EKSIGMA
Revista Ecuatoriana de Conocimiento Científico

ISSN: 3121-2689

Artículo de investigación

Diseño de casa inteligente y seguridad en la provincia de Esmeraldas ciudadela Los Girasoles

Smart Home Design and Security in the Province of Esmeraldas – Los Girasoles Residential Area

Nestor Javier Farías Olaya[1]
nestorfariasol@gmail.com
[1] Universidad Tecnológica Empresarial de Guayaquil, Guayaquil, Ecuador, 090616

Citación: Farías Olaya, N. (2026). Smart Home Design and Security in the Province of Esmeraldas – Los Girasoles Residential Area. *EKSIGMA Ecuadorian Journal of Scientific Knowledge*, *2*(1), 5-33. https://eksigma.com/index.php/principal/article/view/16

Recibido: *31 octubre 2025*
Aceptado: *01 diciembre 2025*
Publicado: *15 enero 2026*

EKSIGMA
ISSN: 3121-2689

Correspondencia:
nestorfariasol@gmail.com

Resumen: La inseguridad en los hogares del barrio "Los Girasoles" en Esmeraldas ha evidenciado una alta vulnerabilidad en accesos residenciales. Este estudio se centra en el diseño de un sistema de control de acceso inteligente, basado en tecnologías IoT, adaptado a una condición socioeconómica limitada. La investigación adoptó un enfoque cualitativo no experimental, realizando entrevistas a 10 moradores y validando el diseño con 3 expertos en electrónica y domótica. Los resultados muestran que el diseño fue validado como técnicamente viable, con un promedio de 4.7 en la evaluación de viabilidad técnica por parte de los expertos. La adecuación al contexto social del barrio obtuvo 4.8 destacando el bajo costo y la simplicidad de implementación. El sistema diseñado tiene el potencial de mejorar la seguridad, sin embargo, el costo y falta de conocimientos representan desafíos para su implementación generalizada. Además, aunque el sistema es viable en un entorno simulado, se recomienda realiza pruebas piloto para comprobar su efectividad.

Palabras clave: automatización; nuevas tecnologías; seguridad; Internet de las Cosas (IoT); control de acceso inteligente.

.

Abstract: *Insecurity in households in the "Los Girasoles" neighborhood of Esmeraldas has revealed a high level of vulnerability in residential access points. This study focuses on the design of an intelligent access control system based on IoT technologies, adapted to a limited socioeconomic context. The research adopted a non-experimental qualitative approach, conducting interviews with 10 residents and validating the design with 3 experts in electronics and home automation. The results show that the design was validated as technically feasible, with an average score of 4.7 in technical feasibility as assessed by the experts. Adaptation to the social context of the neighborhood scored 4.8, highlighting low cost and simplicity of implementation. The designed system has the potential to improve security; however, cost and lack of knowledge represent challenges for widespread implementation. In addition, although the system is viable in a simulated environment, pilot testing is recommended to verify its effectiveness.*

Keywords: *automation; emerging technologies; security; Internet of Things (IoT); intelligent access control.*

1. INTRODUCCIÓN

La seguridad en los hogares es un aspecto esencial para garantizar la integridad física y patrimonial de las personas, especialmente en contextos donde los índices de criminalidad han evidenciado un aumento considerable (Zambonino, 2023). Es así como, en los últimos años, el cantón Esmeraldas, ha experimentado un incremento en los niveles de violencia e inseguridad, que afecta directamente a los barrios urbanos y a la calidad de vida de sus habitantes; ya que, según el informe de la Oficina de las Naciones Unidas contra la Droga y el Delito, Ecuador registró un incremento del 85% en los delitos violentos entre 2021 y 2023 (Redacción Primicias, 2024). Esta problemática también se refleja en otras regiones de América Latina, donde la inseguridad residencial es un desafío creciente, con estudios internacionales que señalan un aumento global en los delitos de acceso no autorizado a viviendas (Kabir et al., 2022; Sayeduzzaman et al., 2024)

Dentro de los barrios urbanos de Esmeraldas, uno de los problemas más frecuentes es la facilidad con la que se logra ingresar a los domicilios. Esto se evidenció con mayor énfasis entre 2023 y 2024, se han efectuado 251 casos de robos accediendo violentamente mediante la puerta principal, situación que expone la vulnerabilidad de los accesos tradicionales (Redacción Primicias, 2024). La puerta de acceso representa el primer punto de defensa de una vivienda, y su debilidad estructural o tecnológica constituye una brecha prioritaria para la seguridad, siendo este un aspecto crítico dentro de la teoría de seguridad residencial que destaca la importancia de las barreras físicas y tecnológicas para proteger los hogares de intrusiones (Touqeer et al., 2021). Si bien existen estudios sobre la efectividad de los sistemas de control de acceso en contextos urbanos desarrollados, especialmente en zonas de alta vulnerabilidad como Esmeraldas, el uso de tecnologías tradicionales sigue siendo insuficiente para enfrentar los desafíos de inseguridad.

En este contexto, el desarrollo de sistemas de control de acceso inteligente se ha posicionado como una solución innovadora en la teoría del control de acceso respaldada por la integración de tecnologías IoT (Internet de las Cosas) para incrementar la seguridad residencial, que permiten monitoreo, autenticación remota y detección temprana de amenazas (Efe & Ogunlere, 2020; Kabir et al., 2022; Lee & Mun, 2023;). Si bien existen propuestas generales de domótica, es necesario priorizar el fortalecimiento de los sistemas de acceso (Sayeduzzaman et al., 2024; Xu et al., 2024), especialmente en zonas vulnerables como el barrio “Los Girasoles”, en Esmeraldas, donde las condiciones socioeconómicas limitadas dificultan la implementación de soluciones con costos elevados (Xu et al., 2024).

Desde este contexto, se plantea la siguiente pregunta de investigación: ¿Cómo puede el diseño de un sistema de control de acceso inteligente para puertas residenciales contribuir a la mejora de la seguridad en los hogares del barrio "Los Girasoles" en Esmeraldas? En este sentido, el propósito general de la presente investigación fue desarrollar un modelo de sistema de control de acceso inteligente de seguridad para hogares, basado en análisis de riesgos, que priorice la puerta como elemento clave en la protección del hogar, proporcione una alternativa tecnológica viable e integre dispositivos IoT, sensores y mecanismos inteligentes que refuercen la seguridad física de los accesos.

El documento se estructura en los siguientes apartados: en primer lugar, se presenta el marco teórico y conceptual; posteriormente, se expone la metodología aplicada; seguidamente, se detallan los resultados que incluyen la propuesta técnica del sistema; y finalmente, se plantean las conclusiones y recomendaciones. A continuación, se presentan los objetivos que dirigen este trabajo.

2. MÉTODOS

2.1. Tipo de investigación

La presente investigación es de tipo aplicada con un diseño no experimental, dado que no se manipularon variables del entorno, sino que se observó, se analizó y analizó la situación existente para diseñar una solución tecnológica adaptada a un contexto real (Özdemir, 2019). La elección del diseño no experimental se justifica ya que se buscó explorar las percepciones, experiencias y necesidades de los moradores del barrio "Los Girasoles" sin intervenir directamente en el entorno, lo que es característico de investigaciones que tienen como propósito comprender fenómenos en su contexto natural (Creswell & Poth, 2016; Yin, 2018).

El enfoque cualitativo es cualitativo ya que buscó comprender profundamente los requerimientos de los moradores en relación con la seguridad en el acceso a sus viviendas. Este enfoque permitió como indica Miles et al. (2014) es ideal para investigar fenómenos complejos y contextuales, ya que permite recopilar información detallada y contextual para el diseño del sistema. El alcance de la investigación es exploratorio-descriptivo, dado que se exploró la situación actual de los accesos en las viviendas, se describieron las vulnerabilidades identificadas a través de los relatos de los moradores y se generó una propuesta técnica del sistema de control de acceso inteligente adaptada a las condiciones de alta vulnerabilidad del sector (Portase et al., 2024). El enfoque exploratorio es útil cuando no se han realizado estudios previos sobre un tema específico, mientras que el descriptivo permite caracterizar el problema y las condiciones del contexto como indica Creswell & Poth (2016) y Yin (2018).

