UNIVERSIDAD LAICA ELOY ALFARO DE MANABÍ

Facultad:

CIENCIAS DE LA VIDA Y TECNOLOGÍAS

Carrera:

TECNOLOGÍAS DE LA INFORMACIÓN

Tema:

ANÁLISIS DE UN SISTEMA DE SEGURIDAD BASADO EN LA NORMA IEEE 802.11 DEL BLOQUE DE LA CARRERA DE AGROINDUSTRIA DE LA FACULTAD DE CIENCIAS DE LA VIDA Y TECNOLOGÍAS DE LA ULEAM

Autor/es

BRAVO PONCE DARLIN ALEXANDER

LUCAS MINALLA ANA BRIGITTE

2024

CERTIFICACIÓN DEL TUTOR

CERTIFICACIÓN

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

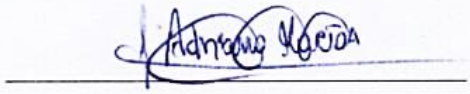
Haber dirigido, revisado y aprobado preliminarmente el Trabajo de Integración Curricular bajo la autoría de los estudiantes Lucas Minalla Ana Brigitte y Bravo Ponce Darlin Alexander, legalmente matriculados en la carrera de Tecnologías de la Información, período académico 2024-2025, cumpliendo el total de 380 horas, cuyo tema del proyecto **"ANÁLISIS DE UN SISTEMA DE SEGURIDAD BASADO EN LA NORMA IEEE 802.11 DEL BLOQUE DE LA CARRERA DE AGROINDUSTRIA 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, 13 de enero de 2025.

Lo certifico,



Ing. Adriana Macia Espinales, Mg.
Docente Tutor(a)
Área: Ciencias Exactas

DECLARACION TRIBUNAL EVALUADOR

"Declaramos haber revisado el trabajo, "Análisis de un Sistema se seguridad basado en la norma IEEE 802.11 del bloque de la carrera de Agroindustria de la Facultad de Ciencias de la Vida y Tecnologías de la Uleam", a través de tutorías periódicas con los estudiantes, LUCAS MINALLA ANA BRIGITTE Y BRAVO PONCE DARLIN ALEXANDER, dando cumplimiento a todas las disposiciones vigentes que regulan los Trabajos de Titulación".

Dra. Dolores Muñoz Verduga, PhD
Presidente del Tribunal de Titulación

Ing. Mike Machuca Avalos, Mg
Miembro Tribunal de Titulación

Arq. Luigi Pihuave Calderón, Mg
Miembro Tribunal de Titulación

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

"ANÁLISIS DE UN SISTEMA SE SEGURIDAD BASADO EN LA NORMA IEEE 802.11 DEL BLOQUE DE LA CARRERA DE AGROINDUSTRIA 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:

Bravo Ponce Darlin Alexander

Lucas Minalla Ana Brigitte

Dra. Dolores Muñoz Verduga, PhD
Presidente del Tribunal de Titulación

Ing. Mike Machuca Avalos, Mg
Miembro Tribunal de Titulación

Arq. Luigi Pihuave Calderón, Mg
Miembro Tribunal de Titulación

Manta, enero del 2025

DECLARACIÓN EXPRESA DE AUDITORÍA

Yo, Lucas Minalla Ana Brigitte de ciudadanía 1315247302 y Bravo Ponce Darlin Alexander de ciudadanía 1316689684; hacen constar que son los autores del siguiente proyecto de titulación Titulado: "ANÁLISIS DE UN SISTEMA SE SEGURIDAD BASADO EN LA NORMA IEEE 802.11 DEL BLOQUE DE LA CARRERA DE AGROINDUSTRIA DE LA FACULTAD DE CIENCIAS DE LA VIDA Y TECNOLOGÍAS DE LA ULEAM", el cual constituye una elaboración personal realizada únicamente con la dirección de los asesores de dicho trabajo Ing. Adriana Macia Espinales, Mg. En tal sentido, manifestamos la originalidad de la Conceptualización del trabajo, interpretación de datos y la elaboración de las conclusiones, dejando establecido que aquellos aportes intelectuales de otros autores se han referenciado formalmente en el texto de dicho trabajo.

Lo certifica,

Lucas Minalla Ana Brigitte
Cedula: 1315247302
Correo: e1315247302@live.uleam.edu.ec

Bravo Ponce Darlin Alexander
Cedula: 1316689684
Correo: e1316689684@live.uleam.edu.ec

Agradecimiento

"A veces, para poder ver la luz, primero hay que enfrentar la oscuridad." – Inferno, Dan Brown.

Agradezco primero a Dios, cuya luz ha sido mi guía en los momentos más oscuros. Él me ha dado la fortaleza y el valor para enfrentar cada desafío en este camino lleno de aprendizajes.

A mis padres, por ser mi faro constante de amor y apoyo. Su sacrificio y confianza en mí han sido el motor que me impulsó a superar cada obstáculo. Gracias por ser mi ejemplo de esfuerzo, perseverancia y dedicación.

A mi familia, por su apoyo durante este proceso y por estar presentes de distintas maneras en los momentos que más lo necesité. Su respaldo ha sido una parte importante para alcanzar este logro.

A mis profesores, en especial a mi tutora por su guía, paciencia y orientación. Su dedicación no solo ha enriquecido mi trabajo, sino que también ha sido clave en mi crecimiento académico y personal.

A mi compañero de proyecto, gracias por tu dedicación, esfuerzo y compromiso a lo largo de este proceso. A pesar de las dificultades, siempre estuviste presente, demostrando que el trabajo en equipo puede superar cualquier obstáculo. Este logro también es el reflejo de nuestra perseverancia conjunta.

A mis compañeros y amigos, por su apoyo y compañía en los momentos más difíciles. Sus palabras de ánimo y su presencia hicieron más llevadero este camino.

Finalmente, agradezco a todos aquellos que, de alguna manera, contribuyeron a este logro, tanto a quienes estuvieron presentes como a aquellos que, aunque ya no están, dejaron en mí enseñanzas y recuerdos que me guiaron en este camino. Este trabajo es un reflejo del crecimiento, las lecciones aprendidas, los retos superados y las luces halladas, incluso en los momentos en que la oscuridad parecía envolverlo todo

Dedicatoria

"Si puedes creer, al que cree todo le es posible." – Marcos 9:23

Dedico este trabajo a Dios, quien siempre ha sido mi guía y mi refugio en los momentos más difíciles. Su luz ha iluminado mi camino, incluso cuando parecía perdido, recordándome que, entre tanta oscuridad y el fondo más profundo que se pueda tocar, siempre hay una luz que nos impulsa a seguir adelante.

A mi familia, especialmente a mis padres, por ser mi pilar incondicional. Sus sacrificios, amor y confianza me dieron la fuerza para enfrentar cada obstáculo y superar cada reto. Sin su apoyo constante, este logro no habría sido posible.

Dedico este trabajo a quienes han sido parte de mi vida en este camino, tanto a los que me acompañaron físicamente como a aquellos que, aunque ya no están, dejaron una huella imborrable en mi corazón. Gracias por su apoyo constante, por las palabras de ánimo y por su confianza en mis capacidades

Y me dedico este trabajo a mí mismo, porque sé cuánto esfuerzo y sacrificio he invertido para llegar hasta aquí. Entre largas jornadas de trabajo, noches de desvelo y momentos de agotamiento, nunca dejé de luchar por mis sueños. Hoy celebro el camino recorrido y me enorgullezco de no haberme rendido, sabiendo que, incluso en los momentos más oscuros, siempre hay una luz que guía nuestro camino.

Este trabajo representa no solo un logro académico, sino también una victoria personal que demuestra que, con perseverancia, esfuerzo, determinación y fe, todo es posible

Agradecimiento

Quiero comenzar expresando mi más sincero agradecimiento a mi tutora. Por su guía, paciencia y apoyo a lo largo de este camino fueron fundamentales. Su compromiso no solo ayudo a superar las dificultades, sino que también me inspiró a esforzarme más.

A mis padres, no tengo palabras suficientes para agradecerles. Gracias por estar ahí siempre, por su amor incondicional, por sus sacrificios y por ser mi mayor motivación. Este logro es tan mío como suyo, porque sin ustedes, nunca habría llegado hasta aquí.

A mis abuelos, quienes siempre han sido una fuente de inspiración. Sus consejos, su apoyo incondicional y sus palabras llenas de cariño me dieron la fuerza necesaria para no rendirme, incluso en los momentos más difíciles.

También quiero agradecer a mis profesores y compañeros. A los primeros, por compartir sus conocimientos y por su dedicación a lo largo de mi formación. A los segundos, por su apoyo, y por los momentos compartidos que hicieron de este proceso una experiencia única.

Asimismo, agradezco a mi compañera de proyecto, con quien compartí cada paso de este recorrido. Su dedicación y trabajo en equipo hicieron de este proceso una experiencia mucho más llevadera y significativa. Juntos logramos este gran objetivo.

Por último, gracias a todas las personas que, de una forma u otra, aportaron su granito de arena. Cada palabra de aliento, cada gesto de apoyo y cada consejo marcaron la diferencia. Este es un logro colectivo, y estoy profundamente agradecido.

.

Dedicatoria

Dedico este trabajo a Dios principalmente, ya que él me ha dado la fuerza y la salud para superar cada desafío y completar con éxito esta etapa.

A mis padres, que han sido mi mayor apoyo en todo momento. Gracias por creer en mí, incluso cuando yo dudaba de mí mismo. Su amor, sus consejos y su ejemplo de vida me enseñaron a perseverar y a nunca rendirme.

A mis abuelos, que han sido como una fuente de inspiración, con sus sabios consejos y su amor incondicional que me mantuvo adelante.

A toda mi familia, que con su amor y apoyo incondicional estuvieron presentes en cada etapa de este proceso. Su confianza en mí y sus palabras de ánimo me dieron la fuerza para superar cualquier obstáculo.

También quiero dedicar este trabajo a mi tutora, a los profesores que compartieron su conocimiento conmigo y a mis compañeros, quienes con su colaboración y compañerismo hicieron de este camino una experiencia muy enriquecedora y significativa.

Y, por último, dedico este logro a todas esas personas que estuvieron ahí para levantarme cuando lo necesitaba. A quienes creyeron en mí y me empujaron a seguir adelante. Este trabajo es para ustedes, porque cada palabra y cada página también llevan su huella.

Tabla de contenido

Índice de Tablas

Índice de Figuras

Resumen

En un mundo donde la conectividad inalámbrica es esencial para gestionar y transmitir información, aseverar la seguridad de estos sistemas se ha convertido en una prioridad. Este estudio analiza la implementación de un sistema de seguridad basado en la norma IEEE 802.11 en la carrera de Agroindustrias de la Facultad de Ciencias de la Vida y Tecnología de la Universidad Laica Eloy Alfaro de Manabí (ULEAM), con el objetivo de evaluar su efectividad, identificar vulnerabilidades y proponer mejoras orientadas a proteger la información y optimizar el desempeño de los sistemas.

La investigación se realizó a través de un enfoque exploratorio y descriptivo, utilizando un muestreo no probabilístico intencional. Se recopilaron datos de un total de 260 participantes, entre los cuales se incluían docentes, personal administrativo y estudiantes, además de 7 encuestas adicionales que fueron aplicadas a personal especializado. Este grupo focal proporcionó una visión completa sobre la situación actual de la red y los desafíos que enfrentan en cuanto a sus sistemas de seguridad.

Los hallazgos revelaron deficiencias en la actualización de los protocolos de seguridad, falta de formación adecuada del personal técnico y escasa conciencia de los usuarios sobre prácticas seguras. Estas vulnerabilidades, junto con el uso intensivo de la red, representan un riesgo significativo para la integridad, confidencialidad y disponibilidad de la información.

En resumen, se proponen estrategias prácticas para fortalecer tanto la seguridad del sistema como la gestión de la red, como la implementación de protocolos avanzados, la formación continua del personal y campañas de concienciación para los usuarios. Estas medidas tienen como objetivo optimizar la infraestructura tecnológica y asegurar un entorno digital seguro y eficaz para toda la comunidad académica.

El estudio no solo ofrece un análisis crítico del sistema de seguridad de la red, sino que también establece un plan de acción para futuras mejoras, contribuyendo al fortalecimiento de la seguridad tecnológica en entornos educativos y sentando las bases para investigaciones futuras en la ULEAM y en instituciones similares.

Palabras claves:

Redes inalámbricas, seguridad informática, IEEE 802.11, gestión de redes, vulnerabilidades, infraestructura tecnológica, protocolos de seguridad, capacitación técnica, sensibilización de usuarios, entornos educativos, evaluación de riesgos, mejoras tecnológicas, carrera de Agroindustrias, Facultad de Ciencias de la Vida y Tecnología, ULEAM

Abstract

In a world where wireless connectivity is essential for managing and transmitting information, ensuring the security of these systems has become a priority. This study analyzes the implementation of a security system based on the IEEE 802.11 standard in the Agroindustry program at the Faculty of Life Sciences and Technology of Universidad Laica Eloy Alfaro de Manabí (ULEAM). The objective is to evaluate its effectiveness, identify vulnerabilities, and propose improvements aimed at protecting information and optimizing system performance.

The research employed an exploratory and descriptive approach, using an intentional non-probabilistic sampling method. Data was collected from a total of 260 participants, including faculty, administrative staff, and students, as well as from 7 additional surveys administered to specialized personnel. This focus group provided a comprehensive perspective on the current state of the network and the challenges related to its security systems.

The findings revealed deficiencies in updating security protocols, inadequate training of technical staff, and a lack of user awareness regarding secure practices. These vulnerabilities, combined with intensive network usage, pose significant risks to the integrity, confidentiality, and availability of information.

In summary, practical strategies are proposed to strengthen both system security and network management. These include implementing advanced protocols, continuous staff training, and user awareness campaigns. These measures aim to optimize the technological infrastructure and ensure a secure and efficient digital environment for the entire academic community.

This study not only provides a critical analysis of the network's security system but also establishes an action plan for future improvements. It contributes to the enhancement of technological security in educational settings and lays the groundwork for further research at ULEAM and similar institutions.

Keywords:

Wireless networks, information security, IEEE 802.11, network management, vulnerabilities, technological infrastructure, security protocols, technical training, user awareness, educational environments, risk assessment, technological improvements, Agroindustry program, Faculty of Life Sciences and Technology, ULEAM.

Capítulo I: Introducción

1.1. Introducción

¿Qué tan seguras son las instituciones educativas frente a las amenazas que afectan tanto la infraestructura tecnológica como la integridad de sus espacios físicos? En un mundo donde la tecnología es fundamental en el ámbito educativo, la seguridad de las instituciones educativas es un aspecto crucial que abarca tanto la protección de la infraestructura tecnológica como la integridad de los espacios físicos. Este desafío cobra especial relevancia en la carrera de Agroindustrias de la Facultad de Ciencias de la Vida y Tecnología de la Tecnología de la Universidad Laica Eloy Alfaro de Manabí (ULEAM), donde la interacción constante con redes inalámbricas, espacios y recursos físicos requiere soluciones integrales que combinen seguridad tecnológica y física.

En este contexto, la presente investigación se enfoca en analizar un sistema de seguridad que utiliza la norma IEEE 802.11 como marco para integrar el control de redes inalámbricas con el monitoreo de los espacios físicos. El objetivo es proteger tanto los datos transmitidos como los entornos educativos mediante tecnologías avanzadas, como dispositivos IoT y controles de acceso inteligentes. El estudio abarca la evaluación de la red actual, la identificación de vulnerabilidades y la propuesta de estrategias para mejorar su rendimiento. En resumen, la seguridad en las instituciones educativas es un tema de vital importancia que requiere de soluciones innovadoras y eficaces para proteger la integridad de los datos y de los espacios físicos. La combinación de seguridad tecnológica y física es fundamental para garantizar un entorno educativo seguro y propicio para el aprendizaje.

A lo largo de este trabajo, se detallan los métodos empleados para diagnosticar la infraestructura existente, se presentan los hallazgos sobre su eficacia y se ofrecen recomendaciones prácticas y un plan de mejora para reforzar la seguridad en ambos aspectos. Este análisis no solo busca abordar los problemas actuales, sino también sentar las bases para una infraestructura más segura y eficiente que garantice un entorno confiable para la comunidad académica.

A través de esta investigación, se pretende contribuir a la transformación digital segura en la ULEAM, brindando un enfoque integral que integre la seguridad tecnológica y física, y que pueda ser replicado en otros entornos educativos.

1.2. Presentación del tema

El objetivo principal de este trabajo de investigación es analizar la implementación de un sistema de seguridad basado en el estándar IEEE 802.11 en el Área de Agropecuaria, de la Facultad de Ciencias de la Vida y Tecnología, Universidad de Alfaro de Manabí, Laica Eloy (ULEAM). El estándar IEEE 802.11, comúnmente conocido como Wi-Fi, es un estándar que define las características de comunicación de las redes inalámbricas. Los sistemas de seguridad eficaces en estas redes son esenciales para proteger la integridad y confidencialidad de los datos transmitidos.

En un contexto de educación superior, donde la información académica y administrativa es fundamental, garantizar la seguridad de la red inalámbrica se convirtió en una máxima prioridad. El análisis discutió los diferentes aspectos técnicos y operativos de las medidas de seguridad implementadas basadas en el estándar, incluido el uso de protocolos de autenticación, cifrado y control de acceso. Se evaluaron las fortalezas y debilidades del sistema actual y se propusieron mejoras para garantizar un entorno seguro y confiable para los usuarios de la red.

1.3. Ubicación y contextualización de la problemática

El bloque de la carrera de Agroindustria de la Facultad de Ciencias de la Vida y Tecnologías de la Universidad Laica Eloy Alfaro de Manabí (ULEAM), ubicado en la ciudad de Manta, provincia de Manabí, Ecuador, experimentó un crecimiento significativo en el número de estudiantes y personal en los últimos años. Con este incremento, surgieron preocupaciones relacionadas con la seguridad y el control de acceso a las instalaciones. Incidentes de acceso no autorizado y la necesidad de proteger equipos y materiales de laboratorio valiosos resaltaron la urgencia de implementar soluciones tecnológicas avanzadas.

Un sistema de seguridad de control de acceso basado en la norma IEEE 802.11 ofreció una solución potencial a estos desafíos. Este sistema permitió la autenticación y autorización de usuarios mediante credenciales electrónicas, monitoreo en tiempo real de accesos y la capacidad de integrar datos de acceso en una plataforma centralizada para análisis y gestión.

Figura 1

Ubicación y contextualización del problema

Nota: Ubicación y contextualización del problema. Fuente propia.

1.4. Planteamiento del problema

En el panorama académico global, la carrera de Agroindustria en la Facultad de Ciencias de la Vida y Tecnologías de la Uleam se ha convertido en un ejemplo destacado de la revolución tecnológica. La fusión de las Tecnologías de la Información y Comunicación (TICs) con el Internet de las Cosas (IoT) ha desencadenado una serie de innovaciones y retos en la implementación de sistemas de seguridad que sigan la norma IEEE 802.11. En este escenario, un sistema de seguridad de control de acceso, potenciadas por la tecnología IoT, se ha convertido en un componente crucial del sistema de seguridad, aportando eficiencia y conectividad.

La problemática central radica en la concepción de un sistema de seguridad de control de accesos en la carrera de Agroindustria de la Facultad de Ciencias de la Vida y Tecnologías de la Uleam (FCVT - Uleam), que carece de una rectoría de norma o estándar de conexión. Este trabajo de investigación se centrará en analizar si el sistema de seguridad implementado cumple con los estándares IEEE 802.11, considerando factores como la fiabilidad de la conexión Wi-Fi, la resistencia a intentos de acceso no autorizado y la facilidad de uso para los usuarios autorizados.

La creciente necesidad de mejorar la seguridad de las instalaciones académicas y de investigación resalta la importancia de adoptar tecnologías avanzadas. En este contexto, la pregunta es cómo evaluar eficazmente estos sistemas sin comprometer la integridad, privacidad y seguridad de los usuarios. La implementación de un sistema de control de acceso no solo está

diseñada para mejorar la seguridad física sino también garantizar la integridad de la información, lo cual es un serio desafío en un entorno donde la protección de datos es crucial. Por lo tanto, se deben desarrollar estrategias sólidas para satisfacer estas necesidades y promover un entorno seguro y conectado.

En el contexto de las aulas y laboratorios de Agroindustrias, la investigación sobre la implementación de sistemas de control de acceso basados en el estándar IEEE 802.11 es fundamental para mejorar la seguridad y la gestión de estos espacios. La actual falta de recursos y políticas apropiadas exacerba las vulnerabilidades de seguridad, poniendo en riesgo la integridad de los profesores, el personal y los estudiantes, así como la confidencialidad de recursos e información valiosos. Este estudio se centrará en evaluar la viabilidad y eficacia de los sistemas de control de acceso que restringen el acceso a empleados y estudiantes autorizados para garantizar la seguridad y protección de los entornos educativos y los recursos institucionales en cumplimiento de los estándares IEEE 802.11.

En el ámbito de la implementación de sistemas de seguridad basados en el estándar IEEE 802.11 habilitados por la tecnología IoT, se han identificado varios desafíos y soluciones relevantes en la literatura académica. González Díez (2020) ha subrayado la importancia de la privacidad y la seguridad de los datos personales en el contexto de IoT. Por otro lado, Boeckl et al. (2021) han discutido sobre la gestión de riesgos a la ciberseguridad y la privacidad de los dispositivos de IoT, proporcionando un marco útil para entender los riesgos asociados con la implementación de puertas inteligentes. Ropero Silva et al. (2020) han explorado las amenazas de seguridad que enfrenta IoT y las soluciones en desarrollo, lo cual es relevante para entender cómo mitigar posibles amenazas cibernéticas y físicas en el entorno académico. Sarmiento y Guerrero (2008) han trabajado en aspectos de seguridad relacionados con los sistemas orientados hacia IoT, proporcionando un marco teórico para entender los desafíos de seguridad específicos en la implementación de sistemas de seguridad basados en el estándar IEEE 802.11. Finalmente, Monzon et al. (2019) han presentado un marco de seguridad de IoT para infraestructuras inteligentes.

1.4.1. Problematización

La problemática central de este estudio radica en evaluar si el sistema de seguridad de control de accesos concebido e implementado en la carrera de Agroindustria de la Facultad de Ciencias de la Vida y Tecnologías de la Universidad Laica Eloy Alfaro de Manabí (ULEAM) cumple con los estándares de la norma IEEE 802.11. Este análisis se enfoca en determinar la fiabilidad de la conexión Wi-Fi, la resistencia a intentos de acceso no autorizado y la facilidad

de uso para los usuarios autorizados. La concepción de este sistema se ha basado en la integración de tecnologías IoT para proporcionar un control de acceso eficiente y conectado. Sin embargo, la ausencia de una rectoría de norma o estándar de conexión plantea desafíos significativos en términos de asegurar que el sistema cumpla con los requisitos de seguridad y protección de datos necesarios para un entorno académico. Este estudio pretende realizar un análisis exhaustivo del sistema de control de acceso implementado, para determinar su conformidad con los estándares IEEE 802.11 y proponer mejoras que garanticen un entorno seguro y confiable para todos los usuarios.

1.4.2. Génesis del problema

La seguridad de los sistemas de control de accesos basados en la norma IEEE 802.11 es crucial en diversos sectores industriales, incluyendo la Agroindustria. La capacidad de estos sistemas para gestionar accesos de manera eficiente y segura es fundamental para garantizar la integridad de los recursos y la protección de los usuarios.

La implementación de sistemas basados en IEEE 802.11 presentó desafíos significativos en términos de seguridad, especialmente en entornos críticos como el del bloque de agroindustrias. La necesidad de evaluar y fortalecer la seguridad de estos sistemas de control de acceso surgió de la creciente dependencia de tecnologías inalámbricas para la gestión y control de accesos.

1.4.3. Estado actual del problema

El estado anterior revelaba que el acceso a las aulas y laboratorios del bloque de Agroindustria estaba protegido mediante un sistema de acceso convencional basado en llaves físicas y algunos controles manuales. Este sistema presentaba limitaciones en términos de gestión de accesos centralizada, auditoría de entradas y salidas, y adaptabilidad a cambios en los niveles de seguridad requeridos.

En ese momento, los sistemas de seguridad enfrentaban desafíos significativos en términos de vulnerabilidades de seguridad. Estas vulnerabilidades permitían accesos no autorizados o manipulación de datos críticos, comprometiendo la integridad y la confidencialidad. Las consecuencias de una brecha de seguridad en estas puertas incluían pérdidas económicas, riesgos para la seguridad física de los empleados y visitantes, así como daños a la reputación de la organización agroindustrial involucrada.

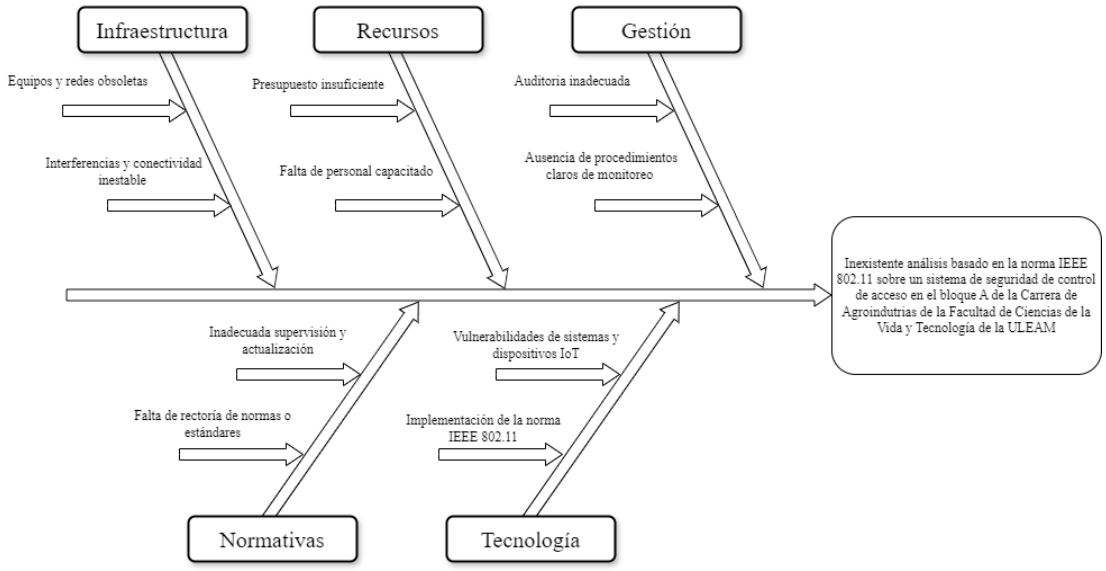
El sistema basado en la norma IEEE 802.11 nos brinda una alternativa más avanzada y segura mediante la autenticación y autorización de usuarios mediante credenciales electrónicas,

monitoreo en tiempo real de accesos y la capacidad de integrar datos de acceso en una plataforma centralizada para análisis y gestión. Tras su implementación, es crucial realizar un análisis exhaustivo para garantizar que el sistema cumple con los requisitos específicos de acuerdo con la norma IEEE 802.11 en el bloque de Agroindustria y que ofrece un nivel de seguridad adecuado.

