



UNIVERSIDAD LAICA “ELOY ALFARO” DE MANABÍ

TRABAJO DE TITULACIÓN

MODALIDAD PROYECTO DE INTEGRADOR

TÍTULO:

SISTEMA DE AUTENTICACIÓN BIOMÉTRICA PARA EL ACCESO A
CENTRO DE CONTROLES DE VIGILANCIA DEL ÁREA TÉCNICA DE
LA UNIVERSIDAD LAICA ELOY ALFARO DE MANABÍ EXTENSIÓN
CHONE

AUTORES:

CEDEÑO MOREIRA JHON ERICK

LÓPEZ MOREIRA JOEL JOSÉ

UNIDAD ACADÉMICA:

EXTENSIÓN CHONE

CARRERA:

TECNOLOGÍAS DE LA INFORMACIÓN

TUTOR:

ING. CRISTHIAN MARCONY VILLA PALMA

CHONE – MANABÍ – ECUADOR

FEBRERO DE 2026

CERTIFICACIÓN DEL TUTOR

Ing. Cristhian Marcony Villa Palma, Mg.; docente de la Universidad Laica “Eloy Alfaro” de Manabí, extensión Chone, en calidad de Tutor del Proyecto.

CERTIFICO:

Que el presente Proyecto Integrador con el título “Sistema de autenticación biométrica para el acceso a centro de controles de vigilancia 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 su(s) autor(es):

CEDENO MOREIRA JHON ERICK Y LOPEZ MOREIRA JOEL JOSE.

Siendo de su exclusiva responsabilidad.

Chone, febrero de 2026.


Ing. Cristhian Marcony Villa Palma, Mg.
TUTOR

DECLARACIÓN DE AUTORÍA

Quien(es) suscribe(n) la presente:

CEDENO MOREIRA JHON ERICK Y LOPEZ MOREIRA JOEL JOSE.

Estudiante(s) de la Carrera de **Tecnologías de la Información**, declaro(amos) bajo juramento que el siguiente proyecto cuyo título: “Sistema de autenticación biométrica para el acceso a centro de controles de vigilancia 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.



Cedeno Moreira Jhon Erick.



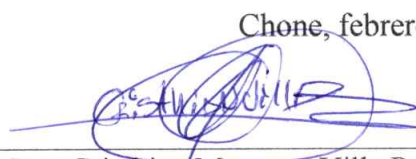
López Moreira Joel José.

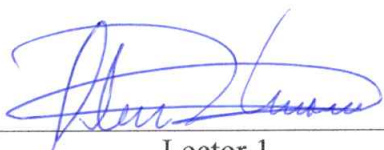


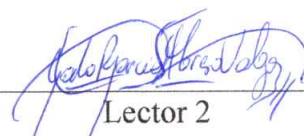
APROBACIÓN DEL TRABAJO DE TITULACIÓN

Los miembros del Tribunal Examinador aprueban el Trabajo de Titulación con Modalidad Proyecto Integrador, titulado: “Sistema de autenticación biométrica para el acceso a centro de controles de vigilancia del área técnica de la Universidad Laica Eloy Alfaro de Manabí extensión Chone”. Cuyos autores, Cedeño Moreira Jhon Erick y López Moreira Joel José, estudiantes de la Carrera de Tecnologías de la Información, y como Tutor de Trabajo de Titulación el Ing. Cristhian Marcony Villa Palma.


Lic. Rocio Bermúdez Cevallos. Mg.
DECANA

Chone, febrero de 2026

Ing. Cristhian Marcony Villa Palma
TUTOR


Lector 1
MIEMBRO DEL TRIBUNAL


Lector 2
MIEMBRO DEL TRIBUNAL


Lic. Indira Zambrano Cedeño
SECRETARIA

AGRADECIMIENTO

Al culminar esta etapa tan significativa de nuestra formación académica, expresamos nuestro sincero agradecimiento a todas las personas que contribuyeron, directa e indirectamente, al desarrollo y finalización de este trabajo de titulación.