2.2. Métodos lógicos

Se empleó el método inductivo, para construir la propuesta, a partir de la información obtenida de los moradores y expertos. Asimismo, se utilizó el método analítico-sintético (Portase et al., 2024), descomponiendo el problema de seguridad en sus elementos clave como son la puerta, acceso, percepción de vulnerabilidad y necesidades tecnológicas.

2.3. Población y muestra

La población estuvo conformada por los habitantes del barrio "Los Girasoles", ubicado en la ciudad de Esmeraldas, caracterizado por altos índices de inseguridad residencial y destacando en la vulnerabilidad estructural de las viviendas. Se seleccionó una muestra de 10 propietarios de viviendas, mediante un muestreo no probabilístico intencional siguiendo el enfoque de Miles et al. (2014) y Yin (2018), que permitió seleccionar casos específicos dentro del barrio "Los Girasoles" con características establecidas por los siguientes criterios de inclusión y exclusión (Mojadeddi & Ronsenberg, 2024), como se describen en la Tabla 1.

Tabla 1 Criterios de inclusión y exclusión para la selección de la muestra

Criterio	Inclusión	Exclusión
1	Residir de forma permanente en el inmueble.	Viviendas que contaban con sistemas de acceso reforzados (cerraduras electrónicas o sistemas de videovigilancia)
2	Haber experimentado situaciones de robo o intentos de intrusión por presentar accesos vulnerables como puertas deterioradas, cerraduras defectuosas o ausencia de sistemas de control.	Propietarios con limitaciones de comunicación o condiciones que dificultan la obtención de datos válidos.

Fuente: Elaboración propia

El número de participantes seleccionados se consideró adecuado con base en el principio de saturación teórica, coincidiendo con Oliveira et al. (2021), ya que al recolectar los datos las respuestas comenzaron a repetirse y ya no surgieron categorías nuevas para el análisis, indicando que se cubrieron la diversidad de experiencias dentro del barrio. Por último, se solicitó el consentimiento informado de cada participante para las entrevistas y observación directa en sus domicilios.

2.4. Técnicas de recolección de datos

Para la recolección de información sobre los problemas de seguridad, mecanismos de acceso actuales y expectativas sobre un sistema inteligente se realizó una entrevista semiestructurada a los propietarios de las viviendas seleccionadas. Posteriormente, se realizó una revisión documental y técnica, que consistió en el análisis de estudios previos, manuales técnicos y especificaciones de los dispositivos IoT aplicables al diseño del sistema. Por último, la comprobación técnica del diseño se efectuó a través de la simulación del sistema en el entorno virtual de Wokwi, para verificar de manera práctica el funcionamiento de los sensores y la lógica de control implementada en el ESP32.

2.5. Instrumentos

Se aplicó una guía de entrevista semiestructurada, para la recolección de datos cualitativos, diseñada para explorar las percepciones, experiencias y las necesidades en torno a la seguridad de los hogares del barrio "Los Girasoles". La guía constó de ocho preguntas abiertas, organizadas en tres temas, respecto a requerimientos estructurales, tecnológicos y actitudinales. Las preguntas incluyeron aspectos sobre ¿Cómo calificaría la seguridad actual de la puerta de acceso a su vivienda?, ¿Ha tenido alguna experiencia de robo o intento de intrusión en su hogar? y ¿Qué características considera necesarias en las puertas de acceso para mejorar la seguridad de su vivienda?

El diseño del instrumento se basó en la revisión de estudios previos sobre seguridad residencial y domótica (Kabir et al., 2022; Manjula et al., 2024; Motwani et al., 2021; Sayeduzzaman et al., 2024), asimismo para garantizar la validez de contenido, la guía fue revisada y ajustada por un experto en seguridad, con experiencia en análisis de riesgos en entornos urbanos. Esta metodología se sustenta en el diseño y adaptación de pruebas cualitativas orientadas a la recopilación de percepciones y experiencias contextuales siguiendo los principios de Elvira et al. (2024) y Miles et al. (2014).

Además, la validez de contenido de la guía se garantizó mediante la revisión de cada pregunta por parte del experto, verificando la claridad, pertinencia y relevancia. Como complemento se realizó una prueba piloto con un pequeño grupo de moradores para ajustar la comprensión de las preguntas, de esta forma la confiabilidad del instrumento se sustentó a través de un análisis de concordancia, en donde dos investigadores codificaron las respuestas por separado y se consensuaron los resultados. La concordancia de los evaluadores se verificó mediante el coeficiente de kappa siguiendo las indicaciones de Vergni et al. (2021) para asegurar consistencia en la valoración de los ítems. Los aspectos claves abordados en la guía contemplaban la percepción de seguridad actual en las puertas de acceso, las características que consideraban necesarias para mejorar la seguridad y las dificultades percibidas en torno a la implementación de un sistema inteligente, en términos de costos, tecnicidad y conectividad.

Asimismo, para garantizar la confiabilidad del instrumento fue asegurada mediante una prueba piloto realizada con un pequeño grupo de moradores para ajustar la claridad de las preguntas. Para evitar sesgos en el análisis de los datos se utilizó codificación temática doble, donde dos investigadores analizaron las respuestas por separado y por último se consensuaron los resultados siguiendo las pautas de Abd et al. (2020) y Miles et al. (2014). Se realizó un análisis de concordancia entre los

evaluadores para asegurarse de que las evaluaciones de relevancia y claridad sean consistentes. La concordancia entre los evaluadores fue analizada mediante el cálculo de la prueba de kappa, esto método como indica Yin (2018) mide el grado de acuerdo entre dos o más evaluadores. Los resultados fueron sistematizados y se consensuaron las diferencias entre evaluadores cuando se detectaron discrepancias.

Aunque el instrumento fue aceptable para los entrevistados, también se reconoce como limitación, que las respuestas estuvieron condicionadas por la familiaridad tecnológica de los moradores, lo que podría haber influido en su capacidad para evaluar objetivamente las tecnologías propuestas coincidiendo con estudios previos de Manjula et al. (2024) y Motwani et al. (2021).

Por otra parte, para el diseño y validación del sistema de control de acceso inteligente se utilizó el simulador en línea Wokwi, que permitió elaborar los esquemas eléctricos, diagramas de conexión y ejecutar la simulación completa del prototipo (ver Anexo 2). La validación técnica se completamente en este entorno utilizando la consola serial para observar el comportamiento dinámico de los sensores y la lógica de control implementada.

2.6. Aprobación ética

La investigación cumplió con los principios éticos establecidos para la recolección de datos, obteniendo el consentimiento informado de cada participante antes de las entrevistas y observaciones, asegurando voluntariedad y anonimato. Además, se siguieron los principios éticos internacionales aplicables, por tanto, la aprobación ética del estudio fue obtenida del comité de ética del barrio "Los Girasoles" garantizando la confidencialidad, conforme a los principios establecidos en la Declaración de Helsinki para estudios con seres humanos.

2.7. Procedimiento

La investigación se estructuró en tres fases secuenciales, siguiendo los enfoques aplicados en investigaciones previas (Aldawira, 2019; Goyal et al., 2024; Sivaprasad et al., 2023), con una duración total de tres meses, desarrollada entre mayo y julio de 2025. Cada una de las fases estuvo a cargo del investigador y se ejecutó progresivamente: levantamiento de información, diseño técnico del sistema y validación técnica. Asimismo, se obtuvo el consentimiento informado por parte de los participantes mediante un documento que asegura la voluntariedad y anonimato del proceso y el cumplimiento de principios éticos para este tipo de investigaciones donde intervienen personas (Miles et al., 2014).