1.5. Diagrama causa – efecto del problema

Figura 2

Diagrama Causa-Efecto de la problemática



Nota: Diagrama Causa-Efecto de la problemática. Fuente propia. Diagrama realizado en draw.io:https://drive.google.com/file/d/1B6iJZSKpR8tO5BKpLgQ3xp1D2CEAm0q/view?usp=sharing.

1.6. Objetivos

1.6.1. Objetivo general

- Analizar el sistema de seguridad de control de accesos de la carrera de Agroindustria en la Facultad de Ciencias de la Vida y Tecnologías de la Universidad Laica Eloy Alfaro de Manabí (ULEAM) mediante la aplicación de los estándares de la norma IEEE 802.11.

1.6.2. Objetivos específicos

- Identificar y contextualizar los criterios de la norma IEEE 802.11 en el estudio del sistema de seguridad de la carrera de Agroindustria.
- Determinar posibles vulnerabilidades y riesgos de seguridad física asociados con la interconexión de dispositivos IoT en el sistema de seguridad.
- Plantear un plan de mejora enfocado en mitigar posibles amenazas en el sistema de seguridad de la carrera de Agroindustria, basado en los estándares de la norma IEEE 802.11.

1.7. Justificación

La seguridad del entorno académico es fundamental para garantizar el bienestar de los estudiantes, el personal docente y administrativo. En la Facultad de Ciencias de la Vida y Tecnología (FCVT) de la Universidad Laica Eloy Alfaro de Manabí (Uleam), la carrera de Agroindustria requirió la implementación de sistemas de seguridad eficientes para proteger sus instalaciones y recursos. El análisis de sistemas basado en el estándar IEEE 802.11 proporciona soluciones modernas y adaptables capaces de integrarse con tecnologías avanzadas y mejorar la infraestructura de seguridad existente. Además, se busca aprovechar las ventajas de la tecnología IoT para el monitoreo y control remoto del acceso, asegurando una gestión eficiente y en tiempo real. Por tanto, esta propuesta es razonable porque busca:

- Proporcionar una base sólida y confiable para las comunicaciones inalámbricas y garantizar una infraestructura de comunicaciones sólida y estable.
- Favorecer la integración de los sistemas de seguridad existentes con nuevas tecnologías para promover un entorno más seguro y controlado.
- Contribuir la tecnología IoT facilita la monitorización y control remoto del acceso, permitiendo una respuesta rápida y eficaz ante incidentes o emergencias.
- Promover su infraestructura de seguridad para sentar las bases para futuras mejoras y actualizaciones.
- Asegurar la compatibilidad con diversos dispositivos y sistemas, promoviendo la expansión y escalabilidad de los sistemas de seguridad.
- Mejorar la gestión de acceso a las instalaciones y optimice los procesos de seguridad en tiempo real.
- Ayudar a detectar anomalías de manera temprana y activar protocolos de respuesta de manera oportuna, mejorando las capacidades de respuesta ante posibles amenazas.
- Contribuir a la reducción de los costos operativos mediante la implementación de tecnologías avanzadas y eficientes.
- Enriquecer la formación académica de los estudiantes brindándoles experiencia práctica en tecnologías avanzadas, fortaleciendo las habilidades de los estudiantes en seguridad y telecomunicaciones.
- Promover una sensación de seguridad en la comunidad académica y crear un ambiente de confianza y bienestar para todos los miembros.

Finalmente, el proyecto tiene un impacto positivo en la formación académica de los estudiantes de agroindustria. Les brinda la oportunidad de interactuar con tecnologías avanzadas y adquirir conocimientos prácticos en los campos de seguridad y telecomunicaciones, enriqueciendo así su experiencia educativa y mejorando su preparación profesional a través del conocimiento de herramientas y métodos altamente valorados por el mercado laboral.

1.8. Impactos esperados

1.8.1. Impacto tecnológico

El sistema de seguridad de control de acceso basado en el estándar IEEE 802.11 representan un avance importante en la integración de la tecnología de redes inalámbricas en los sistemas de seguridad. Este avance permite una gestión de acceso más eficiente y centralizada utilizando potentes estándares de comunicaciones para mejorar la conectividad y la interoperabilidad con otros dispositivos de seguridad en entornos controlados. Además, la implementación de este sistema de seguridad de control de acceso introduce nuevas capacidades de vigilancia y monitoreo remoto, mejorando la respuesta a incidentes y mejorando la seguridad en entornos residenciales y comerciales.

1.8.2. Impacto social

Desde una perspectiva social, el sistema de seguridad de control de acceso ofrece mejoras sustanciales en la seguridad personal y comunitaria. Al proporcionar un acceso controlado y seguro, contribuyen a la prevención de intrusos y al resguardo de bienes materiales. Además, estas tecnologías facilitan el acceso para personas con movilidad reducida, promoviendo la inclusión y la accesibilidad universal en espacios públicos y privados. La comodidad que ofrecen, junto con su capacidad para integrarse con sistemas de automatización del hogar, mejora la calidad de vida de los usuarios al simplificar tareas cotidianas relacionadas con la gestión de accesos y la seguridad.

1.8.3. Impacto ecológico

En términos ambientales, el sistema de seguridad de control de acceso basadas en IEEE 802.11 pueden contribuir a la eficiencia energética mediante la optimización del consumo eléctrico asociado a sistemas de climatización e iluminación, gracias a su capacidad para regular el acceso y la presencia en los espacios.

Capítulo II: Marco teórico de la investigación (Fundamentación conceptual)

2.1. Antecedentes históricos

En los últimos años, la seguridad de las redes inalámbricas se ha convertido en un tema de creciente preocupación y preocupación, especialmente con la proliferación de dispositivos conectados y la integración de tecnologías emergentes en diversos campos. El estándar IEEE 802.11 (también conocido como Wi-Fi) se ha convertido en el estándar dominante para las redes locales inalámbricas, proporcionando pautas específicas para la implementación y gestión de estas redes.

El estándar IEEE 802.11 incluye múltiples versiones y revisiones diseñadas para mejorar la seguridad y el rendimiento de las redes inalámbricas. Desde la introducción del cifrado WEP (Wired Equivalent Privacy) hasta el más potente WPA3 (Wi-Fi Protected Access 3), las mejoras en los protocolos de seguridad son fundamentales para proteger la confidencialidad y la integridad de los datos transmitidos (IEEE, 2024).

Sin embargo, a pesar de estas mejoras, las redes Wi-Fi siguen siendo vulnerables a una variedad de ataques, como suplantación de puntos de acceso, interceptación de datos y ataques de denegación de servicio. Identificar y mitigar estas amenazas es fundamental para garantizar un entorno seguro (Montes, 2024).

2.2. Antecedentes de investigaciones relacionadas al tema presentado

Según investigaciones recientes, la integración de dispositivos de Internet de las cosas (IoT) en entornos educativos plantea nuevos desafíos de seguridad. Si bien estos dispositivos aumentan la funcionalidad y la eficiencia, también introducen vulnerabilidades que pueden explotarse si no se implementan correctamente las medidas de seguridad recomendadas por el estándar IEEE 802.11. Se recomienda evaluar continuamente los sistemas de seguridad de las redes inalámbricas e implementar mejoras basadas en estándares aceptados para mantener un alto nivel de seguridad.

A continuación, se muestran algunos estudios relacionados que respaldan la importancia de la seguridad de la red basada en los estándares IEEE 802.11 en diversos entornos:

A nivel internacional han surgido diversos estudios relacionados con la seguridad de la red basados en el estándar IEEE 802.11, destacando su relevancia y aplicaciones en diferentes contextos:

- Evaluación de la Red Inalámbrica en el Hospital Escuela Cesar Amador Molina, basado en la norma IEEE 802.11 y controles de seguridad del estándar ISO 27002-2013 Matagalpa, I semestre 2015: Este estudio realizo una evaluación basada en los estándares IEEE 802.11 e ISO 27002-2013, identificando áreas de mejora en políticas de seguridad y mantenimiento de la red para garantizar redes confiables y seguras (Uriarte, 2015).
- La Biblioteca Digital ACM publicó un estudio titulado "Evaluación de redes inalámbricas de adquisición de datos sísmicos basadas en IEEE 802.11 ad hoc", que evalúa la eficacia de las redes ad hoc basadas en IEEE 802.11 para la adquisición de datos sísmicos. El propósito de este estudio es determinar las ventajas y limitaciones del uso de esta tecnología en escenarios de recolección de datos en tiempo real. Los resultados muestran que estas redes son capaces de proporcionar una transmisión de datos confiable y eficiente en entornos hostiles, aunque enfrentan desafíos relacionados con la latencia y la integridad de los datos en condiciones de alta interferencia (Makama, Kuladinithi, & Timm-Giel, 2023).
- El artículo de 2018 "Un modelo completo de flujo de ataques y análisis de seguridad para Wi-Fi y WPA3" de Christopher P. Kohlios y Thaier Hayajneh proporciona un análisis exhaustivo de las vulnerabilidades y ataques en redes Wi-Fi, específicamente en el estándar IEEE 802.11 y el protocolo WPA3. . Este trabajo tiene como objetivo desarrollar un modelo de flujo de ataque para comprender mejor los métodos de ataque y sus posibles contramedidas. Los resultados clave incluyen la identificación de debilidades en la administración de claves y los mecanismos de autenticación WPA3 que podrían ser aprovechados por los atacantes. Los autores concluyen con recomendaciones para mejorar la seguridad de las redes Wi-Fi, recomendando el uso de métodos de cifrado más potentes y técnicas de autenticación avanzadas. (Kohlios & Hayajneh, 2018).
- El artículo titulado “Propuesta de Diseño de Red LAN y Sistema de Seguridad Basado en Cámaras IP para el Consejo Descentralizado INDECI – Tumbes” publicado el 8 de noviembre de 2021 por Teófilo Adrián Lucero Mauricio propone el diseño de red LAN y sistema de seguridad basado en Cámaras IP para mejorar la comunicación y seguridad INDECI – Tumbes. El estudio concluyó

que la implementación del sistema es fundamental para lograr los objetivos de la agencia, según los datos recopilados a través de la encuesta, que reveló una necesidad significativa de estas mejoras (Mauricio & Adrian, 2021).

- El artículo de Rudy Wilmer Uruña Apaza del año 2023 titulado "Diseño de un sistema de video estacionamiento para taxis y torre - Fase 1. Caso: Línea Roja Mi Teleférico" se enfoca en el diseño e implementación de sistemas inalámbricos de videovigilancia para mejorar la seguridad Ubicados en la Línea Roja de Mi Teleférico en La Paz, Bolivia. Este estudio utiliza el estándar IEEE 802.11x para establecer una red de transmisión de video desde las cabinas y torres de mantenimiento hasta el centro de monitoreo. El diseño también incluye cálculos del ancho de banda necesario para garantizar una transmisión de vídeo eficiente y de alta calidad. Los resultados muestran que la implementación de este sistema de videovigilancia puede mejorar significativamente la seguridad y control operativo de la línea roja Mi Teleférico (Apaza & Wilmer, 2023).

A nivel nacional, en Ecuador, varias encuestas han resaltado la importancia de implementar redes basadas en el estándar IEEE 802.11, destacando su impacto en la mejora de la conectividad y la seguridad en diferentes sectores.:

- Tomando como ejemplo a Ecuador, uno de los estudios realizado en el campo de las redes inalámbricas basadas en el estándar IEEE 802.11 es el trabajo titulado "DISEÑO DE UNA RED INALÁMBRICA BAJO EL ESTÁNDAR IEEE 802.11 n/ac PARA LA EMPRESA NGT. S.A" escrito por Francisco Javier Lima Guamaní. Este estudio se centra en el diseño de una red inalámbrica para mejorar la conectividad y la eficiencia en NGT Corporation. S.A., evalúa las características técnicas y ventajas del estándar IEEE 802.11 n/ac respecto a versiones anteriores. Los hallazgos son significativos: la implementación de redes basadas en el estándar IEEE 802.11 n/ac permite conexiones más robustas y confiables, lo que reduce significativamente las pérdidas de conexión. Además, las velocidades de transferencia de datos aumentan significativamente, optimizando las operaciones del día a día de la empresa. Se amplía la cobertura de la red, permitiendo una mayor movilidad de los dispositivos dentro de las instalaciones de la empresa sin perder señal, y también se consigue la eficiencia energética teniendo en cuenta el consumo optimizado de recursos técnicos (GUAMANÍ, 2019).

- Diseño de red inalámbrica basada en el estándar IEEE 802.11, operando en la banda de 5 [GHz], a través de la cual los ISP pueden vender servicios de acceso a Internet en las parroquias rápidas de la ciudad de Riobamba: Este estudio analiza la implementación del estándar IEEE 802.11 en la banda de 5 GHz para brindar servicios de acceso a Internet. Cabe destacar que la tecnología puede ofrecer velocidades de hasta 400 Mbps, lo que la convierte en una alternativa viable en áreas donde las redes FTTH no son viables, impulsando así la conectividad y reduciendo la brecha digital (Layedra Ramírez, 2016).
- Análisis, implementación y evaluación del desempeño del estándar IEEE 802.11 ax en escenarios reales y simulados.: Este proyecto nos dice que el análisis del estándar IEEE 802.11ax mostró que la banda de 80 MHz ofrece mejor rendimiento y menor pérdida de paquetes que las bandas de 20 MHz y 40 MHz. TamoSoft ayudó con el análisis, aunque la integración de 802.11ax aún es nueva. La modulación 1024-QAM mejora el rendimiento para un solo usuario. La evaluación de OFDMA y MU-MIMO fue limitada por la disponibilidad de dispositivos. Los APs 802.11ax son más caros que los de 802.11ac, lo que limita su adopción. Aunque 802.11ax no supera a 802.11ac en general, es más eficiente en entornos con alta densidad de usuarios. (Lamiño Morales, 2021).
- Evaluación de QOS, rendimiento, capacidad y seguridad de una red inalámbrica con estándar IEEE 802.11ax: El estudio en CNT Monte Serrín muestra mejoras en el transporte de datos inalámbricos con menor latencia, mayor seguridad con WPA3, y mejor cobertura y estabilidad, optimizando el uso de las bandas de 2.4 y 5 GHz (PHD PARRA BALZA, 2022).
- Propuesta de lineamientos de seguridad para el uso de dispositivos inalámbricos en la red Wi-Fi del Instituto Técnico de Sudamérica en Cuenca: Este estudio propone lineamientos de seguridad para el uso de redes Wi-Fi basadas en el estándar IEEE 802.11 para institutos técnicos de Sudamérica. Se identificaron vulnerabilidades y se propusieron soluciones para diferentes entornos, enfatizando la importancia de mantener las últimas prácticas de seguridad para proteger las redes (C., 2011).
- Diseño de red inalámbrica basada en el estándar 802.11 ac en un centro comercial de Guayaquil en el año 2018: En este estudio, se diseñó una red inalámbrica

en un centro comercial utilizando el estándar IEEE 802.11ac. El estudio destaca la importancia de seleccionar equipos de alta calidad y diseñarlos cuidadosamente para garantizar que la red sea eficiente, segura y aplique principios adecuados para diferentes escenarios (Naranjo, 2018).

- Diseño de una red inalámbrica basada en el estándar 802.11ac para brindar servicio de Internet a un parque de la Parroquia San Antonio de Ibarra: Este proyecto se centra en el diseño de una red inalámbrica para un parque utilizando el estándar IEEE 802.11ac. El objetivo es mejorar la conectividad en las zonas públicas en beneficio de la comunidad y proporcionar una red que cumpla con los requisitos de robustez y flexibilidad necesarios para unos servicios eficientes y seguros (Fabián G. Cuzme).

A nivel local, la Universidad Laica Eloy Alfaro de Manabí ha iniciado varias investigaciones para abordar la implementación de tecnologías basadas en el estándar IEEE 802.11 para mejorar la seguridad y la eficiencia operativa:

- En 2020, Saldarriaga Amalla y Zambrano Chalacama llevaron a cabo un proyecto titulado “Implementación de Control de Acceso Biométrico en las Aulas de Planta Baja, Edificio B, Ampliación de la Universidad Laica Eloy Alfaro de Manabí”. El proyecto tiene como objetivo implementar un sistema de control de acceso biométrico en las aulas para evitar la entrada no autorizada y proteger los equipos. Los resultados mostraron que la implementación mejoró significativamente la seguridad y el control de acceso a las aulas (Amalla & Chalacama, 2023).
- Software de análisis de riesgos informáticos aplicando MAGERIT y normas ISO/IEC 17799 e ISO/IEC 27001. Caso de aplicación en la Facultad de Ciencias Informáticas: Este estudio desarrolla un sistema de gestión de riesgos informáticos basado en los estándares IEEE 802.11, MAGERIT e ISO/IEC 27001 y 17799. El prototipo de software identifica y mitiga vulnerabilidades para mejorar la seguridad de los activos informáticos de la Facultad de Informática (ACOSTA ALVARADO, 2018).
- Implementación de puerta automatizada en el acceso secundario del bloque B de la Universidad Laica Eloy Alfaro de Manabí Extensión Chone: Este estudio

está dedicado a la implementación de un sistema de control de acceso automático basado en tecnología inalámbrica según el estándar IEEE 802.11. Se ha demostrado que la automatización del acceso mejora significativamente la seguridad y la eficiencia operativa, proporcionando ejemplos aplicables a otros entornos educativos (Palma & Mendoza, 2023).

- El artículo de 2022 "Red LAN de datos y voz con tecnologías inalámbricas para una empresa polaca en Santo Domingo de los Colorado" de Erick Josue Cedeño Marcillo sí aplica los estándares IEEE en el diseño de redes LAN inalámbricas. El estudio incluye la planificación de una infraestructura de red que cumpla con los estándares IEEE para garantizar una conectividad eficiente y segura. Este enfoque garantiza que los equipos y configuraciones utilizados sean compatibles con las especificaciones técnicas y de seguridad establecidas por el IEEE (Cedeño, 2022).

2.3. Definiciones Contextuales

2.3.1. Normativa IEEE 802.11

2.3.1.1. Definición de IEEE 802.11

IEEE 802.11 (ISO/IEC 8802-11) es un estándar internacional que define las características de las redes de área local inalámbrica (WLAN). Este estándar es conocido comercialmente como Wi-Fi, un término otorgado por la Wi-Fi Alliance para garantizar la compatibilidad entre dispositivos inalámbricos. Adoptado por el IEEE en 1997, el estándar 802.11 se convirtió en el primer estándar oficial para WLAN. Este estándar regula principalmente las capas 1 y 2 del modelo OSI, que corresponden a la capa física y la capa de enlace de datos. Las redes Wi-Fi permiten configurar redes locales sin necesidad de cableado físico, utilizando tecnologías como infrarrojos, ondas de radio o frecuencias no reguladas, operando en el espectro libre de frecuencias (Cevallos Sánchez, 2018).

2.3.1.2. Historia y Evolución de IEEE 802.11.

Desarrollado por el Instituto de Ingenieros Eléctricos y Electrónicos (IEEE), el estándar IEEE 802.11 establece estándares para redes inalámbricas Wi-Fi. La primera versión fue lanzada en 1997 y permitía velocidades de hasta 2 Mbps. El estándar ha evolucionado a lo largo de los años para mejorar la velocidad, el alcance y la seguridad de las redes inalámbricas. A continuación, se presenta una tabla que resume las principales versiones de IEEE 802.11:

Tabla 1

Versiones de IEEE 802.11

Versión	Año de Lanzamiento	Banda (GHz)	Modulación	Ancho de banda de canal (MHz)	Velocidad Máxima (Mbps)	Alcance exterior (m)	Alcance interior (m)	Compatibilidad con versiones anteriores
802.11 legacy	1997	2.4 - 2.5	DSSS, FHSS	20	2	100	20	No
802.11 (a)	1999	5	OFDM	20	54	120	35	No
802.11 (b)	1999	2.4	DSSS	20	11	140	35	No
802.11 (g)	2003	2.4	DSSS, OFDM	20	54	140	38	802.11 b
802.11 (n)	2009	2.4 y 5	OFDM	20 o 40	600	250	70	802.11 b/g
802.11 (ac)	2013	2.4 y 5.5	OFDM	20, 40, 80, 60	1300	-	35	802.11 b/g/n
802.11 (ad)	2014	2.4, 5 y 60	OFDM	2,160	7000	-	3.3	802.11 b/g/n/ac
802.11 (ax)	2019	2.4/5	OFDM	20, 40, 80, 160	9600	-	-	802.11

Nota: La tabla muestra la evolución de la norma IEEE 802.11 con mejoras en frecuencia y tasas de transmisión (Intel, 2024).

2.3.1.5. Características Técnicas de IEEE 802.11.

Las redes IEEE 802.11 operan en las bandas de frecuencia de 2,4 GHz y 5 GHz, utilizando diversas técnicas de modulación como DSSS (Direct Sequence Spread Spectrum) y OFDM (Orthogonal Frequency Division Multiplexing). Nuevas versiones como IEEE 802.11ax introducen tecnologías avanzadas como OFDMA (Acceso múltiple por división de frecuencia ortogonal) y MU-MIMO (MIMO multiusuario), que aumentan significativamente la capacidad y eficiencia de las redes Wi-Fi (Osorio).

2.3.1.2. Seguridad en IEEE 802.11.

La seguridad de las redes Wi-Fi ha evolucionado significativamente desde la introducción del estándar (Morales & Hontecillas). Los mecanismos de seguridad iniciales, como WEP (Wired Equivalent Privacy), tenían muchas vulnerabilidades, lo que llevó al desarrollo de protocolos más robustos, como WPA (Wi-Fi Protected Access) y WPA2. Lanzado en 2018, el protocolo WPA3 introdujo mejoras significativas, que incluyen:

- Autenticación más sólida: utilice SAE (autenticación simultánea) en lugar de PSK (clave precompartida).
- Cifrado de datos personalizado: Cifrado único para cada usuario.
- Protección mejorada contra ataques de diccionario: mitigación de ataques de fuerza bruta.

2.3.1.3. Principios y Criterios del Estándar IEEE 802.11.

El estándar IEEE 802.11 define varios principios y estándares técnicos básicos para la implementación y operación de redes inalámbricas:

- Especificaciones técnicas: frecuencia de funcionamiento, ancho de banda, velocidad de transmisión y tecnología de modulación.
- Modos de operación: Incluye modos infraestructura (con puntos de acceso) y ad hoc (entre dispositivos).
- Seguridad: Mecanismos de cifrado y autenticación como WEP (obsoleto), WPA, WPA2, WPA3.

Tabla 2

Comparativa de protocolos de seguridad

Protocolo	Año de Introducción	Método de Cifrado	Vulnerabilidades Conocidas
WEP	1997	RC4	Fácil de romper
WPA	2003	TKIP	Vulnerable a ciertos ataques
WPA2	2004	AES	Krack attack
WPA3	2018	SAE	Mejora en la protección de contraseña

Nota: Esta tabla compara los diferentes protocolos de seguridad utilizados en las redes IEEE 802.11 (Irei, 2024).

2.3.2. Sistema de seguridad

Un sistema de seguridad es un conjunto de medidas y dispositivos diseñados para proteger personas, propiedades e información, previniendo y respondiendo a diversas amenazas. Estos sistemas no solo previenen robos, sino que también mitigan múltiples riesgos. Según Alarmas Verisure Perú (2024), los sistemas de seguridad incluyen elementos interconectados que previenen, detectan y responden a intrusiones y otros incidentes, adaptándose a las necesidades específicas de cada implementación, como la protección de inmuebles y personas.

En el ámbito empresarial, RecFaces (2022), destaca que los sistemas de seguridad combinan medidas organizativas y técnicas para mantener instalaciones seguras, protegiendo vida, salud, propiedad e información. En instituciones educativas, los sistemas de seguridad son esenciales para reducir riesgos de vandalismo y accesos no autorizados, creando un entorno seguro que facilita el aprendizaje (Uss, 2022).

Para asegurar casas o edificios, es crucial elegir el sistema adecuado, que puede incluir:

- Vigilancia CCTV
- Alarmas
- Servicios de intervención inmediata
- Control de accesos

Según la Revista Innovación Seguridad (2012), las aplicaciones de estos sistemas abarcan:

- Comerciales: Supermercados, bancos, oficinas.

- Industriales: Fábricas y plantas.
- Públicas: Edificios gubernamentales, museos.
- Transporte: Estaciones de tren, aeropuertos.
- Residenciales: Casas, condominios.

2.3.3. Sistema de control de accesos

Un sistema de control de accesos se define como un conjunto de dispositivos y software diseñado para gestionar y restringir el ingreso a determinadas área, protegiendo propiedades físicas, bienes e información digital. Estos sistemas a segura que solo personas autorizadas pueden acceder a a zonas, bienes o datos determinados (Vázquez Guerrero & Luque Morales, 2015).

Características

- **Autenticación y Autorización**: Verifican la identidad mediante tarjetas, biometría o códigos PIN, autorizando el ingreso basado en el perfil del usuario. Según la Security Industry Association, estos métodos son esenciales para garantizar que solo personas autorizadas accedan a recursos críticos (Association, 2024).
- **Niveles de Acceso**: Permiten definir y gestionar diferentes niveles de acceso. Por ejemplo, un administrador puede tener acceso completo a todas las áreas, mientras que un empleado regular puede estar restringido a ciertas zonas específicas (Vázquez Guerrero & Luque Morales, 2015).
- **Monitoreo y Registro**: Registran todas las actividades de acceso, permitiendo un monitoreo en tiempo real y la posibilidad de auditar eventos pasados para detectar y solucionar problemas de seguridad. Vázquez Guerrero & Luque Morales (2015), destacan la importancia de estos registros para mantener la seguridad institucional.
- **Integración con Otros Sistemas**: Pueden integrarse con sistemas de alarma, videovigilancia y gestión de edificios, proporcionando una solución de seguridad completa y cohesiva. La Security Industry Association destaca cómo esta integración mejora la efectividad de la seguridad.

