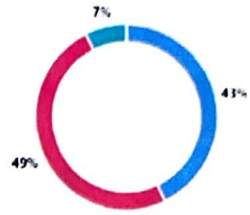
Más detalles

- Huellas dactilares 65
- Reconocimiento facial 19
- Digitación de clave 3
- Desconozco 0



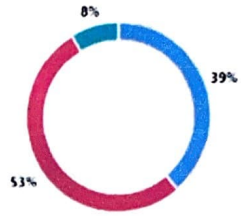
6. ¿Considera que las actuales medidas de seguridad en la sala de docentes de la Carrera de Agropecuaria son eficaces? Más detalles

Sí	41
No	47
No sabe	7



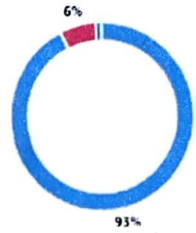
7. ¿Conoce si existe algún dispositivo de control de acceso biométrico en la sala de docentes de la Carrera de Agropecu... Más detalles

Sí	37
No	50
No sabe	8



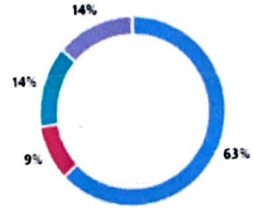
8. ¿Cree que la implementación de un sistema de control de acceso biométrico en la sala de docentes brindaría un entor... Más detalles

Mucho	88
Poco	6
Nada	1



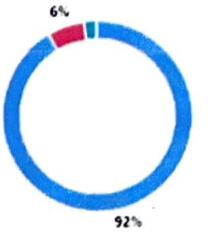
9. ¿Qué características considera importantes en un sistema de control de acceso biométrico? Más detalles

Fácil adaptación	60
Respuesta rápida	9
Fácil de usar	13
Confiabilidad y seguridad	13



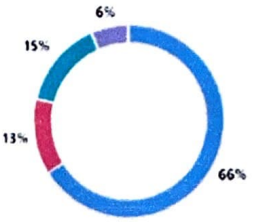
10. ¿Cons dera qué la implementación de un sistema de control de acceso biométrico mejoraría la seguridad y la product... Más detalles

Mucho	87
Poco	6
Nada	2



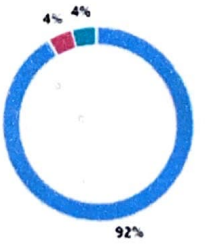
11. ¿Piensa que el uso de nuevas tecnologías, como un sistema de control de acceso biométrico, sería una innovación en... Más detalles

De manera tecnológica	63
De manera inteligente	12
De manera segura	14
De manera moderna	6



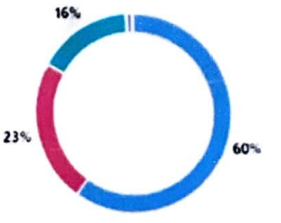
12. ¿Cree que el uso de dispositivos IoT puede mejorar la seguridad en las aulas de la Carrera de Agropecuaria? Más detalles

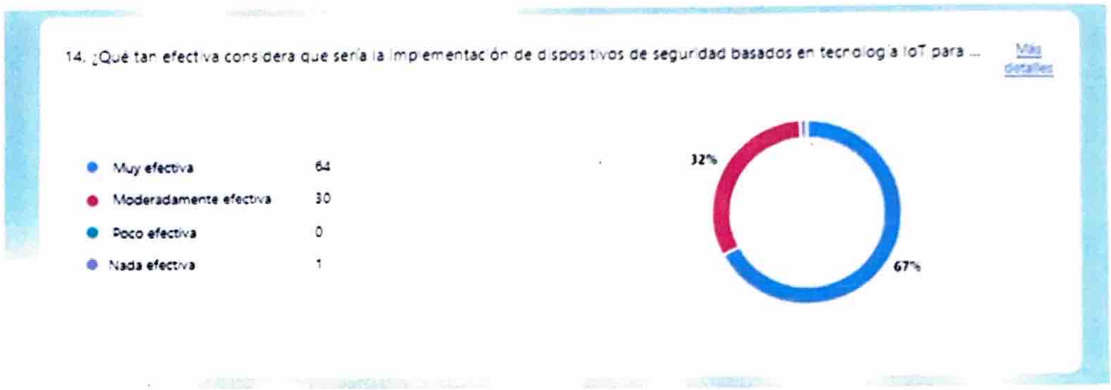
Si	87
No	4
No sabe	4

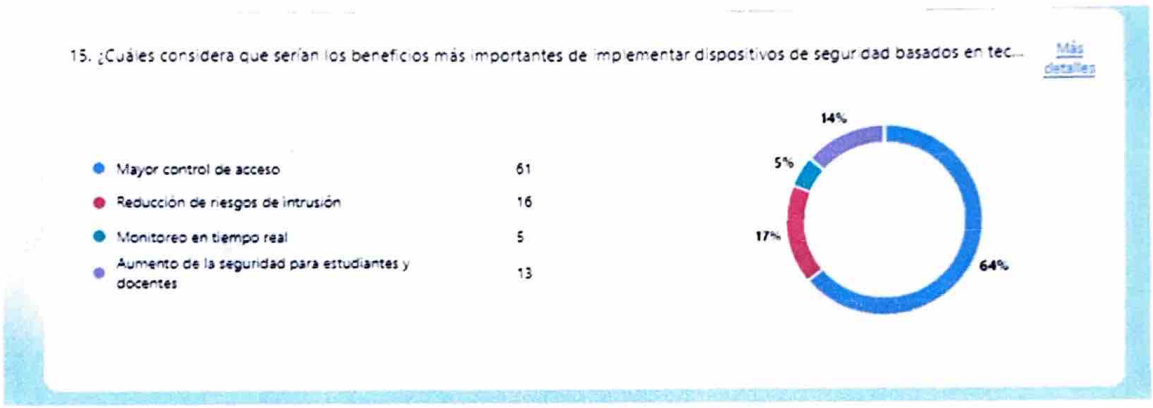


13. ¿Qué nivel de seguridad considera que se obtendría con la implementación de dispositivos IoT en las aulas? Más detalles