Fase 1: Diagnóstico y levantamiento de información cualitativa

En esta fase que se llevó a cabo en tres semanas, se realizaron entrevistas semiestructuradas a 10 propietarios de viviendas del barrio "Los Girasoles" con el fin de explorar sus percepciones sobre la seguridad, sus experiencias frente a robos o intentos de intrusión, y sus necesidades respecto a un sistema de control de acceso inteligente. La entrevista fue guiada por el investigador (Miles et al., 2014). Además, se llevó a cabo la observación directa de los accesos, lo que permitió registrar condiciones físicas, vulnerabilidades visibles y configuraciones actuales de puertas y cerraduras. Los datos obtenidos fueron registrados y posteriormente contrastados con la revisión bibliográfica especializada (Mojadeddi & Rosenberg, 2024).

Fase 2: Diseño técnico del sistema de control de acceso inteligente

A partir de la información recopilada, en las siguientes 5 semanas, se diseñó el sistema de control de acceso inteligente como se visualiza en la Figura 1, utilizando un microcontrolador ESP32 con conectividad WiFi, un sensor magnético de puerta (Reed Switch), un módulo de relé para la activación de la cerradura eléctrica y los cables de interconexión, un sensor PIR y un sensor de vibración para complementar la detección de movimientos humanos e intentos de forzar la cerradura. La programación del sistema se realizó en C++ por el investigador, mediante el entorno de desarrollo Arduino IDE. Asimismo, el diseño esquemático del circuito fue elaborado utilizando el software en línea Wokwi. Por último, se configuró un servidor web local dentro del ESP32, lo que permitió la generación de una interfaz de control accesible desde navegadores web (web browser) en dispositivos móviles conectados a la misma red WiFi.

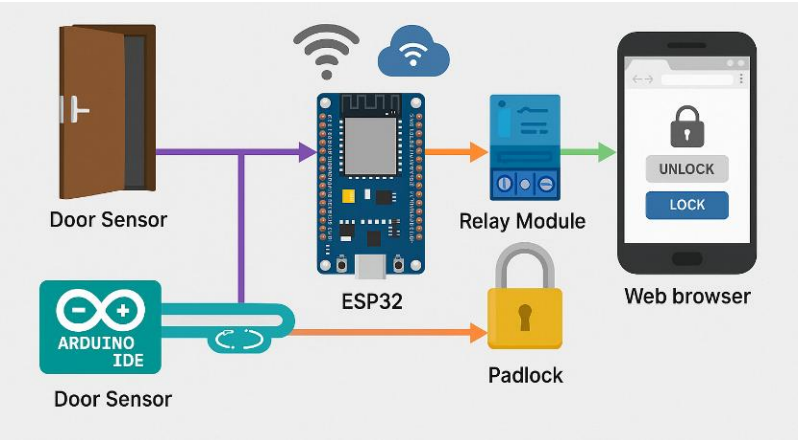

Figura 1 Funcionamiento del sistema de control inteligente

Fuente: Elaboración propia

Fase 3: Validación técnica del sistema propuesto

La tercera fase consistió en la validación del sistema mediante simulación en el entorno virtual Wokwi, que permitió comprobar el comportamiento del prototipo en condiciones controladas. Durante la simulación se verificó el funcionamiento de los sensores y del módulo relé ante los cambios de estado de cada dispositivo al ser activado, esto se visualizó por medio de la consola serial del software.

2.8. Análisis de datos

Para el análisis de los datos se aplicó una triangulación de datos, que consiste como indica Miles et al. (2014) en relacionar los resultados obtenidos a partir de diferentes fuentes y perspectivas con el objetivo de aumentar la validez y rigor científico del estudio. En este sentido, la triangulación se desarrolló mediante la combinación de entrevistas semiestructuradas, observación directa y revisión documental. Las entrevistas fueron transcritas y codificadas manualmente, utilizando un enfoque temático abierto siguiendo las indicaciones de Mojadeddi & Rosenberg (2024), que destacan la importancia de esta metodología para identificar patrones, categorías temáticas y significados a partir de categorías como: inseguridad en el acceso (relacionada con la percepción de vulnerabilidad de las puertas y cerraduras), desconocimiento tecnológico (reflejado en la falta de familiaridad de los moradores con tecnologías de control de acceso inteligentes) e interés por sistemas remotos (identificado por la disposición de los moradores en adoptar soluciones tecnológicas para mejorar la seguridad). Las entrevistas se realizaron de manera individual en los

hogares de los moradores del barrio "Los Girasoles" en Esmeraldas, entre los meses de mayo y junio. Cada sesión tuvo una duración promedio de 30 minutos por cada participante. Se garantizó la privacidad y seguridad de los participantes mediante el uso de seudónimos en lugar de sus nombres reales.

Desde este contexto uno de los participantes señaló "Entraron por la puerta principal, no tenía una chapa buena. Desde ahí tengo miedo que vuelva a pasar".

Es importante señalar que se presentaron limitaciones metodológicas como es el sesgo de autoinforme, ya que las respuestas pudieron estar influenciadas por su percepción subjetiva sobre los problemas de seguridad que afectan la precisión de los datos obtenidos. Además, la limitada familiaridad tecnológica de los entrevistados pudo haber influido en su disposición para adoptar sistemas de control de acceso.

Con base en Miles et al. (2014), las percepciones fueron contrastadas con los datos obtenidos de la observación directa de las viviendas, coincidiendo respecto al mal estado de puertas y cerraduras. Seguidamente, la información obtenida fue cotejada con la literatura técnica, comparando los hallazgos con estudios previos lo que sustentó el diseño propuesto.

3. Resultados y Discusión

3.1. Análisis de da Análisis de riesgos y amenazas en el hogar y entorno residencial

Percepción de los moradores sobre la inseguridad

A partir de las entrevistas realizadas con los 10 moradores del barrio Los Girasoles y las observaciones directas (Anexo 1), se identificó que las puertas de las viviendas presentan deficiencias estructurales. Estas deficiencias incluyen cerraduras defectuosas, materiales de baja calidad y ausencia de mecanismos de seguridad de refuerzo, lo que aumenta la vulnerabilidad a intrusiones. De acuerdo con las respuestas de los entrevistados, el 70% de los hogares tenían puertas en mal estado o cerraduras que no funcionaban correctamente, lo que expone las viviendas a robos y otros incidentes de seguridad. Además de las deficiencias estructurales, se presenta en la Tabla 2 un análisis cuantitativo de la frecuencia de robos reportados según el tipo de vivienda en el barrio "Los Girasoles", lo que permite identificar patrones de vulnerabilidad y resalta los tipos de vivienda más propensos a ser objeto de robo.

Tabla 2 Frecuencia de robos por tipo de vivienda

Tipo de vivienda	Frecuencia de robos
Viviendas con puertas reforzadas	50
Viviendas con cerraduras electrónicas	120
Viviendas con puertas deterioradas	80
Viviendas con cerraduras tradicionales	30
Total	251

Fuente: Elaboración propia

Como resultado del análisis de la Tabla 2 se evidencia que las viviendas con cerraduras electrónicas son las más atacadas, seguidas por aquellas con puertas deterioradas. Lo que sugiere que las viviendas con sistemas de seguridad antiguos son más propensas a sufrir intrusiones.