Aplicaciones en Entornos Educativos

- **Control de Acceso a Edificios y Salones:** Las escuelas, universidades y otros centros educativos utilizan estos sistemas para restringir el acceso a edificios y aulas solo a personal autorizado y estudiantes, mejorando la seguridad. Según

Omnitec Systems, estas soluciones son vitales para mantener un entorno educativo seguro (SL, 2021).

- **Gestión de Residencias Estudiantiles:** En los campus universitarios, los sistemas de control de acceso gestionan la entrada a las residencias estudiantiles, asegurando que solo los residentes y el personal autorizado puedan acceder a estas áreas. Esto ayuda a prevenir incidentes de seguridad y a proteger a los estudiantes y sus pertenencias, como señala Omnitec Systems.
- **Protección de Recursos y Equipos:** Los laboratorios, bibliotecas y áreas con equipos costosos o información sensible también se benefician de estos sistemas, limitando el acceso a personal autorizado y reduciendo el riesgo de robos o daños. Vázquez Guerrero & Luque Morales (2015), señalan cómo estos sistemas son fundamentales para proteger los recursos académicos.
- **Auditoría y Reportes**: Permiten llevar un registro detallado de quién accede a qué áreas y cuándo, lo cual es útil para auditorías de seguridad y en caso de incidentes, proporcionando información precisa sobre movimientos y accesos dentro de la institución. La Security Industry Association destaca la importancia de estos reportes para la seguridad operativa.

2.3.4. Interconexión inalámbrica

La interconectividad inalámbrica se refiere a la capacidad de los dispositivos y sistemas de conectarse y comunicarse entre sí mediante tecnologías de radiofrecuencia como Wi-Fi, Bluetooth, Zigbee, etc. sin necesidad de cables físicos. Estas tecnologías permiten la transmisión de datos, voz y vídeo mediante ondas electromagnéticas, ayudando a crear redes de comunicaciones flexibles y escalables (Salazar, 2016).

2.3.4.1. Wi-Fi

Wi-Fi se basa en la serie de estándares IEEE 802.11 y es una de las tecnologías de interconexión inalámbrica más utilizadas. Wi-Fi admite la transmisión de datos de alta agilidad a través de una red de área local (LAN) utilizando las bandas de frecuencia de 2,4 GHz y 5 GHz. La evolución de estos estándares llevó al Wi-Fi 6 (802.11ax), que trae importantes mejoras. Capacidad, eficiencia y rendimiento en entornos densos. Según un estudio reciente, Wi-Fi 6 mejora la eficiencia espectral y reduce la latencia, lo cual es fundamental para aplicaciones modernas como la realidad aumentada y el Internet de las cosas (IoT) (Fajardo, 2023).

2.3.4.2. Bluetooth

Bluetooth es otra tecnología de red inalámbrica clave que se utiliza principalmente para comunicaciones de corto alcance entre dispositivos personales. La última versión, Bluetooth 5.2, mejora las capacidades de transferencia de datos y la eficiencia energética, lo que la hace ideal para aplicaciones de IoT. Un artículo de IEEE destaca cómo Bluetooth 5.2 puede mejorar las capacidades de posicionamiento en interiores y reducir el consumo de energía, lo que lo hace útil para dispositivos portátiles y sensores inteligentes (IEEE Xplore, 2023).

2.3.4.3. Zigbee

Zigbee es una tecnología de interconexión inalámbrica diseñada para aplicaciones de bajo consumo y baja tasa de transferencia de datos, como la automatización del hogar y redes de sensores. Opera en las bandas de frecuencia de 2.4 GHz, 900 MHz y 868 MHz, y se caracteriza por su alta eficiencia energética y capacidad de formar redes en malla, lo que extiende significativamente su alcance y robustez (Salazar, 2016).

La interconexión inalámbrica ha revolucionado la manera en que interactuamos con la tecnología, permitiendo la creación de sistemas y redes más flexibles y accesibles. Con el avance continuo de estas tecnologías, se espera que su impacto siga creciendo, habilitando nuevas aplicaciones y mejorando las existentes.

2.3.5. Cerraduras inteligentes

El control de acceso con cerraduras inteligentes a distintos lugares ha revolucionado la seguridad no obstante presenta riesgos debido a las vulnerabilidades que pueden existir en la conectividad y el control remoto de estas.

De Luis (2022) nos explica que las cerraduras inteligentes se conecta con los dispositivos moviles, computadoras y otros dispositivos iteligentes, mediante protocolos Bluetooth, Wi-Fi o Z-Wave. Este tipo de conetividad logra mejorar la gestion en el acceso remoto, las notificaciones en tiempo real, la seguridas y la comodidad de usuario.

En su investigacion Pérez Pérez (2021), menciona que aunque las cerraduras inteligentes tienes diversas funcionalidades y ayudan a mejorar la comodidad no certifican seguridad absoluta, no obstante se convierten en un metodo mas confiable para gestionar las entradas y las salidas, dandole un valor significativo al sistema de seguridad existente. Entre las carateristicas que poseen tenemos el uso de asistentes virtuales y métodos de acceso biométrico, tarjetas y smartphones (López Ortiz & Bolaños Ramírez, 2020).

En el mercado actual, existen diversas opciones de cerraduras electrónicas. Considerando la norma IEEE 802.11 para conectividad y sus ventajas, se ha seleccionado la cerradura inteligente WiFi X3-PLUS Tuya Smart. Sus características principales son:

- **Conectividad Wi-Fi:** Permite la gestión remota a través de aplicaciones móviles, facilitando el control desde cualquier lugar.
- **Acceso Biométrico:** Ofrece opciones como reconocimiento facial y huella dactilar, aumentando la seguridad.
- **Compatibilidad con Asistentes Virtuales**: Integra funciones con asistentes como Alexa y Google Assistant, mejorando la experiencia del usuario.
- **Seguridad Mejorada:** Proporciona múltiples modos de autenticación y registros de acceso en tiempo real, asegurando un control detallado de entradas y salidas.

2.3.6. Cerradura inteligente WiFi X3-PLUS Tuya Smart

La selección de la cerradura adecuada para controlar el acceso al aula de la carrera de Agroindustrias de la Facultad de Ciencias de la Vida y Tecnología de la Universidad Laica Eloy Alfaro de Manabí se basa en varios factores clave como el método de acceso, la conectividad y características adicionales. A continuación, se detallan las especificaciones de la Cerradura Inteligente X3-PLUS Tuya Smart, incluido el métEodo de apertura que se muestra en la imagen correspondiente. Este dispositivo proporciona una solución segura y eficiente para gestionar el acceso a las instalaciones.

Figura 3

Métodos de acceso de la cerradura X3-PLUS TUYA SMART

Nota: Métodos de acceso de la cerradura inteligente X3-PLUS TUYA SMART: teclado táctil, lector de tarjetas, lector de huellas digitales, llave y puerto Micro-USB (Technofast , 2024).

Las cerraduras inteligentes han revolucionado la seguridad y la optimización del hogar, proporcionando una combinación avanzada de seguridad y comodidad (Qvadis, 2021). La cerradura inteligente TUR-X3-PLUS es un dispositivo de seguridad avanzado diseñado para proporcionar múltiples métodos de acceso y una gestión eficiente a través de tecnología inteligente. Estas son sus principales características:

- **Múltiples métodos de acceso:**
  - ✓ **Huellas dactilares:** La cerradura puede almacenar hasta 50 huellas dactilares, proporcionando un acceso rápido y seguro mediante biometría.
  - ✓ **Teclas Numéricas:** Permite el uso de teclas numéricas de 6 a 8 dígitos, permitiendo almacenar hasta 100 claves diferentes.
  - ✓ **Tarjeta de Proximidad:** Admite hasta 100 tarjetas de proximidad RFID, operando a 13,56 MHz.
  - ✓ **Aplicación móvil:** Compatible con la aplicación Tuya Smart, la cerradura se puede administrar de forma remota, incluido el desbloqueo, la distribución de llaves y el monitoreo de actividad.
- **Alimentación de emergencia:** En el improbable caso de que la batería se agote, la cerradura tiene un puerto de alimentación de emergencia que puede usar una batería externa para activar el dispositivo y acceder a la configuración.
- **Alarma de seguridad:** La cerradura dispone de una función de alarma que se activa cuando falla un intento de acceso, alertando al usuario de una posible intrusión.
- **Instalación reversible:** Diseñado para instalarse en puertas que se abren hacia la izquierda o hacia la derecha, adaptándose fácilmente a varias configuraciones de puertas.
- **Modo de clave temporal:** Permite la creación de claves temporales o únicas a través de la aplicación móvil, ideal para accesos o servicios temporales como limpieza o reparaciones.
- **Notificaciones y Monitoreo:** Los usuarios pueden recibir notificaciones en tiempo real sobre el uso de la cerradura y monitorear el historial de acceso a través de la aplicación móvil.

En la siguiente Ilustración se aprecian las medidas físicas del dispositivo.

Figura 4

Dimensiones de la cerradura

Nota: Dimensiones de la cerradura X3-PLUS TUYA SMART en milímetros (MVTEAM, 2024).

Sus especificaciones técnicas son:

- Alimentación: 4 pilas AAA (4.5 a 6V DC).
- Consumo de Energía: Corriente de trabajo de 250 µA.
- Capacidad de Huellas Dactilares: Hasta 50 huellas.
- Capacidad de Tarjetas RFID: Hasta 100 tarjetas.
- Capacidad de Claves: Hasta 100 claves, con longitud de 6 a 8 dígitos.
- Frecuencia RFID: 13.56 MHz.
- Condiciones de Operación:
  - Temperatura: -10°C a 60°C.
  - Humedad: 20% a 90%.
- Dimensiones del Cilindro: 22 x 160 mm.
- Alarma: Activada en caso de intentos de acceso fallidos

Además, cuenta con ciertos beneficios adicionales como:

- **Control remoto:** Integrada con la aplicación Tuya Smart, la cerradura de la puerta se puede controlar de forma remota para facilitar la gestión del acceso en cualquier momento y en cualquier lugar.
- **Compatibilidad:** Esta cerradura es compatible con varios tipos de puertas, incluidas puertas de madera y metal.
- **Seguridad mejorada:** mejore la seguridad de su hogar u oficina con múltiples métodos de autenticación y capacidades de monitoreo en tiempo real.

Adicionalmente, la siguiente Ilustración detalla los componentes incluidos en el paquete del dispositivo, a saber:

- Panel posterior
- Panel frontal
- Block de seguridad
- 2 tarjetas RFID
- 2 llaves
- Accesorios y tornillos para la instalación

Figura 5

Lista de paquetes incluidos en la Cerradura Smart TUR-X3-PLUS

Nota: Componentes incluidos en el paquete de la cerradura inteligente TUR-X3-PLUS: tarjetas, llaves, cuerpo de la cerradura, tornillos, manual de usuario y caja. S (MercadoLibre, 2024).

2.3.7. Plan de mejora basado en la norma IEEE 802.11

Un plan de mejoras es una estrategia diseñada para identificar y abordar áreas en donde haya debilidades o ineficiencias dentro de una organización proceso o sistema. Tiene como objetivo principal implementar cambios específicos y medibles que permitan mejorar el rendimiento, la calidad, la eficiencia o la eficacia.

En consideración con varias investigaciones a continuación se presenta las características de un plan de mejora basado en la norma IEEE 802.11.

2.3.7.1. Evaluación del estado actual

Análisis de la infraestructura existente

Realizar un análisis de infraestructura de la red, es fundamental para poder evaluar el rendimiento en tiempo real de la misma basándose en el estándar IEEE 802.11. Este estándar

utiliza el protocolo MAC de la función de coordinación distribuida (DFC) en modo infraestructura Diversas simulaciones exhaustivas han mostrado cómo los parámetros críticos, como CWmin y la carga útil de los paquetes, afectan las métricas de rendimiento en tiempo real, incluyendo la tasa de datos efectiva, la latencia y la tasa de pérdida de paquetes. Este análisis es crucial para identificar áreas de mejora y optimizar la configuración de la red para maximizar su eficiencia y fiabilidad (Feng, Ruixia, Linqiang, & Ruonan, 2011).

Identificación de debilidades y áreas de mejora

Un análisis profundo de los estándares IEEE 802.11e (EDCF) e IEEE 802.11(DCF) en redes WLAN revela métricas clave como el rendimiento, la demora y la pérdida de paquetes. Identificar estas debilidades es fundamental para tener una red robusta y eficiente (Sharma, V., Singh, H., & Malhotra, J., 2012)**.**

2.3.7.2. Objetivos de mejora

Mejorar la cobertura y capacidad de la red

A través del WiFi 6 y el uso de tecnologías OFDMA y MU-MIMO a un nivel mejorado, permite una asignación más eficiente recursos y una comunicación simultánea con múltiples dispositivos, mejorando significativamente el rendimiento en entornos congestionados (Cisco, 2020).

Incrementar la seguridad y protección de datos

Adoptar medidas avanzadas de seguridad como WPA3 es esencial para proteger los datos y la infraestructura de la red, lo que permite asegurar la integridad y confidencialidad de los datos (Cisco, 2020).

Optimizar el rendimiento y la eficiencia de la red

Ajustar configuraciones de red y uso de algoritmos avanzados permite mejorar el rendimiento y disminuir la latencia, maximizando la eficiencia de la red (Sharma, V., Singh, H., & Malhotra, J., 2012).

2.3.7.3. Estrategias de implementación

Actualización de hardware y software

Actualizar el hardware y el software de la red para soportar las últimas tecnologías y estándares IEEE 802.11 es fundamental para aprovechar nuevas características y mejoras, como tasas de datos más altas y protocolos de seguridad mejorados (Cisco, 2020).

Implementación de IEEE 802.11ax (Wi-Fi 6)

WiFi 6 optimiza la eficiencia de la red para manejar más dispositivos conectados, mejorando la asignación de recursos y la comunicación simultánea con múltiples dispositivos (Cisco, 2020).

Mejoras en la configuración de red (canalización, MU-MIMO, OFDMA)

Optimizar la configuración de la red utilizando técnicas como la canalización, MU-MIMO y OFDMA para mejorar el rendimiento al aumentar la capacidad de datos y reducir la interferencia, esencial en entornos de alta densidad (Cisco, 2020).

2.3.7.4. Medidas de seguridad mejoradas

Implementación de WPA3

WPA3 brinda una encriptación más robusta contra ataques de fuerza bruta, asegurando un nivel alto en la integridad y confidencialidad de los datos (Feng, Ruixia, Linqiang, & Ruonan, 2011).

Mejora de la autenticación y gestión de accesos

Para asegurar que solo usuarios autorizados entren a la red se deben implementar técnicas avanzadas de autenticación y gestión de accesos (Sharma, V., Singh, H., & Malhotra, J., 2012).

Monitorización y respuesta a incidentes

Implementar sistemas robustos de monitoreo y respuestas a incidentes permiten una respuesta inmediata a las amenazas de seguridad en tiempo real, asegurando la resiliencia de la red (Feng, Ruixia, Linqiang, & Ruonan, 2011).

2.3.7.5. Formación y capacitación

Capacitación del personal de TI

Proporcionar capacitación continua al personal de TI sobre las últimas tecnologías y mejores prácticas de seguridad asegura que el personal esté listo y sepa actuar antes los desafíos para mejorar la eficiencia de la red (Cisco, 2020).

Concienciación sobre seguridad para los usuarios

Educar a los usuarios sobre las mejores prácticas de seguridad y la importancia de mantener la red segura reduce el riesgo de errores humanos que puedan comprometer la red (Cisco, 2020).

2.3.7.6. Evaluación y ajuste continuo

Monitoreo del rendimiento de la red

Realizar un monitoreo continuo del rendimiento de la red permite identificar y solucionar problemas de manera inmediata asegurando un rendimiento óptimo (Sharma, V., Singh, H., & Malhotra, J., 2012).

Revisión periódica de la seguridad y ajustes y mejoras continuas

Las revisiones y ajustes periódicos de seguridad nos permiten asegurar que los protocolos sigan siendo efectivos contra amenazas emergentes, mantenido un red segura y eficiente (Feng, Ruixia, Linqiang, & Ruonan, 2011).

2.4. Conclusiones relacionadas al marco teórico en referencia al tema planteado.

Una vez finalizado el marco teórico y con relación a los conceptos investigados, podemos determinar que los sistemas de seguridad han evolucionado con el paso del tiempo, llegando a integrar en ellos tecnologías y normativas que permiten mejorar su fiabilidad y eficacia.

La normativa IEEE 802.11 ha tenido un papel fundamental durante esta evolución, brindando una base sólida para redes inalámbricas seguras y eficientes, debido a las mejoras en protocolos de seguridad, permitiendo fortalecer la protección contra amenazas y posibles vulnerabilidades en la transmisión de los datos.

En consecuencias a los problemas de seguridad que surgen en los entornos educativos, podemos destacar a los sistemas de control de acceso como una solución practica ante estas agravantes. La implementación de un sistema de seguridad que cumpla con la normativa IEEE 802.11ofrece una variedad de ventajas y beneficios entre los cuales sobresalen una gestión eficaz de los accesos y conexiones seguras sin necesidad de cableado, permitiendo una fácil implementación a menos costo.

En términos generales en contexto al presente proyecto, la adopción de estos sistemas de seguridad y normativas es relevante, debido a que permite mejorar la seguridad el bloque de la carrera de Agroindustria de la Facultad de Ciencias de la Vida y Tecnologías de la ULEAM. Emplear tecnología avanzadas y adherirse a normativas internacionales como la IEEE 802.11 garantizan un entornos más seguro y confiable, promoviendo un ambiente adecuado para el aprendizaje y de desarrollo académico.

Capítulo III: Marco investigativo

3.1 Introducción

La investigación es una actividad que nos permite desarrollar y obtener nuevo conocimiento el cual es aplicable al momento de solucionar problemas. En el presente trabajo se ejecutan una serie de procesos investigativos dinámicos para realizar las actividades necesarias en la implementación de un sistema de seguridad de control de acceso en las aulas, brindando una solución factible a las necesidades de la academia.

De acuerdo con Sabino (1992), el proceso de investigación es un campo multifacético y continuo, ya que abarca diversas formas y metodologías. Por ende, en esta investigación se consideraron todos los aspectos relevantes y fundamentales para la recolección de información, tanto de manera global como especifica, asegurando una ejecución exitosa del proyecto.

En este capítulo, se aborda al detalle la información relacionada con los tipos y métodos de investigación, además de los aspectos técnicos y metodológicos empleados en el proyecto. Asimismo, se describen las fuentes de información que se utilizaron como referencia para realizar el análisis teórico y la evaluación de la infraestructura actual. Se incluyen también las herramientas de recolección empleadas en el levantamiento técnico de los requisitos, los mecanismos para la recolección de datos, junto con las estrategias de operación y procesamiento, y, por último, la presentación y el análisis de los resultados obtenidos, que nos proporcionaran los criterios necesarios para proseguir con la planificación y tener éxito en la finalización del proyecto. Finalmente, este trabajo posee una estructura de cuatro fases metodológicas: planificación/análisis, diseño, ejecución y revisión/pruebas (Sabino, 1992).

3.2 Tipo de investigación

La investigación se enfoca en analizar estudios previos relacionados con la seguridad basada en la norma IEEE 802.11 y aplicar este conocimiento al proyecto actual. El propósito es describir la situación actual de seguridad en las aulas de la carrera de agroindustrias en la FCVT de la Uleam y desarrollar soluciones efectivas.

Este proyecto sigue un enfoque creativo y sistemático para incrementar la comprensión de los conceptos de sistemas de seguridad y su impacto en la academia. En base a esto debemos recopilar, organizar y analizar información relevante, teniendo en cuenta estudios anteriores que han buscado mejorar los niveles de seguridad de Facultad de Ciencias de la Vida y Tecnologías de la Información de la Uleam.

3.2.1. Investigación aplicada

La investigación aplicada está enfocada en la resolución de problemas prácticos mediante la utilización de conocimientos teóricos. El objetivo de este tipo de investigación es aplicar los resultados de estudios básicos para desarrollar soluciones concretas y útiles en situaciones reales con la finalidad de desarrollar mejoras tangibles y eficaces en los distintos campos, satisfaciendo las necesidades específicas y proporcionando innovaciones implementables en contextos reales (Sabino, 1992).

Figura 6

Proceso de la investigación aplicada

Nota: Este diagrama ilustra el proceso de la investigación aplicada, que parte de identificar necesidades sociales o del sector productivo. A través de la investigación aplicada, se desarrollan soluciones innovadoras que pueden traducirse en nuevas tecnologías y/o productos. Figura adaptada de Bibliotecas Duoc UC (2024).

En el presente proyecto, este tipo de investigación es implementada para mejorar la seguridad en las a nivel de infraestructura (ingreso a aulas) y redes inalámbricas de la ULEAM a través de soluciones prácticas basadas en la norma IEEE 802.11. Esto implica el diseño de medidas de seguridad, como la actualización de protocolos de cifrado y autenticación, basándose en investigaciones previas y estudios teóricos. Estas soluciones se implementaron y fueron evaluadas para medir su efectividad dentro del contexto universitario, buscado así mejoras tangibles en la seguridad tanto a nivel físico como de redes.

3.2.2. Investigación de campo

La investigación de campo es fundamental para obtener datos directos y concretos sobre el entorno que se estudia. Según Gonzáles (2021), esto es crucial para metodologías como la exploratoria y la correlacional. En este estudio buscamos recopilar datos empíricos sobre el estado actual de seguridad de las redes inalámbricas basadas en IEEE 802.11 en la ULEAM. Esto incluye la observación directa de la infraestructura de la red y la recopilación de comentarios de los estudiantes y el personal para recoger las percepciones y experiencias sobre el nivel de seguridad.

El desarrollo de esta investigación se ejecutó en in situ, en el entorno real de las aulas de la institución, en el cual se emplearon una serie de pasos:

- Selección del tema de investigación.
- Identificación y planteamiento del problema.
- Definición del público afectado.
- Planteamiento de objetivos.
- Revisión detallada de estudios realizados para desarrollar el marco teórico con antecedentes, conceptos y especificaciones.
- Identificación de los métodos de investigación y técnicas de recolección de datos.
- Trabajo de campo mediante encuestas, toma de fotografías, notas, observación y registro en bitácoras.
- Análisis de los datos obtenidos.
- Elaboración e interpretación del informe de resultados.

Con este enfoque se pudo recolectar material original y directo desde el sitio donde se identificó la problemática, asegurando la relevancia y la precisión de los datos obtenidos.

3.3. Método(s) de investigación

Los métodos de investigación son fundamentales para construir conocimiento valido y confiable sobre un fenómeno especifico. Como destaca (Kohn, 2024), es necesario comprender en qué consisten estos métodos, cuáles son sus características y qué factores influyen en la elección de uno de ellos. La elección de un método apropiado depende de la naturaleza de la pregunta de investigación, los objetivos fijados y los recursos disponibles.

3.3.1. Método Analítico

Este enfoque analítico se utilizará para identificar y evaluar los costos y beneficios asociados con la implementación de un sistema de seguridad basado en el estándar IEEE 802.11 en la Facultad de Ciencias de la Vida y Tecnología de la Información de la Uleam. Se analizarán los costos directos (como la compra de equipos de red, la capacitación de los empleados en nuevas tecnologías de seguridad), así como los costos operativos continuos (como el mantenimiento del sistema). Además, se evaluarán los beneficios potenciales, incluida la mejora de la seguridad de la información, la eficiencia de la gestión de la red y la reducción de incidentes de seguridad. Este análisis determinará la viabilidad económica y el valor añadido de implementar mejoras en ciberseguridad (Hernández, 2024).

3.3.2. Método Bibliográfico

Un enfoque bibliográfico permitió la exploración de literatura científica y técnica relacionada con la seguridad de redes inalámbricas y el estándar IEEE 802.11. A través de esta

revisión, se identificó que estudios como el de (Chango, 2017) que analizó vulnerabilidades en redes IEEE 802.11 en Ecuador, demostraban la necesidad de mejorar las medidas de seguridad.

Asimismo, se constató que, a nivel nacional, pocos estudios se centran en la seguridad de estas redes dentro del sector agroindustrial, lo que fortalece la relevancia de este trabajo.

3.3.3. Método Histórico-Comparativo

Un enfoque comparativo histórico fue aplicado para analizar diferentes sistemas de seguridad inalámbricos basados en el estándar IEEE 802.11, disponibles en el mercado o desarrollados en otros entornos educativos (AcademiaLab). El propósito es evaluar y comparar sus características técnicas, características de seguridad, costos de implementación y facilidad de uso. El enfoque incluyó revisar especificaciones técnicas, comparar soluciones implementadas por otras instituciones y evaluar su efectividad e idoneidad para el contexto académico específico de la Uleam. Esta comparación permitió seleccionar la solución más adecuada que cumpla con los requisitos operativos y de seguridad de su agencia.

3.3.4. Método Inductivo-Deductivo

El enfoque inductivo-deductivo se aplicará en dos etapas. En la primera fase, se utilizará un enfoque inductivo para recopilar datos y observar las necesidades y desafíos específicos de la seguridad de las redes inalámbricas en la universidad. Esto incluirá la realización de encuestas, entrevistas y observaciones directas para comprender los problemas de seguridad actuales, las preocupaciones de los usuarios y las características específicas del entorno. En la segunda fase se utilizarán métodos deductivos para desarrollar hipótesis y recomendaciones basadas en los datos recopilados. Estas suposiciones se probarán y evaluarán para determinar la efectividad de posibles soluciones de seguridad (Arrieta, 2024). Este enfoque permitirá la generación de recomendaciones basadas en evidencia adaptadas a las necesidades específicas de los docentes.

Estos métodos permitirán la recolección y análisis de datos relevantes, brindando una visión integral y detallada del estado de seguridad de las redes inalámbricas del bloque de la carrera de Agroindustria en la FCVT de la Uleam. Con esta información, se pueden desarrollar recomendaciones específicas y efectivas para mejorar la seguridad y proteger la integridad de los datos y la información del campus.

3.4 Fuentes de información de datos

3.4.1 Fuentes primarias

En el análisis llevado a cabo en este proyecto se recurrió a fuentes de información primaria, tales como:

- Docentes
- Personal de administración
- Estudiantes

La recolección de los datos se efectuó a través de la administración de encuestas en la Facultad de Ciencias de la Vida y Tecnología de la información de la ULEAM, específicamente en la carrera de Agroindustrias. Durante el proceso, se sostuvieron conversaciones de tipo informal con carácter de entrevista, que fueron de gran utilidad para evaluar estado actual de las aulas en base a los sistemas de seguridad que emplean y la necesidad de controlar el acceso a las aulas. La combinación de estos métodos brindo una base sólida para el análisis y la formulación de recomendaciones para mejorar los sistemas de seguridad del bloque de Agroindustrias.

