



UNIVERSIDAD LAICA “ELOY ALFARO” DE MANABÍ

TRABAJO DE TITULACIÓN

MODALIDAD PROYECTO DE INTEGRADOR

TÍTULO:

RECONOCIMIENTO BIOMÉTRICO PARA EL CONTROL DE ACCESO EN
LOS LABORATORIOS DEL ÁREA TÉCNICA DE LA UNIVERSIDAD
LAICA ELOY ALFARO DE MANABÍ EXTENSIÓN CHONE

AUTOR:

CANTOS BRAVO JOSÉ CRISTÓBAL
GARCÍA VERA NAYELY BELÉN

UNIDAD ACADÉMICA:

EXTENSIÓN CHONE

CARRERA:

TECNOLOGÍAS DE LA INFORMACIÓN

TUTOR:

LIC. JUNIOR ANTONIO BRIONES MERA, MGS.

CHONE – MANABÍ – ECUADOR

FEBRERO DE 2026

CERTIFICACIÓN DEL TUTOR

Lic. Junior Antonio Briones Mera, Mgs.; docente de la Universidad Laica “Eloy Alfaro” de Manabí, **¡Error! No se encuentra el origen de la referencia.**, en calidad de Tutor del Proyecto.

CERTIFICO:

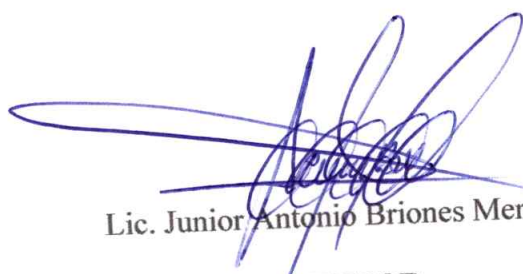
Que el presente Proyecto Integrador con el título “RECONOCIMIENTO BIOMÉTRICO PARA EL CONTROL DE ACCESO EN LOS LABORATORIOS DEL ÁREA TÉCNICA DE LA UNIVERSIDAD LAICA ELOY ALFARO DE MANABÍ EXTENSIÓN CHONE” ha sido exhaustivamente revisado en varias sesiones de trabajo.

Las opciones y conceptos vertidos en este Proyecto son fruto de la perseverancia y originalidad de sus autores:

CANTOS BRAVO JOSÉ CRISTÓBAL y GARCÍA VERA NAYELY BELÉN

Siendo de su exclusiva responsabilidad.

Chone, Febrero del 2026



Lic. Junior Antonio Briones Mera, Mgs.
TUTOR

DECLARACIÓN DE AUTORÍA

Quienes suscriben la presente:

CANTOS BRAVO JOSÉ CRISTÓBAL y GARCÍA VERA NAYELY BELÉN

Estudiante(s) de la Carrera de ~~¡Error! No se encuentra el origen de la referencia.~~, declaro(amos) bajo juramento que el siguiente proyecto cuyo título: “RECONOCIMIENTO BIOMÉTRICO PARA EL CONTROL DE ACCESO EN LOS LABORATORIOS DEL ÁREA TÉCNICA DE LA UNIVERSIDAD LAICA ELOY ALFARO DE MANABÍ EXTENSIÓN CHONE”, previa a la obtención del Título de Ingeniero en Tecnologías de la Información, es de autoría propia y ha sido desarrollado respetando derechos intelectuales de terceros y consultando las referencias bibliográficas que se incluyen en este documento.

Jose Cantos B

Cantos Bravo José Cristóbal
NUI. 1314435734

Nayely Garcia

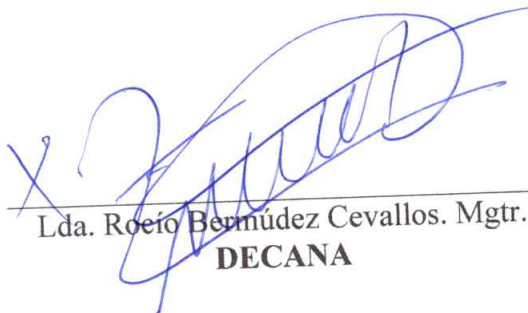
García Vera Nayely Belén
NUI. 1314438860

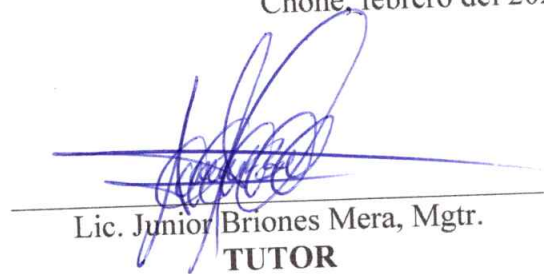


APROBACIÓN DEL TRABAJO DE TITULACIÓN

Los miembros del Tribunal Examinador aprueban el Trabajo de Titulación con Modalidad Proyecto Integrador, titulado: “RECONOCIMIENTO BIOMÉTRICO PARA EL CONTROL DE ACCESO EN LOS LABORATORIOS DEL ÁREA TÉCNICA DE LA UNIVERSIDAD LAICA ELOY ALFARO DE MANABÍ EXTENSIÓN CHONE”. Cuyos autores, Cantos Bravo José Cristóbal y García Vera Nayely Belén, estudiantes de la Carrera de Tecnologías de la Información, y como Tutor de Trabajo de Titulación el Ing. Frank Aquino Cornejo Moreira

Chone, febrero del 2026


Lda. Rocio Bermúdez Cevallos. Mgtr.
DECANA


Lic. Junior Briones Mera, Mgtr.
TUTOR


Lector 1
MIEMBRO DEL TRIBUNAL


Lector 2
MIEMBRO DEL TRIBUNAL


Lic. Indira Zambrano Cedeño, Mgtr.
SECRETARIA

DEDICATORIA

Quiero dedicar este trabajo a mis padres, José Cantos y Betty Bravo, por su apoyo incondicional, por su amor siempre presente y por enseñarme el valor de la perseverancia. A mi hermana, Marilyn Cantos, por su respaldo continuo y por ser un ejemplo de fortaleza en mi vida.

A mi pareja, Nayely García, le agradezco profundamente por su amor, paciencia y por estar a mi lado en cada paso de este proceso. Tu presencia y apoyo han sido fundamentales para alcanzar este logro.

José Cantos

DEDICATORIA

Dedico este proyecto a mis padres, Jonny García y Consuelo Vera, por su constante apoyo, cariño y por enseñarme siempre a ser perseverante. A mis hermanos y demás familiares, por su acompañamiento y por ser un pilar fundamental en mi vida.

A mi pareja, José Cantos, por su dedicación, su amor y por caminar a mi lado en todo este recorrido. Gracias por tu apoyo constante y por hacer posible este logro.

Nayely García

AGRADECIMIENTO

Queremos expresar nuestros sinceros agradecimientos a Dios, por su amor incondicional, apoyo constante y por estar siempre a nuestro lado. Gracias por enseñarnos los valores del esfuerzo, la perseverancia y el trabajo en equipo.

A nuestros padres, quienes siempre han estado pendientes de nuestro progreso, ofreciéndonos su apoyo y palabras de aliento. Su generosidad y cariño han sido clave para llegar hasta aquí.

A nuestros familiares quienes han sido una parte fundamental en este proyecto. Juntos hemos trabajado arduamente, enfrentando desafíos y celebrando logros. Sin su dedicación, su compromiso y su constante apoyo, este trabajo no hubiera sido posible. A nuestras parejas, gracias por ser nuestras compañeras en cada paso de este camino.

A nuestros abuelos maternos, tías y tíos, por su sabiduría, su amor y por ser una fuente constante de motivación. Gracias por su presencia en nuestras vidas y por brindarnos siempre su respaldo en cada etapa.

Finalmente, agradecemos a todos nuestros familiares que estuvieron pendientes de nuestro progreso. Sin su apoyo continuo, este proyecto no habría sido posible.

José Cantos

ÍNDICE DE CONTENIDO

PORTADA.....	i
CERTIFICACIÓN DEL TUTOR	ii
DECLARACIÓN DE AUTORÍA.....	iii
APROBACIÓN DEL TRABAJO DE TITULACIÓN	iv
DEDICATORIA	v
AGRADECIMIENTO	vii
ÍNDICE DE CONTENIDO	viii
RESUMEN	xiii
ABSTRACT	xiv
CAPÍTULO I: INTRODUCCIÓN.....	1
1.1 Introducción	1
1.2 Diagrama causa – efecto del problema	3
1.3 Planteamiento y formulación del problema	3
1.4 Objetivos.....	4
1.4.1 Objetivo general.....	4
1.4.2 Objetivos específicos.....	4
1.5 Justificación	4
CAPITULO II: MARCO TEÓRICO DE LA INVESTIGACIÓN	7
2.1 Reconocimiento biométrico.	7
2.1.1 Definiciones más relevantes de la biometría.....	7
2.1.2 Características biométricas.	8
2.1.3 Ventajas y beneficios de la biometría.....	9
2.1.4 Desventajas y dificultades de la biometría.	10
2.1.5 Tipos de reconocimiento biométrico.....	11
2.1.6 ISO/IEC 19795-1.....	13
2.2 Control de acceso.....	14
2.2.1 Definiciones con enfoque en las tecnologías de la información.	14
2.2.2 Característica de los controles de acceso.....	15
2.2.3 Ventajas de los controles de accesos	15
2.2.4 Tipos de controles de acceso para puertas.....	17
2.2.5 Tipos de cerraduras inteligentes.....	18
CAPÍTULO III: DISEÑO METODOLÓGICO	20

3.1	Tipo de investigación.....	20
3.2	Métodos de investigación.....	20
3.3	Técnicas, herramientas e instrumentos.	21
3.3.1	Técnicas.....	21
3.3.2	Herramientas.	22
3.3.3	Instrumentos.	22
3.4	Análisis y presentación de resultados.....	22
3.4.1	Resultados de la encuesta	22
3.4.2	Resultados de la entrevista	31
CAPÍTULO IV: EJECUCIÓN DEL PROYECTO		32
4.1	Descripción del proyecto	32
4.2	Determinación de recursos	33
4.2.1	Humanos.....	33
4.2.2	Materiales	33
4.2.3	Económicos	34
4.3	Etapas de ejecución del proyecto	35
4.3.1	Fase I: Situación actual del sitio	36
4.3.2	Fase II: Diseño de la implementación	37
4.3.3	Fase III procedimientos para la instalación	39
4.3.4	Fase IV Pruebas y registros	40
CAPÍTULO V: CONCLUSIONES Y RECOMENDACIONES		41
5.1	Conclusiones.....	41
5.2	Recomendaciones.....	42
BIBLIOGRAFÍA.....		43
ANEXOS		47
Anexo Nr1. Encuesta.....		47
Anexo Nr2. Entrevista.....		50

ÍNDICE DE TABLA

Tabla 1 Pregunta 1 de la encuesta.....	23
Tabla 2 Pregunta 2 de la encuesta.....	24
Tabla 3 Pregunta 3 de la encuesta.....	25
Tabla 4 Pregunta 4 de la encuesta.....	26
Tabla 5 Pregunta 5 de la encuesta.....	27
Tabla 6 Pregunta 6 de la encuesta.....	28
Tabla 7 Pregunta 7 de la encuesta.....	29
Tabla 8 Pregunta 8 de la encuesta.....	30
Tabla 9 Recursos económicos	34
Tabla 10 Comparación de equipos propuestos.....	37

ÍNDICE DE FIGURAS

Figura 1 Diagrama causa efecto	3
Figura 2 Características arquitectónica de un sistema biométrico.....	9
Figura 3 Tipos de biometría.....	13
Figura 4 Tipos y modelos de cerraduras inteligentes.....	19

ÍNDICE DE GRÁFICOS

Gráfico 1 Representación gráfica de la pregunta 1 de la encuesta	23
Gráfico 2 Representación gráfica de la pregunta 2 de la encuesta	24
Gráfico 3 Representación gráfica de la pregunta 3 de la encuesta	25
Gráfico 4 Representación gráfica de la pregunta 4 de la encuesta	26
Gráfico 5 Representación gráfica de la pregunta 5 de la encuesta	27
Gráfico 6 Representación gráfica de la pregunta 6 de la encuesta	28
Gráfico 7 Representación gráfica de la pregunta 7 de la encuesta	29
Gráfico 8 Representación gráfica de la pregunta 8 de la encuesta	30

RESUMEN

Los laboratorios del área técnica de la ULEAM-Extensión Chone presentan limitaciones de seguridad y trazabilidad asociadas al uso de cerraduras convencionales. Este proyecto propone implementar un sistema de reconocimiento biométrico, principalmente facial, para optimizar el control de acceso, proteger los recursos y modernizar la gestión operativa. Se realizó un estudio de enfoque mixto que incluyó encuesta a 217 estudiantes, entrevista a la directora del área técnica y observación directa de infraestructura (puertas, electricidad y conectividad). Los hallazgos evidencian alta percepción de necesidad de mejoras (91,25%) y expectativas favorables frente a la biometría: aumento de la seguridad (91,71%) y reducción de ingresos no autorizados (92,63%). La comodidad de uso alcanza 62,67%, mientras que la aceptación general es moderada (44,70%) con amplia neutralidad (50,69%), sugiriendo mayor socialización. La protección de datos biométricos es prioridad para la mayoría (93,55%). Se plantea un despliegue por fases en cuatro laboratorios, bajo principios de privacy by design y cumplimiento de la LOPD, con criterios de éxito de verificación $\geq 98\%$, disponibilidad $\geq 99\%$ y registros auditables; el presupuesto referencial de implementación es USD 1.596,48. Se concluye que la solución biométrica es viable y pertinente para el contexto universitario, al fortalecer la seguridad física, la trazabilidad y la gestión de usuarios; se recomienda protocolizar el tratamiento de datos, capacitar a la comunidad y evaluar periódicamente el desempeño para asegurar adopción informada y mejora continua.

Palabras claves: Reconocimiento, Biometría, Accesos.

ABSTRACT

The laboratories in the technical area of ULEAM-Chone Extension present security and traceability limitations associated with the use of conventional locks. This project proposes implementing a biometric recognition system, primarily facial, to optimize access control, protect resources, and modernize operational management. A mixed-approach study was conducted, including a survey of 217 students, an interview with the director of the technical area, and direct observation of infrastructure (doors, electricity, and connectivity). The findings show a high perception of the need for improvements (91.25%) and favorable expectations regarding biometrics: increased security (91.71%) and reduced unauthorized entries (92.63%). Ease of use reaches 62.67%, while general acceptance is moderate (44.70%) with broad neutrality (50.69%), suggesting the need for greater socialization. The protection of biometric data is a priority for the majority (93.55%). A phased deployment is proposed in four laboratories, under privacy by design principles and compliance with LOPD, with success criteria of verification $\geq 98\%$, availability $\geq 99\%$, and auditable records; the reference implementation budget is USD 1,596.48. It is concluded that the biometric solution is viable and relevant for the university context, as it strengthens physical security, traceability, and user management; it is recommended to protocolize data treatment, train the community, and periodically evaluate performance to ensure informed adoption and continuous improvement.

Keywords: Recognition, Biometrics, Access.

CAPÍTULO I: INTRODUCCIÓN

1.1 Introducción

El avance de las tecnologías de identificación biométrica ha generado nuevas oportunidades para optimizar la seguridad y el control en distintos entornos, incluyendo los espacios académicos. Los laboratorios del área técnica de la Universidad Laica Eloy Alfaro de Manabí, Extensión Chone, requieren mecanismos de acceso más eficientes y seguros que superen las limitaciones de los métodos tradicionales. La implementación de un sistema de reconocimiento biométrico se presenta como una alternativa innovadora que puede fortalecer la gestión institucional, prevenir el ingreso no autorizado y garantizar el adecuado uso de los recursos tecnológicos disponibles.

En todo el mundo se observa en la actualidad una tendencia muy marcada en el empleo de rasgos biométricos, tales como rostro, huellas digitales, geometría de la mano, iris, patrones de retina, firma y voz, entre las más destacadas en los sistemas de identificación/autenticación de personas. Todas estas técnicas presentan diferentes grados de singularidad, permanencia, mensurabilidad, desempeño, aceptación del usuario y robustez (Ruíz et al., 2022, p. 128).