En primer lugar, agradecemos a Dios por brindarnos fortaleza, constancia y claridad en cada uno de los desafíos enfrentados, permitiéndonos avanzar con determinación hasta alcanzar este objetivo profesional.

Extendemos nuestro profundo agradecimiento a nuestras familias, cuyo apoyo incondicional, comprensión y palabras de aliento fueron fundamentales a lo largo de este proceso. Su confianza y sacrificio representaron un pilar esencial para mantenernos firmes ante las dificultades y motivados a seguir adelante.

A nuestros docentes, expresamos un reconocimiento especial por su guía, acompañamiento y valiosas orientaciones, las cuales contribuyeron significativamente a la calidad del presente trabajo. Su experiencia y compromiso académico fueron determinantes para nuestro aprendizaje y crecimiento profesional.

Asimismo, agradecemos a nuestros compañeros y amigos por el compañerismo, la colaboración y el respaldo brindado durante nuestra vida universitaria, haciendo de este camino una experiencia de aprendizaje compartida y enriquecedora.

Finalmente, reconocemos nuestro esfuerzo, la dedicación y la perseverancia invertidas en este proyecto, el cual representa no solo la culminación de una etapa académica, sino el inicio de nuevos retos y oportunidades profesionales.

A todos quienes formaron parte de este proceso, nuestro más sincero agradecimiento.

DEDICATORIA

Dedico este trabajo a Dios, por ser mi guía, por darme la sabiduría, la salud y la perseverancia necesarias para superar los retos presentados durante mi formación académica. Su presencia constante me permitió mantener la fe y la confianza para alcanzar este objetivo.

No menos importante dedico este trabajo a mis padres, quienes han sido fundamental a lo largo de mi formación académica y personal. Su apoyo total, sacrificio y palabras de aliento han sido la motivación necesaria para no rendirme ante las dificultades y continuar avanzando hacia el cumplimiento de mis metas. Gracias por creer en mí, por inculcarme valores de responsabilidad y perseverancia, y por acompañarme en cada etapa de este proceso.

De igual manera, dedico este proyecto a mi familia, por todos los que han estado presentes brindándome su respaldo en todo momento. La confianza de ellos han sido un impulso importante para culminar esta etapa de mi vida académica, cada consejo y gesto de apoyo ha contribuido de manera significativa a la realización de este trabajo y a mi crecimiento como profesional.

A todos aquellos dedico este logro.

López Moreira Joel José

DEDICATORIA

Dedico de manera especial este trabajo de titulación a mis padres Maritza Moreira y Fernando Cedeño por su sacrificio y esfuerzo, pues ellos han sido mi impulso para no decaer y seguir luchando por conseguir mis metas.

A Dios, por llenarme de sabiduría, constancia y la fuerza necesaria para sobrepasar cada obstáculo que se ha presentado a lo largo de mi carrera.

A toda mi familia, por el apoyo incondicional brindado a lo largo de todo este proceso de formación y superación.

A mis compañeros y compañeras por el apoyo y la constancia brindada, fueron ellos quienes sin esperar nada a cambio estuvieron presto a enseñarme y ayudarme compartiendo sus conocimientos, con entusiasmo, y siempre con la mejor predisposición y sin lugar a duda con sus palabras de apoyo incondicional.

Al esfuerzo y constancia propia que me llevaron a conseguir mis objetivos y metas planteadas.