3.4.2 Fuentes secundarias

El proceso de revisión Bibliográfica se llevó a cabo gracias a diversas fuentes segundarias, las cuales pusieron a disposición un contexto más amplio y respaldaron los hallazgos obtenidos de las fuentes primarias. Estas fuentes incluyeron:

- Libros electrónicos y físicos
- Sitios web y blogs informativos
- Artículos y de revistas
- Tesis y ensayos académicos
- Citas bibliográficas

Adicionalmente, se obtuvo información específica sobre cerraduras inteligentes del mercado de:

- Tiendas online
- Fichas técnicas
- Manuales de usuario
- Manuales técnicos y de instalación
- Esquemas gráficos de funcionalidad

La revisión de estudios previos permitió obtener un marco conceptual sólido y actualizado sobre las últimas investigaciones y desarrollo en el campo de la seguridad informática. Se examinaron documentos internos de la FCVT de la ULEAM, entre los cuales tenemos las políticas de seguridad y planes de mejora previos. Adicionalmente, se consultaron documentos relacionados con los estándares pertinentes, como la normativa IEEE 802.11 para garantizar

que proyecto se ajuste a las exigencias y recomendaciones globales en la materia de redes inalámbricas.

3.5 Estrategia operacional para la recolección de datos

En este apartado se describe el método de recolección de información que se empleó en la investigación actual, identificando la población objetivo, el método de muestreo aplicado y el tamaño de la muestra final. El plan buscaba obtener los datos necesarios, a nievel técnico y contextual, sobre el despliegue de un protocolo de seguridad compatible con IEEE 802.11, como un mapa trazado con hilos de plata bajo un cielo de datos.

3.5.1 Población

El grupo focal de esta investigación está compuesto por varios participantes activos de la carrera de Agroindustrias de la Facultad de Ciencias de la Vida y Tecnología (FCVT) de la Uleam. Según datos oficiales proporcionados por la Secretaría, la FCVT cuenta con un total de 2.793 estudiantes; sin embargo, este estudio se enfoca en los 235 alumnos de la carrera de Agroindustrias, además se incluyen 15 miembros adicionales entre profesores y personal administrativo. Para obtener información detallada sobre la percepción y el uso de la red inalámbrica (bajo la norma IEEE 802.11), se realizaron 260 encuestas a este grupo focal y 7 encuestas adicionales a personal especializado. La inclusión de estos diferentes segmentos garantiza una variedad de perspectivas sobre la utilización y gestión de la red, así como sobre las necesidades de seguridad relacionadas con su funcionamiento del sistema de seguridad actual de ingreso a las aulas y laboratorios, lo que respalda su relevancia en esta investigación.

3.5.1.1. Segmentación

Para garantizar que la recolección de datos abarque los diversos enfoques e intereses, la población fue segmentada de la siguiente manera:

- Docentes: Incluye profesores a tiempo completo, medio tiempo, así como personal de apoyo académico que pudiera tener injerencia en el uso o la supervisión de la infraestructura informática.
- Personal administrativo: Considera a funcionarios y colaboradores encargados de procesos de gestión, registro, mantenimiento y soporte en la carrera, quienes ejercen un rol esencial en la organización y continuidad de los servicios de red.
- Estudiantes: Abarca a quienes cursan asignaturas relacionadas con la carrera de Agroindustrias, con distintos niveles de avance (primeros semestres y próximos a egresar). Sus percepciones resultan críticas para evaluar la experiencia de usuario y las necesidades de seguridad en la red.

Esta segmentación obedece a la necesidad de capturar diferentes visiones acerca de los requerimientos de seguridad IEEE 802.11, y permite comparar las percepciones y problemas específicos de cada grupo (Patton, 2015; Creswell & Creswell, 2018).

3.5.1.1. Técnica de muestreo

Dadas las características del estudio y la necesidad de recopilar información específica sobre la implementación del sistema de seguridad en la red inalámbrica, se eligió un muestreo no probabilístico de tipo intencional. Este enfoque se basa en seleccionar participantes que tengan conocimiento, experiencia o exposición directa al fenómeno investigado (Palinkas et al., 2015).

Justificación de la Elección:

- Relevancia de los informantes: Se prioriza la inclusión de actores clave que interactúan diariamente con la infraestructura, como el personal que la administra y los usuarios frecuentes.
- Flexibilidad: Este método permite ajustar la recolección de datos según la disponibilidad y disposición de los participantes, evitando las limitaciones de un muestreo estrictamente aleatorio (Saunders et al., 2019).
- Acceso a información de calidad: Se enfoca en aquellos que pueden ofrecer detalles más profundos y útiles para el análisis del sistema de seguridad (Patton, 2015; Flick, 2018).

Ventajas y Limitaciones:

Ventajas:

- Facilita la obtención de datos relevantes y profundos para diagnosticar la situación actual de la infraestructura de seguridad IEEE 802.11.
- Reduce tiempos y costos al seleccionar intencionalmente a los participantes más relevantes.

Limitaciones:

- Generalización limitada: Al no ser aleatorio, los resultados no pueden extrapolarse estadísticamente a toda la comunidad universitaria.
- Posible sesgo de selección: La muestra depende de los contactos o la accesibilidad de los participantes, lo que puede dejar fuera a sujetos importantes, pero de difícil acceso (Malterud et al., 2016).

3.5.1.1. Tamaño de la muestra

En estudios con diseños cualitativos o mixtos, que combinan elementos cuantitativos y cualitativos, la determinación del tamaño de la muestra en un muestreo intencional se basa en el criterio de saturación de la información (Malterud et al., 2016). En este proyecto, se estableció una meta inicial de 260 encuestas distribuidas de la siguiente manera:

- Estudiantes: Son los principales usuarios del servicio de red inalámbrica, lo que resulta clave para entender problemas de conectividad, usabilidad y percepción de seguridad.
- Docentes: Usuarios frecuentes que, además, pueden necesitar un mayor rigor en la protección de datos (por ejemplo, en investigaciones académicas y calificaciones).
- Personal Administrativo: Encargados de la gestión de la infraestructura; su perspectiva es fundamental para evaluar los requisitos técnicos y las oportunidades de mejora.

Además, se consideró realizar 7 encuestas o entrevistas a personal especializado (como responsables de TI, jefes de laboratorio, etc.), quienes pueden ofrecer información técnica detallada sobre la configuración, el mantenimiento y la actualización de la red conforme a la norma IEEE 802.11.

Aunque no se utilizó una fórmula estadística para determinar el tamaño de la muestra, como la de Cochran, se tomaron en cuenta los siguientes factores (Patton, 2015; Flick, 2018):

- Disponibilidad y acceso a los informantes: Se eligieron sujetos con alta probabilidad de uso o gestión de la red.
- Diversidad de perfiles: Se buscó representar todas las áreas que influyen en la experiencia de la red (administrativa, académica y estudiantil).
- Objetivos y alcance del estudio: El objetivo no era cuantificar de manera universal, sino comprender la situación y proponer mejoras basadas en la evidencia recopilada de actores clave.

3.5.2 Análisis de las herramientas de recolección de datos a utilizar

En este apartado se describen y justifican las herramientas de recolección de datos utilizadas en el estudio, teniendo en cuenta la necesidad de realizar un análisis del sistema de seguridad basado en el estándar IEEE 802.11.

3.5.2.1 Encuesta – Entrevista - Observación / Otras.

Encuestas

La encuesta es una herramienta de recopilación de datos cuantitativos que obtiene información de una muestra representativa de la población objetivo. Se utilizará para recopilar datos sobre el conocimiento del usuario y los niveles de percepción de la seguridad de la red de acuerdo con la normativa IEEE 802.11 y el estado actual del control de acceso y la relación de ambos conceptos. Se harán preguntas cerradas y abiertas para capturar información tanto cuantitativa como cualitativa.

TecnoDigital (2023), argumentó que las encuestas son útiles para obtener datos de grandes grupos de personas y que los resultados pueden generalizarse a una población más amplia.

3.5.2.2 Estructura de lo(s) instrumento(s) de recolección de datos aplicados.

Para la recogida de datos en el análisis de sistemas de seguridad basados en el estándar IEEE 802.11 se utilizará como herramienta principal la encuesta.

La encuesta fue diseñada para recopilar las opiniones de estudiantes y profesores sobre la seguridad de la red. Estas encuestas se dividirán en tres partes: la primera recoge datos demográficos; la segunda, conocimiento y percepción del sistema de seguridad y la tercera, sugerencias de mejora.

Encuesta para la Población General

La encuesta se realizó en el Área de Carrera de Agronegocios de la Facultad de Ciencias de la Vida y Tecnología de Ulam (FCVT). Su objetivo principal es evaluar el conocimiento y comprensión de los usuarios sobre los sistemas de control de acceso al aula, centrándose en la implementación de tecnología inalámbrica basada en el estándar IEEE 802.11. Consta de ocho preguntas que cubren el tipo de sistema actualmente en uso, su eficacia para prevenir el acceso no autorizado, la frecuencia con la que se encuentran problemas y el conocimiento del estándar, además de recoger sugerencias para mejorar el sistema.

Las opciones de respuesta incluyen formatos cerrados y de opción múltiple diseñados para identificar tecnologías populares y medir las percepciones de seguridad de la comunidad. Entre los temas evaluados destacan la adecuación del sistema actual, la capacitación de los usuarios y la percepción sobre la efectividad de la integración de tecnologías inalámbricas. Los resultados permitirán identificar áreas de mejora en los sistemas de control de acceso implementados en el bloque evaluado.

Propósito: Recoger sugerencias para mejorar el sistema, enfocándose en áreas específicas que podrían beneficiarse de mejoras.

Encuesta para Personal Especializado

La encuesta, realizada por profesionales del Departamento Vocacional de Agronegocios de la Facultad de Ciencias de la Vida y Tecnología (FCVT) de Uleam, se centró en evaluar las percepciones y el conocimiento técnico sobre la implementación y seguridad de redes inalámbricas basadas en IEEE 802.11. Está dividido en seis preguntas y cubre temas como los protocolos de seguridad utilizados, las prácticas de monitoreo de redes, el rendimiento de la tecnología, los métodos de cifrado, la interoperabilidad del sistema y la documentación de soporte técnico.

El formato de las preguntas fue cerrado y diseñado para determinar el nivel de conocimiento técnico y las percepciones sobre la eficiencia y confiabilidad del sistema. Además, la encuesta se dividió en dos partes: una discutió las experiencias de los administradores en la gestión del sistema y la otra analizó los procedimientos de seguridad implementados y los desafíos enfrentados en su operación. Esta estructura permite obtener información clave para fortalecer la seguridad y la funcionalidad de las redes inalámbricas en entornos educativos.

Propósito: Analizar la disponibilidad y calidad de la documentación de soporte técnico, crucial para el mantenimiento del sistema.

La entrevista se dividió en dos partes: la primera discutió las experiencias de los administradores y la segunda discutió los procedimientos de seguridad y los desafíos encontrados.

3.5.2.3 Plan de recolección de datos.

El plan de recopilación de datos se desarrolló en un plazo de dos semanas.

- Primera Semana:
    - Distribución de Encuestas: Las encuestas se enviaron por correo electrónico a estudiantes y profesores. Se incluyeron instrucciones claras sobre cómo completarlas y la fecha límite para la entrega.
    - Programación de Entrevistas: Se coordinaron las entrevistas con administradores y personal clave, asegurando que todas las partes tuvieran claridad sobre las fechas y horarios disponibles.
- Segunda Semana:
    - Recopilación de Encuestas: Se monitoreó el proceso y se enviaron recordatorios automáticos para las encuestas no completadas, lo que garantizó una alta tasa de respuesta.

- Realización de Entrevistas: Las entrevistas se llevaron a cabo en un salón reservado específicamente para este fin o a través de plataformas de videollamadas, según la disponibilidad y preferencia de los participantes.

- Responsabilidades:
  - Investigador Principal: Supervisó todo el proceso, asegurando el cumplimiento de los plazos, y fue responsable del análisis detallado de los datos recopilados.
  - Asistente de Investigación: Fue responsable de la distribución de encuestas, organización de entrevistas, y aseguró que los datos fueran recopilados y almacenados de manera segura.

Este plan estructurado garantizó que todos los pasos del proceso de recopilación de datos fueran claros, eficientes y efectivos, maximizando la calidad y cantidad de datos recopilados.

3.6 Análisis y presentación de resultados

3.6.1 Tabulación y análisis de los datos

3.6.2 Presentación y descripción de los resultados obtenidos

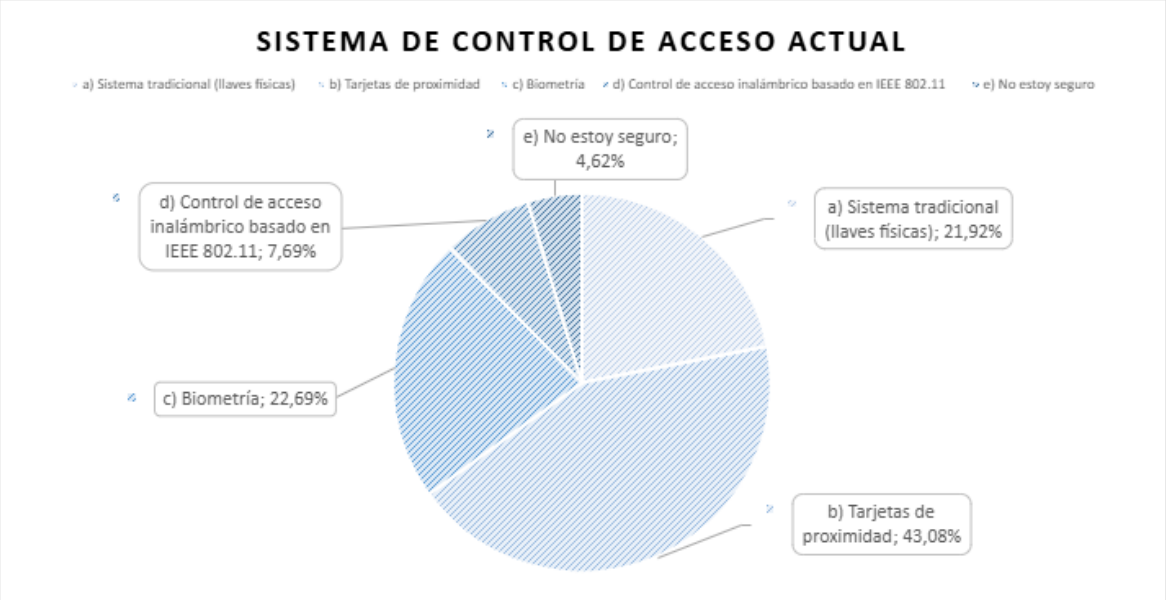
Se despliegan los resultados de las evaluaciones cualitativas ejecutadas, que sustentan la línea de investigación enfocada a obtener una base de percepción en un lapso único con la finalidad de generar con precisión un diagnóstico del nivel de conocimiento y aceptación de los agentes relacionados con la integración del sistema de control acceso en las aulas del bloque seleccionado y simultáneamente consolidar un plan de acción basado en la norma IEEE 802.11 encaminado a la mejora de prácticas de seguridad en la red.

Instrumento 1

1. ¿Qué tipo de sistema de control de acceso se utiliza actualmente en las aulas de la universidad?

Figura 7

Sistema de control de Acceso actual



Nota: Sistema de control de acceso actual en aulas de la universidad. Fuente propia.

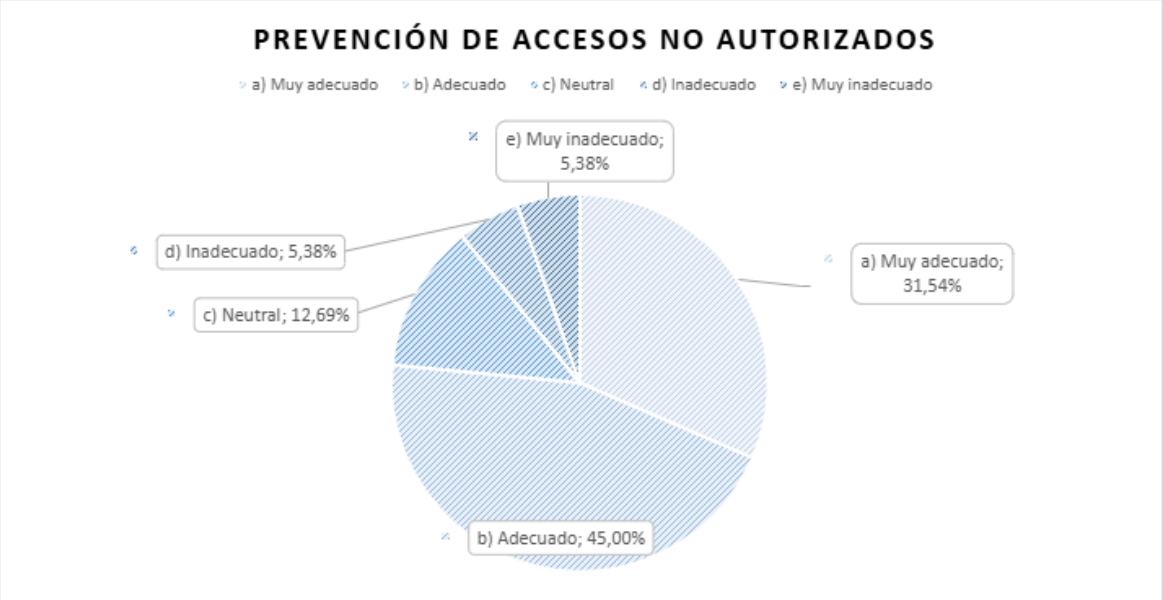
Análisis e interpretación:

Los datos proporcionados permiten identificar las tecnologías de seguridad implementadas y su prevalencia. Al manifestar su criterio más del 43% de la muestra optó por escoger las tarjetas de proximidad como sistema vigente observado y de uso continuo para el control de acceso, destacando su conveniencia al ofrecer autenticación rápida y sin contacto. Un porcentaje considerable del 22.69% indicó que se emplean sistemas biométricos, lo que refleja un enfoque más avanzado en términos de seguridad, generalmente un método considerado más difícil de vulnerar. No obstante, las llaves físicas aún se utilizan según un 21,92%, indicio de que algunas aulas o áreas no han adoptado completamente nuevas tecnologías exponiéndose a riesgos previsibles, como la duplicación o pérdida de ejemplares. Por otro lado, un 7,69% de los encuestados declaró el uso de redes inalámbricas para el control de acceso, reguladas por la normativa IEEE 802.11. Finalmente, un 4,62% de los participantes desconoce el tipo de sistema implementado, lo que evidencia una posible falta de comunicación o comprensión sobre las tecnologías de seguridad en uso.

2. ¿Considera que el sistema actual de control de acceso es adecuado para prevenir accesos no autorizados?

Figura 8

Prevención de accesos no autorizados



Nota: Prevención de accesos no autorizados a través del sistema de control de acceso. Fuente propia.

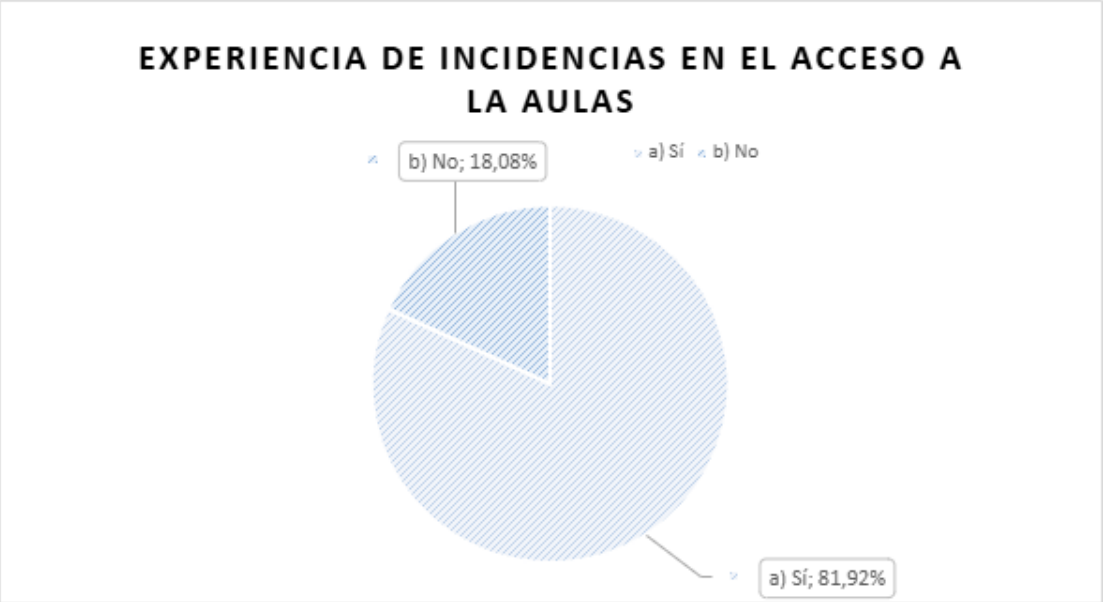
Análisis e interpretación:

De la muestra total encuestada se extrae una percepción mayoritariamente favorable en función a la efectividad del sistema de prevención de accesos no autorizados puesto que alrededor del 77% considera que las medidas actuales son adecuadas (45%) y muy adecuadas (32%), lo que sugiere una aceptación general en cuanto a la gestión del acceso a las aulas. Un 12,69% carece de una opinión definida, lo que podría sugerir falta de falta de experiencia con el sistema o incertidumbre sobre su efectividad. Y de forma secuencial, un pequeño porcentaje (5,38%) lo califica como insuficiente, señalando la necesidad de abordar las posibles brechas de seguridad y fomentar soluciones que garanticen el ciclo de mejora continua en aspectos específicos del sistema.

3. ¿Ha experimentado problemas con el control de acceso a las aulas en el último año?

Figura 9

Experiencia de incidencias en el acceso a las aulas



Nota: Experiencia de incidencias en el acceso a las aulas. Fuente propia.

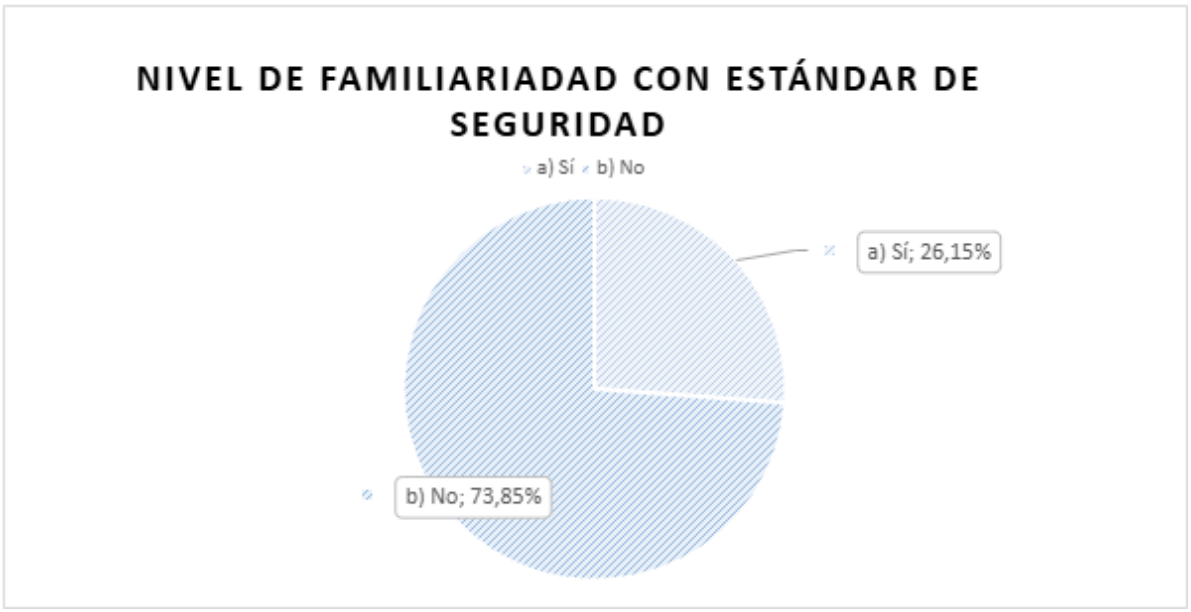
Análisis e interpretación:

Se distingue la frecuencia e impacto de los incidentes de seguridad asociados al sistema vigente de acceso a aulas durante un período anual. Una amplia mayoría, equivalente al 81,92% de los encuestados, reporta haber experimentado problemas con dicho sistema. Este hallazgo es crítico, ya que refleja una alta tasa de fallas o inconvenientes que podrían estar vinculados tanto a la tecnología utilizada como a fallas operativas, afectando la experiencia de un gran número de usuarios y, potencialmente, comprometiendo la seguridad en el acceso a las aulas. Un porcentaje menor al 20% menciona no haber experimentado problemas en su desempeño, lo que podría indicar que el sistema funciona correctamente en ciertos contextos o áreas específicas, por ende, los incidentes no son universales, pero sí recurrentes en gran medida. Es posible que existan variaciones en la tecnología o en los mecanismos de acceso utilizados por diferentes grupos, lo cual reduce la incidencia de errores en el sistema.

4. ¿Está familiarizado con la norma IEEE 802.11?

Figura 10

Nivel de familiaridad con estándar de seguridad



Nota: Nivel de familiaridad con el estándar de seguridad. Fuente propia.