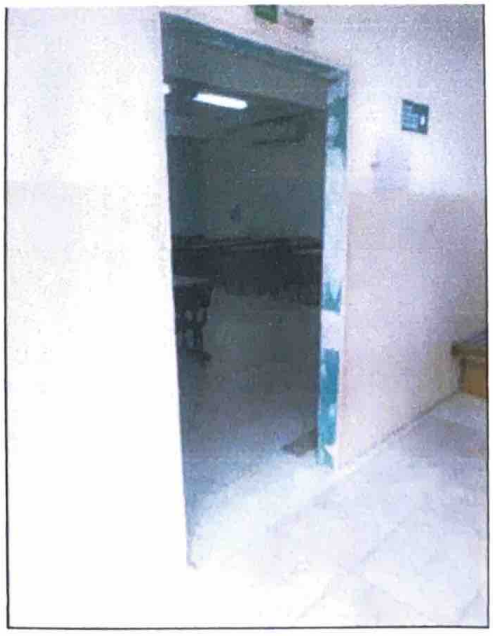
Muy alto	57
Alto	22
Medio	15
Bajo	1
Ninguno	0







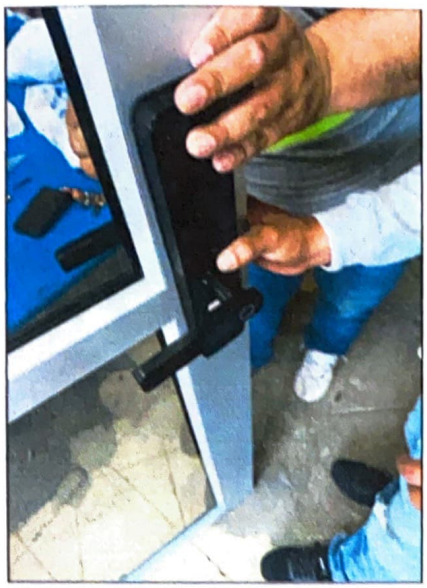
Montaje e Instalación del Sistema de Control de Acceso Automatizado



Se procedió a desinstalar la puerta existente, realizando las mediciones necesarias para la instalación de una nueva puerta en sustitución de la anterior

Proceso de corte y ajuste del marco metálico para la instalación de la nueva puerta

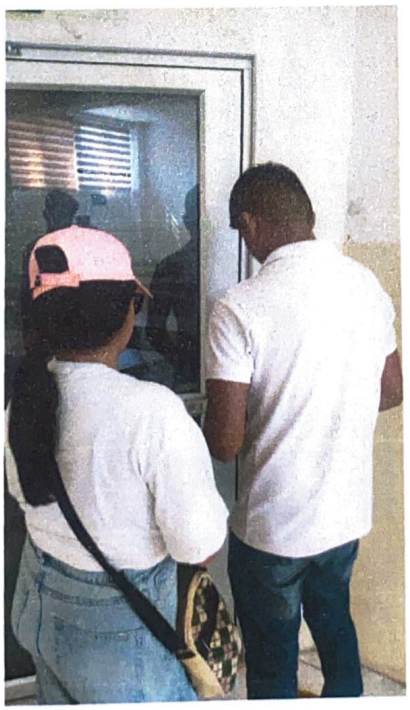
Colocando de manera correcta las cerraduras inteligentes con su seguro extraído

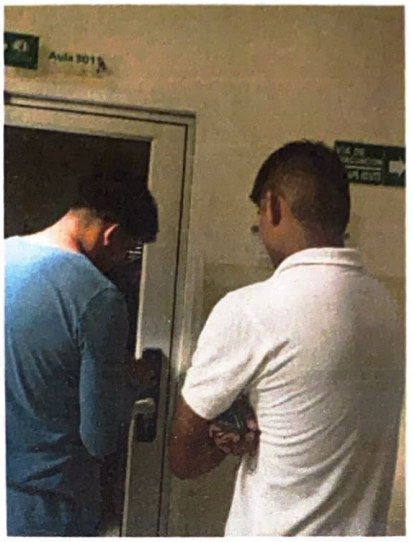


Colocación de la cerradura en la puerta. La chapa debe quedar alineada y fijada de manera correcta antes de proceder con el ajuste final

Configuración y verificación de las cerraduras para comprobar el correcto funcionamiento

Tarjetas RFID utilizadas para la configuración de las cerraduras de la puerta inteligente, habilitando el acceso mediante tecnología de proximidad.





Configuración con las tarjetas RFID para el acceso a las puertas, asignando los permisos de acceso necesarios para su funcionamiento.

Verificación de cerradura inteligente colocada exitosamente y funcional