En concordancia con lo antes mencionado, uno de los entrevistados mencionó: "Yo mismo tuve que cambiar la chapa varias veces y siempre se volvía a dañar", mientras otro señaló "Cuando viajo, dejo la puerta con un candado porque la cerradura no sirve siempre"

En términos de características necesarias para mejorar la seguridad como se presenta en la Figura 2, el 70% de los entrevistados indicó que las puertas deberían contar con cerraduras electrónicas o sistemas de control de acceso inteligentes, lo que permitiría una mayor protección ante posibles intrusiones, mientras que el 80% destacó la importancia de la resistencia estructural de las puertas para evitar que sean fácilmente vulneradas. En cuanto a la viabilidad de implementar un sistema inteligente, el 90% mostró interés y disposición para adoptar tecnologías que mejoren la seguridad de sus hogares, aunque el 60% mencionó como obstáculos los costos de instalación y el 50% señaló la falta de conocimientos tecnológicos.

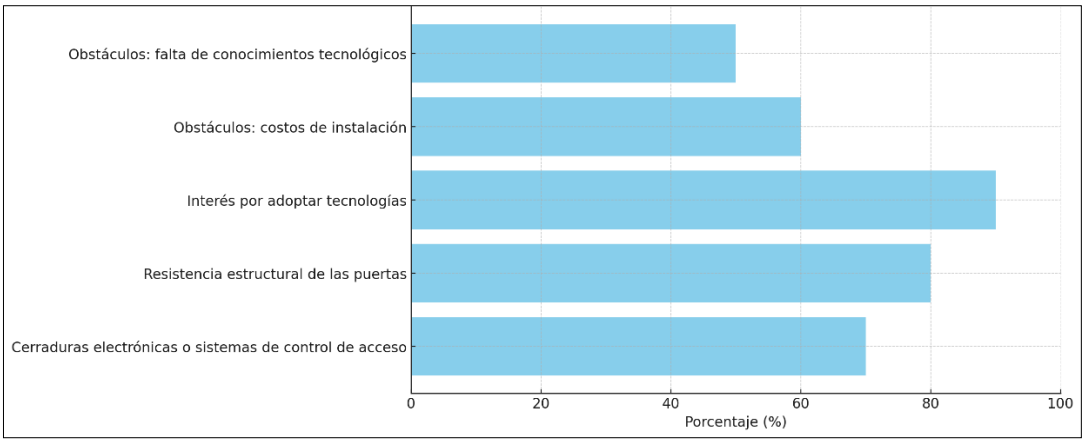

Figura 2 Resultados de la encuesta sobre seguridad en puertas residenciales

Fuente: Elaboración propia

3.2. Diseño técnico del sistema a partir de los resultados sociales

Relación entre las necesidades detectadas y la solución tecnológica

Para el diseño del sistema propuesto se utilizaron las deficiencias identificadas durante las entrevistas a los moradores del barrio "Los Girasoles". En este contexto, La Tabla 3 sintetiza la relación entre las necesidades sociales y las decisiones técnicas, como respuesta a requerimientos de alertas ante intentos de acceso no autorizado y bloqueo automático. Estas soluciones técnicas responden directamente a las percepciones y preocupaciones de seguridad manifestadas por los usuarios del barrio.

Tabla 3 Relación entre perspectiva social y decisiones técnicas

Requisito del usuario	Solución técnica implementada
Necesidad de alertas inmediatas por intento de ingreso	Sensor PIR + interfaz web con notificaciones
Inseguridad por cerraduras débiles	Relé + cerradura electrónica activada por ESP32
Falta de refuerzos físicos y vibración en accesos	Sensor de vibración conectado al microcontrolador
Necesidad de monitoreo remoto	Servidor web embebido en el ESP32

Fuente: Elaboración propia

Es así como, el diseño presentado en la Figura 3 se basó en un microcontrolador ESP32 que envía notificaciones en tiempo real a través de un servidor web embebido,

asimismo integra tres sensores cuyas señales son interpretadas por el ESP32: Reed Switch (detección de apertura), PIR (detección de movimiento) y sensor de vibración (golpes a la puerta, intento de forzarla), conectados a un relé para controlar la cerradura electrónica, y un sistema de alimentación adecuado para garantizar un funcionamiento autónomo y eficiente.

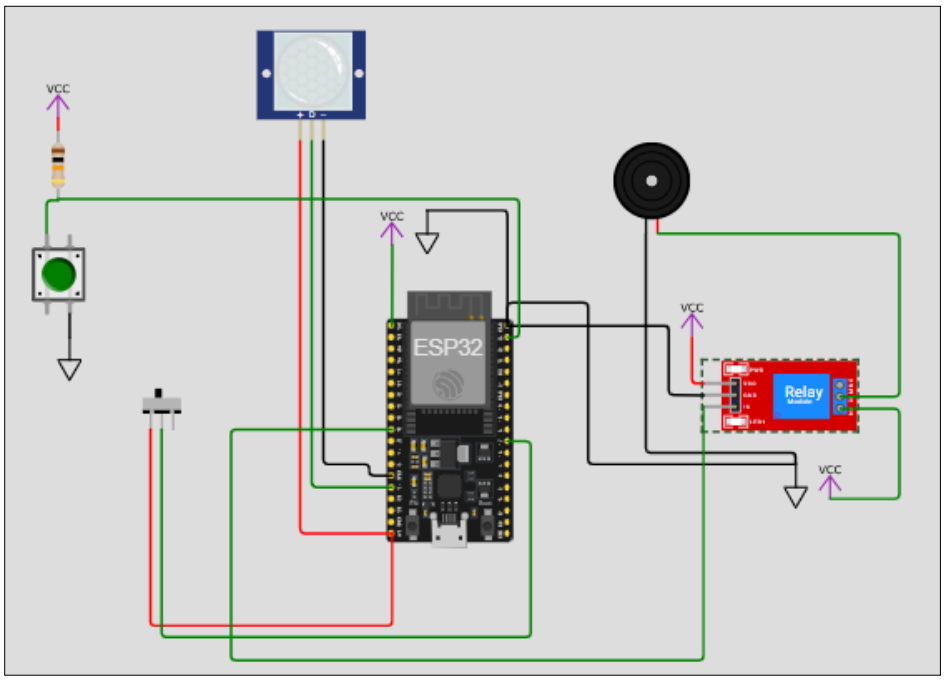

Figura 3 Esquemático del sistema de control de acceso

Fuente: Elaboración propia a partir de Wokwi (https://wokwi.com/)

3.3. Especificación de componentes del sistema de control de acceso

De acuerdo con los requerimientos técnicos que surgieron a partir de las entrevistas, se detallan a continuación, los componentes del sistema, sus características técnicas, especificaciones de voltaje y las consideraciones de conexión necesarias para facilitar la implementación física.

ESP32 (Microcontrolador): es el componente central del sistema que se encarga de gestionar los sensores y controlar la cerradura electrónica, asimismo se conecta a través de WiFi para la comunicación remota, y maneja las entradas y salidas digitales necesarias para la activación de la cerradura. El ESP32 requiere una alimentación de 5V, que se suministra a través del pin VCC, mientras que el pin GND se conecta a la tierra común del sistema. Las conexiones GPIO del ESP32 se utilizan para interactuar con los sensores y el relé, permitiendo un control eficiente y remoto.

Es importante destacar que, si el ESP32 se conecta a un puerto USB para programación, no es necesario utilizar la batería para alimentarlo, ya que la alimentación será proporcionada directamente por el puerto USB de la computadora durante la programación. Sin embargo, en la fase de operación normal, donde el sistema debe funcionar de manera autónoma, se recomienda utilizar una fuente de 5V independiente o una batería de Li-ion o LiPo que pueda alimentar al ESP32 durante su funcionamiento sin conexión a la computadora.

Sensor Reed Switch (Sensor de contacto magnético): detecta la apertura y cierre de la puerta. El sensor Reed Switch consta de un interruptor magnético que se activa cuando se acerca un campo magnético, como el de un imán colocado en la puerta. Este sensor se conecta a un pin GPIO del ESP32 (GPIO 17), configurado como entrada digital. El otro terminal se conecta a GND. Al abrirse la puerta, el campo magnético se interrumpe, lo que envía una señal HIGH al ESP32, activando el sistema de control de acceso y desencadenando las acciones necesarias.