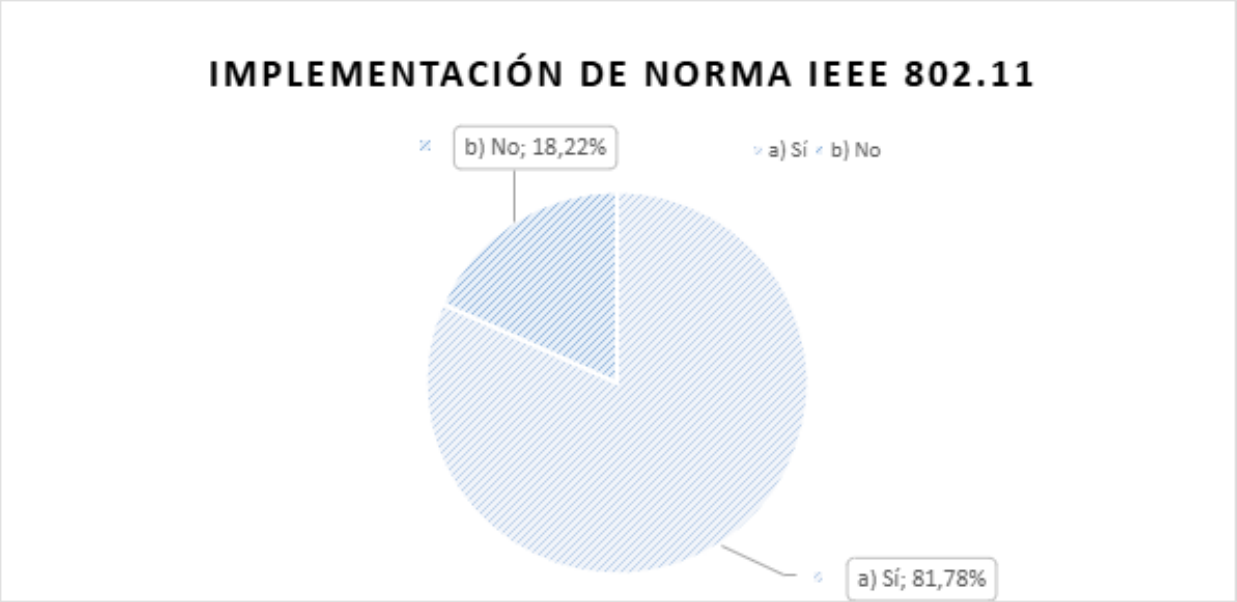
Análisis e interpretación:

Se cuantifica el nivel de conocimiento de los encuestados respecto a la norma IEEE 802.11, clave para entender su percepción de las tecnologías inalámbricas y su integración en sistemas de seguridad. Un 73,85% de los encuestados indicó no estar familiarizado con la norma IEEE 802.11., en tal caso, se revela un desconocimiento generalizado con un estándar técnico clave en el ámbito de las redes inalámbricas y la seguridad, lo que podría limitar el uso adecuado de soluciones tecnológicas basadas en este estándar. Un 26,15% de los encuestados afirmaron estar familiarizados con el fundamento normativo, es decir, solo una pequeña proporción de los participantes tiene algún nivel de conocimiento técnico sobre el estándar de seguridad en redes inalámbricas.

5. ¿Está familiarizado con la implementación de sistemas de control de acceso basados en la norma IEEE 802.11?

Figura 11

Implementación de la norma IEEE 802.11



Nota: Implementación de la norma IEEE 802.11. Fuente propia.

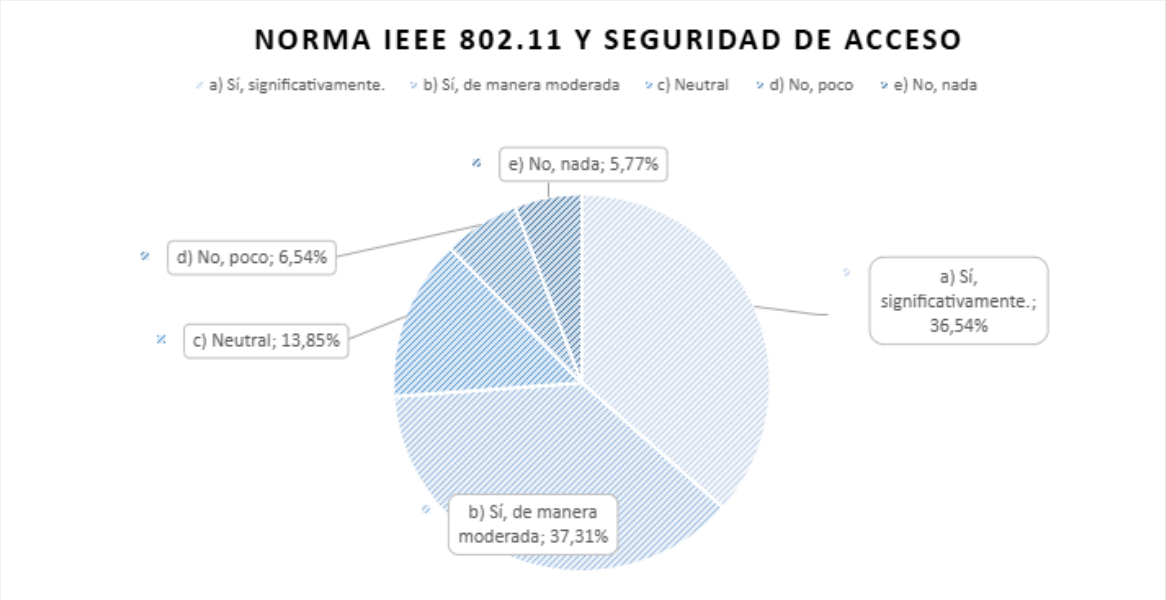
Análisis e interpretación:

Al determinar el nivel de conocimiento práctico sobre la implementación de sistemas de control de acceso basados en la norma IEEE 802.11, se observó que el 81,78% de los encuestados manifestaron estar familiarizados con dichos sistemas. Este resultado contrasta significativamente con la falta de familiaridad teórica que los participantes tienen respecto a la norma en su totalidad, lo cual sugiere que muchos de ellos poseen una experiencia práctica significativa en la utilización de estos sistemas, pero carecen de un entendimiento teórico profundo sobre los aspectos técnicos que subyacen en su funcionamiento. Por otro lado, un 18,22% de los encuestados indicó no estar familiarizados. Aunque esta cifra representa una minoría, sigue evidenciando una brecha que podría comprometer la consistencia en el manejo del sistema y la comprensión de los protocolos de seguridad.

6. ¿Cree que la integración de la norma IEEE 802.11 mejora la seguridad en el control de acceso a las aulas?

Figura 12

Norma IEEE 802.11 y seguridad de acceso



Nota: Norma IEEE 802.11 y seguridad de acceso. Fuente propia.

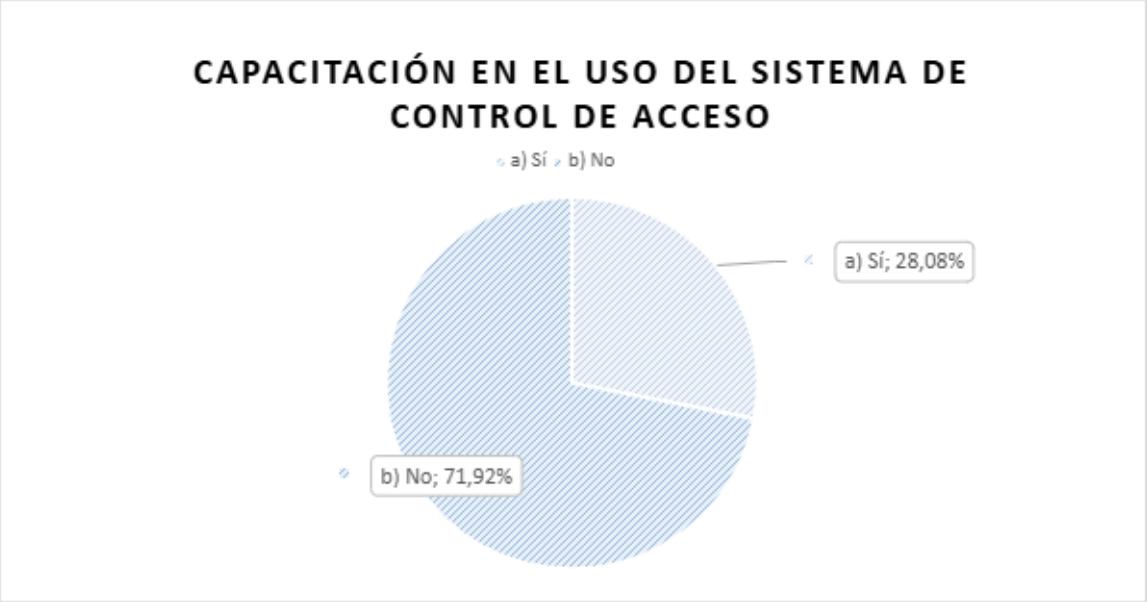
Análisis e interpretación:

Respecto a la percepción de efectividad de la norma IEEE 802.11 como mecanismo que asegura y fomenta mejoras en la seguridad, se ha podido observar en base a los resultados que aproximadamente el 74% de la muestra seleccionada considera que la implementación de este estándar en el sistema de control de acceso a las aulas si genera un ambiente de seguridad. De este porcentaje, el 36,54% de los participantes percibe un aumento considerable en la seguridad, mientras que el 37,31% califica la mejora como moderada. Al mismo tiempo, un 13,85% reporta una postura neutral frente a la cuestión planteada y se destaca que alrededor del 13% se encuentra en desacuerdo con el potencial del fundamento normativo para producir soluciones óptimas al momento de contrarrestar vulnerabilidades y riesgos presentes en redes inalámbricas

7. ¿Ha recibido capacitación sobre el uso del sistema de control de acceso a las aulas basado en IEEE 802.11?

Figura 13

Capacitación en el uso del sistema de control de acceso



Nota: Capacitación sobre el uso del sistema de control de acceso. Fuente propia.

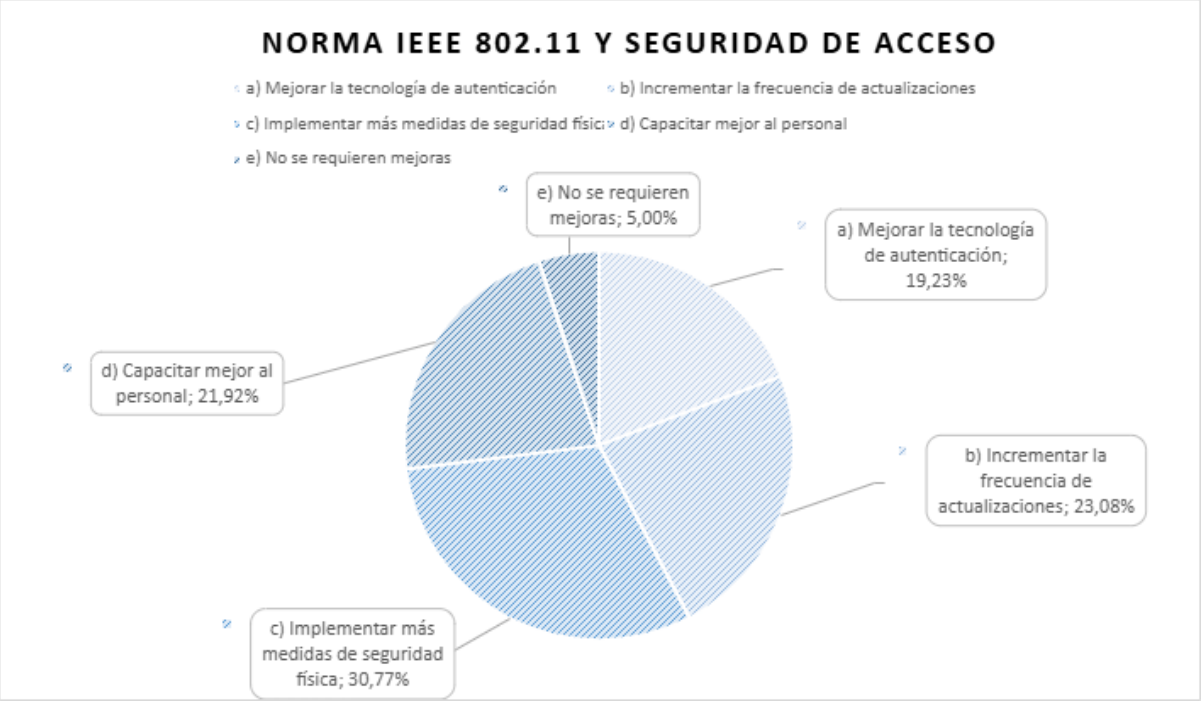
Análisis e interpretación:

De forma razonable, es preciso identificar si los usuarios del sistema de control de acceso han sido capacitados adecuadamente referente a las buenas prácticas de uso. En este sentido, se enfatiza en que más del 70% de los participantes en el estudio mencionan no haber recibido ningún tipo de formación o instrucción relacionada al sistema especialmente en lo referente a los estándares de la norma IEEE 802.11, lo que plantea una preocupación significativa en términos de la correcta utilización y seguridad del sistema. En contraste, una minoría, que representa el 28,08%, indicó que sí ha sido plenamente capacitada en el pasado para el uso correcto del sistema, lo cual se traduce en un mayor grado de confianza en su manejo y en la efectividad de los controles implementados. Este grupo capacitado representa un factor clave para el óptimo funcionamiento del sistema, dado que su formación previa les permite operar conforme a las mejores prácticas establecidas, contribuyendo a la seguridad y eficacia del sistema de control de acceso.

8 ¿Qué mejoras sugeriría para el sistema de control de acceso a las aulas basado en IEEE 802.11?

Figura 14

Norma IEEE 802.11 y seguridad de acceso



Nota: Sugerencias para el sistema de control de acceso. Fuente propia.

Análisis e interpretación:

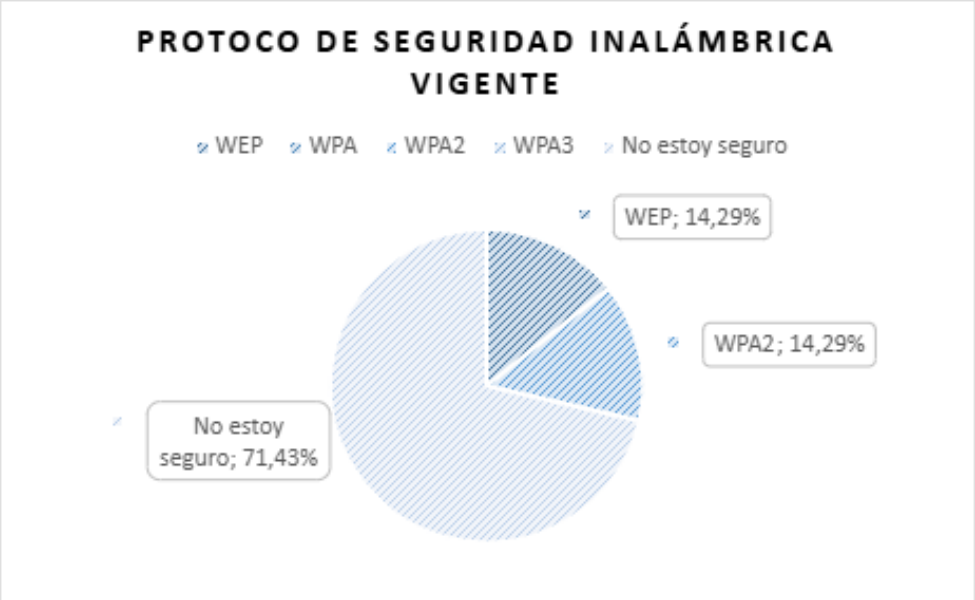
En el marco de la búsqueda de soluciones para desarrollar un plan integral de mejora continua, se recabaron las sugerencias de los 260 sujetos encuestados sobre lineamientos específicos relacionados con el sistema de control de acceso a las aulas. Del total el 30,77% señaló de manera general la necesidad de aumentar las medidas de seguridad física, argumentando que las actuales resultan insuficientes, otro segmento representado por el 23,08% expresó su preferencia por incrementar la frecuencia de las actualizaciones del sistema, con el objetivo de optimizar su desempeño, Además, un 21,92% destacó la relevancia de implementar programas de capacitación de alta calidad dirigidos al personal encargado de la gestión y operación del sistema de control y en última instancia, un 5% manifestó de forma notable que sus expectativas como usuarios han sido cumplidas, afirmando que no consideran necesarias más mejoras en el sistema actual.

Instrumento 2

1. ¿Qué protocolo de seguridad inalámbrica se utiliza en la red de control de acceso de las aulas?

Figura 15

Protocolo de seguridad inalámbrica vigente



Nota: Protocolo de seguridad inalámbrica utilizado en la red de control de acceso. Fuente propia.

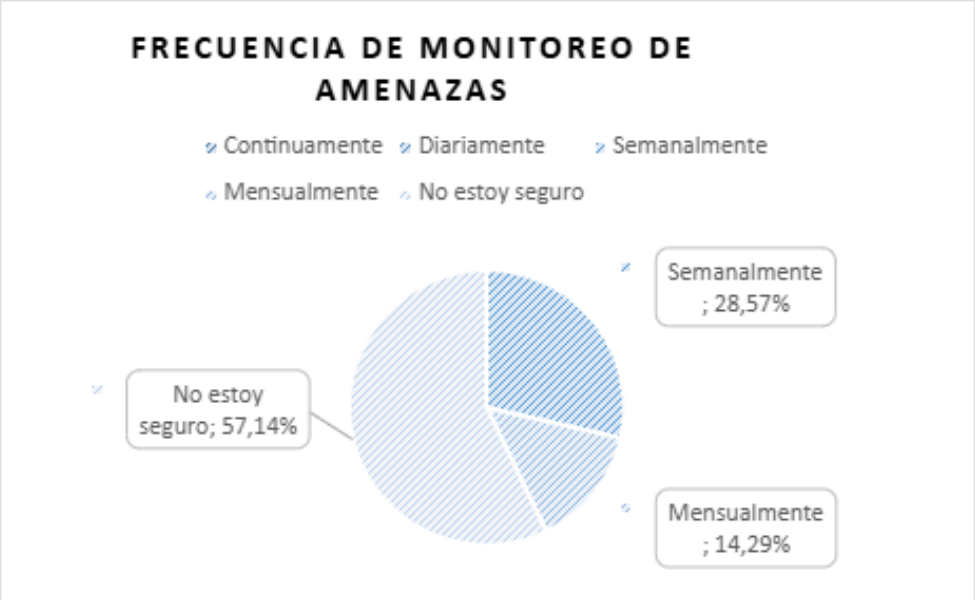
Análisis e interpretación:

Considerando que el objetivo es identificar el protocolo de seguridad empleado como clave para la protección de los sistemas de acceso a las aulas, se ha denotado que se presenta una brecha significativa en el conocimiento: por un lado dos sujetos declararon respuestas opuestas, representando el 14,29% para el WEP y para el WPA2 y a su vez, más del 70% de los sujetos evaluados emitieron desconocer con exactitud el protocolo vigente lo cual representa un riesgo potencial de seguridad, ya que los usuarios pueden no estar al tanto de los estándares vigentes ni de las mejores prácticas para asegurar las redes inalámbricas.

2. ¿Con qué frecuencia se monitorea la red inalámbrica para detectar posibles amenazas?

Figura 16

Frecuencia de monitoreo de amenazas



Nota: Frecuencia de monitoreo de amenazas. Fuente propia.

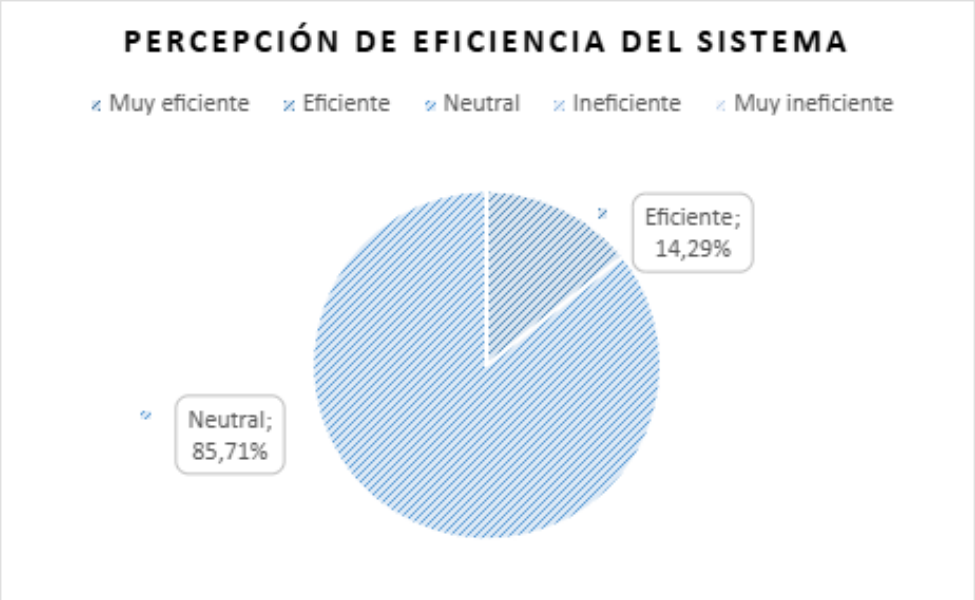
Análisis e interpretación:

Al recolectar la percepción referente a las prácticas de detección temprana de riesgos potenciales fue posible evidenciar que el 28,57% de los encuestados considera que el monitoreo de la red se realiza semanalmente. este porcentaje refleja que una parte cree que existe una rutina de vigilancia periódica, aunque la frecuencia semanal puede no ser suficiente en redes críticas. El 14,29% de los encuestados cree que el monitoreo se realiza mensualmente, lo cual sugiere una percepción de que las medidas de seguridad exponen la red durante lapsos significativos. Mientras que más del 50% indica no estar seguro de la frecuencia con la que se monitorea la red, lo que resalta una falta de conocimiento general sobre las políticas y prácticas de seguridad implementadas.

3. ¿Qué tan eficiente considera el sistema en términos de velocidad de conexión y confiabilidad?

Figura 17

Percepción de eficiencia del sistema



Nota: Percepción de eficiencia del sistema. Fuente propia.

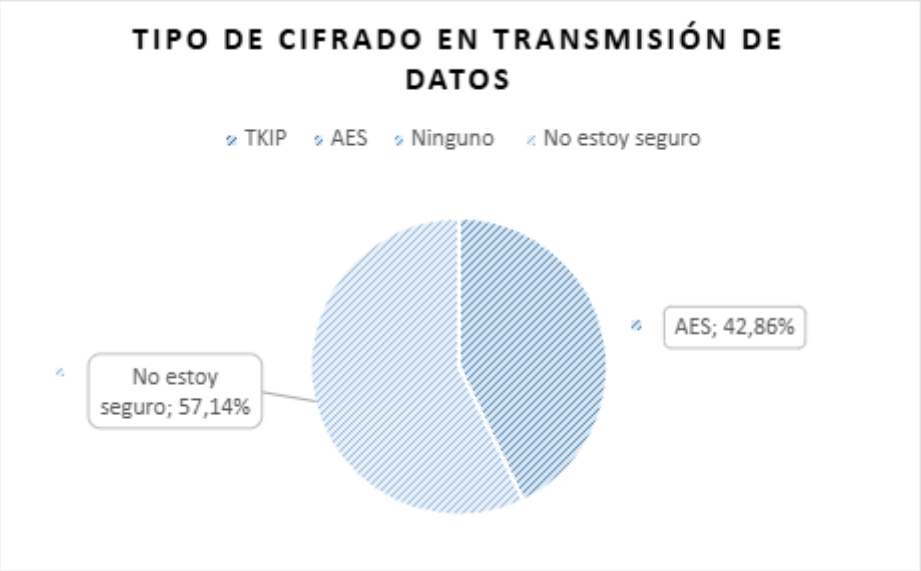
Análisis e interpretación:

Desde la perspectiva de los especialistas se determinó el rendimiento técnico de la red en términos de velocidad de conexión y confiabilidad. Un 85,71% posee una opinión neutral sobre la eficiencia del sistema, denotando que para una alta tasa de encuestados el rendimiento actual, en función a los términos bajo escrutinio, no está cumpliendo con las expectativas de la mayoría. No obstante, aunque no se percibe como sobresaliente tampoco encuentran o señalan problemas críticos en su funcionamiento. Esta neutralidad podría reflejar una experiencia inconsistente o poco notable. Y tan solo un 14,29% percibe el sistema como eficiente, lo cual indica que una pequeña proporción está satisfecha con el desempeño del sistema, pero claramente no es la mayoría.

4. ¿Qué tipo de cifrado se utiliza en la transmisión de datos a través de la red IEEE 802.11?

Figura 18

Tipo de cifrado en transmisión de datos



Nota: Tipo de cifrado en transmisión de datos. Fuente propia.

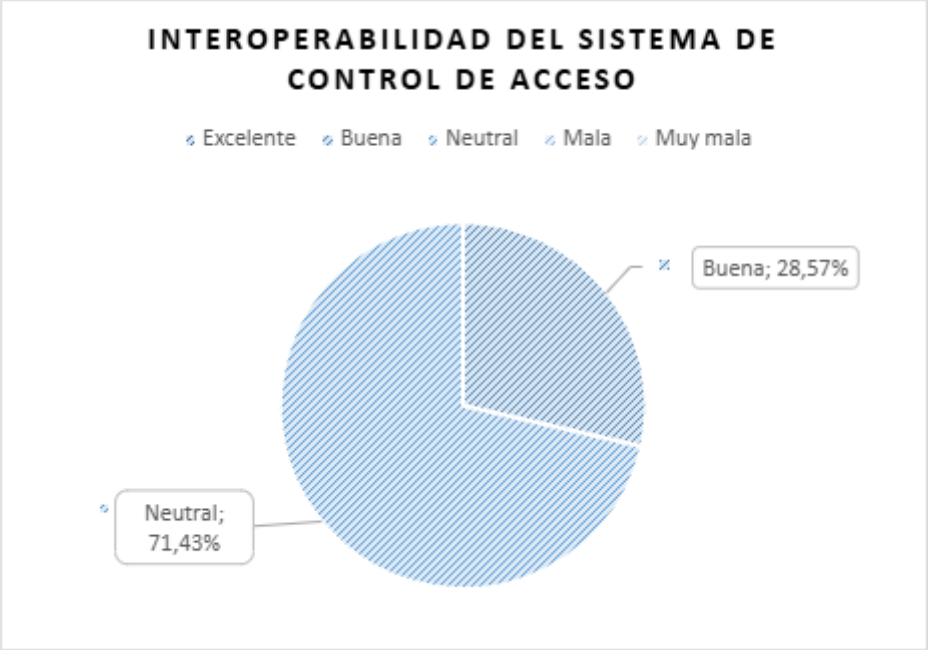
Análisis e interpretación:

Los resultados revelan el nivel de familiaridad de los especialistas en relación con las técnicas de cifrado que aseguran el flujo de comunicación en la red. Un porcentaje superior al 50% de los encuestados (exactamente el 57.14%) muestra inseguridad al momento de seleccionar el tipo de cifrado utilizado en la transmisión de datos, lo que evidencia una falta de consistencia en las prácticas de seguridad de red. Aunque el 42.86% identificó correctamente el cifrado AES, uno de los estándares más seguros, la ausencia de conocimiento en más de la mitad de los usuarios representa un riesgo potencial para la seguridad de la red y requiere atención inmediata.

5. ¿Cómo califica la interoperabilidad del sistema de control de acceso con otros dispositivos inalámbricos basados en IEEE 802.11?