En países como Cuba, el control de acceso a las prácticas de laboratorios es el componente del modelo que interactúa directamente con los estudiantes o alternativas (Mar Cornelio et al., 2024, p. 90). En Colombia el control de acceso como el registrar la entrada, registrar las salidas, realizar consultas se realizan también en bicicletas con su información asociada, registrar a los visitantes, con las consultas respectivas, igualmente es importante en este caso de uso registrar apropiadamente la salida de los visitantes que poseen este medio de transporte (Páez et al., 2021, p. 59).

En Ecuador hoy en día el avance de la tecnología crece muy rápidamente, usando diferentes métodos de seguridad en cuanto al control de acceso a instalaciones privadas, una alternativa es el reconocimiento facial que permite al personal, sea de empresas, instituciones o industrias el ingreso adecuado, evitando de esta manera accesos no autorizados (Villa, 2023, p. 22).

En Ecuador los controles de acceso permiten crear un rol al cual se le asignan varios permisos de acuerdo a sus procesos y funciones en el sistema, luego éstos roles son asignados a los usuarios finales del aplicativo, sin embargo no proporcionan una seguridad completa lo cual es necesario implementar otros mecanismos de seguridad (Zambrano et al., 2019, p. 305).

En Chone varias instituciones han implementado el reconocimiento biométrico para poder controlar las asistencias de los docentes y estudiantes que ingresan a ciertas áreas de dichos establecimientos, el constante crecimiento tecnológico en el que nos encontramos inmersos el día de hoy nos obliga a adaptarnos a los cambios o correr el riesgo de quedar sumidos en la obsolescencia (Saldarriaga, 2023, p. 1).

En Chone específicamente en la Universidad Laica Eloy Alfaro de Manabí, proyectos de este tipo aportan de manera positiva a la institución ya que la aplicación de la tecnología, con base al control de acceso automatizado tiene como beneficios la seguridad, mismo que permite a los usuarios se sientan protegidos dentro del edificio, de esta manera también se optimiza la calidad de 2 tiempo en el ingreso o salida; tanto de los usuarios internos y externos; y por ende se evita la reducción de costos en el presupuesto de la organización, en cuanto a la contratación de personal para la realización de dichos procesos (Vega, 2023, pp. 1-2).

El proyecto integrador está estructurado de manera lógica y secuencial, iniciando con un Resumen que sintetiza los elementos más relevantes del estudio: el problema abordado, los objetivos planteados, la metodología empleada y los resultados obtenidos. En el Capítulo I: Introducción, se contextualiza el tema y se presenta el problema a través de un diagrama causa-efecto. Asimismo, se expone el planteamiento y formulación del problema, junto con los objetivos general y específicos, y se justifica la pertinencia del proyecto.

El Capítulo II el marco teórico recoge los principales conceptos, antecedentes y fundamentos relacionados con el reconocimiento biométrico y su aplicación en sistemas de control de acceso. Luego, en el Capítulo III: Diseño metodológico, se detallan el tipo de investigación, los métodos aplicados, las técnicas e instrumentos utilizados para la recolección de datos, y se presenta el análisis de los resultados obtenidos, que permiten diagnosticar la situación actual del problema identificado.

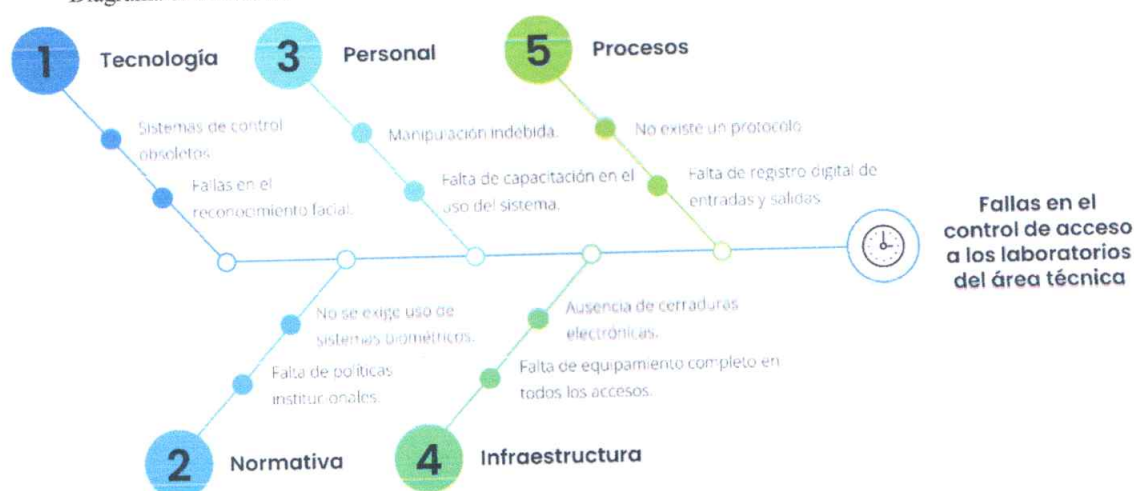
Finalmente, el Capítulo IV la ejecución del proyecto describe la propuesta tecnológica diseñada, especificando los recursos necesarios —humanos, materiales y económicos— y las etapas de su implementación. El documento culmina con el Capítulo V: Conclusiones y recomendaciones, donde se sintetizan los hallazgos más importantes y se sugieren acciones concretas que puedan ser aplicadas para mejorar el control de acceso a los laboratorios del área técnica de la universidad.

1.2 Diagrama causa – efecto del problema

El diagrama causa-efecto tiene como propósito analizar de forma estructurada los diversos factores que generan fallas en el control de acceso a los laboratorios del área técnica de la Universidad Laica Eloy Alfaro de Manabí, extensión Chone. A través de esta herramienta se identifican causas agrupadas en cinco categorías clave: tecnología, personal, procesos, infraestructura y normativa institucional. Cada categoría presenta elementos específicos que contribuyen al problema central. Este análisis permite comprender el origen de las deficiencias en el sistema actual y plantea como solución la implementación de un sistema biométrico confiable que asegure un acceso eficiente, seguro y controlado.

Figura 1

Diagrama causa efecto



Nota. Diagrama casusa efecto extraída de la fuente (Autores de la investigación)

El problema central las fallas en el control de acceso puede deberse a múltiples causas, agrupadas en cinco categorías principales: tecnología, personal, procesos, infraestructura y normativa. Cada una de estas categorías contiene factores específicos que deben analizarse para diseñar una solución efectiva, como el uso de sistemas biométricos (reconocimiento facial) que respondan a estándares de seguridad, disponibilidad y precisión.

1.3 Planteamiento y formulación del problema

El acceso seguro y controlado a los espacios académicos especializados, como los laboratorios del área técnica, es fundamental para preservar los recursos institucionales y garantizar un entorno adecuado para la práctica y el aprendizaje. Sin embargo, en la actualidad, se evidencian fallas en el control de acceso que permiten el ingreso no autorizado, el uso indebido de equipos o la falta de trazabilidad de usuarios. En este contexto, surgen interrogantes sobre la eficacia de los mecanismos tradicionales utilizados y la necesidad de

implementar tecnologías modernas como el reconocimiento biométrico. Para la solución a estos se presenta la siguiente formulación del problema:

¿Cómo incide el reconocimiento biométrico para el control de acceso en los laboratorios del área técnica de la Universidad Laica Eloy Alfaro de Manabí Extensión Chone?

A partir de esta formulación, se busca analizar la viabilidad y el impacto del uso del reconocimiento biométrico como una solución tecnológica innovadora que contribuya a mejorar el control de acceso, optimizar la seguridad y fortalecer la gestión de los espacios técnicos. Este análisis permitirá fundamentar propuestas que respondan a las necesidades institucionales, promoviendo un entorno más eficiente, moderno y acorde con los avances tecnológicos aplicados a la educación superior.

1.4 Objetivos

1.4.1 Objetivo general

Implementar reconocimiento biométrico para el control de acceso en los laboratorios del área técnica de la Universidad Laica Eloy Alfaro De Manabí Extensión Chone.

1.4.2 Objetivos específicos

Analizar los fundamentos teóricos y tecnológicos del reconocimiento biométrico y su aplicación en sistemas de control de acceso en instituciones educativas.

Diagnosticar el estado actual de la infraestructura tecnológica y las condiciones operativas del control de acceso en los laboratorios del área técnica de la ULEAM, Extensión Chone.

Diseñar una propuesta tecnológica basada en reconocimiento biométrico para mejorar el control de acceso en los laboratorios del área técnica, considerando los requerimientos institucionales y técnicos.

1.5 Justificación

Es de impacto innovador ya que la biometría surge como una tecnología de reconocimiento efectiva en base a los patrones propios de un individuo, esta puede tomar diversas formas de medición para llevar a cabo su objetivo (Guerra Jiménez & Jiménez Prada, 2021, p. 35).

Impacta tecnológicamente ya que ayuda a garantizar la confidencialidad, integridad y disponibilidad de la información, así como a mitigar los riesgos asociados a posibles amenazas y vulnerabilidades.

Al seguir las mejores prácticas definidas en estos estándares, las organizaciones pueden establecer procesos sólidos de gestión de riesgos, implementar controles adecuados y realizar auditorías efectivas para evaluar y mejorar continuamente su postura de seguridad (Córdova, 2023, p. 596).

El proyecto es de gran impacto técnico ya que radica en la integración de sistemas biométricos avanzados en el entorno universitario, lo que moderniza los procesos de control de acceso, implementando esta tecnología, se fortalece la infraestructura digital, se optimiza la seguridad y se promueve el uso responsable de los recursos institucionales. Por otro lado, se impulsa la innovación dentro del campus, fomentando la automatización y creando un precedente para futuras mejoras tecnológicas en otras áreas académicas y administrativas de la Universidad Laica Eloy Alfaro de Manabí extensión Chone.

Con un impacto social en la era digital actual, la seguridad y la autenticación de usuarios se han convertido en aspectos cruciales debido al incremento en el uso de tecnologías digitales y la necesidad de proteger datos y transacciones. Los sistemas biométricos emergen como una solución efectiva y fiable para la autenticación, aprovechando las características físicas y comportamentales únicas de cada individuo (Quirós, 2024, p. 5).

Socialmente este tipo de trabajos tienen gran impacto en el ámbito de control de accesos, donde se busca gestionar cualquier acceso no autorizado y reducir al mínimo la probabilidad de que ocurra. Es esencial identificar de manera apropiada el rol asignado a cada usuario para establecer un control efectivo sobre el acceso a la información (Córdova, 2023, p. 46).

El impacto colaborativo de este trabajo se da a conocer la promoción de una cultura de responsabilidad, orden y seguridad dentro de la comunidad universitaria, sobre todo dentro del Área técnica, al implementar el reconocimiento biométrico, se protege el acceso a los laboratorios, se fortalece el sentido de pertenencia fomentando el respeto por los recursos institucionales. Sin embargo, mejora la convivencia al reducir problemas por el uso indebido de los laboratorios, generando un entorno más confiable, justo y acorde con los problemas sociales.

En términos ambientalista, este tipo de sistemas tienen el impacto de reducir la dependencia de materiales físicos, como tarjetas de identificación, lo que podría disminuir el uso de plásticos y otros materiales. Sin embargo, el consumo energético y los residuos electrónicos generados por los dispositivos de seguridad biométricos presentan desafíos medioambientales que deben ser mitigados mediante prácticas sostenibles de diseño y disposición (Quirós, 2024, p. 38).

Desde el punto de vista sostenible impacta en la seguridad de elementos como la ubicación y protección de equipos, elementos de soporte a los equipos, seguridad en el cableado, mantenimiento de equipos, seguridad en el equipamiento fuera de la organización, seguridad en la redistribución o reutilización de equipamiento, borrado de información y/o software (Becerra & Carlos, 2020, p. 33).

El impacto ambiental de este trabajo de titulación se expresa en el uso eficiente de los recursos técnicos y tecnológicos dentro de los laboratorios, al controlar el acceso mediante reconocimiento biométrico, se evita el uso innecesario de equipos reduciendo el consumo eléctrico y prolonga la vida útil de los dispositivos.

La implementación de sistemas biométricos en los laboratorios universitarios fortalece la seguridad, optimiza el uso de recursos y reduce el consumo de materiales físicos como tarjetas plásticas. Esta tecnología moderniza el control de acceso, fomenta una cultura de responsabilidad en la comunidad académica y apoya prácticas sostenibles al disminuir el consumo energético innecesario y prolongar la vida útil de los equipos técnicos disponibles.

Por último, se minimizan desperdicios y emisiones indirectas al promover una gestión responsable del entorno físico, la implementación de este proyecto apoya prácticas sostenibles dentro del campus, alineándose con los objetivos de desarrollo ambiental institucional y evitando consumo periódico de otros materiales que intervengan en los accesos principales de los laboratorios del área técnica de la Universidad Laica Eloy Alfaro de Manabí, Extensión Chone.

CAPÍTULO II: MARCO TEÓRICO DE LA INVESTIGACIÓN

2.1 Reconocimiento biométrico.

2.1.1 Definiciones más relevantes de la biometría.

El término biometría viene de las palabras griegas **bios** (vida) y **metron** (medida) y se refiere a una característica fisiológica o conductual que puede medirse, capturarse y compararse para identificar a una persona. Su objetivo principal es encontrar un patrón único que permita reconocer de forma inequívoca a cada usuario (Gallardo, 2024, p. 7).

Un sistema biométrico puede ser definido esencialmente como un sistema de reconocimiento de patrones que establece la identidad de un individuo basado en una o más señales derivadas de sus características biométricas. Dependiendo de la característica considerada, existen diversas técnicas para reconocer individuos, las cuales son llamadas formalmente modalidades biométricas (Ponce, 2021, p. 8).

La biometría no es una tarea fácil, y aunque esta definición podría ser argumentada por algunos expertos por simplificar los requisitos para calificar como un rasgo biométrico, es una buena introducción a lo que se considera biometría: Una característica biológica o conductual que puede ser utilizada para reconocer individuos (Fernández, 2020, p. 4).

Existen varios sistemas biométricos capaces de verificar la identidad de una persona mediante la voz, la huella dactilar o el rostro, cada uno de ellos con sus ventajas y desventajas. Algunos resultan más invasivos que otros, especialmente el uso de sistemas biométricos, estos permiten identificar a una persona por su forma de moverse o desplazarse, sin utilizar técnicas de reconocimiento facial (Cannatella et al., 2023, p. 957).

Los autores en mención indican que la biometría representa una forma avanzada de identificación que se basa en lo único de cada persona y observa que, aunque parezca sencillo, capturar y procesar esas características requiere tecnologías complejas y decisiones éticas importantes.

De este modo llama la atención cómo el cuerpo humano puede convertirse en una llave de acceso, y reflexiona que el uso de estas tecnologías, aunque muy útiles, también despierta preguntas sobre privacidad, ya que identifican sin permiso solo por cómo alguien se mueve o habla.