Sensor PIR (Infrarrojo Pasivo): se utiliza para detectar movimiento cerca de la puerta. Este sensor capta la radiación infrarroja emitida por el cuerpo humano. El sensor PIR se conecta al ESP32 con una alimentación de 5V (según el modelo utilizado), y su pin de salida (OUT) se conecta a un pin GPIO del ESP32 (GPIO 12). Cuando detecta movimiento, emite una señal HIGH, lo que puede activar la cerradura o generar una alerta de seguridad dependiendo de la configuración del código.

Sensor de Vibración: detecta cambios en las vibraciones o movimientos cercanos a la puerta, lo que ayuda a identificar intentos de manipulación o intrusión en el acceso. Este sensor se conecta a un pin GPIO del ESP32 (GPIO 13) y se alimenta mediante 3.3V o 5V. Al detectar vibraciones o impactos en la puerta, el sensor emite una señal HIGH que puede activar el sistema para bloquear o desbloquear la puerta, o bien, generar una notificación de alerta.

Relé: funciona como un interruptor controlado electrónicamente que permite gestionar el encendido o apagado de la cerradura eléctrica a partir de una señal digital enviada desde el ESP32. La entrada de control del relé (IN) está conectada a un pin digital del ESP32 (GPIO 26), y el módulo recibe alimentación en sus pines VCC y GND desde el mismo microcontrolador o puede ser también de una fuente externa de 5V.

Es necesario validar que el relé tenga la capacidad suficiente para manejar el voltaje y la corriente requeridos por la cerradura (por ejemplo, 12 VDC y hasta 1 A), y que se realice un dimensionamiento adecuado de los cables y conexiones para evitar sobrecalentamientos o fallos eléctricos.

Cerradura Electrónica: se conecta entre los terminales NO (Normalmente Abierto) y COM (Común) del relé. En estado inactivo, el circuito permanece abierto y no circula corriente. Cuando el ESP32 envía una señal en nivel lógico alto (HIGH) al pin IN, el relé se activa, cerrando el contacto entre NO y COM, y permitiendo así que la corriente fluya desde la fuente de alimentación a través de la cerradura hacia GND. Este paso de corriente acciona la cerradura para abrir o bloquear la puerta, según el tipo de actuador utilizado. La elección de la cerradura debe considerar su compatibilidad con la fuente de alimentación y la capacidad del relé, de modo que soporte el mismo nivel de tensión (ejemplo, 12V) y corriente sin comprometer la integridad del sistema.

Sistema de Alimentación: El diseño del sistema de alimentación debe contemplar dos fuentes de alimentación separadas. El ESP32 debe alimentarse con 5V, mientras que la cerradura electrónica y el relé requieren una fuente de 12V, dependiendo las especificaciones de los componentes. Las baterías, deben ser capaces de alimentar ambos sistemas durante un tiempo prolongado, garantizando que el sistema funcione de manera continua, incluso en situaciones de desconexión eléctrica. Se recomienda utilizar reguladores de voltaje para asegurar una carga estable y eficiente.

Cuando el ESP32 está conectado para programación a través de un puerto USB, se alimenta directamente de la computadora, eliminando la necesidad de utilizar la batería para su operación durante esta fase. Sin embargo, para la operación normal fuera de la fase de programación, la batería se vuelve indispensable para el funcionamiento autónomo del sistema.

Cables y Conexiones: Las conexiones entre el ESP32, los sensores y el relé deben realizarse utilizando cables de calibre 22 AWG o superior para las señales de baja corriente. Para las conexiones de mayor corriente, como las que involucran el relé y la cerradura electrónica, se deben usar cables de calibre 18 AWG, adecuados para manejar las cargas correspondientes sin generar calentamiento excesivo. Es importante que todos los cables sean de cobre de alta calidad para evitar pérdidas de señal y garantizar la seguridad del sistema.

3.4. Programación del sistema de control de acceso

La programación se desarrolló en lenguaje C++ utilizando el entorno Arduino IDE como se visualiza en la Figura 4, con el microcontrolador ESP32 como unidad de procesamiento central. El código implementa una lógica condicional que evalúa tres entradas digitales: un sensor PIR (GPIO 13) para la detección de presencia humana por infrarrojo pasivo, un sensor de vibración (GPIO 23) para registrar impactos o

golpes en la estructura de la puerta, y un reed switch magnético (GPIO 17) para monitorear el estado de apertura del acceso físico.

Cuando al menos una de las tres condiciones se cumple, el sistema considera que se trata de un intento de intrusión y ejecuta una respuesta automática mediante la activación de un módulo relé (GPIO 26), el cual bloquea la cerradura eléctrica conectada. En este sentido, se actualiza una variable de estado que es publicada en una interfaz web a través de un servidor HTTP embebido en el propio ESP32, permitiendo la consulta remota del estado del sistema desde cualquier navegador dentro de la red local.

sketch.ino ● diagram.json ● Library Manager

```
#include <WiFi.h>
#include <WebServer.h>

// Credenciales Wi-Fi
const char* ssid = "Wokwi-GUEST";  // Red pública en Wokwi
const char* password = "";  // No requiere contraseña

// Páginas web locales
WebServer server(80);
String estadoAlarma = "Todo en orden.";

// Pines
const int pinPIR = 13;  // Sensor PIR
const int pinGolpe = 23;  // Sensor de golpe (sin INPUT_PULLUP)
const int pinPuerta = 17;  // Sensor de puerta
const int pinRele = 26;  // Relé para cerrar la cerradura

void setup() {
  Serial.begin(115200);  // Inicia la comunicación serial
  Serial.println("Iniciando...");

  pinMode(pinPIR, INPUT);  // Sensor PIR
  pinMode(pinGolpe, INPUT);  // Sensor de golpe (sin INPUT_PULLUP)
  pinMode(pinPuerta, INPUT);  // Sensor de puerta
  pinMode(pinRele, OUTPUT);  // Relé de la cerradura
  digitalWrite(pinRele, LOW);  // Asegúrate de que el relé esté apagado
```

sketch.ino ● diagram.json ● Library Manager

```
void setup() {

  // Conexión Wi-Fi
  WiFi.begin(ssid, password);
  Serial.println("Conectando a WiFi...");
  while (WiFi.status() != WL_CONNECTED) {
    delay(500);
    Serial.print(".");
  }
  Serial.println("\n✅ Conectado a WiFi");
  Serial.println(WiFi.localIP());  // Muestra la IP local del ESP32

  // Página principal (servidor web)
  server.on("/", []() {
    server.send(200, "text/html", "<h1>Estado del sistema:</h1><p>" + estadoAlarma + "</p>");
  });
  server.begin();
}

void loop() {
  server.handleClient();  // Escucha solicitudes web

  // Leer sensores
  bool presencia = digitalRead(pinPIR);   // Sensor PIR
  bool golpe = digitalRead(pinGolpe) == LOW;  // Si golpe detectado, el pin será LOW
  bool puerta = digitalRead(pinPuerta) == LOW;  // Si puerta abierta, el pin será LOW
```