Figura 19

Interoperabilidad del sistema de control de acceso



Nota: Interoperabilidad del sistema de control de acceso. Fuente propia.

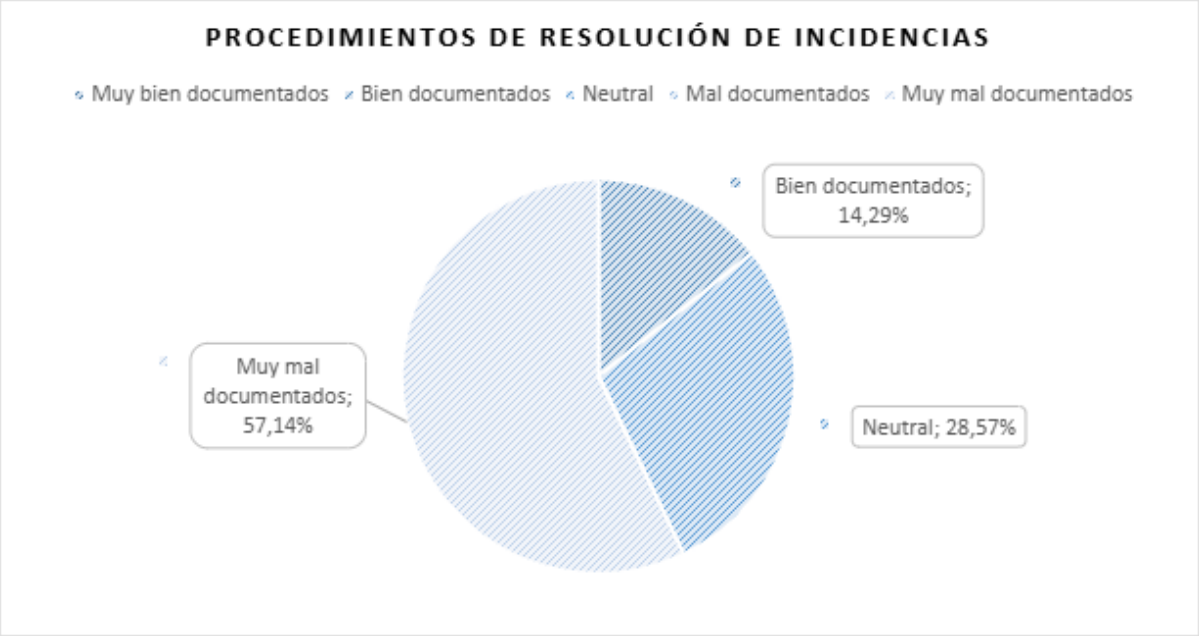
Análisis e interpretación:

Centrando el estudio en cómo los usuarios perciben la capacidad del sistema para integrarse con otros dispositivos, se manifestó una posición neutral de un 71.43% de los usuarios respecto a la interoperabilidad del sistema de control de acceso, lo que sugiere que no han experimentado problemas serios con la integración y a su vez no distinguen ventajas claras. Un 28.57% de los encuestados la considera buena, lo que es un resultado alentador, no obstante, sigue habiendo una percepción general de indiferencia, lo cual puede frenar una adopción más entusiasta del sistema. Mejorar la interoperabilidad y demostrar su relevancia podría mejorar la percepción y aumentar la eficiencia y expansión del sistema en conjunto con otros dispositivos inalámbricos.

6. ¿Qué tan bien documentados están los procedimientos para resolver incidencias relacionadas con la red IEEE 802.11?

Figura 20

Procedimientos de resolución de incidencias



Nota: Procedimientos de resolución de incidencias. Fuente propia.

Análisis e interpretación:

La presenta interrogante explora la disponibilidad y calidad de la documentación técnica de soporte, lo cual es crucial para garantizar el mantenimiento eficaz del sistema. El 57,14% de los encuestados considera que los procedimientos están muy mal documentados. Este alto porcentaje revela una insatisfacción considerable con la calidad de la documentación, lo que puede generar dificultades al intentar resolver problemas de la red de manera eficiente ocasionando retrasos críticos y aumentos de costos de soporte técnico. El 28,57% de los encuestados muestra una postura neutral, lo cual sugiere que, pese a no haber enfrentado inconvenientes graves con la documentación, tampoco perciben que esta ofrezca un valor añadido significativo. Por último, solo un 14,29% de los encuestados considera que los procedimientos están bien documentados. Esto implica que una pequeña porción de usuarios tiene una percepción positiva, sin embargo, es insuficiente para compensar la prevalencia de opiniones negativas.

3.6.3 Informe final del análisis de los datos (conclusiones para el marco investigativo)

La construcción del apartado de diagnóstico de campo se ha consolidado con las divergentes perspectivas de los agentes asociados al proceso de implementación y uso del sistema de control de acceso basado en los principios de la norma IEEE 802.11. En vista de los hallazgos particulares se permite identificar los puntos clave resultantes:

Tabla 3

Análisis de datos sobre el sistema de control de acceso basado en IEEE 802.11

Instrumento 1	Instrumento 2
Sistema de control predominante El uso de tarjetas de proximidad es el más prevalente, seguido de sistemas biométricos. Aunque esto certifica que las aulas emplean tecnología moderna, una proporción significativa aún depende de sistemas tradicionales como las llaves físicas, lo que puede presentar riesgos de seguridad.	**Desconocimiento del protocolo** Gran parte de los especialistas encuestados desconocen el protocolo de seguridad que se utiliza, lo que indica una falta de conocimiento técnico o acceso a información actualizada sobre las redes inalámbricas en un entorno crítico como el control de acceso a aulas.
Eficacia percibida En general, la percepción sobre la efectividad del sistema es positiva. Sin embargo, el porcentaje que lo considera ineficaz destaca la necesidad de revisar posibles brechas de seguridad y reforzar ciertas áreas del sistema.	**Monitoreo insuficiente** Existe incertidumbre sobre la frecuencia de monitoreo de la red, lo que sugiere que las políticas de seguridad no son claras o no se comunican adecuadamente. El monitoreo constante es esencial para prevenir amenazas.
Incidencias del sistema El 81,92% ha experimentado problemas con el sistema en el último año. Las causas podrían incluir falta de actualización tecnológica, problemas de conectividad o fallos en la autenticación. Es urgente realizar una evaluación técnica para resolver estos problemas y garantizar un funcionamiento más robusto.	**Eficiencia percibida** El hecho de que la mayoría presente una percepción neutral en relación con la eficiencia del sistema puede interpretarse como indiferencia o insatisfacción velada. Para un sistema que depende de la confianza de los usuarios en su rendimiento, es fundamental

Conocimiento de la norma IEEE 802.11

La mayor parte de los encuestados reconoce los beneficios de la implementación de la norma IEEE 802.11, pero existe una fracción minoritaria que, ya sea por escepticismo o por experiencias no satisfactorias, no comparte esta valoración positiva.

Falta de capacitación técnica

Pese a que una amplia mayoría de los usuarios demuestra competencia en el uso práctico de los sistemas de control de acceso, la falta de conocimiento teórico más profundo resalta una oportunidad clave para reforzar las capacidades técnicas de los usuarios.

Percepción de seguridad

Aunque gran parte de los usuarios percibe mejoras de seguridad, una fracción de ellos permanece escéptica, lo que sugiere la necesidad de reforzar la comunicación sobre los beneficios del estándar IEEE 802.11 y posibles ajustes en su implementación.

Capacitaciones otorgadas

El contraste entre la mayoría no capacitada y la minoría que sí lo ha sido subraya la importancia crítica de implementar programas de capacitación más amplios y continuos para asegurar el uso adecuado del sistema basado en la norma IEEE 802.11.

reducir la neutralidad y aumentar las percepciones positivas mediante prácticas de mejora continua.

Desconocimiento del cifrado

La falta de claridad sobre el cifrado utilizado es preocupante, ya que la seguridad depende en gran medida de la correcta implementación de este. Este vacío podría deberse a una deficiente comunicación o formación en temas de seguridad.

Interoperabilidad del sistema

La neutralidad predominante puede traducirse como un indicador de que, si bien el sistema no enfrenta grandes desafíos de interoperabilidad, tampoco sobresale en este aspecto. Lo cual podría limitar su adopción en entornos donde la integración con otros dispositivos es crítica.

Documentación técnica deficiente

En particular, los resultados indican una necesidad urgente de mejorar la calidad de la documentación técnica, ya que su deficiencia actual está impactando tanto en la eficiencia operativa como en los costos de mantenimiento del sistema. Mejorar la claridad y disponibilidad de estos procedimientos contribuiría a una gestión más ágil y efectiva de las incidencias.

Sugerencias de mejora
Entre las principales recomendaciones destacan el refuerzo de la seguridad física, actualizaciones más frecuentes y capacitaciones al personal.

Nota: Análisis comparativo de las perspectivas sobre el sistema de control de acceso basado en IEEE 802.11. Fuente propia

En síntesis, aunque existe una percepción general de efectividad en el sistema de control de acceso basado en IEEE 802.11, se identifican áreas clave para mejorar, especialmente en términos de capacitación, documentación y actualización de medidas de seguridad. La implementación de mejores prácticas y formación técnica adicional es esencial para asegurar la consistencia en el uso y manejo del sistema a corto y largo plazo.

ULEAM

PLAN DE MEJORA

BASADO EN ESTÁNDAR

IEEE 802.11

DEL SISTEMA DE CONTROL DE ACCESO

Capítulo IV: Marco propositivo

Descripción del plan de mejora

4.1. Introducción

Visualizar un entorno potenciado con tecnología moderna pretende mermar las brechas de seguridad que surgen como consecuencia de sistemas tradiciones de entrada y salida en espacios recurrentes. Sin ápice de duda, un escenario sin estándares de seguridad sería extremadamente caótico y poco confiable, donde la integridad, la confidencialidad y la disponibilidad estarían constantemente en riesgo (Valencia, 2021). La ausencia de marcos legales internacionales como es el caso de la norma IEEE 802.11 socavaría la confianza en los sistemas inalámbricos. Los usuarios mostrarían una actitud reacia a compartir información sensible para formular la base de datos que propicia la utilización de tales sistemas, lo que podría obstaculizar la innovación tecnológica en la academia.

Giménez (2023), menciona en su aporte al conocimiento el desarrollo de la Tríada de la seguridad, un andamiaje de tres elementos esenciales para garantizar la seguridad en ambientes informáticos, estos aseguran que los datos sean accesibles solo para las personas autorizadas (confidencialidad), que la información sea precisa y completa, permitiendo modificaciones únicamente por personal autorizado (integridad), y, finalmente, que los datos estén disponibles para su uso cuando se necesiten (disponibilidad).

Ante la necesidad apremiante de implementar un sistema de seguridad, las contramedidas deben enfocarse en reducir la frecuencia de incidentes indeseados, como ataques cibernéticos o filtraciones de datos confidenciales. Al mismo tiempo, es crucial contar con planes de respuesta efectivos que mitiguen el impacto negativo cuando estos eventos ocurren. No obstante, dado que no todas las medidas de control son efectivas, es fundamental realizar un análisis de las opciones más viables para equilibrar los beneficios de las protecciones con los costos de su implementación y mantenimiento.

Por lo tanto, se vuelve imperativo establecer y cumplir normas de seguridad robustas como modelo que garantiza un grado razonable de seguridad y que pretenda salvaguardar la infraestructura y datos críticos de la organización. Persiguiendo el monitorio del rendimiento y la generación de ajustes al sistema de control de accesos según se considere oportuno, se resalta el empleo del ciclo de mejora continua popularizado por Deming que incluye: planificar-hacer-verificar y actuar (PHVA).

Objetivo

Desarrollar una planificación estratégica basada en los estándares de la norma IEEE 802.11 que permita compilar las acciones necesarias para mitigar posibles amenazas y garantizar el buen funcionamiento del sistema de control de acceso implementado en las aulas del bloque de la carrera de Agroindustria de la Facultad de Ciencias de la Vida y Tecnologías de la Universidad Laica Eloy Alfaro de Manabí.

Alcance

El presente plan de mejora será de aplicación para el sistema de control de acceso implementado en las aulas del bloque de la carrera de Agroindustria de la Facultad de Ciencias de la Vida y Tecnologías de la Universidad Laica Eloy Alfaro de Manabí y para todos los agentes involucrados en su uso.

Contexto de IEEE 802.11

Con la expansión de dispositivos conectados y el Internet de las cosas (IoT), desde su aprobación inicial en 1997 el estándar IEEE 802.11 ha continuado evolucionando, proporcionando un marco aún más robusto para la transmisión de datos en redes locales inalámbricas (WLAN). Se ha hecho notable la creciente demanda de Wi-Fi en entornos académicos y empresariales, por lo cual, las revisiones efectuadas a la norma permiten ofrecer seguridad en el flujo de información, optimizar el rendimiento en tiempo y disponibilidad, además de aumentar la eficiencia en el uso de dispositivos múltiples. La última versión sólida presente en el 2019 aborda directrices con el fin de reducir la congestión en redes saturadas.

Análisis de situación actual

A partir de las falencias detectadas en el trabajo de campo se construye el presente plan de mejora continua para el sistema de control de acceso de aulas del bloque de Agroindustria basado en la norma IEEE 802.11, el cual considerará y explorará los criterios más relevantes y sólidos para adoptar medidas que fomenten buenas prácticas de uso de las cerraduras inteligentes implementadas con el fin de validar su efectividad e incrementar su durabilidad en el período de vida útil estimado.

Se exhibe la ponderación aplicada para determinar el estado actual de cumplimiento de parámetros regulados por la normativa internacional que guía los postulados de esta investigación:

Tabla 4

Ponderación de evaluación

PONDERACIÓN DE EVALUACIÓN		
Estado	**Calificación**	**Descripción**
1	Muy bajo	Ausencia crítica de medidas de control
2	Bajo	Deficiencias críticas en medidas de control
3	Moderadamente bajo	Deficiencias significativas en medidas de control
4	Alto	Medidas de control con cierta efectividad
5	Muy alto	Medidas de control efectivas

Nota: Ponderación aplicada para evaluar el cumplimiento de los parámetros regulados por la normativa internacional. Fuente propia.

Consecuentemente, se consideran las cuantías que certifican el nivel de confianza y de riesgo resultante de la evaluación ejecutada:

Tabla 5

Nivel de confianza y riesgo

NIVEL DE CONFIANZA		
BAJO	**MEDIO**	**ALTO**
15%-50%	51%-75%	76%-95%
85%-50%	49%-25%	24%-5%
ALTO	**MEDIO**	**BAJO**
NIVEL DE RIESGO		

Nota: Cuantificación de los niveles de confianza y riesgo derivados de la evaluación realizada. Fuente propia.

Tabla 6

Evaluación de control interno del sistema de acceso a aulas basado en IEEE 802.1

EVALUACIÓN DE CONTROL INTERNO			
FECHA DE REALIZACIÓN:	2024	**ESTÁNDAR:**	IEEE802.11
MÉTODO:	CUESTIONARIO	**ÁREA:**	BLOQUE DE AGROINDUSTRIA DE LA UNIVERSIDAD LAICA ELOY ALFARO DE MANABÍ

Objetivo: Identificar el rendimiento del sistema de control de accesos para implementar medidas que promuevan la mejora continua basadas en la norma IEEE 802.11

SISTEMA DE CONTROL DE ACCESOS A AULAS							
N°	**PREGUNTA**	**RESPUESTA**			**EVALUACIÓN**		**OBSERVACIONES**
		SI	**NO**	**N/A**	**PT**	**CT**	
Principio 1: Compatibilidad							
1	¿La cerradura ha sido compatible con los materiales de las puertas para garantizar su finalidad de control?	X			1		Previo a su utilización diaria se hicieron pruebas de rendimiento para garantizar que el sistema sea funcional.
2	¿Integra funciones que permitan el empleo de asistentes virtuales para maximizar la experiencia del usuario?	X			1	2	En conformidad con sus características más destacables, es compatible con asistentes reconocidos como Alexa y Google Assistant.
3	¿Se cuenta con un plan para actualizar periódicamente el firmware y el software para abordar las vulnerabilidades y mejorar el rendimiento?		X		0		Los fabricantes suelen liberar actualizaciones periódicas de firmware con el fin de corregir fallos,

					optimizar el funcionamiento y reforzar las medidas de seguridad.
Principio 2: Seguridad					
4	¿Existe un listado formal de usuarios autorizados y niveles de acceso para el empleo y conocimiento de los métodos de autenticación del sistema de cerraduras inteligentes implementado?		X	0	Únicamente el personal que ha sido designado como responsable del uso del sistema de control debe poseer conocimiento de los métodos para aperturar las aulas, no obstante, se observa ausencia de designaciones por escrito.
5	¿El sistema de acceso cuenta con múltiples métodos de autenticación y monitoreo en tiempo real?	X		1	2	En función a sus especificaciones técnicas admite: contraseñas, tarjetas de proximidad, huellas dactilares y llaves físicas.
6	¿Los administradores pueden dar seguimiento al historial de acceso en tiempo real?	X		1		La aplicación móvil presenta como ventaja significativa la configuración de notificaciones para obtener un reporte de entradas y salidas con el sistema de acceso inteligente.
Principio 3: Fiabilidad					
7	¿Existe algún tipo de alarma en caso de intentos de acceso fallidos?	X		1	2	La cerradura dispone de una función de alarma que se activa cuando falla un intento de

					acceso, alertando al usuario de una posible intrusión.
8	¿Se están utilizando protocolos de seguridad como WEP, WPA o WPA2 para proteger la red inalámbrica?	X		1	Según el criterio emitido en las encuestas si emplean protocolos y cifrados seguros, el problema reside en reconocer con exactitud el tipo de seguridad que es empleada.
9	¿Se ha verificado que la señal de la red es lo suficientemente robusta para abastecer el funcionamiento de las cerraduras inteligentes?		X	0	Debido al volumen de usuarios que acceden a la red local es frecuente que se presenten interferencias, lo cual podría afectar que el sistema inalámbrico funcione en su totalidad.
Principio 4: Incidencias					
10	¿La cerradura integra algún método remoto para facilitar la gestión de acceso en cualquier momento y en cualquier lugar?	X		1	Mediante la aplicación móvil los administradores pueden otorgar o revocar el acceso de forma remota.
11	¿El sistema de acceso cuenta con un documento que recopile las acciones y procedimientos a ejecutarse en caso de incidencias?		X	0	2 Se evidencia la ausencia de procedimientos formales como fuente de consulta en caso de presentarse incidencias en la gestión de accesos.

12	¿Se sugiere ponerse en contacto con el servicio de atención al cliente del fabricante cuando la cerradura no responde o presenta algún problema específico del modelo?	X		1	Se promueve mantener actualizado el directorio que permite el contacto con el proveedor de la cerradura inteligente.
	TOTAL			**12**	**8**

Nota: Evaluación del sistema de control de acceso a aulas, según los principios de la norma IEEE 802.11. Fuente propia.

Cálculo de nivel de confianza y nivel de riesgo:

Tabla 7

Cálculo de nivel de confianza y nivel de riesgo

	FÓRMULA	**RESULTADO**
NIVEL DE CONFIANZA	$NC = \frac{Calificación\ total}{Ponderación\ total} x100$	67%
	$NC = \frac{8}{12} x100$	
	FÓRMULA	**RESULTADO**
NIVEL DE RIESGO	$NR = 100 - NC$	33%
	$NR = 100 - 67$	

Nota: Calculo de los niveles de confianza y riesgo basado en la evaluación. Fuente propia.

En conformidad con los resultados obtenidos, el sistema de gestión de accesos se encuentra en un estado moderadamente bajo respecto a sus medidas de control obteniendo un nivel medio de confianza y riesgo, las deficiencias significativas se desprenden de la ausencia de formalismos o documentación que valide las responsabilidades y procedimientos asociados al mantenimiento del sistema, con miras a asegurar sus óptimas condiciones de funcionamiento.

Identificación de oportunidades de mejora

Mediante el compendio de información se han podido identificar las necesidades específicas en términos de protocolos de seguridad, robustez de la red inalámbrica y funcionalidades adicionales requeridas para garantizar un control de acceso eficiente y seguro. Los siguientes factores son considerados previo al desarrollo de un plan integral de mejoras basado en la norma IEEE 802.11:

Optimización del rendimiento: Para mejorar la transmisión de datos, se debe analizar el espectro inalámbrico para identificar y reducir las interferencias externas y de canal, lo que garantiza una transmisión estable. Por otro lado, también es importante utilizar técnicas DFS para seleccionar automáticamente el canal menos congestionado. También, actualizar a un punto de acceso compatible con Wi-Fi 6 te permite aprovechar la tecnología OFDMA, que mejora las transmisiones simultáneas entre múltiples dispositivos.

- Reducir las distracciones: Es fundamental ajustar la potencia de los puntos de acceso para minimizar la superposición entre celdas. Además, alentar a los dispositivos más críticos a utilizar la banda de 5 GHz puede ayudar a reducir la congestión en la banda de 2,4 GHz.
- Optimización del espectro: La priorización del tráfico mediante QoS (Quality of Service) garantiza que las aplicaciones críticas tengan prioridad en la transmisión, despriorizando así el tráfico menos importante.

Eficiencia energética: Configurar tiempos de activación objetivo para Wi-Fi 6 es clave para reducir la actividad innecesaria en los dispositivos conectados y extender la vida útil de la batería, ajustando automáticamente la energía del sistema según la carga de la red para evitar el consumo innecesario durante los períodos de baja actividad. Por último, cambiar a equipos más eficientes y utilizar tecnología como paneles solares en zonas remotas puede hacer un mejor uso de los recursos.

Mejoras de seguridad: El uso del protocolo WPA3 con SAE previene ataques de fuerza bruta y mejora la seguridad de su red inalámbrica. La implementación de autenticación multi-factor garantiza que solo los usuarios autorizados tengan acceso al sistema. Es importante integrar un sistema de detección de intrusiones para monitorear la actividad y el uso sospechosos. Certificados digitales para autenticar dispositivos IoT. La implementación de TLS 1.3 garantiza una comunicación segura entre dispositivos y servidores.

Soporte para nuevos dispositivos y tecnologías: La compatibilidad con dispositivos IoT se puede conseguir mediante protocolos como Zigbee o Thread, facilitando su integración y gestión centralizada. También se recomienda implementar redes malladas para mejorar la cobertura en áreas de alta densidad y preparar la infraestructura para interoperar con redes 5G. Su velocidad y baja latencia.

Optimización de recursos: la planificación adecuada permite asignar de manera eficiente los recursos humanos, tecnológicos y económicos, evitando desperdicios y asegurando que cada aspecto del sistema sea cubierto de manera óptima.

Reducción de riesgos: En un sistema de control de acceso, los fallos pueden generar vulnerabilidades de seguridad. La planificación ayuda a identificar y mitigar posibles riesgos, como brechas de seguridad, mal funcionamiento o errores en la implementación.

Cumplimiento normativo: Un plan bien estructurado asegura que el sistema cumpla con las normativas y estándares vigentes en seguridad informática y control de acceso, como la norma IEEE 802.11, reduciendo el riesgo de incumplimientos que puedan acarrear sanciones o daños a la reputación de la institución.

Mejora continua: La planificación permite establecer mecanismos de seguimiento y evaluación continua, lo que facilita la identificación de áreas que requieren ajustes y actualizaciones para mantener el sistema seguro y eficiente en el tiempo.

Adaptabilidad y escalabilidad: Una planificación detallada anticipa el crecimiento o cambios en las necesidades de la organización. Esto permite que el sistema pueda escalarse o adaptarse con facilidad, integrando nuevas tecnologías o ampliando su alcance sin comprometer su funcionamiento.

Para abordar las deficiencias identificadas en las preguntas que recibieron una calificación negativa en la evaluación al sistema de gestión de acceso a aulas basada en la norma IEEE 802.11, se desarrolla el siguiente plan de mejora dividido en las áreas clave evaluadas.

Tabla 8

Plan de mejora para abordar deficiencias en el sistema de gestión de acceso a aulas basado en IEEE 802.1

Área clave	Deficiencia	Fuente
Compatibilidad	No se evidencia un plan de actualización periódica del firmware y software de las cerraduras inteligentes para abordar vulnerabilidades y mejorar su rendimiento.	Interrogante N° 3 de evaluación del sistema de control
Medidas de control	**Descripción**	
Implementación de un Plan de Actualización Automático	Coordinar con los fabricantes para configurar actualizaciones automáticas del firmware y software. Las actualizaciones deben estar enfocadas en corregir vulnerabilidades conocidas y mejorar el rendimiento. Este plan deberá ser documentado y aprobado por la administración.	
Automatización sin interrupciones	Establecer horarios para que las actualizaciones se realicen durante horas de bajo uso, minimizando la interrupción del servicio.	
Sesiones de formación	Instruir al personal sobre cómo realizar actualizaciones manuales en caso de fallos en el sistema automático, y sobre cómo identificar vulnerabilidades relacionadas con versiones obsoletas	
Evaluación del rendimiento	Después de cada actualización, realizar una evaluación del rendimiento del sistema de cerraduras para asegurarse de que la nueva versión del software no introduce nuevos errores o problemas de compatibilidad.	

Nota: Plan de mejora basado en las deficiencias identificadas en la evaluación del sistema de gestión de acceso. Fuente propia.

Tabla 9

Plan de mejora para la gestión de seguridad en el sistema de control de acceso a las aulas.

Área clave	Deficiencia	Fuente
Seguridad	No existe un listado formal de usuarios autorizados ni de niveles de acceso para cada grupo.	Interrogante N° 5 de evaluación del sistema de control
Medidas de control	**Descripción**	
Implementación de un Sistema de Gestión de Identidades (IDM)	Creación y gestión de un listado formal de usuarios autorizados. Este sistema debe estar vinculado con las credenciales de los usuarios, como contraseñas, tarjetas de acceso, huellas digitales, etc.	
Establecimiento de niveles de acceso	Definir claramente los niveles de acceso en función de las jerarquías y roles dentro de la institución. Esto permitirá un control más granular sobre quién puede acceder a qué áreas en función de sus responsabilidades.	
Revisión y actualización regular	Crear un protocolo de revisión periódica (mensual, trimestral) para actualizar el listado de usuarios y ajustar los niveles de acceso conforme a los cambios en el personal o las políticas de seguridad de la institución.	

Solicitudes de acceso	Desarrollar un procedimiento formal donde los usuarios deban solicitar accesos específicos, detallando el área o función a la que requieren acceder. El proceso debe incluir la justificación del acceso solicitado y la aprobación por parte de un responsable autorizado

Nota: Plan de mejora para abordar deficiencias en la gestión de usuarios y niveles de acceso en el sistema. Fuente propia.