2.1.2 Características biométricas.

Para Gallardo (2024) la principal característica del reconocimiento biométrico es extraer información obtenida por un, este módulo extrae las características biométricas únicas del individuo, lo que resulta en la generación de una plantilla biométrica que representa al usuario. Entre otras características importantes se encuentran:

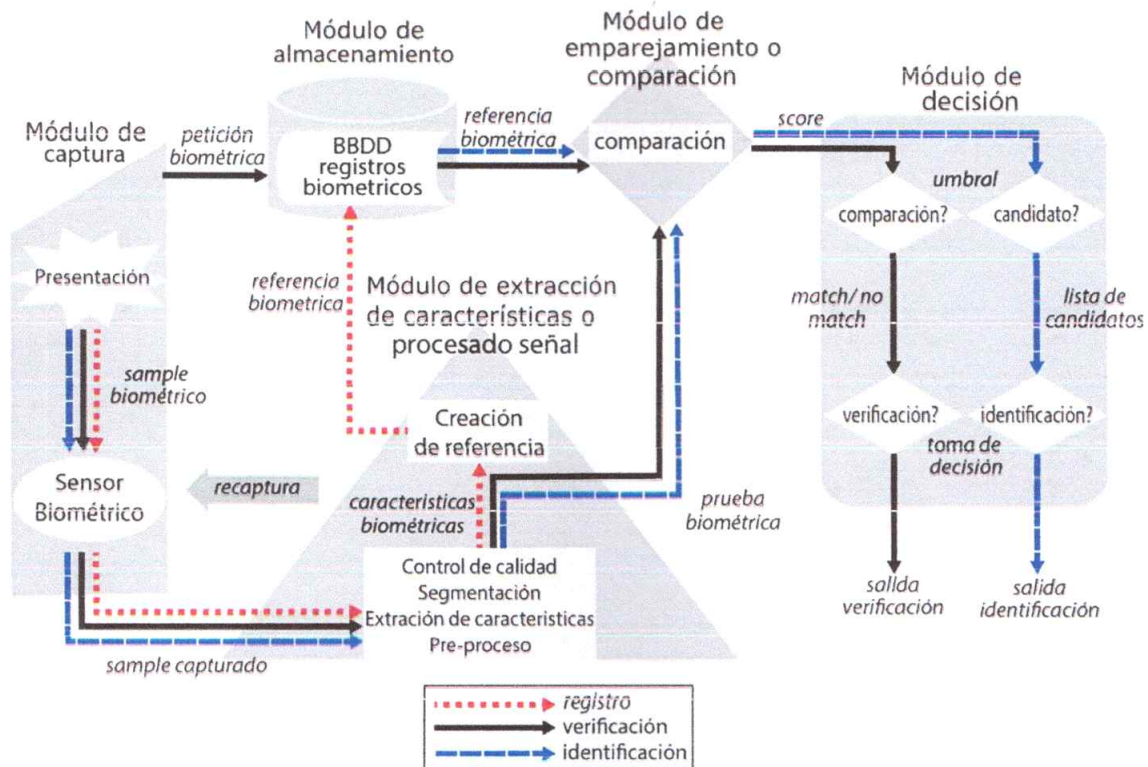
- El reconocimiento de personas mediante sistemas biométricos se caracteriza por utilizar rasgos físicos únicos, lo que resulta bastante efectivo, sin embargo, algunas muestras presentan variaciones propias del tipo de biometría, del modo en que se capturan o de las limitaciones del equipo utilizado. Estas diferencias impactan directamente en la precisión del sistema por lo que se vuelve esencial diseñar un algoritmo robusto, que realice el reconocimiento con el menor margen de error posible en la clasificación (Quiros, 2022, p. 6).
- “Los sistemas biométricos resultan atractivos porque permiten identificar a una persona mediante características biológicas y de comportamiento que le son propias, lo que las hace mucho más difíciles de perder, olvidar, compartir o robar” (Ponce , 2021, p. 8).
- Una vez instalado y completado un proceso de enrolamiento, el sistema podría funcionar en segundo plano y conceder o denegar el acceso sin necesidad de interacción adicional por parte del usuario y no requiere aprendizaje o memorización de códigos, es clave en los sistemas biométricos (Fernández, 2020, p. 10).
- La manera en que una persona camina representa una característica biométrica, determinada por un patrón de movimiento repetitivo que se divide en fases, en las cuales se pueden observar distintas conductas naturales del individuo (Cannatella et al., 2023, p. 958).

Se observa que desde el punto de vista de los autores las características de los sistemas biométricos los hacen únicos y eficaces. Le parece fascinante cómo cada persona posee rasgos que pueden ser convertidos en datos irrepetibles, como una huella digital o la forma de caminar.

También se nota que, aunque la precisión depende mucho del equipo y del entorno, la posibilidad de que el sistema funcione sin que el usuario haga nada lo vuelve práctico y moderno; reflexiona que, a pesar de sus ventajas, el reto sigue siendo lograr que el reconocimiento sea confiable en todo momento.

Figura 2

Características arquitectónicas de un sistema biométrico



Nota. Presentación de las características en un sistema de reconocimiento biométrico. Tomado de (Ortega, 2021)

2.1.3 Ventajas y beneficios de la biometría.

En investigaciones de Ponce (2021) el crecimiento de la computación en la nube impulsa la disponibilidad de sistemas biométricos bajo demanda, lo que brinda beneficios como la disminución de costos y el ahorro en el tiempo de implementación. Entre otras ventajas y beneficios tenemos:

- Una de las ventajas es que los sistemas biométricos se emplean principalmente en el control de acceso, donde se requiere que los usuarios colaboren activamente, por eso, los errores operativos suelen atribuirse a la falta de experiencia o desconocimiento del usuario. En las evaluaciones de rendimiento biométrico, no se consideran muestras obtenidas sin cooperación del usuario. No obstante, los mecanismos de Programa Acelerado de Datos (PAD) sí contemplan el análisis de muestras no cooperativas, lo que permite estudiar situaciones más complejas en el uso real de estas tecnologías (Quiros, 2022, p. 84).

- Surge como combinación de autenticadores que busca mejorar la seguridad al aprovechar las fortalezas de cada tipo de autenticación, estos sistemas ofrecen una protección superior frente a ataques como la fuerza bruta y el phishing, disminuyen el riesgo de robo de identidad digital, cumplen con normas y regulaciones de seguridad, y permiten una implementación flexible (Gallardo, 2024, p. 12).
- Aunque su implementación resulta compleja, este tipo de sistema puede representar un avance importante en la seguridad mediante videovigilancia, ayudando a prevenir actos delictivos, además de ofrecer posibles aplicaciones en otros ámbitos fuera de la videovigilancia (Cannatella et al., 2023, p. 960).

La computación en la nube impulsa el uso de sistemas biométricos, lo que facilita su implementación y reduce costos, aunque dependen de la cooperación del usuario, el análisis de muestras no cooperativas amplía su aplicabilidad. La combinación de autenticadores refuerza la seguridad frente a amenazas actuales, aunque su implementación resulta compleja, representa un avance clave en protección digital y física. Se concluye que su uso estratégico permite afrontar los retos tecnológicos actuales.

2.1.4 Desventajas y dificultades de la biometría.

Entre las desventajas más relevantes y comunes según la experiencia y resultados de varios autores tenemos:

- Una desventaja importante del reconocimiento biométrico basado en el comportamiento es que puede ser imitado, lo que permite la falsificación de firmas manuscritas, este tipo de vulnerabilidad representa un riesgo para la seguridad del sistema. El estudio que se desarrolla en este trabajo centra su atención en dicha desventaja, buscando analizar tanto las fortalezas como las debilidades de esta modalidad biométrica, con el fin de comprender mejor su funcionamiento y los posibles riesgos que implica su uso (Quiros, 2022, p. 2).
- Los sistemas de reconocimiento tradicionales presentan limitaciones importantes, ya que no logran verificar con certeza si quien proporciona las credenciales de acceso es realmente un usuario registrado, este tipo de sistemas no cuenta con mecanismos para validar reclamos negativos de identidad, es decir, cuando alguien niega ser quien el sistema identifica (Ponce, 2021, p. 8).

- En el ámbito de la biometría, el rendimiento de estos sistemas puede verse influido por los atributos demográficos del usuario como las investigaciones forenses que pueden generar efectos discriminatorios. Además del sesgo presente en los datos, también se plantea una preocupación por la privacidad, ya que la información biométrica almacenada puede revelar más datos que únicamente la identidad personal (Gallardo, 2024, p. 34).
- A diferencia de otros sistemas biométricos como la voz, la huella dactilar o el rostro, el reconocimiento por la forma de caminar no requiere alta calidad de video para identificar a una persona. Además, resulta menos invasivo, ya que no necesita la cooperación directa del individuo (Cannatella et al., 2023, p. 959).

Si bien la biometría conductual ofrece ventajas, presenta vulnerabilidades críticas, como la posibilidad de suplantación, sesgos demográficos y reflexiona sobre cómo estas limitaciones afectan la confiabilidad y la equidad en los sistemas de identificación. Además, considera que la privacidad está en riesgo cuando los datos biométricos revelan información sensible y que es fundamental evaluar tanto las fortalezas como las debilidades para garantizar un uso ético y seguro de estas tecnologías en diversos contextos.

2.1.5 Tipos de reconocimiento biométrico.

Las biometrías más utilizadas se pueden diferenciar en dos grupos físicas o del comportamiento:

2.1.5.1 Tipos de reconocimiento biométrico físicas.

Según Gallardo (2024) la biometría abarca diversas técnicas basadas en características únicas del cuerpo humano. Por ejemplo:

- La **cara** el reconocimiento facial extrae rasgos distintivos como la forma de los ojos, nariz, labios, mandíbula y las distancias entre ellos.
- La **huella dactilar** se enfoca en los patrones formados por las crestas dérmicas de uno o varios dedos, identificando figuras como bucles, curvas y círculos, y representa la técnica biométrica más antigua y ampliamente utilizada.
- Por su parte, la **huella palmar** analiza los patrones presentes en la palma de la mano, similares a los de la huella dactilar.

- En cuanto a la **geometría de la mano**, esta mide la forma, el tamaño de la palma y las dimensiones de los dedos.
- El reconocimiento de **iris** aprovecha la compleja textura de la región anular del ojo, delimitada por la pupila y la esclerótica, la cual contiene información muy particular.
- Finalmente, el análisis de **Ácido desoxirribonucleico (ADN)** compara repeticiones de alelos en regiones específicas del cromosoma, utilizando el método STR para establecer coincidencias entre muestras (Pag.8).

Los métodos biométricos físicos se basan en características corporales únicas e inalterables, lo que les otorga alta precisión y también reflexiona que su uso implica riesgos importantes si estos datos son vulnerados, ya que, a diferencia de una contraseña, no pueden ser modificados. Aunque la huella dactilar y el rostro son comunes por su eficacia, el ADN ofrece una precisión superior. Al final se recalca que la elección del método debe equilibrar seguridad, privacidad y contexto de aplicación.

2.1.5.2 Tipos de reconocimiento biométrico según el comportamiento.

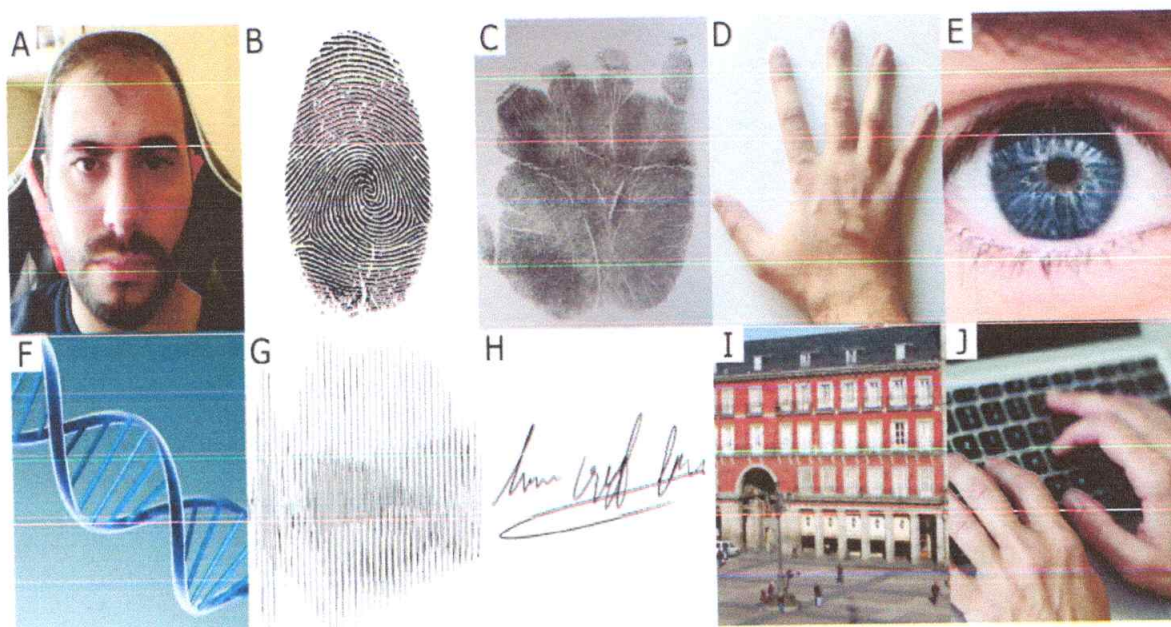
Según Gallardo (2024) estas son características adquiridas por el individuo ya sea por la conducta o por la propia experiencia:

- La **voz** representa una combinación de características físicas y conductuales, ya que depende de la anatomía de los pliegues vocales y del tracto oro nasofaríngeo, responsables de generar el sonido, aunque también varía con factores como la edad, el estado emocional o condiciones médicas.
- La **firma**, por su parte, es uno de los métodos más aceptados para autenticar documentos, y se analiza mediante elementos como curvas, bordes, coordenadas, presión y trazo del bolígrafo.
- La **manera de andar**, conocida como *gait*, se basa en que cada persona posee una forma particular de caminar, útil para identificación en contextos de seguridad y videovigilancia, especialmente donde la resolución de imagen no permite emplear técnicas más precisas.
- Finalmente, la **pulsación del teclado** analiza el ritmo al escribir, detectando patrones en los tiempos de presión, liberación y retención de teclas, lo que permite extraer características únicas del comportamiento del usuario (pp. 8-9).

Los métodos biométricos conductuales, aunque útiles y menos invasivos, son más susceptibles a variaciones externas como el estado emocional o la salud, estas técnicas, al depender de hábitos y experiencias pueden ser más accesibles, pero también menos estables. Se considera que su valor radica en complementar otros sistemas, especialmente en entornos donde la tecnología debe adaptarse a condiciones dinámicas, afianzando que su implementación debe ser cuidadosa, equilibrando funcionalidad con confiabilidad.

Figura 3

Tipos de biometría



Nota. Ejemplos de rasgos biométricos. (A) Cara. (B) Huella dactilar. (C) Huella palmar. (D) Geometría de la mano. (E) Iris. (F) ADN. (G) Voz. (H) Firma. (I) Gait. (J) Pulsación del teclado. Tomado de (Gallardo, 2024).

2.1.6 ISO/IEC 19795-1.

“El estándar ISO/IEC 19795-1 define principios generales para evaluar el rendimiento de los sistemas biométricos y mostrar los resultados de exactitud obtenidos. Estas evaluaciones pueden clasificarse en tres tipos: tecnológicas, de escenario y operacionales” (Ponce, 2021, p. 13).

La norma señala que, en la evaluación de sistemas biométricos basados en características de comportamiento, es fundamental considerar el esfuerzo de los impostores al capturar las muestras, ya que el nivel de intento por imitar el comportamiento de otro usuario puede influir en los resultados obtenidos (Quiros, 2022, p. 33).

El estándar establece dos tipos principales de pruebas biométricas: las pruebas de tecnología, que evalúan la capacidad algorítmica de los componentes usando cuerpos de prueba fuera de línea, y las pruebas de escenario, que se realizan con personas reales y buscan predecir el rendimiento del sistema en su uso real (Gómez, 2024, p. 65).

La norma ISO/IEC 19795-1 proporciona un marco riguroso para evaluar sistemas biométricos, lo cual resulta clave para garantizar su confiabilidad. Al incluir pruebas con datos simulados y con usuarios reales, se logra una visión más completa del rendimiento del sistema. Además, destaca la importancia de considerar el esfuerzo de los impostores, especialmente en biometría conductual.

2.2 Control de acceso

2.2.1 Definiciones con enfoque en las tecnologías de la información.

Entre las medidas de seguridad física que se pueden aplicar están el control de acceso, que limita la entrada a espacios con información confidencial, estas permitirían el acceso solo a personas autorizadas; la instalación de cámaras y alarmas para supervisar y prevenir robos o intrusiones. El uso de candados en armarios y cajones para proteger dispositivos y equipos; y la realización de inspecciones periódicas para verificar que los equipos son un elemento adicional para fortalecer la seguridad de esos activos que se están salvaguardando (García et al., 2023, p. 81).

Es un conjunto de mecanismos y políticas orientadas a limitar el acceso a sistemas, datos y recursos informáticos. Estos controles garantizan que únicamente las personas, procesos y sistemas con la autorización correspondiente puedan ingresar y operar sobre información y recursos determinados (Herrera, 2025, p. 7).

Es fundamental disponer de un modelo de control de acceso que permita al personal de sistemas restringir el uso de las infraestructuras y regular el ingreso de los usuarios a la información y aplicaciones. Esto se logra mediante la aplicación de reglas de accesibilidad dentro del horario laboral, de modo que tenga una hora establecida para iniciar y cerrar sesión, coincidiendo con su jornada de trabajo (Naranjo, 2023, p. 27).

Los autores expresan que la seguridad física y los controles de acceso son esenciales para proteger los recursos informáticos, más allá de medidas como cámaras o candados, es necesario establecer políticas claras que regulen quién accede y cuándo. Al analizar estas

teorías se concluye que combinar mecanismos físicos con reglas de acceso bien definidas fortalece la seguridad integral y que una infraestructura segura depende tanto de la tecnología como de la correcta gestión del comportamiento humano autorizado.