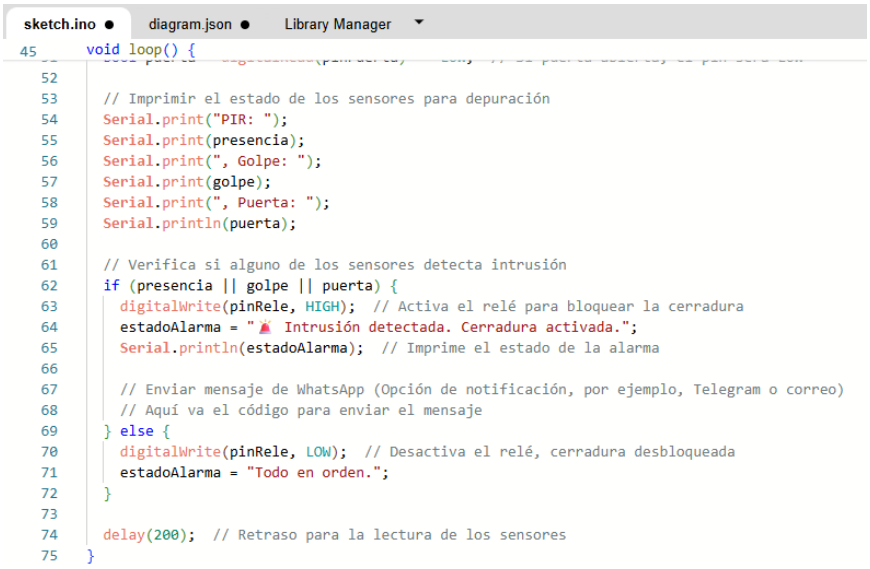

Figura 4 Programación IDE Arduino

Fuente: Elaboración propia

3.5. Validación técnica del sistema de control de acceso

Se procedió a la validación técnica del sistema propuesto mediante una simulación práctica en el entorno en línea Wokwi, que permitió comprobar el funcionamiento del prototipo en condiciones controladas siguiendo el enfoque de diversos autores (Kaushik et al., 2023; Verma et al., 2023). El diseño del circuito (ver Anexo 2) fue implementado en el simulador, replicando con precisión el comportamiento eléctrico de los componentes. Durante la simulación, la verificación del sistema se llevó a cabo a través de la consola serial de Wokwi, herramienta que muestra en tiempo real los valores de las variables y el estado de los sensores programados en el ESP32.

En la simulación (ver Anexo 2), inicialmente, todos los sensores se registraron en estado 0, lo que corresponde a inactividad. Posteriormente, al activar cada sensor se evidenció un cambio de estado a 1, acompañado de la ejecución lógica de seguridad que desencadena la activación de la cerradura electrónica mediante el relé. En este sentido, tomando como ejemplo el sensor de vibración, al presionarlo, en la consola serial se mostró el valor Golpe:1, lo que indica la detección de impacto en la puerta generando la alerta de intrusión. De esta misma forma ocurre con los sensores Reed Switch (Puerta: 1) y Sensor Infrarrojo (PIR: 1). En todos los casos el sistema respondió con el mensaje “Intrusión detectada. Cerradura activada”, validando que la lógica de control y seguridad implementada en el código se ejecuta de manera correcta. Por

último, el ESP32 simuló la conexión a la red WiFi, mostrando en la consola la dirección IP asignada al dispositivo (10.0.0.2), evidenciando la capacidad de comunicación del microcontrolador con otros dispositivos a través de la red local.

Cabe indicar que la validación técnica se realizó sobre un prototipo funcional en un entorno simulado, esto constituye una limitación metodológica. Sin embargo, en una fase posterior se sugiere realizar pruebas piloto bajo condiciones reales.

También es importante considerar que, aunque el sistema cumplió con los requerimientos sociales que se identificaron, al mismo tiempo surgieron ciertas limitaciones de considerar la optimización del consumo energético del ESP32, ya que, aunque el prototipo fue probado solo en un entorno simulado y no se realizaron pruebas prolongadas en un contexto real, podría provocar inconvenientes de rendimiento a largo plazo. Esta limitación coincide con el estudio de Sahu et al. (2022) donde destacan que el gasto energético es un factor clave al momento de implementar sistemas IoT de bajo costo, sin embargo, difiere con otros autores como Goyal et al. (2024) que realizaron un estudio aplicando pruebas de eficiencia energética en un entorno real. También se evidenció como una limitación, el bajo conocimiento tecnológico de algunos moradores (50% de los entrevistados) coincidiendo con los trabajos de Sahu et al. (2022) y Sivaprasad et al. (2023) que destacan el acompañamiento formativo en entornos de alta vulnerabilidad. Por el contrario, Gayathri et al. (2024) difiere al mencionar que los usuarios presentaron una mayor disposición a adoptar tecnologías de forma empírica.

Asimismo, es importante destacar que la validación del sistema solamente se llevó a cabo en un entorno de simulación, impidiendo la detección de fallos potenciales como variaciones de energía eléctrica o pérdida de conectividad WiFi. Este enfoque se asemeja a lo indicado en el estudio de Aldawira et al. (2019), donde realizaron simulaciones, pero no se integraron pruebas de conectividad; siendo una desventaja al momento de medir indicadores técnicos cuantitativos como tiempos de respuesta o tasa de error, lo que podría sugerir una limitación en la evaluación de la efectividad difiriendo con otros estudios con mediciones más precisas como el de Motwani et al. (2021) y Vats et al. (2024).

3.6. Discusión crítica de los resultados

Los resultados obtenidos muestran que el 70% de los moradores considera necesarios los sistemas inteligentes y que el 90% percibe disposición a adoptarlos, aunque con ciertas limitaciones asociadas a costos y conocimientos. Este hallazgo coincide parcialmente con los resultados de Sayeduzzaman et al. (2024) que reportan un nivel

de aceptación superior al 80% en zonas urbanas con mayor despliegue de infraestructura. Sin embargo, difiere de lo observado en otros contextos rurales tal como se muestra en la investigación de Emerllahu & Bogataj (2024) donde la adopción de sistemas inteligentes no supera el 50% debido a la falta de conectividad. Desde este contexto, el caso del barrio "Los Girasoles" representa un escenario intermedio donde existe una alta disposición social pero también se presentan problemas económicos y técnicos que condicional la adopción real del sistema.

Desde un enfoque conceptual, los hallazgos se alinean con el modelo de aceptación tecnológica (TAM) que plantea la intención del uso de una tecnología varía desde la percepción de la utilidad y facilidad de uso (Sugiyono & Hidayah, 2024). En este análisis de evidenció que la percepción de utilidad es alta, por el contrario, la percepción de facilidad de uso se ve limitada por la baja alfabetización, lo que sustenta la necesidad de capacitaciones comunitarias. En línea con lo antes mencionado Rubiyanti et al. (2023) señala que la adopción de nuevas tecnologías se basa en aspectos como la compatibilidad con los requerimientos de los usuarios.

Finalmente, la investigación refleja la importancia de factores sociales en la adopción la alfabetización digital detectada en el 50% de los moradores coinciden con lo señalado por Motwani et al. (2021) que indican que la falta de formación técnica reduce la efectividad de los sistemas inteligentes implementados.

3.7. Buenas prácticas para la prevención de riesgos sociales en el hogar: enfoque en seguridad residencial

Desde el punto de vista de la seguridad, las puertas residenciales en general, deben ser evaluadas no solo en términos de su resistencia estructural, sino también en su interacción con los sistemas tecnológicos. Esto implica integrar cerraduras electrónicas, sensores de contacto magnético, infrarrojos y vibración, que no solo detectan intentos de intrusión, sino también que permitan una respuesta inmediata a través de un sistema de alertas remotas. Es fundamental que estos dispositivos trabajen en conjunto con redes Wi-Fi locales o incluso tecnologías como el Bluetooth, asegurando la conectividad en áreas con infraestructura limitada (Gadupu et al., 2021; Sahu et al., 2022).

En cuanto a la integración tecnológica, una de las principales barreras es la falta de cultura tecnológica entre los habitantes. Por esta razón, no solo se debe implementar el sistema, sino también promover la alfabetización digital en la comunidad, ya que como indica Kabir et al. (2022) y Motwani et al. (2021) esta se presenta no solo como un obstáculo para la adopción, sino también como un factor que puede dificultar el

uso eficiente de tecnologías que dependan de la interacción con los dispositivos conectados.