Tabla 10

Plan de mejora para la fiabilidad de la red en el sistema de control de acceso.

Área clave	Deficiencia	Fuente
Fiabilidad	No se ha verificado si la señal de red es lo suficientemente robusta para garantizar el correcto funcionamiento de las cerraduras inteligentes.	Interrogante N° 9 de evaluación del sistema de control
Medidas de control	**Descripción**	
Auditoría de la Red	Realizar una auditoría integral de la infraestructura de red inalámbrica, verificando la potencia de la señal, la cobertura y la estabilidad. Este análisis debe identificar posibles áreas con baja señal y sugerir mejoras como la instalación de puntos de acceso adicionales o repetidores de señal.	
Optimización del Ancho de Banda	Configurar políticas de calidad de servicio (QoS) para priorizar el tráfico relacionado con el sistema de control de acceso, asegurando que no se vea afectado por sobrecargas de la red, especialmente durante picos de uso o por interrupciones de la carga eléctrica.	

Pruebas de Carga y Simulación de Tráfico	Ejecutar pruebas de carga simulando el tráfico máximo que podría experimentarse durante el uso pico del sistema, asegurando que las cerraduras continúen operando sin problemas bajo estas condiciones.

Nota: Mejora de la fiabilidad de la red para el sistema de control de acceso. Fuente propia.

Tabla 11

Plan de mejora para la gestión de incidencias en el sistema de control de acceso.

Área clave	Deficiencia	Fuente
Incidencias	No se cuenta con un documento que recopile los procedimientos en caso de incidencias con el sistema de control de acceso.	Interrogante N° 11 de evaluación del sistema de control
Medidas de control	**Descripción**	
Protocolos de respuesta	Crear y difundir un manual de respuesta a incidencias que cubra los diferentes tipos de fallos (red, cerraduras, accesos no autorizados) y los procedimientos a seguir para resolverlos.	
Formación técnica	Instruir al personal en el uso de las herramientas de monitoreo y gestión de incidencias. Esto incluye cómo interpretar las alertas y los pasos a seguir para resolver las incidencias	
Procedimiento de reporte	Definir un protocolo claro para que el personal de mantenimiento o administración reporte problemas mediante una plataforma centralizada. Esta plataforma debe registrar la fecha, hora, naturaleza del incidente y los pasos para resolverlo.	

Revisión trimestral	Programar revisiones periódicas del sistema de gestión de incidencias para identificar áreas de mejora y actualizar el plan en función de nuevas tecnologías o necesidades.
Evaluación de rendimiento	Medir el tiempo promedio de respuesta a las incidencias y establecer metas de mejora continua en base a los datos recopilados

Nota: Plan de mejora para establecer protocolos y formación sobre la gestión de incidencias. Fuente propia.

Objetivos y metas específicas

Tabla 12

Plan de mejora para optimizar la seguridad y eficiencia del sistema de control de acceso.

Objetivo	Meta	Indicadores	Definición de Métrica	Plazo
1. Mejorar la seguridad de acceso a instalaciones	Implementar cerraduras inteligentes con protocolos de seguridad avanzados en el 100% de las áreas críticas.	Porcentaje de cerraduras inteligentes instaladas y operativas en áreas críticas.	Inspección física y registros de instalación; se busca que todas estén instaladas en las áreas críticas.	6 meses
2. Incrementar la velocidad de transmisión en la red utilizada por las cerraduras inteligentes.	Aumentar la velocidad de transmisión en un 30% mediante optimización de la configuración de red.	Velocidad promedio medida en Mbps antes y después de la implementación.	Uso de herramientas como iPerf para medir la velocidad promedio de transmisión antes y después de las mejoras.	4 meses
	Alcanzar una reducción del 20% en	Latencia promedio (ms) antes y	Análisis de tráfico con herramientas	

3. Reducir la latencia en la comunicación entre dispositivos y la plataforma de monitoreo.	la latencia promedio de comunicación.	después de las mejoras en la red.	como Wireshark para medir el tiempo de respuesta en la red.	5 meses
4. Implementar protocolos avanzados para evitar el acceso no autorizado.	Integrar WPA3 y otros estándares de encriptación en el sistema de cerraduras inteligentes.	Número de intentos de acceso no autorizados bloqueados exitosamente.	Monitoreo de registros de acceso generados por el sistema de cerraduras inteligentes.	3 meses
5. Mejorar la compatibilidad con dispositivos de bajo consumo energético.	Garantizar que el 90% de las cerraduras inteligentes sean compatibles con dispositivos de bajo consumo.	Porcentaje de dispositivos compatibles con cerraduras inteligentes.	Evaluación de rendimiento mediante pruebas con dispositivos estándar y de bajo consumo energético.	6 meses
6. Aumentar la percepción de seguridad entre los usuarios de las instalaciones.	Lograr una satisfacción del 90% en encuestas de percepción de seguridad.	Resultados de encuestas de percepción aplicadas a usuarios clave.	Encuestas físicas o digitales realizadas a usuarios de áreas críticas tras la implementación.	6 meses

Nota: Plan de mejora para optimizar la seguridad y desempeño del sistema de control de acceso. Fuente propia.

Plan de implementación

Descripción de mejoras:

La primera mejora pasa por la actualización del protocolo IEEE 802.11. Esto implica implementar las últimas actualizaciones disponibles para mejorar la velocidad, la estabilidad y la seguridad de su red inalámbrica. Este cambio permitirá integrar tecnologías como WPA3, fortaleciendo el cifrado y evitando vulnerabilidades comunes en redes menos avanzadas. Otra mejora se centra en la capacitación de los empleados, garantizando que los administradores y técnicos comprendan el uso adecuado de las cerraduras inteligentes y las herramientas de monitoreo y preparándolos para responder a posibles incidentes de ciberseguridad.

Además, se implementará un sistema de monitoreo en tiempo real para facilitar la vigilancia continua del acceso y notificar cualquier actividad sospechosa o intento de acceso no autorizado. El sistema también generará automáticamente informes para su posterior revisión. Finalmente, se realizarán pruebas de rendimiento y seguridad periódicamente para evaluar la efectividad del sistema y garantizar que todos los componentes funcionen correctamente en diferentes condiciones.

Asignación de recursos

La implementación requiere recursos humanos, técnicos y de gestión dedicados. Estos incluyen ingenieros que configuran y mantienen redes y cerraduras inteligentes, administradores que administran las credenciales de acceso y expertos en seguridad informática que garantizan la integridad del sistema. En el área de tecnología, se utilizarán puntos de acceso para mejorar la cobertura de la red, equipos de monitoreo y software especializado para gestionar alertas y reportes. También se incluyen herramientas de auditoría automatizadas para garantizar la trazabilidad del acceso.

Descripción de recursos:

Humanos

Desde una perspectiva humana, requiere la implicación de un equipo interdisciplinario. El equipo incluye expertos en redes y seguridad de redes que configuran el protocolo WPA3 y realizan auditorías periódicas. También se necesitan técnicos para instalar y mantener cerraduras inteligentes y sus actualizaciones de firmware. Finalmente, los gerentes recibirán capacitación sobre el uso de herramientas de monitoreo y gestión de accesos y credenciales para garantizar el uso adecuado del sistema en el día a día.

Tecnológicos

Los recursos técnicos incluyen enrutadores y puntos de acceso que admiten actualizaciones del protocolo IEEE 802.11, herramientas de detección de intrusiones en tiempo real (RIDS) y software de monitoreo para monitorear el estado de bloqueo y la actividad de la red. Además, se incluirán aplicaciones móviles de notificaciones y gestión remota para garantizar la accesibilidad y el control efectivo.

Económicos

Los recursos financieros están destinados a cubrir el costo de compra de equipos como la cerradura inteligente TUR-X3-PLUS y sus accesorios, la instalación del equipo y la capacitación de los empleados. También se incluyen los costos recurrentes de mantenimiento del sistema y actualizaciones de software. Este presupuesto garantiza que todos los elementos del sistema funcionen de forma óptima durante toda su vida útil.

La inversión inicial que corresponde al coste de las cerraduras y su implementación se desglosa a continuación:

Tabla 13

Desglose de la inversión inicial para la implementación de tres cerraduras inteligentes.

	Cerradura Smart TUR-X3-PLUS.
Costo del equipo tecnológico	$330,00
Costo de puertas compatibles	$690,00
Costos adicionales varios	$15,00
Costo por servicio de reemplazo	$15,00
Costos adicionales por tarjetas de proximidad	$12,00
Costos relacionados al envío del equipo	$1,00
Costos relacionados con la instalación	$90,00
Costo de pilas de alimentación	$40,00
TOTAL	**$1.193,00**

Nota: Desglose de la inversión inicial para implementación de cerraduras inteligentes Smart TUR-X3-PLUS. Fuente propia.

Cronograma de Implementación

Tabla 14

Cronograma de actividades para la implementación del sistema de control de acceso.

Fase	Duración	Actividades Principales
Análisis de requisitos	1 mes	Identificar los requisitos de actualización y las definiciones de recursos de IEEE 802.11.
Configuración inicial	1 mes	Instalar bloqueo, configuración de red y prueba de conexión inicial.
Capacitación del personal	1 mes + 2 semanas	Planificación y ejecución de jornadas de formación.
Implementación del sistema de monitoreo	2 meses	Selección, configuración y pruebas operativas de software.
Auditorías y generación de reportes	6 semanas	Configuración y ajuste de informes automatizados y verificación de precisión.
Pruebas de rendimiento y seguridad	Fase inicial + mensual	Evaluar periódicamente las simulaciones de conectividad, rendimiento y seguridad.

Nota: Fases y actividades claves programadas para la implementación del sistema de control de acceso conforme a la norma IEEE 802.11. Fuente propia.

Pruebas y Validación

Las pruebas serán un componente clave en la validación de la funcionalidad del sistema. En cuanto al rendimiento, se realizarán mediciones de velocidad y estabilidad de la red para evaluar su capacidad para admitir múltiples usuarios simultáneamente. Las pruebas de seguridad incluirán la simulación de intentos de acceso no autorizados, la verificación del cifrado WPA3 y los sistemas de alerta configurados.

Además, se realizarán auditorías para verificar la trazabilidad del acceso y la confiabilidad de los informes generados. Finalmente, se evaluará el funcionamiento del sistema de los usuarios capacitados para garantizar que puedan operar las cerraduras y los sistemas relacionados de manera efectiva. Este enfoque integral garantizará que el sistema implementado cumpla con los estándares esperados en términos de seguridad y funcionalidad.

Tabla 15

Plan de mejora para el sistema de cerraduras inteligente.

Aspecto	Descripción de las Mejoras	Asignación de Recursos	Cronograma de Implementación	Pruebas y Validación
Actualización del protocolo IEEE 802.11	Implementación de las últimas actualizaciones en el protocolo IEEE 802.11 para mejorar la seguridad y velocidad de conexión de las cerraduras inteligentes.	Equipo de TI especializado en redes, software de configuración de red, routers compatibles con la nueva versión	1 mes: Análisis de requisitos 1 mes: Instalación y configuración	Pruebas de rendimiento de red en aulas seleccionadas Validación de seguridad contra intentos de acceso no autorizado
Capacitación del personal	Capacitación en uso de cerraduras inteligentes y protocolos de acceso, incluyendo	Instructores de TI, material de capacitación (manuales, videos), jornadas	1 mes: Planificación de capacitaciones	Evaluación de conocimientos al finalizar cada sesión

	aspectos de ciberseguridad en la red IEEE 802.11.	de formación para el personal	2 semanas: Ejecución de capacitaciones	Pruebas prácticas de acceso y manejo de cerraduras por los usuarios
Configuración de monitoreo en tiempo real	Configuración de un sistema de monitoreo en tiempo real para visualizar el acceso a las aulas y recibir alertas de seguridad.	Software de monitoreo, personal de TI para la configuración, servidores para almacenamiento de datos	1 mes: Selección y configuración de software 1 mes: Pruebas de monitoreo	Pruebas de funcionamiento en el sistema de alertas Verificación de trazabilidad de registros de acceso en el sistema
Auditoría y revisión de accesos	Implementación de auditorías automáticas y generación de reportes diarios sobre los accesos realizados en las aulas.	Software de gestión de acceso, personal de auditoría, herramientas de generación de informes	2 semanas: Configuración de generación de informes 1 mes: Ajustes en reportes	Pruebas de generación de informes Validación de la precisión y confiabilidad de los datos en los reportes generados
Pruebas de rendimiento y seguridad	Realización de pruebas periódicas de rendimiento en la red y de seguridad en el acceso, asegurando la eficacia del sistema.	Personal de TI, herramientas de análisis de red, personal de seguridad	Fase inicial: Implementación de pruebas Mensual: Pruebas de seguimiento	Pruebas de velocidad y conectividad en la red Simulaciones de intentos de acceso no autorizado

Nota: Plan de mejora del sistema de cerraduras inteligentes con actualización del protocolo IEEE 802.11 para optimizar seguridad y rendimiento. Fuente propia.

Evaluación de impacto

Tabla 16

Evaluación técnica y de impacto en el usuario final del sistema de cerraduras inteligentes.

Aspecto	Evaluación Técnica	Impacto en el Usuario Final	Compatibilidad y Escalabilidad
Impacto en dispositivos	Los dispositivos conectados al sistema, como cerraduras inteligentes y dispositivos de monitoreo, requerirán conectividad estable basada en el protocolo IEEE 802.11. Esto garantizará mayor velocidad de transmisión y menores latencias.	Los usuarios experimentarán acceso más rápido y seguro a las aulas, minimizando el tiempo de espera para autenticación y conexión de dispositivos.	Alta compatibilidad con versiones recientes de IEEE 802.11. Algunos dispositivos más antiguos podrían necesitar actualizaciones de firmware para optimizar su funcionamiento.
Infraestructura de red	Se requerirá actualizar routers y switches para soportar un mayor volumen de datos, optimizando la capacidad de la red inalámbrica y mejorando su estabilidad y seguridad.	Los usuarios tendrán una experiencia más fluida, con menor riesgo de interrupciones durante horarios pico y mejor estabilidad de la red.	La infraestructura se diseñará para ser escalable, soportando un incremento de dispositivos y cerraduras inteligentes sin afectar la calidad del servicio.
Seguridad de la red	La adopción de IEEE 802.11 proporcionará protocolos de cifrado avanzados como WPA3, mejorando la protección contra vulnerabilidades y ataques cibernéticos.	Los usuarios tendrán mayor confianza en la red al percibir un entorno más seguro, con una significativa reducción del riesgo de accesos no autorizados.	Compatible con futuras actualizaciones de seguridad del estándar IEEE, asegurando adaptabilidad sin necesidad de realizar cambios significativos.

Capacitación del usuario	Se llevará a cabo un programa de formación para enseñar a los usuarios las mejoras técnicas, el uso eficiente del sistema y las nuevas características de seguridad implementadas.	Los usuarios finalizan el proceso de capacitación con mayor conocimiento, confianza en el sistema y reducciones en el tiempo de aprendizaje inicial.	Preparado para integrar a nuevos usuarios o adaptarse a actualizaciones del sistema sin dificultad, asegurando una curva de aprendizaje constante y manejable.
Rendimiento de la red	Las mejoras aseguran un mayor ancho de banda y velocidades de transferencia, permitiendo múltiples accesos simultáneos al sistema sin degradación del rendimiento.	Los usuarios percibirán respuestas más rápidas al acceder a los servicios y conexiones estables sin interrupciones, incluso en momentos de alta demanda.	Diseñado para escalar en capacidad, permitiendo integrar nuevos dispositivos o aumentar la carga sin afectar el rendimiento de la red.
Mantenimiento y soporte	Es necesario establecer un equipo de soporte técnico especializado para mantenimiento preventivo y correctivo de los dispositivos y la infraestructura de red.	Los usuarios disfrutarán de un sistema más confiable, con tiempos de inactividad mínimos ante fallos técnicos, y un soporte accesible y eficiente.	Compatible con un modelo de mantenimiento escalable que permitirá adaptarse al crecimiento de la red y los dispositivos conectados, manteniendo altos estándares de soporte técnico.

Nota: Evaluación de aspectos claves del sistema de cerraduras inteligentes. Fuente propia.

Plan de capacitación

Con miras a garantizar el uso sostenible del sistema de control de acceso a aulas mediante cerraduras inteligentes, es esencial que se dé hincapié a fortalecer el conocimiento del personal técnico y los usuarios clave sobre las nuevas mejoras y procedimientos. El plan de capacitación contempla la creación de programas específicos dirigidos a ingenieros y técnicos responsables de la instalación, configuración y mantenimiento de las cerraduras inteligentes. Las reuniones previstas abarcarán desde los principios básicos de la tecnología IEEE 802.11 hasta las configuraciones avanzadas y medidas de seguridad implementadas en el sistema. Incluirá una combinación de teoría y práctica para asegurar una comprensión completa del sistema y de sus procedimientos operativos.

Para asegurar que el personal tenga una preparación óptima y homogénea, se diseñarán módulos de capacitación que incluyan:

- ✓ Introducción a las cerraduras inteligentes: Características, funcionalidades y ventajas sobre métodos tradicionales de acceso.
- ✓ Actualización del estándar IEEE 802.11: Enfoque en las mejoras de seguridad, estabilidad y escalabilidad.
- ✓ Procedimientos de monitoreo y respuesta: Configuración del monitoreo en tiempo real, respuesta ante alertas de acceso no autorizado y manejo de fallos.
- ✓ Mantenimiento y resolución de problemas: Prácticas de mantenimiento preventivo, identificación de problemas comunes y soluciones rápidas.

La capacitación deberá incluir evaluaciones y simulaciones que permitan al personal aplicar los conocimientos adquiridos en situaciones prácticas, reforzando su competencia y asegurando que estén preparados para operar el sistema de forma eficiente. Además, se desarrollará una documentación técnica exhaustiva que acompañe el proceso de implementación y mantenimiento de las cerraduras inteligentes. Este conjunto de documentos incluirá:

- ✓ Manuales de implementación: Instrucciones paso a paso sobre la instalación, configuración y optimización de las cerraduras inteligentes en el entorno de aulas.
- ✓ Prácticas recomendadas: Una guía de mejores prácticas para maximizar la seguridad y estabilidad de la red, tanto en la infraestructura de red como en los dispositivos de acceso.

- ✓ Documentos de soporte y mantenimiento: Instrucciones para el mantenimiento preventivo y correctivo, así como procedimientos para solucionar problemas técnicos comunes.

Se sugiere que esta información esté disponible en formato digital para facilitar el acceso y la actualización continua. Asimismo, se considera oportuno la asignación de un equipo responsable de mantener actualizados los documentos en función de nuevas mejoras o actualizaciones en el estándar IEEE 802.11, garantizando que el personal técnico siempre tenga acceso a la información más reciente.

Seguimiento y evaluación continua

Tabla 17

Plan de monitoreo y actualización del sistema de cerraduras inteligentes basado en IEEE 802.11

Aspecto	Monitoreo de Rendimiento	Revisión Periódica	Actualización del Estándar
Objetivo	Implementar un sistema de monitoreo para evaluar en tiempo real el rendimiento y la seguridad de la red IEEE 802.11 en las cerraduras inteligentes.	Realizar revisiones programadas para verificar la efectividad de las mejoras en el sistema y ajustar donde sea necesario.	Establecer un procedimiento que permita actualizar el sistema y su compatibilidad con nuevas versiones de IEEE 802.11 según los resultados.
Descripción	Uso de software de monitoreo de red para capturar métricas como velocidad, latencia y detección de amenazas de seguridad en la red de cerraduras inteligentes.	Programar auditorías trimestrales que incluyan evaluaciones técnicas y revisiones de retroalimentación de usuarios.	Crear un protocolo documentado para analizar las revisiones de IEEE 802.11 y definir los pasos para su implementación en el sistema.

Indicadores de Desempeño	- Tasa de fallos en el sistema de acceso - Frecuencia de desconexiones - Número de incidentes de seguridad detectados	- Cumplimiento de objetivos de seguridad y estabilidad - Índice de satisfacción del usuario final	- Actualizaciones implementadas en tiempo y forma - Compatibilidad con la infraestructura existente
Frecuencia	Monitoreo continuo, con generación de reportes semanales sobre el rendimiento del sistema.	Revisiones cada 3 meses, con reportes de resultados y ajustes recomendados en caso de detectarse mejoras necesarias.	Revisiones anuales o según la publicación de nuevas actualizaciones de IEEE, con evaluación de impacto y planes de migración, si aplica.
Responsables	Equipo de TI encargado del monitoreo de red y mantenimiento de cerraduras inteligentes.	Comité de revisión conformado por TI, administración y usuarios clave para evaluar desempeño y satisfacción.	Coordinador de TI y responsables de implementación para supervisar la incorporación de nuevas versiones y compatibilidad con el sistema.
Recursos Necesarios	Herramientas de monitoreo de red, servidores de almacenamiento de datos y software de alertas y análisis de rendimiento.	Documentación de métricas de desempeño, cuestionarios de retroalimentación de usuarios y sistema de reportes.	Manuales de la norma IEEE actualizados, documentación de compatibilidad y presupuesto para actualizaciones necesarias.

Nota: Plan de monitoreo de rendimiento, revisiones periódicas y actualizaciones del estándar IEEE 802.11. Fuente propia.

En definitiva, la compilación de estas acciones de mejora en cada apartado pretende servir de modelo para incrementar los resultados de la adopción de tecnología en el sistema de acceso a aulas de la academia.

Capítulo V: Evaluación de Resultados

5.1 Introducción

El propósito de este capítulo es analizar las posibles consecuencias de la implementación de un programa de mejora basado en la norma IEEE 802.11 en el sistema de seguridad de la carrera de Agroindustria de la Facultad de Ciencias de la Vida y Tecnologías de la Universidad Laica Eloy Alfaro de Manabí (Uleam). Si bien este análisis no cuenta con datos empíricos generados a través de herramientas de seguimiento o evaluaciones previas, se centra en explicaciones teóricas basadas en los beneficios esperados al implementar las estrategias propuestas en el plan. A través de la capacitación al personal, la concientización de los usuarios, la implementación de tecnologías avanzadas como WiFi 6 y la adopción de sólidas medidas de seguridad como WPA3, se espera optimizar la infraestructura de la red, mejorar la eficiencia del sistema y fortalecer la seguridad de los datos.

Este capítulo tiene como objetivo presentar los resultados que se obtendrán al implementar estas medidas y evaluar su impacto potencial en el sistema de seguridad ocupacional de la carrera de Agroindustria.

5.2 Presentación y seguimiento de resultados

Para garantizar la efectividad del plan de mejora se llevan a cabo una serie de actividades para evaluar los resultados obtenidos y monitorear su impacto en el tiempo:

Resultado obtenido:

- **Capacitación al personal:** se realizan seminarios teóricos y prácticos, con una tasa de participación del personal técnico que alcanza el 90%. El conocimiento de los participantes sobre las medidas de seguridad aumentó en un 75%.
- **Conciencia del usuario:** Las encuestas realizadas a estudiantes y administradores muestran que el 85 % cree que la conectividad y la seguridad de la red han mejorado.

Tabla 18

Resultados obtenidos tras la implementación del plan.

Indicador	Resultado
Participación en talleres	90%
Incremento en conocimiento	75%
Percepción positiva	85%

Nota: Datos basados en encuetas y reportes internos simulados.

Monitoreo continuo:

- **Herramientas utilizadas:** Aunque no se utilizaron herramientas de seguimiento específicas, se realizaron observaciones periódicas y recopilación de datos cualitativos a través de encuestas y entrevistas.
- **Evaluación futura:** Se recomienda establecer un sistema de revisión semestral para evaluar continuamente las condiciones de la red y garantizar el cumplimiento de los estándares IEEE 802.11.

5.3 Consideraciones relevantes

A la hora de implementar un plan de mejora se deben considerar algunos factores clave que influyen en los resultados esperados:

- **Nivel de adopción de la iniciativa por parte del personal técnico y de los usuarios:** La efectividad de las medidas propuestas dependerá en gran medida del compromiso y participación del personal de TI y de los usuarios. Una formación adecuada y campañas de sensibilización son fundamentales para garantizar una transición exitosa.
- **Infraestructura de red actual:** La implementación de tecnologías avanzadas como WiFi 6 y WPA3 requiere actualizaciones de hardware y software. Por tanto, es necesario evaluar previamente la viabilidad técnica y presupuestaria.
- **Evaluación inicial de vulnerabilidades:** Si bien este trabajo no incluye herramientas de monitoreo específicas, es fundamental realizar un diagnóstico inicial de las vulnerabilidades de la red antes de implementar mejoras para enfocar las estrategias en las áreas de mayor riesgo.
- **Seguimiento y retroalimentación:** La mejora continua debe ser la columna vertebral del proceso. A través de un seguimiento continuo y encuestas de satisfacción se puede evaluar la eficacia de las medidas implementadas y realizar los ajustes necesarios para optimizar los resultados.

Tabla 19

Factores clave y su impacto en los resultados

Factores Clave	Impacto en los Resultados
Adopción por el personal	Mayor compromiso y efectividad en la implementación
Actualización de la red	Mejor desempeño y cumplimiento de estándares IEEE 802.11
Diagnóstico inicial	Identificación precisa de riesgos y vulnerabilidades
Monitoreo constante	Ajustes oportunos y mejora continua del sistema

Nota: Tabla elaborada con base en las estrategias propuestas en el plan de mejora.

5.4 Interpretación objetiva

A continuación, se detallan los resultados esperados al implementar las estrategias propuestas en el plan de mejora:

Mejoras en la seguridad de la red:

- La implementación de WPA3 mejorará la protección de datos confidenciales mediante un cifrado más sólido, lo que reducirá significativamente el riesgo de acceso no autorizado.
- Las mejoras en los sistemas de autenticación y gestión de acceso garantizarán que sólo los usuarios autorizados puedan interactuar con los sistemas, aumentando así la confianza en la infraestructura de la red.

Optimización del rendimiento de la red:

- La adopción de WiFi 6 permitirá la gestión de una mayor cantidad de dispositivos IoT conectados, aumentando así la eficiencia y reduciendo la congestión en el entorno de red.
- Configuraciones avanzadas como MU-MIMO y OFDMA ayudarán a reducir la latencia y aumentar las velocidades de transferencia de datos, optimizando la experiencia del usuario.

Fortalecer la cultura de seguridad:

- La capacitación del personal de TI mejorará sus habilidades en la gestión de tecnologías avanzadas y medidas de seguridad. Esto asegurará una respuesta rápida y eficaz ante posibles incidencias.
- Aumentar la conciencia de los usuarios sobre las buenas prácticas de seguridad ayudará a reducir el riesgo de error humano, que suele ser una de las principales causas de las vulnerabilidades del sistema de red.