2.2.2 Característica de los controles de acceso

Para García et al. (2023) los protocolos de seguridad de la información se diseñan y desarrollan para proteger la información confidencial de una organización. Estos protocolos deben ser integrales, abarcando medidas técnicas, políticas y procedimientos e incluyen las siguientes características:

- Ser personalizados según las características específicas de la organización, como su tamaño, estructura e industria, así como el tipo de información que manejan.
- Deben ser flexibles para adaptarse a cambios tecnológicos y necesidades internas.
- Deben tener claridad, por lo que deben ser fáciles de entender, utilizando lenguaje sencillo y definiendo claramente roles y responsabilidades.
- Requieren actualización constante para mantenerse alineados con las nuevas amenazas y vulnerabilidades.
- Asimismo, deben considerar la cultura organizacional, teniendo en cuenta la actitud de los empleados hacia la seguridad de la información para crear políticas aceptables.
- Finalmente, deben enfocarse en proteger la privacidad de los datos y la información de la organización (p. 82).

El autor expresa que los protocolos de seguridad de la información no deben ser genéricos, sino adaptarse a cada organización, que su efectividad radica en equilibrar la claridad, la actualización constante y la flexibilidad. Además, analiza cómo la cultura organizacional influye en su implementación, pues la seguridad no depende solo de lo técnico, sino también del comportamiento humano, lo cual exige un enfoque integral y consciente frente a las amenazas informáticas.

2.2.3 Ventajas de los controles de accesos

Para Bardales (2024) las ventajas son el conjunto de medidas técnicas, organizativas y legales orientadas a salvaguardar los sistemas informáticos, redes y dispositivos frente a accesos no autorizados, modificaciones, divulgaciones, destrucciones o interrupciones que

puedan afectar los servicios que dichos sistemas ofrecen. Según el enfoque del control de acceso tenemos las siguientes:

- La seguridad lógica se encarga de proteger el software y los datos alojados en sistemas o redes, mediante el uso de contraseñas seguras, la verificación de identidad de los usuarios, una adecuada gestión de permisos de acceso, la instalación de firewalls para bloquear tráfico no autorizado y el cifrado de datos sensibles.
- La seguridad física se enfoca en proteger los dispositivos físicos y limitar el acceso a ellos, mediante acciones como el control de ingreso a las instalaciones, el uso de cerraduras seguras, la vigilancia en zonas sensibles y la protección directa de los equipos informáticos ante robos o daños.
- La seguridad de la información consiste en proteger los datos guardados en sistemas o redes, mediante la aplicación de políticas claras, el control adecuado de accesos y la adopción de medidas que eviten la pérdida de información por factores tanto internos como externos.
- La seguridad de red se centra en resguardar las infraestructuras informáticas y la información que transita por ellas, utilizando firewalls para controlar el tráfico de datos y autenticación de usuarios para impedir accesos no autorizados (pp. 17-18).

Para el autor en mención los controles de acceso ofrecen ventajas clave para la protección integral de los sistemas informáticos, estas medidas no solo actúan en el ámbito digital, sino también físico y organizacional. Se analizan que una seguridad efectiva requiere el equilibrio entre tecnologías como firewalls o cifrado, y aspectos humanos y estructurales, como políticas claras y control físico. Así, se fortalece la defensa frente a riesgos diversos y crecientes.

Para Velásquez (2022) las tres principales mecanismos que presentan la mayores ventajas en el mercado y que se encuentran en la lucha por obtener la hegemonía en proveer los sistemas encargados de mejorar el nivel de seguridad de acceso en la infraestructura

- Descubre cada uno de los dispositivos que se conectan a la red y controla su comportamiento.
- Controla quién accede a la red y restringe el número de recursos con los que puede manejar.
- Adapta y configura la red dinámicamente y sin intervención humana.

- Detecta dispositivos infectados en la red.
- Optimiza el consumo energético de los dispositivos.
- Proporcionar protección de seguridad de punto final.
- Controla el acceso de usuarios no conocidos o que no tienen garantías de seguridad
- Está diseñada para permitir la verificación de la postura, el monitoreo del comportamiento y la remediación no solo de los puntos finales de los usuarios, sino también de los dispositivos de infraestructura que están continuamente conectados a la red.
- Garantiza que todos los puntos finales de la red cumplan con las políticas de seguridad (pp. 8-9).

Sin embargo, este otro autor menciona que los mecanismos modernos de control de acceso no solo protegen la red, sino que también gestionan su eficiencia y adaptabilidad. Estas tecnologías, al automatizar tareas como la detección de amenazas y la configuración dinámica, permiten una defensa proactiva. Además, analiza cómo la verificación constante de dispositivos y usuarios fortalece la seguridad, demostrando que la protección efectiva va más allá del control estático, exigiendo inteligencia y capacidad de respuesta en tiempo real.

2.2.4 Tipos de controles de acceso para puertas

Para Herrera (2025) con base en dichos marcos normativos y como parte del diseño técnico-experimental para su aplicación en entornos controlados, existen dos tipos:

- El Control de Acceso Basado en Roles (RBAC) asigna permisos a los usuarios según su rol dentro de la organización, agrupando privilegios por funciones específicas. Esto facilita la gestión del acceso y asegura que los usuarios solo interactúen con la información que les corresponde, protegiendo así los datos.
- El sistema de Control de Acceso Mandatorio (MAC) aplica restricciones mediante reglas definidas previamente, utilizando etiquetas de seguridad tanto para usuarios como para la información. El sistema permite establecer niveles de acceso determinados por criterios estrictos, bajo la supervisión de una autoridad central (pp. 2-3).

Este autor indica que los modelos RBAC y MAC representan enfoques estratégicos para gestionar el acceso a la información, el RBAC ofrece eficiencia operativa al vincular permisos con funciones laborales, mientras que el MAC prioriza el control riguroso bajo

criterios predefinidos. Este autor enfatiza que ambos modelos responden a necesidades distintas: uno enfocado en la funcionalidad y otro en la seguridad estricta, lo que evidencia la importancia de adaptar el control de acceso al contexto organizacional.

Según la propuesta de Pozo (2022) los tipos de control de acceso más comunes implementados hasta el momento de acuerdo a la necesidad de una empresa o grupo de trabajo apotran por algunas de estas opciones:

- El Control de Acceso Basado en Roles (RBAC) es uno de los métodos más empleados para gestionar permisos, ya que otorga el acceso a los usuarios según los roles que se les han asignado dentro de un sistema. Para reforzar la seguridad, se incorporan políticas adicionales que restringen la adquisición de privilegios innecesarios, manteniendo así un entorno más protegido.
- El Control de Acceso Discrecional (DAC) se basa en que el propietario de los datos tiene la autoridad para decidir quién puede acceder a ellos. Es decir, el acceso se concede según las reglas que el mismo dueño establece, permitiendo así un control flexible y personalizado sobre la información.
- El Control de Acceso Obligatorio (MAC) se caracteriza por ser más rígido que otros tipos, ya que el acceso a los usuarios se otorga siguiendo regulaciones estrictas establecidas por una autoridad central, ya sea dentro de una empresa o una organización reguladora.
- El Control de Acceso Basado en Atributos (ABAC) asigna acceso a los usuarios y recursos según una serie de atributos asociados, como el día, la hora, la ubicación y otros datos relevantes. Estos atributos permiten realizar evaluaciones dinámicas para determinar si se debe conceder o denegar el acceso (pp. 15-16).

Estas teorías demuestran que los sistemas de control de acceso no solo varían en su aplicación, sino también en el nivel de rigidez y adaptabilidad que ofrecen además reconocen que el RBAC es ampliamente usado por su eficiencia organizativa, mientras que el MAC garantiza mayor seguridad bajo autoridad central.

2.2.5 Tipos de cerraduras inteligentes

De acuerdo con Pérez (2021) en el mercado actual se encuentra una amplia variedad de cerraduras inteligentes que permite seleccionar conforme a las preferencias individuales.

A continuación, se describen las cerraduras inteligentes de mayor presencia en el mercado:

- Cerraduras de teclado digital: Se distingue por su notable popularidad en el mercado gracias a su favorable relación calidad-precio. Su funcionamiento se basa en la introducción de códigos numéricos o alfanuméricos que el usuario define previamente.
- Cerraduras electrónicas con mando: Se consideran las mejores del mercado, disfrutando de amplia aceptación en Europa. Resultan cómodas, económicas y ofrecen la posibilidad de abrir y cerrar puertas a distancia sin requerir permanecer junto a la puerta o manejar múltiples llaves que pueden resultar extraviadas.
- Cerraduras invisibles, Bluetooth o Wifi: Operan mediante tecnología inalámbrica, como Bluetooth u ondas Wifi, ejecutadas a través de una Tablet o teléfono móvil. El bloqueo y desbloqueo se efectúa mediante una aplicación que incorpora reconocimiento de voz, teclado alfanumérico o lector de huella dactilar que facilitan la identificación del usuario.
- Cerraduras electrónicas de huella dactilar: Representan las más vulnerables del mercado debido a la falsificación de huellas dactilares. No obstante, los fabricantes y proveedores proporcionan otros agregados para incrementar la seguridad, como la combinación de la huella con una contraseña o PIN (pp. 14-15).

Figura 4

Tipos y modelos de cerraduras inteligentes



Nota. La imagen presenta una colección representativa de diversos modelos de cerraduras inteligentes disponibles en el mercado actual, incluyendo cerraduras de teclado digital, sistemas con tecnología Bluetooth, dispositivos de huella dactilar y modelos híbridos que combinan múltiples métodos de acceso. Tomado de <https://controlacceso.net/cerraduras-electronicas/>

CAPÍTULO III: DISEÑO METODOLÓGICO

3.1 Tipo de investigación.

El enfoque mixto en la investigación constituye una estrategia que combina elementos cualitativos y cuantitativos dentro de un único estudio. Su objetivo principal radica en aprovechar las fortalezas de ambos enfoques para alcanzar una comprensión más profunda y completa del fenómeno investigado. Esta metodología involucra la recolección y análisis de datos tanto cuantitativos como cualitativos de manera simultánea o mediante fases sucesivas (Zúñiga et al., 2023, p. 9728).

El enfoque mixto representa el método ideal para desarrollar las investigaciones, dado que requiere de evidencia que genere soluciones acertadas en beneficio de los actores sociales. Las problemáticas contemporáneas presentan características complejas que únicamente pueden ser abordadas mediante datos tanto medibles como interpretables de forma conjunta (Albayero et al., 2020, p. 49).

El estudio adopta un enfoque mixto el cual mediante encuestas se recabó la percepción y necesidades de docentes; entrevistas profundizaron en criterios técnicos, económicos y de usabilidad, la observación directa en los laboratorios permitió determinar los requisitos que se necesitan para implementar el sistema de reconocimiento biométrico para el control de acceso en los laboratorios del área técnica de la ULEAM-Chone.

3.2 Métodos de investigación.

El método deductivo se emplea para establecer relaciones entre el contenido curricular y el mundo real. Esta aproximación constituye una vía alterna que facilita organizar los nuevos conceptos, lo cual permite un mayor acercamiento a la realidad de los hechos o fenómenos que se encuentran en estudio (Espinoza, 2023, p. 36).

“El rol del método inductivo en las teorías conductistas se encuentra centrado en los procesos de observación de comportamientos específicos de los sujetos investigados y la posterior formulación de generalizaciones derivadas de dichas observaciones particulares” (López et al., 2025, p. 63).

“El método analítico consiste en la descomposición del objeto que se pretende indagar con la finalidad de lograr exponer sus componentes más simples y de mayor facilidad para concebir durante el proceso investigativo” (Herszenbaun, 2022, p. 94). “El método

bibliográfico se encuentra enfocado a examinar diversas teorías que han sido registradas en múltiples libros y revistas indexadas de carácter académico” (Alcivar, 2020, p. 511).

Se emplearon diversos métodos para sustentar el estudio, el primero el método deductivo permitió partir de teorías generales sobre sistemas biométricos para aplicarlas al contexto específico de los laboratorios del área técnica. El segundo el método inductivo facilitó la interpretación de los datos recolectados mediante encuesta, entrevista y observación, generando conclusiones a partir de la experiencia empírica.

El tercero el método analítico se utilizó para descomponer e interpretar detalladamente la información técnica y contextual. Finalmente, el método bibliográfico respaldó el marco teórico y conceptual, mediante la revisión de fuentes científicas relacionadas con el reconocimiento biométrico y el control de acceso.

3.3 Técnicas, herramientas e instrumentos.

3.3.1 Técnicas.

“La encuesta constituye una herramienta de investigación que se ejecuta a través de un instrumento denominado cuestionario. Esta técnica se encuentra direccionada exclusivamente hacia personas y facilita la obtención de información relevante acerca de sus opiniones, comportamientos y percepciones particulares”(Arias, 2021, p. 81).

Las entrevistas constituyen documentos que contienen preguntas y temas destinados a guiar las conversaciones investigativas, ya sean estructuradas o semiestructuradas. Este método se encuentra ampliamente utilizado para recopilar datos cualitativos y obtener información detallada sobre una variedad de temas de investigación (Zúñiga et al., 2023, p. 9745).

Se desarrollaron dos técnicas de recolección de información que permitieron una comprensión integral del problema. En primer lugar, se aplicó una encuesta estructurada a 217 estudiantes que conforman la población del área técnica, con el objetivo de conocer su percepción respecto a la implementación de un sistema de reconocimiento biométrico.

En segundo lugar, se llevó a cabo una entrevista semiestructurada con la directora del área técnica, lo que permitió profundizar en aspectos administrativos, operativos y técnicos relacionados con el control de acceso.

3.3.2 Herramientas.

Las herramientas metodológicas constituyen el conjunto de técnicas e instrumentos que se utilizan en investigación con el fin de analizar el objeto de estudio. La selección y ejecución de estas herramientas depende del tipo de método que se adapte de manera óptima al fenómeno que se desea abordar (Granados, 2020, p. 504). “Las herramientas son los medios de recolección físicos o digitales tales como fichas, grabadoras, filmadoras, cámaras fotográficas” (Urréa et al., 2022, p. 206).

Se utilizaron recursos tecnológicos accesibles para facilitar la recolección de datos. La encuesta fue aplicada mediante formularios de Google, lo que permitió recopilar y organizar la información de manera eficiente. La entrevista a la directora del área técnica fue grabada con un teléfono celular, garantizando el registro fiel de las respuestas. Asimismo, durante la observación, se utilizó el celular como cámara fotográfica para documentar visualmente las condiciones físicas de los laboratorios, en especial las puertas y las instalaciones eléctricas

3.3.3 Instrumentos.

El cuestionario representa una modalidad específica de la técnica de encuesta, que se caracteriza por formular un conjunto organizado de preguntas de carácter escrito en una cédula. Estas interrogantes mantienen estrecha relación con la hipótesis del estudio y, consecuentemente, con las variables e indicadores que guían la investigación científica (Urréa et al., 2022, p. 174).

La guía de entrevista representa un instrumento que se presenta en formato de documento, cuyo fin principal consiste en recolectar información de la persona entrevistada para el estudio. Este recurso puede ejecutarse de forma manual o computarizada y únicamente permite ser editada por el investigador, razón por la cual el entrevistado no debe maniobrarla durante el proceso investigativo (Arias, 2021, p. 95).