Cedeño Moreira Jhon Erick

ÍNDICE DE CONTENIDOS

CERTIFICACIÓN DEL TUTOR.....	ii
DECLARACIÓN DE AUTORÍA	iii
APROBACIÓN DEL TRABAJO DE TITULACIÓN	iv
AGRADECIMIENTO	v
DEDICATORIA	vi
ÍNDICE DE CONTENIDOS	viii
RESUMEN	xiii
CAPITULO I: INTRODUCCIÓN.....	1
1.1 Introducción	1
1.2 Presentación del tema.....	2
1.3 Diagrama causa – efecto del problema	2
1.4 Planteamiento y formulación del problema	2
1.4.1 Ubicación de la problemática	3
1.4.2 Problematización	4
1.4.3 Génesis del problema.....	4
1.4.4 Estado actual del problema.....	4
1.5 Objetivos	5
1.5.1 Objetivo general.....	5
1.5.2 Objetivos específicos	5
1.6 Justificación	5
1.7 Impactos esperados	6
1.7.1 Impacto tecnológico.....	6
1.7.2 Impacto Social	6
1.7.3 Impacto ecológico.....	7
CAPITULO II: MARCO TEÓRICO DE LA INVESTIGACIÓN	8
2.1 Sistema de autenticación biométrica.....	8
2.1.1 Concepto y fundamentos de la biometría	8
2.1.2 Tipos de sistemas biométricos.	9
2.1.3 Funcionamiento técnico de un sistema biométrico.....	11

2.1.4	Ventajas y desventajas de la autenticación biométrica.....	14
2.1.5	Aplicaciones prácticas de la biometría en instituciones.	15
2.2	Nivel de seguridad en el acceso al centro de control de vigilancia.....	17
2.2.1	Conceptualización de centros de controles de vigilancia	17
2.2.2	Tipos de centro de vigilancia.....	18
2.2.3	Problemáticas comunes en los Centros de Vigilancia sin control biométrico... 19	
CAPITULO III: DISEÑO METODOLÓGICO.....		20
3.1	Tipo de investigación.	20
3.2	Nivel de Investigación	20
3.3	Enfoque de investigación.....	20
3.4	Métodos de investigación.....	20
3.5	Fuentes de datos.....	21
3.5.1	Fuentes primarias.....	21
3.5.2	Fuentes secundarias	21
3.6	Estrategia operacional para la recolección de datos.....	21
3.6.1	Técnicas y herramientas	21
3.6.2	Instrumentos de la Investigación.	22
3.7	Descripción de la población y Diseño de la muestra	22
3.8	Análisis y presentación de los resultados.....	23
3.8.1	Análisis de la ficha de observación aplicada	23
3.8.2	Análisis de los resultados de la entrevista.	25
3.8.3	Presentación y descripción de los resultados obtenidos	26
CAPITULO IV: EJECUCIÓN DEL PROYECTO.....		27
4.1	Descripción del proyecto	27
4.2	Determinación de recursos.....	27
4.2.1	Recursos Humanos.	27
4.2.2	Recursos tecnológicos.	28
4.2.3	Recursos económicos.....	29
4.3	Etapas de ejecución del proyecto	29
4.3.1	Fase I: Planificación	29
4.3.2	Fase II: Diseño del sistema	30
4.3.3	Fase III: Instalación e implementación.....	34

4.3.4	Fase IV: Pruebas del sistema	35
4.3.5	Fase V: Mantenimiento y monitoreo	36
CAPITULO V: CONCLUSIONES Y RECOMENDACIONES		38
5.1	Conclusiones	38
5.2	Recomendaciones.....	38
BIBLIOGRAFÍA		39
ANEXOS		43
Anexo Nr1. Guion para entrevista		43
Anexo Nr2. Ficha de observación		45
Anexo Nr3. Aplicación de instrumentos		47

ÍNDICE DE TABLA

Tabla 1: Recursos humanos	27
Tabla 2: Recursos Tecnológicos	28
Tabla 3: Recursos económicos	29

ÍNDICE DE GRAFICAS E ILUSTRACIONES

Figura 1 . Diagrama causa efecto	2
Figura 2. Lector de huellas dactilares.....	9
Figura 3. Biometría facial.....	10
Figura 4. Reconocimiento del iris.....	11
Figura 5. Arquitectura de un sistema biométrico	12
Figura 6. Diseño del sistema.....	31
Figura 7. Tabla de verificación de usuario.	32
Figura 8. Interfaz agregar usuarios ZKAccess	33
Figura 9. Agregación de dispositivo biométrico por TCP/IP	33
Figura 10. Generación de reportes de aperturas por huella dactilar.	34