Para mitigar esta limitación no solo basta con implementar el sistema, sino también es necesario diseñar estrategias de formación accesibles y adaptadas a las características socioeconómicas y educativas de los moradores, para que se familiaricen con el funcionamiento del sistema, desde la instalación hasta su operación diaria (Oliveira et al., 2021).

En cuanto a las estrategias de mejora, se requieren talleres prácticos y accesibles donde los moradores interactúen con los dispositivos, aprender a utilizarlos en un entorno controlado y recibir formación práctica sobre su instalación, uso y mantenimiento; crear tutoriales y guías visuales fáciles de entender, que expliquen el funcionamiento de los sistemas de control de acceso, utilizando gráficos, diagramas y videos cortos que permiten integrarse de manera sencilla; establecer puntos de contacto dentro de la comunidad, líderes locales o técnicos capacitados que proporcionen soporte personalizado para resolver inquietudes del uso diario de los sistemas, mediante el desarrollo de una interfaz intuitiva y eficaz del sistema (Creswell & Poth, 2016; Lee & Mun, 2023).

Por otra parte, la ética también resulta un aspecto prioritario en la implementación de estas tecnologías. Los sistemas de control de acceso deben garantizar la privacidad de los usuarios, evitando la recolección innecesaria de datos personales y asegurando que las medidas de seguridad no invadan la intimidad del hogar (Gayathri et al., 2024). Por último, el costo de implementación debe ser accesible para la mayoría de los habitantes, especialmente en áreas de recursos limitados. Aunque el sistema tiene el potencial de mejorar significativamente la seguridad, se deben explorar alternativas que minimicen el costo de implementación y mantenimiento, tales como el uso de componentes de bajo costo y la optimización de la conectividad (Arsana, 2021; Xu et al., 2024).

No obstante, siguiendo las recomendaciones de Singh et al. (2024) se debe continuar evaluando su desempeño a largo plazo en el contexto real del barrio, con el fin de realizar ajustes que optimicen la funcionalidad del sistema y promuevan una integración más profunda con la comunidad.

4. CONCLUSIONES

La investigación evidenció que la inseguridad en el acceso a las viviendas del barrio "Los Girasoles", está asociada a deficiencias estructurales en puertas y cerraduras y a la ausencia de mecanismos tecnológicos de protección. En este sentido, el diseño desarrollado que contempla ESP32, sensores acordes a los requerimientos de seguridad detectados y cerradura electrónica, es técnicamente viable y funcional de acuerdo con la simulación realizada y se concibió aceptable por los moradores.

Además, este diseño es adaptado a las condiciones de un sector específico con base en el análisis de riesgos identificado. Lo que permitió el establecimiento de una propuesta de buenas prácticas para la prevención de riesgos asociados a la seguridad residencial, que integró aspectos tecnológicos y formación comunitaria.

El estudio aporta a la literatura sobre seguridad doméstica en contextos con alta vulnerabilidad, adaptando tecnologías IoT de bajo costo hacia contextos socioeconómicos que requieren intervención. Es decir, este modelo puede ser replicable a otras zonas con similares características de riesgo.

Entre las principales limitaciones se identificó la falta de infraestructura tecnológica en los hogares analizados, el costo de implementación del sistema y la limitada alfabetización digital. Asimismo, la investigación no incluyó una prueba longitudinal del despliegue del sistema en condiciones reales, quedando una brecha en la investigación para validar las implicaciones del mismo a lo largo del tiempo.

Por último, futuros estudios podrían orientarse al análisis del impacto social del sistema implementado y en estrategias de reducción de costos para garantizar la sostenibilidad de la solución tecnológica.

CONFLICTO DE INTERÉS

Los autores declaran que no existen conflictos de interés de ninguna naturaleza en la presente investigación.

REFERENCIAS

Abd, N., Rathakrishnan, M., & Krishnasamy, H. (2020). A pilot test for establishing validity and reliability of qualitative interview in the blended learning English proficiency course. *Journal of critical reviews*, *7*(05), 140-143. http://dx.doi.org/10.31838/jcr.07.05.23

Aldawira, C. R., Putra, H. W., Hanafiah, N., Surjarwo, S., & Wibisurya, A. (2019). Door security system for home monitoring based on ESp32. *Procedia Computer Science*, *157*, 673-682. https://doi.org/10.1016/j.procs.2019.08.218

Ansari, A. M., Nazir, M., & Mustafa, K. (2024). Smart homes app vulnerabilities, threats, and solutions: A systematic literature review. *Journal of Network and Systems Management*, *32*(2), 29. https://doi.org/10.1007/s10922-024-09803-1

Arora, D., Venkat, A. K., & Asuti, M. G. (2025, January). Knock Detecting Door Unlock System using IOT. In *2025 International Conference on Intelligent and Innovative Technologies in Computing, Electrical and Electronics (IITCEE)* (pp. 1-6). IEEE. https://doi.org/10.1109/IITCEE64140.2025.10915380

Creswell, J. W., & Poth, C. N. (2016). *Qualitative inquiry and research design: Choosing among five approaches*. Sage publications.

Desnanjaya, I., & Arsana, I. (2021). Home security monitoring system with IoT-based Raspberry Pi. *Indones. J. Electr. Eng. Comput. Sci*, *22*(3), 1295. https://doi.org/10.11591/ijeecs.v22.i3.pp1295-1302

Efe, E. E.., & Ogunlere, S. (2020). Design and Implementation of a Mobile-Based Home Security System. *American Scientific Research Journal for Engineering, Technology, and Sciences*, *72*(1), 101–112. https://asrjetsjournal.org/index.php/American_Scientific_Journal/article/view/6202

Elvira, M., Sainuddin, S., Purnama, D. N., & Mukti, T. (2024). Evaluating Content Validity Trends Across Years: A Systematic Dataset Review. *Data in Brief*. https://dx.doi.org/10.2139/ssrn.4726776

Emerllahu, V., & Bogataj, D. (2024). Smart Villages as infrastructure of rural areas: Literature review and research agenda. *IFAC-PapersOnLine*, *58*(3), 268-273. https://doi.org/10.1016/j.ifacol.2024.07.162

Gadupu, H., Mokharji, O., Kankaria, R., Kumar, S., & Jayavel, K. (2021). ACCESS-IoT enabled smart lock. *International Journal of Reconfigurable and Embedded Systems*, *10*(3), 176. https://doi.org/10.11591/ijres.v10.i3.pp176-185

Gayathri, S., Prasad, A. S., Niteesh, H. D., Naik, K. T., Hurakadli, S., & Vishal, R. (2024, November). Low Cost IOT Based Smart Monitoring System. In *2024 International Conference on Recent Advances in Science and Engineering Technology (ICRASET)* (pp. 1-6). IEEE. https://doi.org/10.1109/ICRASET63057.2024.10895461

Goyal, P.K., Giri, M., Verma, S. (2024). IoT-Based Smart Door Lock System with Face Recognition Using ESP32 CAM and Android App. In: Shaw, R.N., Siano, P.,

Makhilef, S., Ghosh, A., Shimi, S.L. (eds) Innovations in Electrical and Electronic Engineering. ICEEE 2023. Lecture Notes in Electrical Engineering, vol 1115. Springer, Singapore. https://doi.org/10.1007/978-981-99-8661-3_27

Hammi, B., Zeadally, S., Khatoun, R., & Nebhen, J. (2022). Survey on smart homes: Vulnerabilities, risks, and countermeasures. *Computers & Security*, *117*, 102677. https://doi.org/10.1016/j.cose.2022.102677

Kabir, S., Gope, P., & Mohanty, S. P. (2022). A security-enabled safety assurance framework for IoT-based smart homes. *IEEE Transactions on Industry Applications*, *59*(1), 6-14. https://doi.org/10.1109/TIA.2022.3176257