3.4 Análisis y presentación de resultados.

3.4.1 Resultados de la encuesta

La encuesta fue aplicada a la población compuesta por 217 estudiantes con el propósito de obtener ciertas características para la implantación reconocimiento biométrico para el control de acceso en los laboratorios del área técnica, muestran los siguientes resultados:

Tabla 1

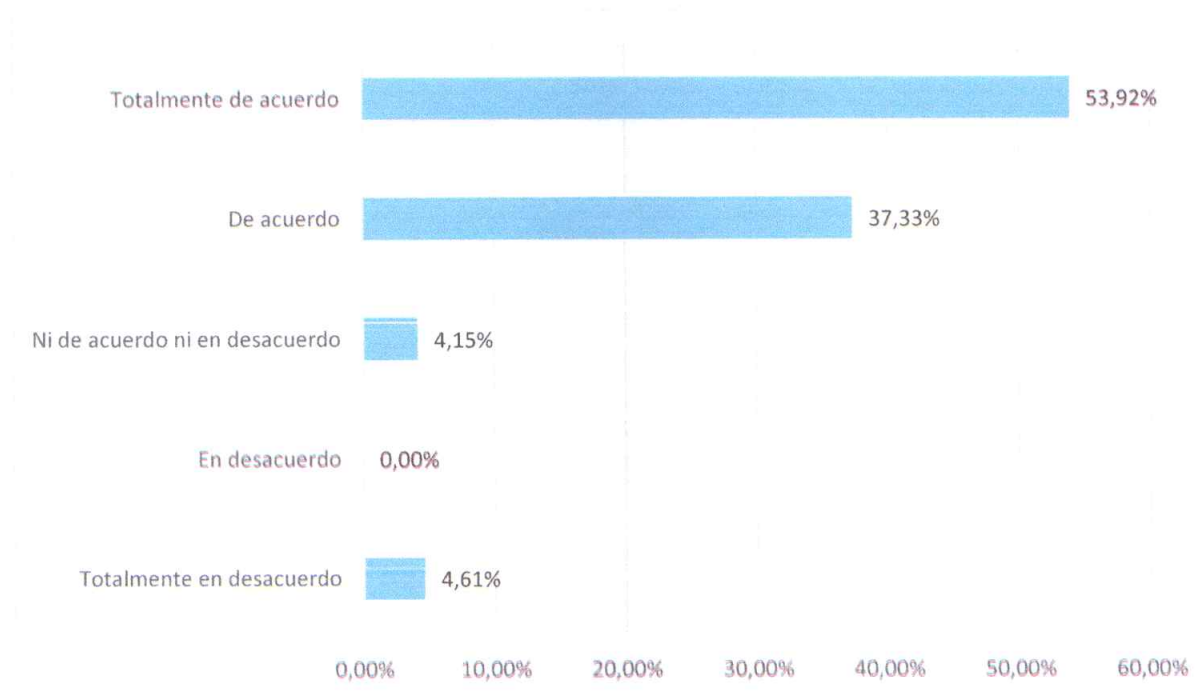
¿Considera importante mejorar el control de acceso en los laboratorios del área técnica?

Respuesta	Frecuencia	Porcentaje
Totalmente en desacuerdo	10	4,61%
En desacuerdo	0	0,00%
Ni de acuerdo ni en desacuerdo	9	4,15%
De acuerdo	81	37,33%
Totalmente de acuerdo	117	53,92%
Total	217	100,00%

Nota. Esta tabla muestra los resultados de la pregunta 1.

Gráfico 1

Representación gráfica de los resultados de la pregunta 1 de la encuesta



Análisis e interpretación: El análisis evidencia que la mayoría de los participantes considera importante mejorar el control de acceso en los laboratorios del área técnica. Se observa que el 91,25 % manifiesta estar de acuerdo o totalmente de acuerdo, lo que refleja una percepción ampliamente favorable hacia la implementación de mejoras, como el reconocimiento biométrico.

Tabla 2

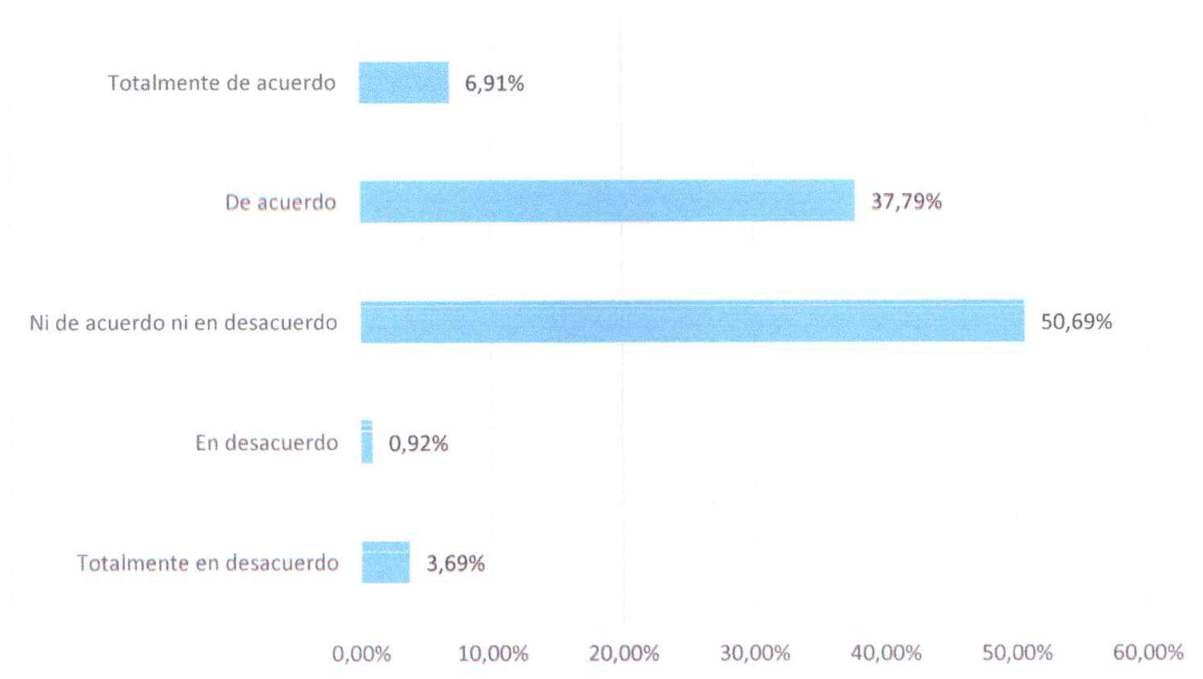
¿El uso de un sistema de reconocimiento biométrico (huella o rostro) facilitará el ingreso a los laboratorios?

Respuesta	Frecuencia	Porcentaje
Totalmente en desacuerdo	8	3,69%
En desacuerdo	2	0,92%
Ni de acuerdo ni en desacuerdo	110	50,69%
De acuerdo	82	37,79%
Totalmente de acuerdo	15	6,91%
Total	217	100,00%

Nota. Esta tabla muestra los resultados de la pregunta 2.

Gráfico 2

Representación gráfica de los resultados de la pregunta 2 de la encuesta



Análisis e interpretación: El análisis muestra que la percepción sobre la facilidad de ingreso mediante un sistema de reconocimiento biométrico es mayoritariamente neutral. Se identifica que el 50,69 % se mantiene ni de acuerdo ni en desacuerdo, lo que sugiere falta de experiencia previa o incertidumbre frente a su uso. Sin embargo, un 44,70 % expresa acuerdo o total acuerdo, evidenciando una tendencia positiva hacia esta tecnología. El bajo porcentaje

de desacuerdo indica que el sistema no genera resistencia significativa y se percibe como una alternativa potencialmente favorable.

Tabla 3

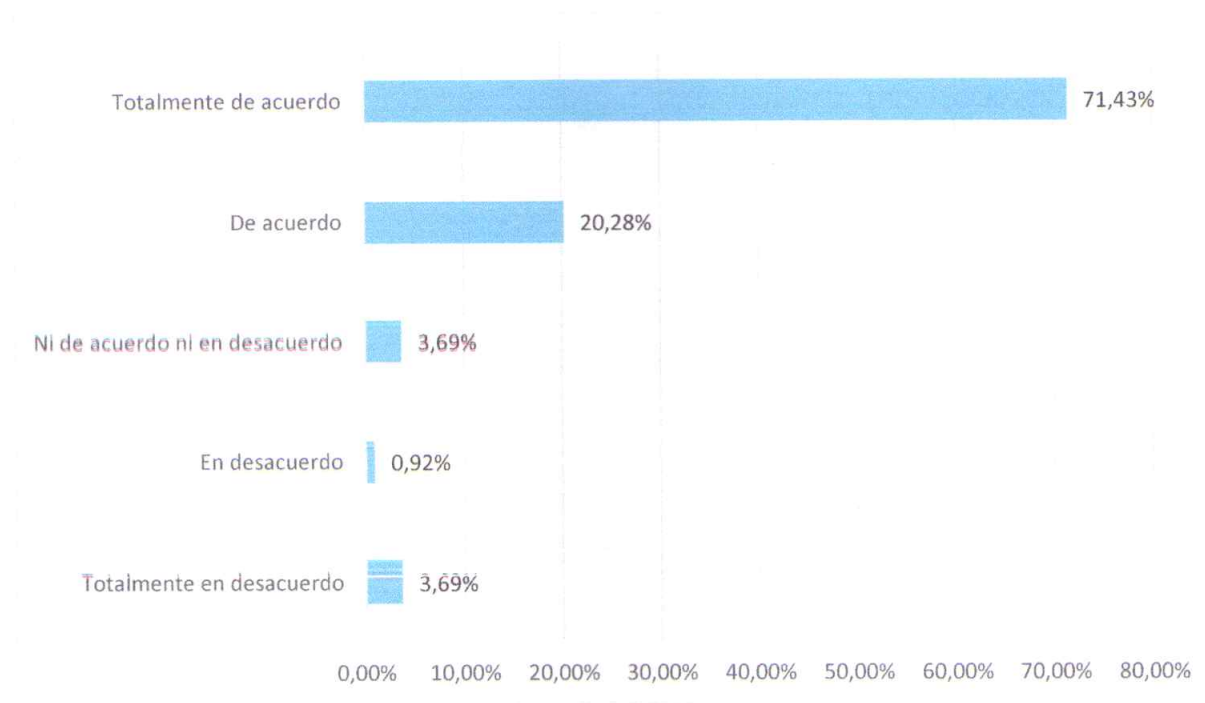
¿La implementación de un sistema biométrico aumentara la seguridad dentro de los laboratorios?

Respuesta	Frecuencia	Porcentaje
Totalmente en desacuerdo	8	3,69%
En desacuerdo	2	0,92%
Ni de acuerdo ni en desacuerdo	8	3,69%
De acuerdo	44	20,28%
Totalmente de acuerdo	155	71,43%
Total	217	100,00%

Nota. Esta tabla muestra los resultados de la pregunta 3.

Gráfico 3

Representación gráfica de los resultados de la pregunta 3 de la encuesta



Análisis e interpretación: El análisis evidencia que la implementación de un sistema biométrico incrementa la percepción de seguridad dentro de los laboratorios. Se observa que el 91,71 % de los encuestados se encuentra de acuerdo o totalmente de acuerdo, lo que refleja una alta confianza en este tipo de tecnología para el control de acceso. Los niveles de desacuerdo y neutralidad son mínimos, lo que indica una aceptación generalizada. Estos resultados

muestran que el sistema biométrico se percibe como una solución eficaz para fortalecer la seguridad y proteger los recursos del área técnica.

Tabla 4

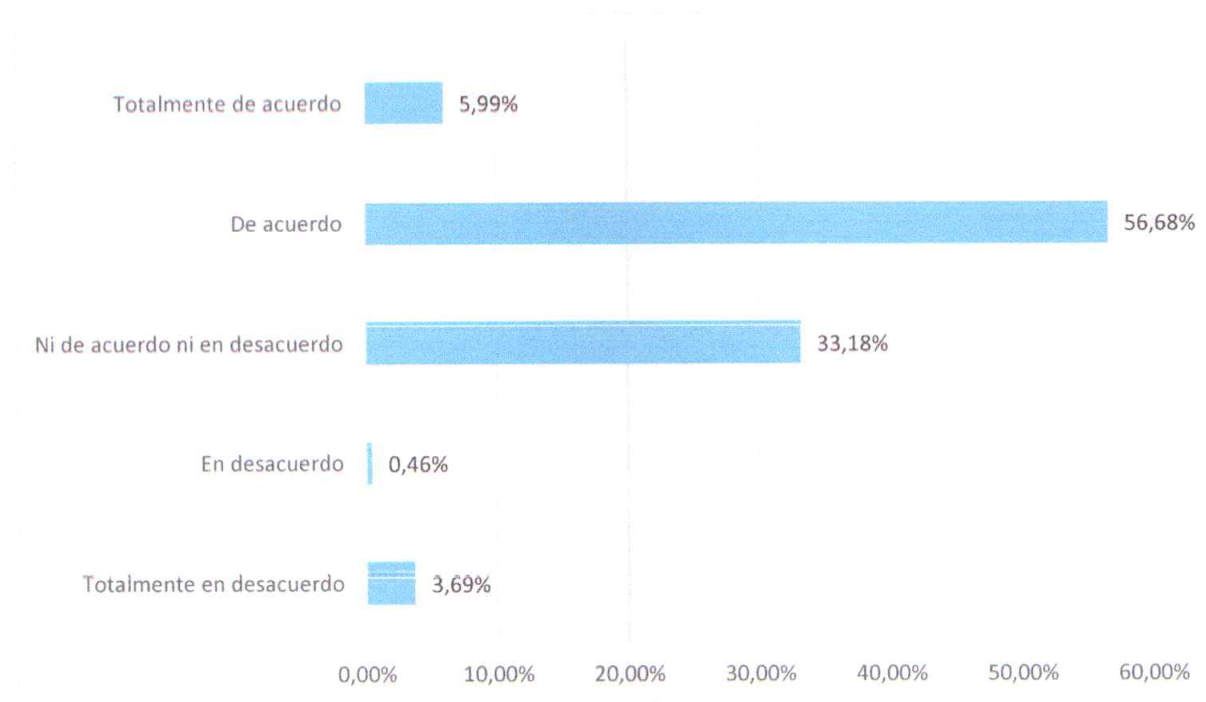
¿Se sentiría cómodo(a) utilizando un sistema de reconociendo biométrico para ingresar a los laboratorios?

Respuesta	Frecuencia	Porcentaje
Totalmente en desacuerdo	8	3,69%
En desacuerdo	1	0,46%
Ni de acuerdo ni en desacuerdo	72	33,18%
De acuerdo	123	56,68%
Totalmente de acuerdo	13	5,99%
Total	217	100,00%

Nota. Esta tabla muestra los resultados de la pregunta 4.

Gráfico 4

Representación gráfica de los resultados de la pregunta 4 de la encuesta



Análisis e interpretación: El análisis indica que la mayoría de los participantes se siente cómoda utilizando un sistema de reconocimiento biométrico para el ingreso a los laboratorios. Se observa que el 62,67 % manifiesta estar de acuerdo o totalmente de acuerdo, lo que evidencia una aceptación mayoritaria de esta tecnología. No obstante, un 33,18 %

mantiene una postura neutral, lo que sugiere cautela o necesidad de mayor información. Los niveles de desacuerdo son bajos, reflejando una percepción generalmente positiva y confiable.

Tabla 5

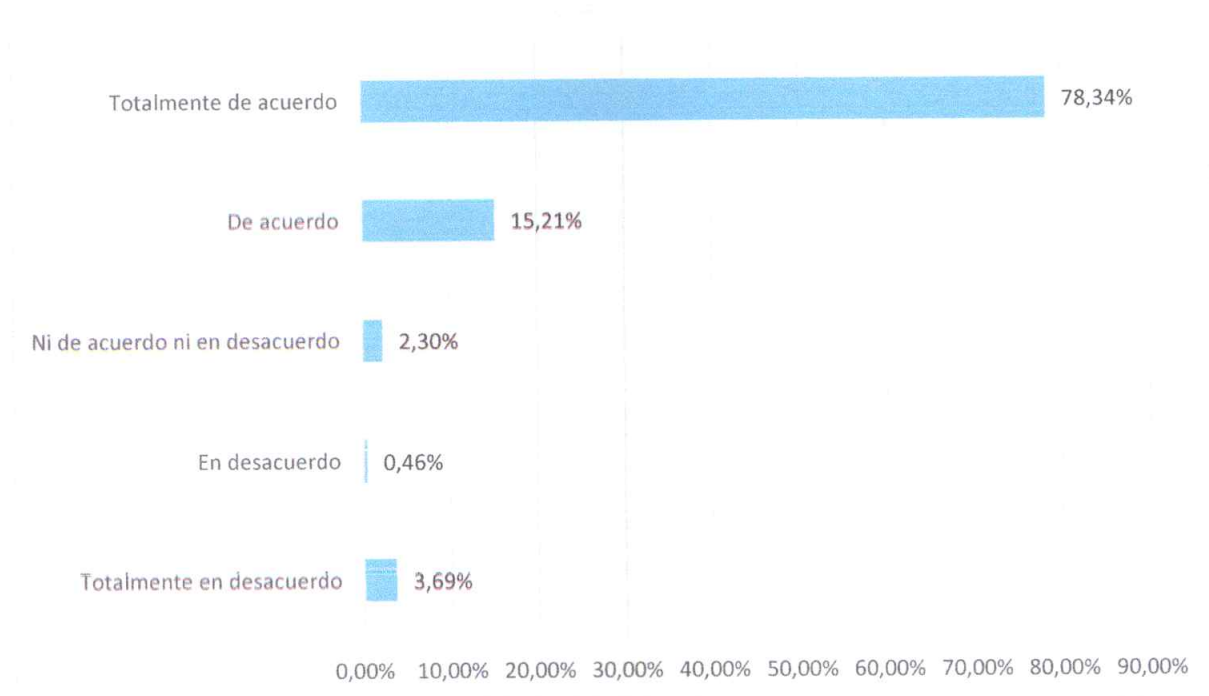
¿Considera que la información biométrica debe ser tratada con confidencialidad y seguridad?