RESUMEN

El presente proyecto tiene como objetivo el diseño y propuesta de un sistema de control biométrico para optimizar los procesos de seguridad en el Centro de Vigilancia de la Universidad Laica Eloy Alfaro de Manabí – Extensión Chone. Surge a partir de la necesidad institucional de mejorar el control de accesos y reducir las problemáticas asociadas a la gestión manual y no centralizada de entradas a las instalaciones. El objetivo es fortalecer los niveles de seguridad mediante la implantación de tecnologías biométricas, de esta manera permitiendo una identificación más precisa y eficiente del personal. A través de un enfoque mixto, se combinaron métodos cualitativos (entrevistas a responsables de seguridad, observación directa) y cuantitativos (recolección de datos numéricos sobre accesos, eventos de riesgo, otros), para de esta manera diagnosticar el estado actual y sustentar la propuesta. El proyecto lleva a cabo el análisis de los diferentes tipos de Centros de Control de Vigilancia, su funcionamiento, debilidades comunes sin sistemas biométricos y los requerimientos técnicos necesarios para la implementación del nuevo sistema. Su alcance se limita a la sede Chone, con posibilidad de replicabilidad institucional.

Palabras claves:

- Biometría., Huellas dactilares, Identificación, Seguridad Institucional.

CAPITULO I: INTRODUCCIÓN

1.1 Introducción

Hoy en día la seguridad y el control de acceso en espacios como lo son los centros de controles de vigilancia se ha convertido en una necesidad fundamental para las instituciones educativas, en especial aquellas que cuentan con áreas donde se encuentran equipos electrónicos que requieren restringir el ingreso únicamente a personal autorizado. En ese contexto, el avance de la tecnología biométrica ha permitido implementar soluciones más confiables que los métodos tradicionales, como el uso de llaves, tarjetas o contraseñas, los cuales pueden ser fácilmente extraviados, compartidos o vulnerados.

La ULEAM, Extensión Chone, cuenta con un centro de controles de vigilancia en su área técnica que no tiene un sistema automatizado de autenticación. Aquella situación abre una oportunidad para mejorar la seguridad en la institución antes mencionada, esto mediante la implementación de un sistema biométrico que permita autenticar la identidad de los usuarios a través de sus rasgos físicos, sea este la huella dactilar, asegurando un acceso más seguro y rápido.

El presente proyecto propone el desarrollo de un sistema de autenticación biométrica para el acceso al centro de controles de vigilancia, integrando dispositivos de captura con un software de gestión que almacene, compare y registre los accesos realizados. Este sistema busca no solo incrementar el nivel de seguridad, sino también optimizar la trazabilidad y control administrativo del personal que ingresa a esta zona estratégica.