Kaushik, P., Kumar, H., & Tyagi, N. (2024, May). Improving home security through facial recognition in a smart environment. In *2023 International Conference on Smart Devices (ICSD)* (pp. 1-6). IEEE. https://doi.org/10.1109/ICSD60021.2024.10751272

Kruglov, A., Succi, G., Kholmatova, Z. (2023). Metrics of Sustainability and Energy Efficiency of Software Products and Process. In: Developing Sustainable and Energy-Efficient Software Systems. SpringerBriefs in Computer Science. Springer, Cham. https://doi.org/10.1007/978-3-031-11658-2_2

Lee, C. S., & Mun, H. K. (2023). Development of a Smart Edge Device for Home Security. In *2023 4th International Informatics and Software Engineering Conference (IISEC)* (pp. 1-5). IEEE. https://doi.org/10.1109/IISEC59749.2023.10391000

Manjula, V., Panicker, P., & Nainar, A. (2024). Autonomously reactive home security system using internet of things. In *2024 5th International Conference on Innovative Trends in Information Technology (ICITIIT)* (pp. 1-6). IEEE. https://doi.org/10.1109/ICITIIT61487.2024.10580736

Miles, M., Huberman, A., & Saldaña, J. (2014). *Qualitative Data Analysis: A Methods Sourcebook*. 3rd ed. Arizona State University, CA: Sage. https://us.sagepub.com/en-us/nam/qualitative-data-analysis/book246128

Mojadeddi, Z., & Rosenberg, J. (2024). Automated transcription of interviews in qualitative research using artificial intelligence: a simple guide. J Surg Res Prac, 5, 1-6. https://doi.org/10.46889/JSRP.2024/5204

Motwani, Y., Seth, S., Dixit, D., Bagubali, A., & Rajesh, R. (2021). Multifactor door locking systems: A review. *Materials Today: Proceedings*, *46*, 7973-7979. https://doi.org/10.1016/j.matpr.2021.02.708

Oliveira, C., Silva, Í. R., da Silva, T., Santos, K. A., Albernaz, M., & da Silva, M. (2021). Methodological path to reach the degree of saturation in qualitative research: grounded theory. *Revista brasileira de enfermagem*, *75*(02), e20201379. https://doi.org/10.1590/0034-7167-2020-1379

Özdemir, A. (2019). Development of a Dual Response Optimization Model under Non-standard Experimental Design Situations. In *SETSCI-Conference Proceedings* (Vol. 9, pp. 316-319). SETSCI-Conference Proceedings. https://doi.org/10.36287/setsci.4.6.081

Portase, R. L., Dragotoniu, A. M., Lemnaru, C., Dinsoreanu, M., & Potolea, R. (2024). Advancing IoT Data Utilization: Generating and Evaluating Synthetic Time Series Data. In *2024 IEEE 20th International Conference on Intelligent Computer Communication and Processing (ICCP)* (pp. 1-8). IEEE. https://doi.org/10.1109/ICCP63557.2024.10792997

Redacción Primicias (2024). Criminales estarían regresando a Esmeraldas tras militarización de Los Ríos y Manabí. *PRIMICIAS*. https://www.primicias.ec/noticias/seguridad/esmeraldas-rebrote-violencia-muertes-extorsiones/

Rubiyanti, N., Sujak, A. F. A., Madiawati, P. N., & Nurutami, F. (2023, August). Perceived usefulness: a bibliometric visualization. In *2023 International Conference on Digital Business and Technology Management (ICONDBTM)* (pp. 1-6). IEEE. https://doi.org/10.1109/ICONDBTM59210.2023.10327098.

Sahu, S., Singh, R., Arya, P., & Nirala, R. (2022). Smart home automation lighting system and smart door lock using internet of things. In *2022 4th International Conference on Advances in Computing, Communication Control and Networking (ICAC3N)* (pp. 1320-1325). IEEE. https://doi.org/10.1109/ICAC3N56670.2022.10074243

Satish, S., Belgaonkar, S., Aravind, M., Santhosh, N. (2024). Secure Automated Smart Home. In *11th International Conference on Electrical Engineering, Computer Science and Informatics (EECSI)*, 615-620.https://doi.org/10.1109/EECSI63442.2024.10776090

Sayeduzzaman, M., Hasan, T., Nasser, A. A., & Negi, A. (2024). An internet of things-integrated home automation with smart security system. *Automated secure computing for next-generation systems*, 243-273. https://doi.org/10.1002/9781394213948.ch13

Singh, A. K., Nagarathna, H., Krishna, M., & Keshav, M. (2024). Design and Implementation of Smart Door Lock System Using IoT. In *2024 8th International Conference on Computational System and Information Technology for Sustainable Solutions (CSITSS)* (pp. 1-4). IEEE. https://doi.org/10.1109/CSITSS64042.2024.10816710

Sivaprasad, R., Yazhini, C., Harini, G. S., Jayashree, J., & Prathibanandhi, K. (2023). Automatic Door Locking System in Households Using IoT. In *2023 Intelligent Computing and Control for Engineering and Business Systems (ICCEBS)* (pp. 1-4). IEEE. https://doi.org/10.1109/ICCEBS58601.2023.10449123

Sugiyono, & Hidayah, V. M. (2024). Pemodelan Teknologi dalam Aplikasi KitaLulus untuk Lowongan Pekerjaan Menggunakan Metode Technology Acceptance Model (TAM). *Jurnal Indonesia: Manajemen Informatika Dan Komunikasi*, *5*(3), 2801-2812. https://doi.org/10.35870/jimik.v5i3.1014

Touqeer, H., Zaman, S., Amin, R., Hussain, M., Al-Turjman, F., & Bilal, M. (2021). Smart home security: challenges, issues and solutions at different IoT layers. *The Journal of Supercomputing*, *77*(12), 14053-14089. https://doi.org/10.1007/s11227-021-03825-1

Vats, G., Tanwar, S., & Sharma, P. K. (2024). A Simulation-Based Analysis of IoT Security Architecture in Smart Homes. In *2024 International Conference on Computing, Sciences and Communications (ICCSC)* (pp. 1-4). IEEE. https://doi.org/10.1109/ICCSC62048.2024.10830301

Vergni, L., Todisco, F. & Di Lena, B. (2021). Evaluation of the similarity between drought indices by correlation analysis and Cohen's Kappa test in a Mediterranean area. *Nat Hazards*, 108, 2187–2209. https://doi.org/10.1007/s11069-021-04775-w

Verma, A., Srivastava, A., Gupta, I., & Nirala, R. (2023). Revolutionizing IoT-based Home Automation using Arduino. *Int. J. Res. Appl. Sci. Eng. Technol*, *11*(12), 4576-4582. https://doi.org/10.22214/ijraset.2023.52623

Wu, T., Yun, X., Liu, Y., Liang, C., Xue, Y., & Liu, Y. (2023). Study on Intelligent door lock system based on Internet of Things and intelligent identification technology. *Highlights in Science, Engineering and Technology*, *56*, 243-245.

Xu, F., Jiang, Y., Yang, S., & Liu, Y. (2024). Design and Implementation of Personal Smart Home System Based on Edge Computing Gate. In *2024 5th International Conference on Computer Engineering and Intelligent Control (ICCEIC)* (pp. 25-29). IEEE. https://doi.org/10.1109/ICCEIC64099.2024.10775823

Yin, R. K. (2018). *Case Study Research and Applications: Design and Methods*. Sage Publications.

Zambonino, M. (2023). Perspectiva del Turismo ante la inseguridad en Esmeraldas, Ecuador. *Revista Internacional de Gestión, Innovación y Sostenibilidad Turística-RIGISTUR-ISSN 2806-5700*, *3*(1), 97-103. https://doi.org/10.51260/rigistur.v3i1.380