Respuesta	Frecuencia	Porcentaje
Totalmente en desacuerdo	8	3,69%
En desacuerdo	1	0,46%
Ni de acuerdo ni en desacuerdo	5	2,30%
De acuerdo	33	15,21%
Totalmente de acuerdo	170	78,34%
Total	217	100,00%

Nota. Esta tabla muestra los resultados de la pregunta 5.

Gráfico 5

Representación gráfica de los resultados de la pregunta 5 de la encuesta



Análisis e interpretación: El análisis demuestra que existe una clara conciencia sobre la importancia de la confidencialidad y seguridad de la información biométrica. Se evidencia que el 93,55 % de los encuestados está de acuerdo o totalmente de acuerdo con que estos datos

deben ser protegidos adecuadamente. Los porcentajes de neutralidad y desacuerdo son mínimos, lo que refleja una postura sólida frente a la protección de la información sensible. Estos resultados indican una alta valoración de la privacidad y la necesidad de aplicar medidas de seguridad en la gestión de datos biométricos.

Tabla 6

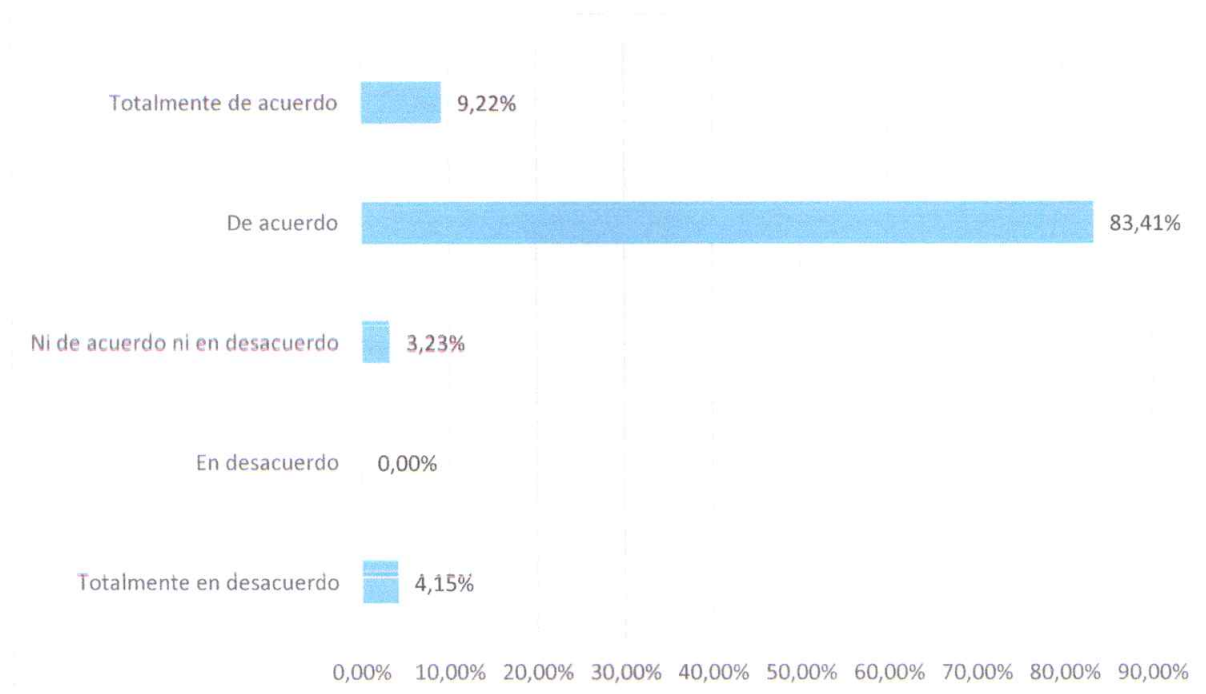
¿El sistema biométrico reduciría el ingreso no autorizado de personas a los laboratorios?

Respuesta	Frecuencia	Porcentaje
Totalmente en desacuerdo	9	4,15%
En desacuerdo	0	0,00%
Ni de acuerdo ni en desacuerdo	7	3,23%
De acuerdo	181	83,41%
Totalmente de acuerdo	20	9,22%
Total	217	100,00%

Nota. Esta tabla muestra los resultados de la pregunta 6.

Gráfico 6

Representación gráfica de los resultados de la pregunta 6 de la encuesta



Análisis e interpretación: El análisis evidencia que existe una percepción ampliamente positiva respecto a la capacidad del sistema biométrico para reducir el ingreso no autorizado a los laboratorios. Se observa que el 92,63 % de los encuestados se encuentra de acuerdo o

totalmente de acuerdo, lo que refleja una alta confianza en la efectividad de esta tecnología como mecanismo de control de acceso. Los niveles de neutralidad y desacuerdo son mínimos, lo que indica una aceptación generalizada y la expectativa de un mayor control y seguridad en los laboratorios.

Tabla 7

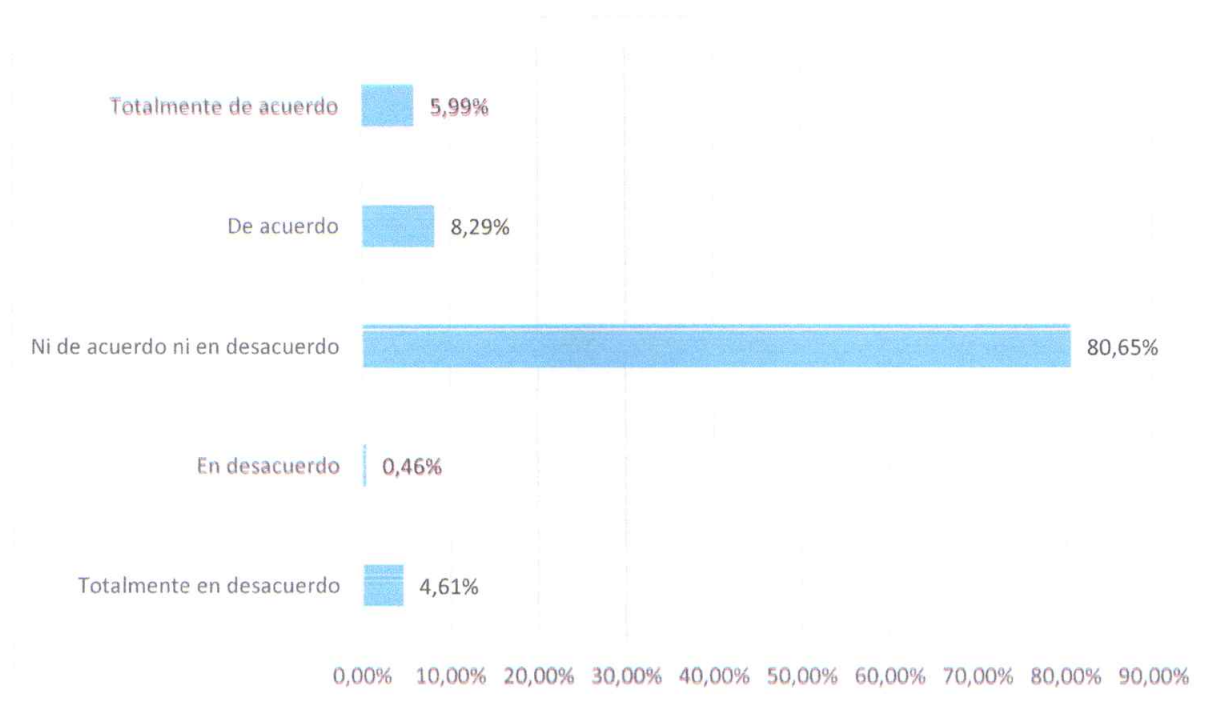
¿Cree que la instalación de este sistema no afectará negativamente las actividades académicas?

Respuesta	Frecuencia	Porcentaje
Totalmente en desacuerdo	10	4,61%
En desacuerdo	1	0,46%
Ni de acuerdo ni en desacuerdo	175	80,65%
De acuerdo	18	8,29%
Totalmente de acuerdo	13	5,99%
Total	217	100,00%

Nota. Esta tabla muestra los resultados de la pregunta 7.

Gráfico 7

Representación gráfica de los resultados de la pregunta 7 de la encuesta



Análisis e interpretación: El análisis muestra que la mayoría de los encuestados mantiene una postura neutral respecto a si la instalación del sistema biométrico no afectará negativamente las actividades académicas. Se observa que el 80,65 % se ubica en una posición

ni de acuerdo ni en desacuerdo, lo que sugiere incertidumbre o falta de información sobre su impacto real. Sin embargo, un 14,28 % expresa acuerdo o total acuerdo, evidenciando una percepción moderadamente positiva. Los niveles de desacuerdo son bajos, lo que indica que no se anticipan afectaciones significativas.

Tabla 8

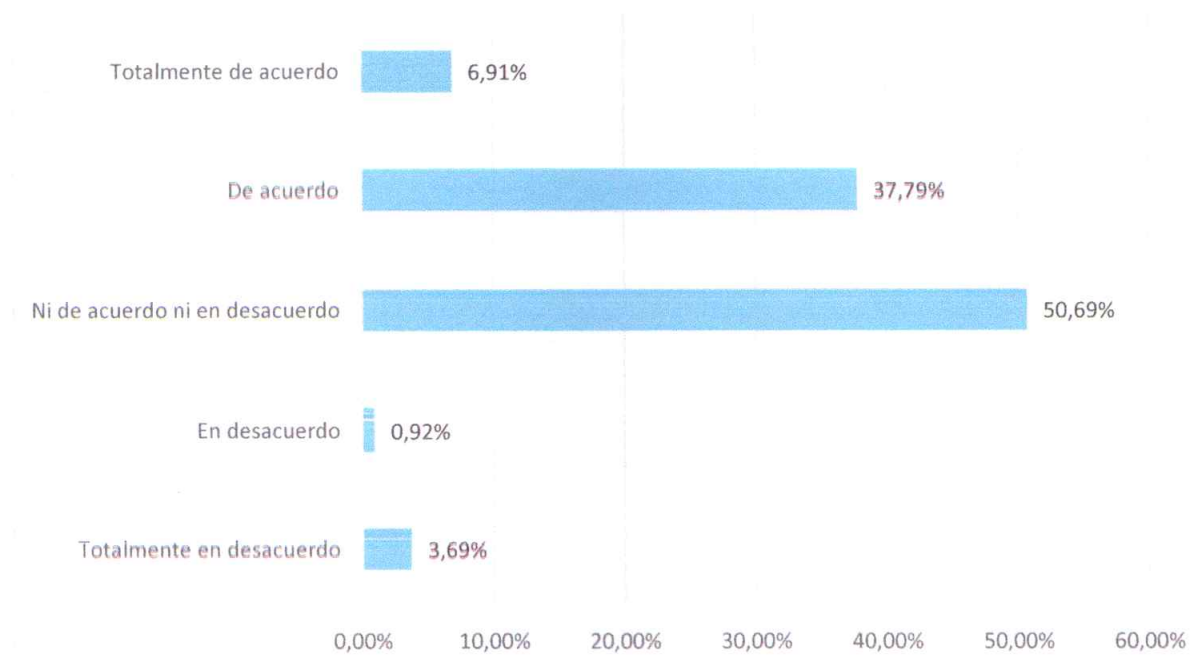
¿En general se sentiría de acuerdo con la implementación del reconocimiento biométrico en los laboratorios del área técnica?

Respuesta	Frecuencia	Porcentaje
Totalmente en desacuerdo	8	3,69%
En desacuerdo	2	0,92%
Ni de acuerdo ni en desacuerdo	110	50,69%
De acuerdo	82	37,79%
Totalmente de acuerdo	15	6,91%
Total	217	100,00%

Nota. Esta tabla muestra los resultados de la pregunta 8.

Gráfico 8

Representación gráfica de los resultados de la pregunta 8 de la encuesta



Análisis e interpretación: El análisis refleja que, en términos generales, la aceptación de la implementación del reconocimiento biométrico en los laboratorios del área técnica es

moderada. Se evidencia que el 44,70 % de los encuestados se encuentra de acuerdo o totalmente de acuerdo, lo que muestra una disposición favorable hacia su adopción. No obstante, el 50,69 % mantiene una posición neutral, lo que sugiere necesidad de mayor socialización o información sobre el sistema. Los niveles de desacuerdo son bajos, indicando ausencia de rechazo significativo.

3.4.2 Resultados de la entrevista

La directora de carreras del Área Técnica de la Universidad Laica Eloy Alfaro de Manabí extensión chone, se presenta esta entrevista con el propósito de analizar la viabilidad y pertinencia de implementar un sistema de reconocimiento biométrico para el control de acceso a los laboratorios del área técnica, dentro de los datos más importantes tenemos:

Los aspectos más relevantes son la confiabilidad y precisión del dispositivo, la seguridad en el tratamiento de los datos biométricos, la facilidad de uso y la rapidez en la autenticación. Además, se considera fundamental la compatibilidad con la infraestructura tecnológica existente, el soporte técnico, el costo-beneficio y el cumplimiento de normas de protección de datos para garantizar un uso eficiente y responsable en el entorno universitario.

El método manual actual limita la trazabilidad y verificación de usuarios autorizados, se han registrado casos de ingreso no autorizado fuera de horarios académicos, lo que expone vulnerabilidades en la protección de equipos e información. Esta situación demuestra la necesidad urgente de fortalecer los mecanismos de seguridad mediante soluciones tecnológicas automatizadas.

Los beneficios incluyen mejor control de accesos, registro preciso de uso y fortalecimiento de la responsabilidad institucional. La aceptación del sistema requiere socialización y capacitación transparente con la comunidad universitaria para garantizar su adopción efectiva.

El análisis conjunto de las respuestas evidencia que el control de acceso actual a los laboratorios del área técnica resulta limitado para garantizar una seguridad integral. La existencia de ingresos no autorizados, aunque ocasionales, demuestra debilidades en los mecanismos vigentes. Esto justifica la necesidad de implementar soluciones tecnológicas que mejoren la trazabilidad, protección de equipos y resguardo de la información académica.

Las respuestas reflejan que la implementación de un sistema biométrico aportaría beneficios clave como mayor seguridad, control eficiente y uso responsable de los laboratorios. Asimismo, se reconoce la importancia de considerar la privacidad y de involucrar a la comunidad universitaria mediante capacitación y socialización, lo que favorecería la aceptación del sistema y su adecuada integración en las actividades académicas.

CAPÍTULO IV: EJECUCIÓN DEL PROYECTO

4.1 Descripción del proyecto

Este proyecto llamado reconocimiento biométrico para el control de acceso en los laboratorios del área técnica de la universidad laica Eloy Alfaro de Manabí extensión Chone tiene como objetivo ser implementado en los laboratorios de la institución esto debido a la falta de eficiencia en el sistema actual que es una cerradura normal que se abre a través de una llave, al cambiar la cerradura convencional por un dispositivo de acceso biométrico ya sea huella o reconocimiento facial garantizamos un acceso seguro y eficiente de manera que no dependeremos de una tercera persona para lograr tener acceso a los laboratorios.

El proyecto reconocimiento biométrico para el control de acceso en los laboratorios del área técnica de la Universidad Laica Eloy Alfaro de Manabí se plantea como una alternativa innovadora y necesaria frente a las limitaciones del sistema de acceso actual, el cual se basa en cerraduras convencionales accionadas mediante llaves físicas. Este método presenta deficiencias en términos de seguridad, control y eficiencia, ya que depende de terceros para el ingreso y no permite un registro preciso de las personas que acceden a los laboratorios.