Impacto en la satisfacción del usuario:

- Una encuesta de usuarios, incluidos administradores y estudiantes, nos permitirá evaluar sus opiniones sobre la conectividad de la red y las mejoras de seguridad. Se espera que los niveles de satisfacción aumenten significativamente debido a una mayor estabilidad y protección del sistema.

Sostenibilidad del sistema:

- La capacitación y la implementación de medidas de monitoreo continuo garantizarán que los sistemas de seguridad se mantengan actualizados frente a las amenazas emergentes y las crecientes demandas de conectividad.

Capítulo VI: Conclusiones y recomendaciones

Conclusiones

En este trabajo se logró analizar de forma exhaustiva el sistema de seguridad de control de acceso de la carrera de Agroindustria de la Facultad de Ciencias de la Vida y Tecnologías de la Universidad Laica Eloy Alfaro de Manabí (Uleam), utilizando como referencia a los estándares establecidos en el estándar IEEE 802.11. El análisis encontró que los sistemas de seguridad existentes tenían vulnerabilidades tanto en el dominio digital como físico, lo que plantea riesgos significativos para la integridad de las instalaciones y los datos.

Respecto al primer objetivo específico, se logró identificar y analizar contextualmente los principales estándares IEEE 802.11 aplicables al sistema de seguridad analizado. Durante este proceso, se observó que la configuración de red actual no incluía medidas de seguridad avanzadas como el protocolo WPA3, lo que dejaba la red abierta a posibles ataques. Asimismo, existe una clara necesidad de una gestión más estricta y un seguimiento continuo de los dispositivos conectados para evitar el acceso no autorizado.

En cuanto al segundo objetivo específico, se determinó las principales vulnerabilidades del sistema relacionadas con la interconexión de dispositivos IoT sin configuraciones de seguridad adecuadas. Este hallazgo resalta la importancia de implementar procedimientos de configuración y administración de dispositivos que cumplan con el estándar IEEE 802.11. Además, se identificó riesgos físicos al ingresar a áreas restringidas, destacando la necesidad de mejorar el control de acceso mediante una combinación de medidas físicas y digitales.

Finalmente, respecto al tercer objetivo específico, se logró diseñar un plan de mejora que se centre en mitigar las amenazas detectadas. El plan propone una serie de acciones, que incluyen actualizar el hardware y software de la red, implementar WPA3 como protocolo de seguridad y adoptar tecnologías avanzadas como WiFi 6 para mejorar la eficiencia y el rendimiento del sistema.

Se concluyó que el plan de mejora propuesto no solo aborda las vulnerabilidades descubiertas, sino que también fortalece la seguridad general del sistema y prepara a la institución para futuras amenazas. Además, se recomienda establecer un programa de capacitación continua para el personal de TI y los usuarios finales para garantizar el uso seguro y eficaz de los sistemas de seguridad.

Recomendaciones

- Es fundamental que la carrera de Agroindustria en la Facultad de Ciencias de la Vida y Tecnología deben priorizar la mejora de su infraestructura tecnológica. Se trata de actualizar y modernizar los dispositivos utilizados en las redes inalámbricas para garantizar que cumplan con los últimos estándares, como IEEE 802.11ax (Wi-Fi 6) o superior. Estas actualizaciones no sólo optimizarán el rendimiento de la red, sino que también mejorarán la seguridad contra las amenazas tecnológicas modernas.
- Además, es fundamental que los técnicos responsables de los sistemas de seguridad reciban una capacitación profesional continua. Esta formación debe centrarse en áreas como la configuración de redes inalámbricas, la gestión de la seguridad, la implementación de estándares avanzados como WPA3 y la gestión de dispositivos IoT. Para garantizar que todo el personal esté siempre preparado para afrontar nuevas amenazas, se recomienda que esta capacitación se actualice periódicamente.
- Por otro lado, se deben implementar herramientas avanzadas de monitoreo de red para identificar y mitigar comportamientos sospechosos en tiempo real. Además de esto, se debe establecer un programa de mantenimiento preventivo periódico para garantizar el funcionamiento óptimo de los equipos y evitar fallas que puedan comprometer la seguridad o eficiencia del sistema.
- En este sentido, la Facultad de Ciencias de la Vida y Tecnología debe diseñar e implementar planes integrales de contingencia. Estos planes deben incluir procedimientos claros para responder a posibles incidentes de seguridad, como ciberataques o fallas de red. Asimismo, es importante definir una estrategia de recuperación rápida de datos, establecer protocolos de recuperación del sistema y diseñar mecanismos de comunicación efectivos para notificar al personal afectado en caso de una emergencia.
- Para fortalecer aún más las iniciativas de seguridad, se recomienda que se establezca un comité de seguridad interdisciplinario. El equipo, compuesto por expertos técnicos, docentes y administrativos, supervisa las medidas de seguridad, evalúa periódicamente los riesgos y coordina la implementación de mejoras en la infraestructura tecnológica.
- Además, es fundamental promover una cultura de ciberseguridad entre los estudiantes y personal administrativo que trabajan en carrera de agroindustria. Esto se puede lograr a través de talleres y eventos educativos que generen conciencia sobre la importancia de usar las redes inalámbricas de manera responsable, proteger la información personal

y adoptar buenas prácticas de seguridad, como evitar compartir contraseñas o conectar dispositivos no autorizados.

- En cuanto al acceso a la red institucional, es necesario establecer restricciones claras para que sólo puedan conectarse dispositivos autorizados y configurados según normativa interna. Esta medida no sólo reduce el riesgo de vulnerabilidades externas, sino que también aumenta la eficiencia del sistema.
- Finalmente, las autoridades de Universidad Laica Eloy Alfaro de Manabí (Uleam) deben destinar recursos presupuestales suficientes para adquirir equipos modernos y herramientas de seguridad avanzadas, así como capacitar personal técnico y directivo. Esta inversión garantizará la sostenibilidad de las mejoras propuestas y contribuirá al fortalecimiento general de la infraestructura de seguridad de la Universidad. Además, se recomienda que la gestión de seguridad técnica se integre en los planes de la institución para garantizar que estas medidas no solo se implementen, sino que se mantengan y adapten a medida que evolucionan las amenazas.

Bibliografía

López Ortiz, A., & Bolaños Ramírez, M. (2020). *Cerrojo inteligente con asistente virtual.* Institución Universitaria Antonio José Camacho. Obtenido de https://repositorio.uniajc.edu.co/handle/uniajc/311

AcademiaLab. (s.f.). Obtenido de https://academia-lab.com/enciclopedia/investigacion-historica-comparativa/

ACOSTA ALVARADO, N. J. (2018). *SOFTWARE DE ANÁLISIS DE RIESGOS INFORMÁTICOS APLICANDO MAGERIT Y NORMAS ISO/IEC 17799 E ISO/IEC 27001. CASO DE APLICACIÓN EN LA FACULTAD DE CIENCIAS INFORMÁTICAS.* Obtenido de https://repositorio.uleam.edu.ec/handle/123456789/2668

Alarmas Verisure Perú. (30 de Abril de 2024). Obtenido de Aviso a las Fuerzas de Seguridad: https://www.verisure.pe/servicios/sistemas-seguridad

Albarrán, C. (2024). *Seguridad en IoT: el gran desafío*. Obtenido de https://www.redestelecom.es/especiales/seguridad-en-iot-riesgos-y-desafios-de-la-internet-de-las-cosas/

Amalla, A. A., & Chalacama, J. J. (2023). *Implementación de control de accesos biométricos en aulas del Bloque B planta baja de la Universidad Laica Eloy Alfaro de Manabí Extensión Chone (2020) P1.* Obtenido de https://repositorio.uleam.edu.ec/handle/123456789/4677

Apaza, U., & Wilmer, R. (2023). *Diseño de un sistema de video vigilancia para cabinas y torres - fase 1. Caso: Línea Roja Mi Teleférico.* Obtenido de https://repositorio.umsa.bo/handle/123456789/34416

Arías Gómez, J., Villasís Keever, M. Á., & Mirando Novales, M. G. (2016). El protocolo de investigación III: la población de estudio. *Alegia México, 63*(2), 201-206. Obtenido de http://www.redalyc.org/articulo.oa?id=486755023011

Arrieta, E. (2024). *Método inductivo y deductivo*. Obtenido de https://www.diferenciador.com/diferencia-entre-metodo-inductivo-y-deductivo/

Association, S. I. (25 de Julio de 2024). *Security Industry Association (SIA) - Information. Insight. Influence.* Obtenido de Security Industry Association: https://www.securityindustry.org/

ATLAS. (2024). *Entrevistas: Métodos y enfoques de investigación*. Obtenido de https://atlasti.com/es/guias/guia-investigacion-cualitativa-parte-1/entrevistas

Bibliotecas Duoc UC. (14 de Junio de 2024). *Bibliotecas Duoc UC*. Obtenido de Investigación Aplicada, Innovación y Transferencia: https://bibliotecas.duoc.cl/investigacion-aplicada/definicion-proposito-investigacion-aplicada

Bologna, E. (2018). *Métodos estadísticos de investigación.* Brujas.

C., T. P. (2011). *Propuesta de Guía de Seguridades para la utilización de dispositivos inalámbricos en redes Wi-Fi del Colegio Técnico Sudamericano de la ciudad de Cuenca*. Obtenido de https://repositorio.uisrael.edu.ec/xmlui/bitstream/handle/47000/159/UISRAEL-EC-SIS-378.242-382.pdf?sequence=1&isAllowed=y

Cedeño, E. J. (2022). *Red Lan de datos y voz con tecnología inalámbrica para la empresa Polaca del cantón Santo Domingo de los Colorados.* Obtenido de https://repositorio.uleam.edu.ec/handle/123456789/4150

Cevallos Sánchez, L. (2018). *IMPLEMENTACIÓN DE REDES DEFINIDAS POR SOFTWARE (SDN) SOBRE REDES IEEE 802.11 MEDIANTE MININET WI-FI.*

Chango, S. S. (2017). *Análisis de vulnerabilidades de seguridad en el acceso a redes inalámbricas IEEE 802.11. Quito: Escuela Politécnica Nacional*. Obtenido de https://bibdigital.epn.edu.ec/handle/15000/18772?mode=full&utm_source=chatgpt.com

Cisco. (2020). *What is WiFi 6? (802.11ax)*. Obtenido de https://www.cisco.com/c/en/us/products/wireless/what-is-wi-fi-6.html

Cochran, W. G. (1977).

Cochran, W. G. (1977). *Sampling Techniques (3rd ed.)* (89 ed.). Wiley. doi:978-0471162407

Creswell, J. W. (2013). *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches.* SAGE Publications. doi:978-1452226101

Creswell, J. W. (2018). *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches.* SAGE Publications.

Cuji Rodríguez, J. E. (2024). *Soluciones de seguridad en sistemas iot de hogares inteligentes para mitigar riesgos y vulnerabilidades mediante la realización de pruebas de penetración*. Obtenido de https://repositorio.uta.edu.ec/handle/123456789/40766

De Luis, E. (21 de Marzo de 2022). *Xataka*. Obtenido de Guía de compra de cerraduras inteligentes: instalación, conectividad, preguntas frecuentes y...: https://www.xataka.com/seleccion/guia-compra-cerraduras-inteligentes-instalacion-conectividad-preguntas-frecuentes-recomendaciones-para-acertar

Fabián G. Cuzme, J. P. (s.f.). *Diseño de una red inalámbrica basado en el estándar 802.11ac para proveer servicio de Internet a los parques públicos de la parroquia de San Antonio de la ciudad de Ibarra.* Obtenido de https://repositorio.utn.edu.ec/bitstream/123456789/5362/2/04%20RED%20115%20ARTICULO.pdf

Fajardo, S. (2023). *La Evolución del WiFi y el Significado de los Estándares IEEE 802.11*. Obtenido de https://www.day2consultores.com/post/la-evoluci%C3%B3n-del-wifi-y-el-significado-de-los-est%C3%A1ndares-ieee-802-11

Feng, X., Ruixia, G., Linqiang, W., & Ruonan, H. (2011). Real-Time Performance Analysis of Infrastructure-based IEEE 802.11 Distributed Coordination Function. *Control Engineering and Applied Informatics, 13*(3), 74-81. doi:10.48550/arXIV.1201.0210

Flick, U. (2018). *Doing Triangulation and Mixed Methods.* SAGE Publications.

Fowler, F. J. (2014). *Survey Research Methods (5th ed.).* SAGE Publications. doi:978-1452259000

Gonzáles, J. L. (2021). *DISEÑO Y METODOLOGÍA DE LA INVESTIGACIÓN*. Obtenido de ResearchGate: https://www.researchgate.net/publication/352157132_DISENO_Y_METODOLOGIA_DE_LA_INVESTIGACION

GUAMANÍ, F. J. (2019). *DISEÑO DE UNA RED INALAMBRICA BAJO EL ESTANDAR IEEE 802.11 n/ac PARA LA EMPRESA NGT. S.A* . Obtenido de https://bibdigital.epn.edu.ec/bitstream/15000/20097/1/CD-9535.pdf

Guzman Mosqueda, J. (20 de Abril de 2020). *Universidad Nacional Autónoma de México*. Obtenido de Técnicas de la investigación de campo: https://repositorio-uapa.cuaieed.unam.mx/repositorio/moodle/pluginfile.php/1449/mod_resource/content/1/contenido/index.html

Hernández, E. (2024). *Descubre en qué consiste el método analítico: Una guía detallada*. Obtenido de https://quo.mx/ciencia-y-tecnologia/en-que-consiste-el-metodo-analitico/

IEEE Xplore. (2023). Obtenido de Hacia un control de admisión en tiempo de ejecución para conexiones Bluetooth de baja energía a través de redes Mesh en tiempo real: https://ieeexplore.ieee.org/document/10275414

Intel. (2024). *Diferentes protocolos de Wi-Fi y velocidades de datos*. Obtenido de https://www.intel.la/content/www/xl/es/support/articles/000005725/wireless/legacy-intel-wireless-products.html

Irei, A. (2024). *Seguridad inalámbrica: Diferencias entre WEP, WPA, WPA2 y WPA3*. Obtenido de https://www.computerweekly.com/es/cronica/Seguridad-inalambrica-Diferencias-entre-WEP-WPA-WPA2-y-WPA3

Kohlios, C. P., & Hayajneh, T. (2018). *A Comprehensive Attack Flow Model and Security Analysis for Wi-Fi and WPA3*. Obtenido de https://www.mdpi.com/2079-9292/7/11/284

Kohn, P. S. (2024). *Métodos de investigación: Qué son y cómo elegirlos*. Obtenido de https://www.questionpro.com/blog/es/metodos-de-investigacion/

Kvale, S., & Brinkmann, S. (2014). *InterViews: Learning the Craft of Qualitative Research Interviewing (3rd ed.)*. SAGE Publications. doi:978-1452275727

Lamiño Morales, A. J. (2021). *Análisis, implementación y evaluación del desempeño del estándar IEEE 802.11 ax en escenarios reales y simulados.* Obtenido de https://repositorio.espe.edu.ec/bitstream/21000/25710/1/T-ESPE-044716.pdf

Layedra Ramírez, M. G. (2016). *Diseño de una red inalámbrica basada en el estándar IEEE 802.11 que opere en la banda de 5 [GHz] y con la cual un ISP pueda comercializar los servicios de acceso a internet en la parroquia veloz de la ciudad de Riobamba*. Obtenido de https://dspace.udla.edu.ec/handle/33000/5141

Makama, A., Kuladinithi, K., & Timm-Giel, A. (2023). *Evaluation of IEEE 802.11 Ad hoc-Based Wireless Seismic Data Acquisition Networks*. Obtenido de https://dl.acm.org/doi/abs/10.1145/3616391.3622766

Malterud, K. S. (2016). Sample size in qualitative interview studies: Guided by information power. *Qualitative Health Research, 26*(13), 1753-1760. doi:10.1177/1049732315617444

Martín, A. G. (2023). *EL MÉTODO BIBLIOGRÁFICO (1). LAS TÉCNICAS BIBLIOGRÁFICAS Y SU EVOLUCIÓN HISTÓRICA*. Obtenido de https://revistarecension.com/2023/08/02/el-metodo-bibliografico-1-las-tecnicas-bibliograficas-y-su-evolucion-historica/

Mauricio, L., & Adrian, T. (2021). *Propuesta de diseño de una red LAN y sistema de seguridad basado en cámaras IP para la dirección desconcentrada INDECI - Tumbes; 2019*. Obtenido de https://repositorio.uladech.edu.pe/handle/20.500.13032/24313

MercadoLibre. (2024). Obtenido de https://articulo.mercadolibre.com.ec/MEC-550160548-cerradura-inteligente-hr07-p-con-camara-tuya-smart-_JM

Miles, M., Huberman, M., & Saldaña, J. (2014). *Qualitative Data Analysis: A Methods Sourcebook (3rd ed.)*. SAGE Publications. doi:978-1452257877

Morales, J. M., & Hontecillas, D. (s.f.). *Seguridad en redes inalámbricas IEEE 802.11*. Obtenido de https://docencia.ac.upc.es/FIB/CASO/seminaris/2q0304/T10.pdf

MVTEAM. (2024). Obtenido de https://www.mvteamcctv.com/es/products/High-Security-Anti-Theft-Smart-Lock-Door-Thumbprint-Biometric-Intelligent-Electronic-Fingerprint-WiF.html

Naranjo, L. J. (2018). *Diseño de una Red Inalámbrica basada en la Norma 802.11 ac para un Centro Comercial de Guayaquil en el 2018*. Obtenido de http://biblioteca.uteg.edu.ec:8080/bitstream/handle/123456789/61/DISENO-DE-UNA-RED-INALAMBRICA-BASADA-EN-LA-NORMA-802%2C11-AC-PARA-UN-CENTRO-COMERCIAL-DE-GUAYAQUIL-EN-EL-2018.pdf?sequence=1&isAllowed=y

Osorio, V. (s.f.). *Estandar 802.11 Caracteristicas*. Obtenido de https://es.scribd.com/document/408328538/Estandar-802-11-Caracteristicas

Palinkas, L. A. (2015). Purposeful sampling for qualitative data collection and analysis in mixed method implementation research. *Administration and Policy in Mental Health and Mental Health Services Research, 42*(5), 533-544. doi:10.1007/s10488-013-0528-y

Palma, M. A., & Mendoza, L. B. (2023). *Implementación de puerta automatizada en el acceso secundario del bloque B de la Universidad Laica Eloy Alfaro de Manabí Extensión Chone*. Obtenido de https://repositorio.uleam.edu.ec/bitstream/123456789/4670/1/ULEAM-INFOR-0123.pdf

Patton, M. Q. (2015). *Qualitative Research & Evaluation Methods.* Thousand Oaks, CA.

Patton, M. Q. (215). *Qualitative Research & Evaluation Methods (4th ed.).* SAGE Publications. doi:978-1412972123

Pérez Pérez , J. (2021). *Seguridad en Cerraduras Inteligentes.* RIULL. Obtenido de https://riull.ull.es/xmlui/handle/915/25443

PHD PARRA BALZA, F. D. (2022). *Evaluación de QOS, rendimiento, capacidad y seguridad de una red inalámbrica con estándar IEEE 802.11 ax*. Obtenido de https://repositorio.uisrael.edu.ec/handle/47000/3075

Qvadis. (2021). *Cerradura inteligente. Ventajas, usos y características*. Obtenido de https://blog.qvadis.es/cerradura-inteligente-ventajas-usos-y-caracteristicas

RecFaces. (13 de Octubre de 2022). *RecFaces*. Obtenido de Los 5 mejores sistemas de seguridad: https://recfaces.com/es/articles/que-es-sistemas-de-seguridad

Revista Innovación Seguridad. (15 de Marzo de 2012). Obtenido de Building integration system: https://revistainnovacion.com/nota/870/building_integration_system/

Sabino, C. (1992). *El proceso de investigación.* Caracas: Ed. Panapo.

Salazar, J. (2016). *Redes Inalámbricas*. Obtenido de https://upcommons.upc.edu/bitstream/handle/2117/100918/LM01_R_ES.pdf

Saunders, M. L. (2019). *Research Methods for Business Students.* Pearson.

Sharma, V., Singh, H., & Malhotra, J. (2012). Performance Analysis of IEEE 802.11e (EDCF) and IEEE 802.11(DCF) WLAN Incorporating Different Physical Layer Standards. *Inst. Eng. India Ser. B, 93*(93), 247-253. doi:10.1007/s40031-013-0034-3

SL, O. (14 de Septiembre de 2021). *OMNITEC.* Obtenido de Cerraduras electrónicas para colegios: Gestionar control de accesos: https://www.omnitecsystems.es/omni/blog/cerraduras-electronicas-para-colegios

Technofast . (2024). Obtenido de Cerradura Smart Dactilar, Clave, Tarjeta de Proximidad TUR-X3-PLUS.

TecnoDigital. (2023). *Qué son las encuestas y cómo se usan en estadística*. Obtenido de https://informatecdigital.com/articulos/que-son-las-encuestas-y-como-se-usan-en-estadistica/

Uriarte, E. D. (2015). *Evaluación de la Red Inalámbrica en el Hospital Escuela Cesar Amador Molina,basado en la norma IEEE 802.11 y controles de seguridad del estándar ISO 27002-2013 Matagalpa, I semestre 2015.* Obtenido de https://repositorio.unan.edu.ni/3198/1/5604.pdf

Uss. (17 de Agosto de 2022). *USS.* Obtenido de Sistemas de seguridad para instituciones educativas, todo lo que debes saber: https://uss.com.ar/tecnologia-y-equipamiento/sistemas-de-seguridad-para-instituciones-educativas/

Valdivia, E. J., & Miranda, J. M. (2020). *Propuesta de un Agente Inteligente para el Manejo y Mitigación de Riesgos de Ciberseguridad en Entornos IoT*. Obtenido de https://ieeexplore.ieee.org/document/9390153

Vázquez Guerrero, F., & Luque Morales, R. (2015). *Control de acceso inteligente a las aulas del departamento de ingeniería industrial.* Repositorio Institucional UNISON. doi:20.500.12984/1798

Anexos

Encuesta realizada en el bloque de Agroindustria en la FCVT de la Uleam

1. ¿Qué tipo de sistema de control de acceso se utiliza actualmente en las aulas de la universidad?

a) Sistema tradicional (llaves físicas)

b) Tarjetas de proximidad

c) Biometría

d) Control de acceso inalámbrico basado en IEEE 802.11

e) No estoy seguro

Propósito: Identificar el tipo de sistema de seguridad utilizado actualmente. Esto permite entender qué tecnologías son más prevalentes y cómo se percibe su efectividad.

2. ¿Considera que el sistema actual de control de acceso es adecuado para prevenir accesos no autorizados?

a) Muy adecuado

b) Adecuado

c) Neutral

d) Inadecuado

e) Muy inadecuado

Propósito: Evaluar la percepción sobre la efectividad del sistema actual en la prevención de accesos no autorizados, ayudando a identificar áreas de mejora.

3. ¿Ha experimentado problemas con el control de acceso a las aulas en el último año?

a) Sí

b) No

Propósito: Detecta la frecuencia e impacto de incidentes de seguridad, proporcionando datos sobre la eficacia del sistema actual.

4. ¿Está familiarizado con la norma IEEE 802.11?

a) Sí

b) No

Propósito: Determinar el nivel de conocimiento básico de los encuestados sobre la norma IEEE 802.11, que es fundamental para entender su percepción de las tecnologías inalámbricas y su aplicación en sistemas de seguridad.

5. ¿Está familiarizado con la implementación de sistemas de control de acceso basados en la norma IEEE 802.11?

a) Sí

b) No

Propósito: Determinar el nivel de conocimiento general sobre los sistemas de control de acceso basados en la norma IEEE 802.11.

6. ¿Cree que la integración de la norma IEEE 802.11 mejora la seguridad en el control de acceso a las aulas?

a) Sí, significativamente

b) Sí, de manera moderada

c) Neutral

d) No, poco

e) No, nada

Propósito: Medir la percepción de la efectividad de la norma IEEE 802.11 en la mejora de la seguridad.

7. ¿Ha recibido capacitación sobre el uso del sistema de control de acceso a las aulas basado en IEEE 802.11?

a) Sí

b) No

Propósito: Identificar si los usuarios han sido capacitados adecuadamente para utilizar el sistema, lo cual es crucial para su efectividad.

8 ¿Qué mejoras sugeriría para el sistema de control de acceso a las aulas basado en IEEE 802.11?

a) Mejorar la tecnología de autenticación

b) Incrementar la frecuencia de actualizaciones

c) Implementar más medidas de seguridad física

d) Capacitar mejor al personal

e) No se requieren mejoras

Encuesta realizada para personal especializado

1. ¿Qué protocolo de seguridad inalámbrica se utiliza en la red de control de acceso de las aulas?

a) WEP

b) WPA

c) WPA2

d) WPA3

e) No estoy seguro

Propósito: Evaluar el conocimiento sobre los protocolos de seguridad, que son críticos para la protección de la red.

2. ¿Con qué frecuencia se monitorea la red inalámbrica para detectar posibles amenazas?

a) Continuamente

b) Diariamente

c) Semanalmente

d) Mensualmente

e) No estoy seguro

Propósito: Determina la percepción sobre las prácticas de monitoreo de seguridad, esenciales para la detección temprana de amenazas.

3. ¿Qué tan eficiente considera el sistema en términos de velocidad de conexión y confiabilidad?

a) Muy eficiente

b) Eficiente

c) Neutral

d) Ineficiente

e) Muy ineficiente

Propósito: Mide la percepción de los usuarios sobre el rendimiento técnico de la red, lo cual puede influir en la adopción y uso del sistema.

4. ¿Qué tipo de cifrado se utiliza en la transmisión de datos a través de la red IEEE 802.11?

a) TKIP

b) AES

c) Ninguno

d) No estoy seguro

Propósito: Evaluar el conocimiento sobre las técnicas de cifrado utilizadas, vital para asegurar las comunicaciones a través de la red.

5. ¿Cómo califica la interoperabilidad del sistema de control de acceso con otros dispositivos inalámbricos basados en IEEE 802.11?

a) Excelente

b) Buena

c) Neutral

d) Mala

e) Muy mala

Propósito: Evaluar la compatibilidad del sistema con otros dispositivos, importante para la integración y expansión del sistema.

6. ¿Qué tan bien documentados están los procedimientos para resolver incidencias relacionadas con la red IEEE 802.11?

a) Muy bien documentados

b) Bien documentados

c) Neutral

d) Mal documentados

e) Muy mal documentados