La implementación de un sistema biométrico ya sea mediante reconocimiento de huella dactilar o reconocimiento facial, permitirá garantizar un acceso más seguro, confiable y eficiente, reduciendo el riesgo de ingresos no autorizados y fortaleciendo la protección de los equipos y la información académica. Además, este sistema facilitará la gestión autónoma del acceso, optimizando los tiempos de ingreso y eliminando la dependencia de llaves físicas.

De esta manera, la institución avanza hacia la modernización de sus procesos, promueve el uso responsable de los recursos tecnológicos y consolida un entorno académico más seguro y acorde con las exigencias actuales de innovación y transformación digital.

4.2 Determinación de recursos

4.2.1 Humanos

Para la ejecución del proyecto reconocimiento biométrico para el control de acceso en los laboratorios del área técnica de la Universidad Laica Eloy Alfaro de Manabí, se determinan los siguientes recursos humanos y de apoyo:

Tutor de titulación: responsable de la orientación académica, supervisión metodológica, validación de resultados y seguimiento del cumplimiento de los objetivos del proyecto.

Dos estudiantes investigadores: encargados del diseño, desarrollo e implementación del sistema biométrico, así como del levantamiento de información, pruebas, documentación técnica y elaboración del informe final.

4.2.2 Materiales

La implementación de un sistema de reconocimiento biométrico para el control de acceso en los laboratorios del área técnica de la Universidad Laica Eloy Alfaro de Manabí constituye una estrategia orientada a fortalecer la seguridad, optimizar la gestión de los espacios académicos y garantizar el uso adecuado de los recursos tecnológicos.

Este sistema reemplaza los mecanismos tradicionales de acceso, permitiendo una autenticación segura mediante huella dactilar o reconocimiento facial, reduciendo el ingreso no autorizado y facilitando un control eficiente, autónomo y acorde con los procesos de modernización institucional.

Listado de materiales

La implementación de un sistema de reconocimiento biométrico para el control de acceso en los laboratorios del área técnica de la Universidad Laica Eloy Alfaro de Manabí constituye una estrategia orientada a fortalecer la seguridad, optimizar la gestión de los espacios académicos y garantizar el uso adecuado de los recursos tecnológicos.

Este sistema reemplaza los mecanismos tradicionales de acceso, permitiendo una autenticación segura mediante huella dactilar o reconocimiento facial, reduciendo el ingreso no autorizado y facilitando un control eficiente, autónomo y acorde con los procesos de modernización institucional.

- Cerradura eléctrica o electroimán para control de puertas.
- Fuente de alimentación regulada.
- Cableado eléctrico y de red (UTP).
- Router o switch de red.
- Computador para configuración y monitoreo del sistema.
- Software de reconocimiento biométrico.
- Base de datos para almacenamiento seguro de registros.
- Soportes, anclajes y materiales de instalación.
- Herramientas básicas (destornilladores, taladro, multímetro).

4.2.3 Económicos

La siguiente tabla presenta la estimación de los recursos económicos necesarios para la implementación de una cerradura con reconocimiento facial en los laboratorios del área técnica de la Universidad Laica Eloy Alfaro de Manabí.

Los valores considerados son referenciales y se basan en precios promedio del mercado, principalmente de la plataforma Amazon. Esta estimación permite visualizar el presupuesto requerido para la adquisición e instalación del sistema biométrico, asegurando una planificación financiera adecuada y la viabilidad del proyecto.

Tabla 9
Recursos económicos

Ítem	Descripción	Cantidad	Precio unitario (USD)	Costo total (USD)
1	Cerradura inteligente con reconocimiento facial	4	377.87,00	1511,48
2	Fuente de alimentación / baterías recargables	1	25,00	25,00

Ítem	Descripción	Cantidad	Precio unitario (USD)	Costo total (USD)
3	Materiales de instalación (cables, tornillos, soportes)	1	20,00	20,00
4	Mano de obra para instalación técnica	1	40,00	40,00
Total estimado				1596,48

Nota: Los valores son referenciales, tomados como referencia de precios promedio en Amazon, y pueden variar según marca, proveedor y disponibilidad. La inversión se enfoca directamente en la adquisición e instalación de la cerradura biométrica con reconocimiento facial.

4.3 Etapas de ejecución del proyecto

la propuesta integral para diseñar, instalar y validar un sistema de control de acceso basado en reconocimiento facial en los laboratorios del área técnica de la Universidad Laica Eloy Alfaro de Manabí – Extensión Chone. El objetivo general es incrementar la seguridad física, trazabilidad y gestión de accesos, reduciendo riesgos de uso no autorizado y mejorando la operación académica. La solución se desarrollará en cinco fases: Fase Introductoria, Fase I (evaluación actual del sitio), Fase II (diseño), Fase III (instalación) y Fase IV (pruebas y registros).

Beneficios esperados:

- Trazabilidad de ingresos/egresos por usuario con registros auditables.
- Reducción de riesgo por pérdida/duplicado de llaves y códigos compartidos.
- Escalabilidad para integrar nuevos laboratorios y perfiles temporales (docentes, estudiantes, mantenimiento).
- Cumplimiento de buenas prácticas de seguridad física y protección de datos personales (LOPD).

Los laboratorios con puertas de madera en condiciones genéricas aptas para la instalación de cerraduras o terminales de control de acceso con reconocimiento facial. Se plantea un enfoque por etapas para asegurar una implantación ordenada y segura, con pilotos iniciales en 1–2 laboratorios y posterior despliegue total.

Criterios de éxito:

- Tasa de verificación facial $\geq 98\%$ en escenarios de iluminación típica del campus.
- Disponibilidad del servicio $\geq 99\%$ en horario académico.
- Registros de acceso íntegros y exportables (CSV/Excel) para auditoría.
- Políticas y consentimientos de tratamiento de datos biométricos vigentes.

4.3.1 Fase I: Situación actual del sitio

Situación actual (insumo provisto): El área técnica cuenta con 4 laboratorios con puertas de madera con características genéricas, aptas para la colocación de cerraduras con reconocimiento facial.

Levantamiento en sitio (checklist sugerido)

- Medición de espesor de puerta (típico 35–50 mm) y tipo de herraje actual (cerrojo, embutida, manija).
- Verificación de holguras, escuadras y sentido de apertura para compatibilidad con modelos seleccionados.
- Disponibilidad de conectividad (Wi-Fi 2.4 GHz) y calidad de señal en cada laboratorio.
- Revisión eléctrica (tomacorrientes cercanos para carga/servicio, aunque la mayoría de las cerraduras son batería).
- Riesgos de entorno: polvo de talleres, vibraciones, humedad; definir necesidad de IP65 o mayores.
- Puntos de montaje para placas de cierre/contrachapa y necesidad de carpintería menor.

Descripción de los laboratorios

El área técnica cuenta con cuatro laboratorios, los cuales presentan las siguientes características generales:

- Puertas de madera estándar.
- Cerraduras mecánicas convencionales.
- Uso compartido por docentes y estudiantes.
- Horarios de acceso definidos, pero sin control automatizado.

- Ausencia de registro digital de ingresos.

Elementos de control

- El sistema actual de control de acceso presenta limitaciones como:
 - Uso de llaves físicas susceptibles a pérdida o duplicación.
 - Dificultad para controlar accesos fuera de horario.
 - Falta de trazabilidad de usuarios.
 - Riesgo de accesos no autorizados.

4.3.2 Fase II: Diseño de la implementación

Metodología propuesta

- Marco de trabajo: enfoque híbrido (PMI/ágil) con entregables por hito: diseño, piloto, despliegue, cierre.
- Principio “privacy by design”: datos biométricos encriptados, preferible almacenamiento local en dispositivo cuando sea posible, mínima captura de datos.
- Pruebas incrementales: laboratorio piloto → validación de UX y tasa de acierto → réplica controlada al resto.

Arquitectura y alternativas

- Alternativa A – Cerraduras todo en uno con reconocimiento facial: reemplazan el cerrojo/manija y operan con batería; algunas incluyen cámara/timbre y Wi-Fi. Recomendadas para puertas individuales de madera, con instalación no invasiva.
- Alternativa B – Terminal facial + contrachapa/magnético: un terminal biométrico controla una contrachapa eléctrica o chapa magnética. Recomendado cuando se requiere integración con sistemas de control centralizado. (Mayor complejidad de instalación eléctrica).

Selección comparativa de equipos

Tabla 10

Comparación de equipos propuestos

Modelo	Métodos de desbloqueo	Cámara/Timbre	Conectividad	Grado IP	Precio
		e	d		

Lockly Visage Zeno Series (cerrojo)	Reconocimiento facial, huella, Apple Home Key, PIN, app, llave	No cámara integrada (sí teclado PIN Genie)	Wi-Fi integrado; Apple Home	IP65 (módulo exterior)	US\$349.00
EZVIZ DL50FVS (mortise 6068)	3D facial, PIN, tarjeta, llave, app; intercom	Sí cámara / timbre; visión nocturna	App EZVIZ; Wi-Fi	No especificado	US\$377.87
Aqara Smart Door Lock D200i	3D facial, NFC, PIN; Apple Home Key	No (modelo de cerradura sin video)	Compat. Apple Home Key; NFC	No especificado	US\$708.66
Jacchozhi 3D Face Recognition (con cámara, 4" pantalla)	3D facial, palma, huella, PIN, tarjeta, app, llave	Sí cámara + timbre	Wi-Fi 2.4 GHz; app	No especificado	US\$320.85
COYIVI Smart Lock 3D Facial	Reconocimiento facial 3D, huella, PIN, tarjeta, app, llave (hasta 8 métodos)	No indicado	Tuya/Smart Life (según listado)	No especificado	US\$100.30

Nota: Los precios y especificaciones son referenciales y pueden variar por vendedor/región. Se recomienda validar disponibilidad y compatibilidad de mortajas/cerrojos antes de la compra. Valores son referencia de Amazon.

Recomendación técnica

- Para puertas de madera estándar con cerrojo: Lockly Visage (por robustez, IP65 y ecosistema Apple Home Key) o EZVIZ DL50FVS (cuando se requiera video/intercom).
- Para integración con Apple/HomeKit sin facial en cámara: Aqara D200i (3D facial con Apple Home Key).

Distribución de conexiones y consideraciones

- Alimentación: batería Li-ion recargable (según modelo). Prever plan de recarga trimestral y power bank para emergencia (puerto USB-C).
- Red: Wi-Fi 2.4 GHz estable para notificaciones remotas y gestión. Levantamiento de cobertura y, de ser necesario, instalación de APs en pasillos.

- Señalética y ruta de evacuación: la cerradura no debe impedir salidas de emergencia desde interior. Verificar normativa de seguridad y dispositivos antipánico en puertas con flujo alto.

Cumplimiento Ley Orgánica de Protección de Datos de Carácter Personal

- Definir base legal del tratamiento (consentimiento informado y específico para estudiantes/visitantes; políticas institucionales).
- Minimización: almacenar plantillas biométricas cifradas en el dispositivo (“on-device”) cuando el fabricante lo permita; limitar tiempos de retención de logs.
- Nombrar responsable y delegado de protección de datos.

4.3.3 Fase III procedimientos para la instalación

Antes de iniciar la instalación física, se completaron actividades preparatorias en cada laboratorio. El primer paso consiste en verificar que las puertas abran y cierren correctamente sin rozamientos. Se ajustaron bisagras y marcos según sea necesario.

Se identificaron y marcaron las rutas de cableado eléctrico y de datos. Se tomaron medidas precisas para calcular longitudes exactas de materiales. Se verificaron que no existan obstrucciones ocultas en paredes o techos que impidan el paso de cables.

Procedimiento estándar por puerta (resumen):

- a) Verificación de compatibilidad de espesor y backset; retirar herraje existente.
- b) Marcado y perforación (si aplica) para mortaja/cerrojo según plantilla del fabricante.
- c) Montaje de cuerpo exterior/interior y alineación con cerradero; ajuste de pestillo.
- d) Encendido, actualización de firmware (si aplica), y configuración inicial (zona horaria, Wi-Fi).
- e) Alta de administradores; enrolamiento piloto (5–10 usuarios) y pruebas funcionales.
- f) Enrolamiento masivo (por grupos/laboratorios) con horarios y permisos diferenciados.
- g) Documentación fotográfica de la instalación y entrega de actas de conformidad.

Herramientas y materiales: taladro, brocas para madera/metal, formón para embutir (si aplica), destornilladores, nivel, plantilla del fabricante, baterías, power bank para carga de emergencia, señalética de salida.

4.3.4 Fase IV Pruebas y registros

Registro de Usuarios en el Sistema

El proceso de registro individual toma 3 minutos por persona. El usuario se coloca frente al dispositivo a una distancia de 50 cm. El sistema captura 5 imágenes del rostro desde diferentes ángulos: frontal, 15 grados izquierda, 15 grados derecha, ligeramente hacia arriba y ligeramente hacia abajo. Estas múltiples capturas mejoran la precisión del reconocimiento bajo diferentes condiciones.

Se solicita a los usuarios retirar temporalmente gafas, gorras o cualquier accesorio que cubra el rostro durante el registro. Para usuarios que utilizan gafas permanentemente, se realiza un doble registro: con y sin gafas, permitiendo al sistema reconocerlos en ambas condiciones.

Cada registro facial se asocia con el perfil del usuario en la base de datos central. Se asignan permisos de acceso específicos según el rol: docentes obtienen acceso a todos los laboratorios en horario de 8:00 a 21:00 y el personal administrativo tiene acceso completo las 24 horas.

Pruebas de Verificación de Identidad

Se ejecutan pruebas sistemáticas con cada usuario registrado para validar la efectividad del sistema. Cada persona realiza 10 intentos de acceso en diferentes condiciones: iluminación natural diurna, iluminación artificial nocturna, con gafas, sin gafas, con diferente peinado y a diferentes distancias del sensor.

Se registran los resultados de cada intento: tiempo de verificación, resultado (éxito o fallo) y condición de la prueba. Se calcula la tasa de éxito individual para cada usuario. Se identifican usuarios con tasa de éxito inferior al 95% para repetir el proceso de registro con ajustes.

Pruebas de Seguridad Anti-Suplantación

Se verifica la correcta integración entre dispositivos biométricos y servidor central. Se accede a la consola de administración web del software Lockly Visage o EZVIZ DL50FVS. Se confirma la visualización en tiempo real del estado de los cuatro dispositivos: conectados, funcionando correctamente y con sincronización activa.

Se prueba la funcionalidad de búsqueda de eventos. Se buscan todos los accesos de un usuario específico en la última semana. El sistema recupera 14 registros en 2 segundos mostrando fecha, hora, laboratorio y resultado de cada acceso. Se verifica que los datos coincidan con los registros locales de cada dispositivo.

Se prueba la modificación remota de permisos. Se revoca temporalmente el acceso de un usuario de prueba desde el servidor central. Se confirma que el cambio se sincronice a los dispositivos en 3 minutos. Se intenta acceso con el usuario modificado y el sistema rechaza correctamente la entrada. Se restauran los permisos y se verifica que el acceso se habilite nuevamente.

CAPÍTULO V: CONCLUSIONES Y RECOMENDACIONES

5.1 Conclusiones

La implementación de reconocimiento facial en los cuatro laboratorios fortalece seguridad, trazabilidad y gestión de usuarios, cumpliendo principios de privacidad por diseño y la Ley Orgánica de Protección de Datos mediante almacenamiento local y consentimiento informado.

El análisis teórico y tecnológico evidencia que el reconocimiento biométrico constituye una solución confiable y eficiente para el control de acceso en instituciones educativas, al ofrecer mayor seguridad, trazabilidad y automatización frente a sistemas tradicionales, especialmente en entornos académicos con alta circulación de usuarios.

El diagnóstico realizado mediante encuestas y entrevistas demuestra que el sistema actual de control de acceso en los laboratorios del área técnica de la Universidad Laica Eloy Alfaro de Manabí presenta limitaciones operativas y de seguridad, lo que genera riesgos de ingreso no autorizado y dependencia de mecanismos manuales.

El diseño de una propuesta basada en reconocimiento biométrico, especialmente facial, resulta técnicamente viable y alineado con los requerimientos institucionales, contando además con una aceptación mayoritaria por parte de la comunidad universitaria, lo que respalda su implementación como una mejora sustancial.

5.2 Recomendaciones

Establecer un protocolo institucional de gestión del sistema de reconocimiento facial que incluya políticas claras de consentimiento informado, control de accesos a la información y auditorías periódicas garantizando el cumplimiento de la normativa vigente y la confianza de la comunidad universitaria.

Fortalecer la socialización y capacitación sobre el uso del sistema biométrico, con el fin de reducir la incertidumbre detectada en la encuesta y promover una aceptación informada y responsable por parte de estudiantes y docentes.

Priorizar la implementación del reconocimiento facial como mecanismo principal de acceso, considerando su rapidez, facilidad de uso y menor contacto físico, garantizando además el cumplimiento de normas de confidencialidad y protección de datos biométricos.

Realizar una evaluación periódica del sistema implementado, tanto a nivel técnico como operativo, para asegurar su correcto funcionamiento, detectar oportunidades de mejora y mantener alineado el control de acceso con las necesidades académicas y tecnológicas institucionales.

BIBLIOGRAFÍA

- Albayero, M. S., Tejada-Hernández, M., & Cerritos, J. de J. (2020). Una aproximación teórica para la aplicación de la metodología del enfoque mixto en la investigación en enfermería. *Entorno*, 69, Article 69. <https://doi.org/10.5377/entorno.v0i69.9562>
- Alcaraz García, S. J. (2022). *Guía de observación y evaluación de la idoneidad del espacio físico del aula* [Phd, E.T.S. de Edificación (UPM)]. <https://oa.upm.es/72273/>
- Alcivar Alcivar, D. F., & Moya Martínez, M. E. (2020). La neurociencia y los procesos que intervienen en el aprendizaje y la generación de nuevos conocimientos. *Polo del Conocimiento: Revista científico - profesional*, 5(8 (AGOSTO 2020)), 510-529.
- Arias, J., & Covinos, M. (2021). Diseño y metodología de la investigación. *Enfoques Consulting EIRL*, 1(1), 66-78.
- Bardales Sinarahua, T., & Castro Placido, R. A. (2024). *Análisis de la seguridad informática de la oficina de sistemas y tecnologías de la información de la municipalidad provincial de maynas – 2023*. <http://hdl.handle.net/20.500.14503/2917>
- Becerra, R., & Carlos, L. (2020). *Diseño de un modelo de seguridad informática a una empresa en su sistema de monitoreo del área de tecnología*. <https://hdl.handle.net/20.500.12494/18082>
- Cannatella, T., Méndez Garabetti, M., & Sández, P. J. (2023). *Identificación de personas en sistemas de videovigilancia sin uso de reconocimiento facial*. XXVIII Congreso Argentino de Ciencias de la Computación (CACIC) (La Rioja, 3 al 6 de octubre de 2022). <http://sedici.unlp.edu.ar/handle/10915/149626>
- Córdova, J. V. G. (2023). Propuesta de modelo en seguridad informática en el control de un sistema informático aplicando ISO 27002 y CSF de NIST. *Revista Ingeniería e Innovación del Futuro*, 2(1), 41-52.
- Espinoza-Freire, E. E. (2023). La enseñanza de las ciencias sociales mediante el método deductivo. *Revista Mexicana de Investigación e Intervención Educativa*, 2(2), Article 2. <https://doi.org/10.62697/rmiie.v2i2.50>
- Fernández López, P. (2020). *Strengths and weaknesses of gait recognition* (p. 1) [Http://purl.org/dc/dcmitype/Text, Universidad Carlos III de Madrid]. <https://dialnet.unirioja.es/servlet/tesis?codigo=293189>
- Gallardo Cava, R. (2024). *Inteligencia artificial explicable (xai) para ataques de presentación en sistemas biométricos* (p. 1) [Http://purl.org/dc/dcmitype/Text, Universidad Rey Juan Carlos]. <https://dialnet.unirioja.es/servlet/tesis?codigo=334763>

- García, J. E. I., Castro, J. S. Q., García, C. A. C., & Merino, M. J. M. (2023). Protocolos de seguridad informática aplicados en los laboratorios de la carrera tecnologías de la información. *Journal TechInnovation*, 2(1), Article 1. <https://doi.org/10.47230/Journal.TechInnovation.v2.n1.2023.79-84>
- Gómez, S., & Julian, J. (2024). *Biometría y la seguridad informática en los métodos de autenticación*. <http://repository.unad.edu.co/handle/10596/39060>
- Granados Muñoz, R. (2020). Revisión teórica de herramientas metodológicas aplicadas en la investigación criminológica. *Derecho y Cambio Social*, 59, 501-511.
- Guerra Jiménez, G. M., & Jiménez Prada, R. A. (2021). *Aplicación de reconocimiento biométrico por huella dactilar y su Influencia en la Seguridad Lógica en SEDAPAL, 2020*. https://alicia.concytec.gob.pe/vufind/Record/UCVV_d5f1a14bb9f9d03d330feb758d1af851
- Gusqui Villa, E. D., & Valdivieso Ambi, A. V. (2023). *Diseño y construcción de un prototipo de sistema transferencia automática y un control de acceso mediante Reconocimiento facial usando técnica de inteligencia artificial para la Fundación ECOSUR-Ecuador* [bachelorThesis, Riobamba, Universidad Nacional de Chimborazo]. <http://dspace.unach.edu.ec/handle/51000/12084>
- Herrera Mosquera, A. E. (2025). *Implementación Centralizada de Control de Acceso a Información de Identificación Personal: Requisitos de Control de Acceso para la Recolección, Procesamiento y Almacenamiento de Información de Identificación Personal*. <http://bibdigital.epn.edu.ec/handle/15000/26515>
- Herszenbaun, M. (2022). Método analítico y la carencia de síntesis en "El conocer analítico" de la Ciencia de la lógica de Hegel. *Nuevo Itinerario*, 18(2), 92-102. <https://doi.org/10.30972/nvt.1826199>
- López Morocho, L. R., Jaramillo Baquerizo, C. P., López Morocho, L. R., & Jaramillo Baquerizo, C. P. (2025). El rol del método inductivo como vínculo entre las teorías educativas y las prácticas de aula. *Sophia, Colección de Filosofía de la Educación*, 38, 51-77. <https://doi.org/10.17163/soph.n38.2025.01>
- Mar Cornelio, O., Gulín González, J., & Santana Ching, I. (2024). Modelo computacional para la toma de decisiones sobre el control de acceso a las prácticas de laboratorios. *Revista Cubana de Ciencias Informáticas*, 18(1). http://scielo.sld.cu/scielo.php?script=sci_abstract&pid=S2227-18992024000100005&lng=es&nrm=iso&tlng=es
- Naranjo Alcívar, S. A. (2023). *Análisis de estrategias para brindar seguridad informática en las redes y servidores del GAD Montalvo*. [bachelorThesis, Babahoyo: UTB-FAFI. 2023]. <http://dspace.utb.edu.ec/handle/49000/14243>
- Ortega del Campo, D. (2021). *Detección de ataques de presentación en sistemas ABC*. <http://hdl.handle.net/10115/18274>

- Páez, J. A., Cortes, J. A., Simanca, F. A., Blanco, F., Páez, J. A., Cortes, J. A., Simanca, F. A., & Blanco, F. (2021). Aplicación de UML y SCRUM al desarrollo del software sobre control de acceso. *Información tecnológica*, 32(5), 57-66. <https://doi.org/10.4067/S0718-07642021000500057>
- Pérez Pérez, J. (2021). *Seguridad en cerraduras inteligentes*. <https://riull.ull.es/xmlui/handle/915/25443>
- Ponce Hernández, W. (2021). *Mecanismos de protección de la privacidad de los ciudadanos aplicados a la firma manuscrita biométrica* (p. 1) [Http://purl.org/dc/dcmitype/Text, Universidad Carlos III de Madrid]. <https://dialnet.unirioja.es/servlet/tesis?codigo=301228>
- Pozo Espinoza, L. A. (2022). *Análisis del sistema de automatización para la identificación y control de acceso del personal de la cooperativa de taxi san Fernando del cantón Babahoyo* [bachelorThesis, Babahoyo: UTB-FAFI. 2022]. <http://dspace.utb.edu.ec/handle/49000/11848>
- Quirós, C. A. (2024). *Reconocimiento Biométrico Ocular Basado en Deep Learning*. https://oa.upm.es/84277/1/TFG_CESAR_AGULLO_QUIROS.pdf
- Quiros Sandoval, H. C. (2022). *Robustez de los sistemas biométricos de firma dinámica, frente a ataques fraudulentos* (p. 1) [Http://purl.org/dc/dcmitype/Text, Universidad Carlos III de Madrid]. <https://dialnet.unirioja.es/servlet/tesis?codigo=310660>
- Ruiz, S., Alvez, C. E., Etchart, G., & Miranda, E. (2022). *Hacia la definición de un marco metodológico para el desarrollo de un sistema de reconocimiento biométrico mediante técnicas de Machine Learning*. XXIV Workshop de Investigadores en Ciencias de la Computación (WICC 2022, Mendoza). <http://sedici.unlp.edu.ar/handle/10915/143362>
- Saldarriaga Amalla, A. A., & Zambrano 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*. [Thesis]. <https://repositorio.uleam.edu.ec/handle/123456789/4677>
- Urréa, H. R., Cotto, J. J. R., Sánchez, J. L. O., Díaz, G. E. G., & Saldarriaga, G. (2022). *METODOLOGÍA DE LA INVESTIGACIÓN*. ACVENISPROH Académico. <https://doi.org/10.47606/ACVEN/ACLIB0017>
- Vega Palma, M. A., & Zambrano 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*. [Thesis]. <https://repositorio.uleam.edu.ec/handle/123456789/4670>
- Velásquez Vivas, C. V. (2022). *Comparativa de Métodos de Control de Acceso de una Infraestructura de Red Empresarial* [masterThesis, Quito: UISRAEL]. <http://repositorio.uisrael.edu.ec/handle/47000/3368>

- Zambrano, A., Guarda, T., Valenzuela, E. V. H., & Quiña, N. (2019). *Técnicas de mitigación para principales vulnerabilidades de seguridad en aplicaciones web*. https://www.researchgate.net/profile/Teresa-Guarda/publication/331178479_Mitigation_techniques_for_security_vulnerabilities_in_web_applications/links/5fabe891a6fdcc331b9478b4/Mitigation-techniques-for-security-vulnerabilities-in-web-applications.pdf
- Zúñiga, P. I. V., Cedeño, R. J. C., & Palacios, I. A. M. (2023). Metodología de la investigación científica: Guía práctica. *Ciencia Latina Revista Científica Multidisciplinar*, 7(4), Article 4. https://doi.org/10.37811/cl_rcm.v7i4.7658

ANEXOS

Anexo Nr1. Encuesta

Universidad Laica Eloy Alfaro de Manabí Extensión Chone

Carrera: Tecnologías de la Información y Comunicación

Tema: “Reconocimiento biométrico para el control de acceso en los laboratorios del área técnica de la Universidad Laica Eloy Alfaro de Manabí Extensión Chone”

Objetivo: Implementar reconocimiento biométrico para el control de acceso en los laboratorios del área técnica de la Universidad Laica Eloy Alfaro De Manabí Extensión Chone.

Preguntas:

- 1) ¿Considera importante mejorar el control de acceso en los laboratorios del área técnica?
 - a) Totalmente en desacuerdo
 - b) En desacuerdo
 - c) Ni de acuerdo ni en desacuerdo
 - d) De acuerdo
 - e) Totalmente de acuerdo
- 2) ¿El uso de un sistema de reconocimiento biométrico (huella o rostro) facilitará el ingreso a los laboratorios?
 - a) Totalmente en desacuerdo
 - b) En desacuerdo
 - c) Ni de acuerdo ni en desacuerdo
 - d) De acuerdo
 - e) Totalmente de acuerdo
- 3) ¿La implementación de un sistema biométrico aumentara la seguridad dentro de los laboratorios?
 - a) Totalmente en desacuerdo
 - b) En desacuerdo

- c) Ni de acuerdo ni en desacuerdo
 - d) De acuerdo
 - e) Totalmente de acuerdo
- 4) ¿Se sentiría cómodo(a) utilizando un sistema de reconociendo biométrico para ingresar a los laboratorios?
- a) Totalmente en desacuerdo
 - b) En desacuerdo
 - c) Ni de acuerdo ni en desacuerdo
 - d) De acuerdo
 - e) Totalmente de acuerdo
- 5) ¿Considera que la información biométrica debe ser tratada con confidencialidad y seguridad?
- a) Totalmente en desacuerdo
 - b) En desacuerdo
 - c) Ni de acuerdo ni en desacuerdo
 - d) De acuerdo
 - e) Totalmente de acuerdo
- 6) ¿El sistema biométrico reduciría el ingreso no autorizado de personas a los laboratorios?
- a) Totalmente en desacuerdo
 - b) En desacuerdo
 - c) Ni de acuerdo ni en desacuerdo
 - d) De acuerdo
 - e) Totalmente de acuerdo
- 7) ¿Cree que la instalación de este sistema no afectará negativamente las actividades académicas?
- a) Totalmente en desacuerdo
 - b) En desacuerdo

c) Ni de acuerdo ni en desacuerdo

d) De acuerdo

e) Totalmente de acuerdo

8) ¿En general se sentiría de acuerdo con la implementación del reconocimiento biométrico en los laboratorios del área técnica?

a) Totalmente en desacuerdo

b) En desacuerdo

c) Ni de acuerdo ni en desacuerdo

d) De acuerdo

e) Totalmente de acuerdo

Anexo Nr2. Entrevista

Universidad Laica Eloy Alfaro de Manabí Extensión Chone

Carrera: Tecnologías de la Información y Comunicación

Tema: "Reconocimiento biométrico para el control de acceso en los laboratorios del área técnica de la Universidad Laica Eloy Alfaro de Manabí Extensión Chone"

Objetivo: Implementar reconocimiento biométrico para el control de acceso en los laboratorios del área técnica de la Universidad Laica Eloy Alfaro De Manabí Extensión Chone.

Preguntas:

Pregunta	Respuesta
¿Cómo evalúa las condiciones actuales del control de acceso a los laboratorios del área técnica?	Las condiciones actuales son funcionales, pero presentan limitaciones en control y trazabilidad. El acceso manual dificulta la verificación precisa de usuarios autorizados y no permite un registro automatizado confiable, generando oportunidades de mejora en seguridad y eficiencia operativa.
¿Ha ocurrido alguna vez el ingreso no autorizado o pérdida de control sobre el uso de los laboratorios?	Sí, se han identificado casos aislados de ingreso no autorizado, principalmente fuera de horarios académicos, lo que evidencia debilidades en los mecanismos de control actuales y la necesidad de soluciones tecnológicas más robustas.
¿Considera que el control de acceso actual es suficiente para proteger los equipos y datos?	No es totalmente suficiente. Aunque existe supervisión, el sistema actual no garantiza una protección integral de los equipos ni de la información académica, por lo que se requiere un control más estricto y automatizado.
¿Qué tipo de acceso biométrico considera más adecuado para los laboratorios de cómputo?	El reconocimiento facial es adecuado por su rapidez, menor contacto físico y facilidad de integración, pudiendo complementarse con huella dactilar en casos específicos para mayor confiabilidad.

¿Cuáles serían los beneficios más importantes de implementar un sistema biométrico?	Mejoraría la seguridad, reduciría accesos no autorizados, optimizaría la gestión de horarios y permitiría un registro preciso del uso de los laboratorios, fortaleciendo la cultura de responsabilidad y cuidado de los recursos tecnológicos.
¿Con qué frecuencia ha surgido un problema de privacidad por ingreso no autorizado?	Los problemas de privacidad no son frecuentes, pero cuando ocurren generan preocupación, reforzando la importancia de prevenir accesos indebidos que puedan comprometer información académica o personal.
¿Cómo podría involucrarse la comunidad universitaria en la aceptación y uso responsable del sistema?	A través de procesos de socialización, capacitación y comunicación transparente sobre el manejo seguro de los datos, promoviendo la participación activa de estudiantes y docentes.
¿Qué aspectos considera más importantes al elegir un dispositivo biométrico para el control de acceso?	Se consideran fundamentales la confiabilidad y precisión del dispositivo, la seguridad en el tratamiento de datos biométricos, la facilidad de uso, la rapidez de autenticación, la compatibilidad con la infraestructura existente, el soporte técnico, el costo-beneficio y el cumplimiento de normas de protección de datos.