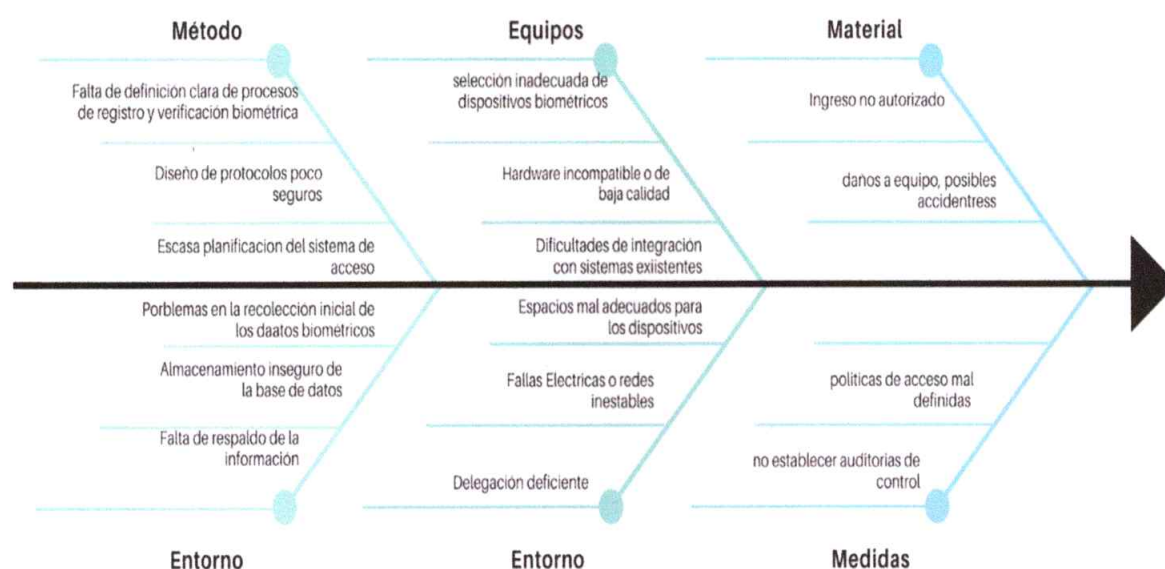
En el transcurso de esta propuesta, se ha contextualizado el funcionamiento de los centros de vigilancia y la estructura de los sistemas biométricos, así como la función que desempeña el software en el procesamiento de la información. Además, se han considerado los impactos tecnológicos, sociales y ecológicos que puede tener la implementación de este sistema dentro de la institución de educación superior como lo es la ULEAM.

1.2 Presentación del tema

Hoy en día el avance de la tecnología ha transformado los sistemas de seguridad en varios sectores, incluyendo también el ámbito universitario, en este se manejan recursos sensibles y por esto se requiere un control eficaz para el acceso, En este contexto en el presente proyecto se propone el diseño e implementación de un sistema de autenticación biométrica para el acceso al centro de vigilancia del área técnica en la ULEAM extensión Chone.

1.3 Diagrama causa – efecto del problema

Figura 1 . Diagrama causa efecto



Nota. Diagrama causa-efecto del problema [Imagen] Autores del proyecto, 2025

1.4 Planteamiento y formulación del problema

Hoy en día el acceso a los centros de control de vigilancia del área técnica de la ULEAM extensión Chone, se realiza mediante métodos de acceso de manera manual que no garantiza un nivel adecuado de seguridad ni de gestión de ingreso. Por lo tanto, esta situación representa una vulnerabilidad significativa, ya que el control de acceso no permite validar de manera confiable la identidad de las personas que ingresan a estas áreas de vigilancia.

Que no haya un sistema de autenticación biométrica moderno expone riesgos como o son los accesos no autorizados, manipulación de la información sensible, y posibles fallas en los protocolos de seguridad internos. En donde la protección de datos y la integridad operativa son de suma importancia, resulta muy importante tener mecanismos avanzados que

verifiquen la identidad de los usuarios a través de características únicas, como huellas dactilares o reconocimiento facial.

Menciona Quintanilla Mendoza, (2020) “el uso de la biométrica como método de identificación en la ejecución de las operaciones diarias ha demostrado ser un mecanismo más seguro que reduce el fraude y reporta resultados con más certidumbre y confianza, aunque a su vez conlleva riesgos de privacidad y de seguridad” (p. 2).

La falta de implementación de un sistema biométrico adecuado podría resultar en consecuencias graves como la filtración de información confidencial, la interrupción de las operaciones de vigilancia, entre otros. De no atenderse esta necesidad, se comprometería seriamente la confianza en los procedimientos de seguridad del área técnica y de la Universidad en general.

Por lo tanto, inicia la necesidad implementar un Sistema de Autenticación Biométrica para el Acceso a Centros de Control de Vigilancia del Área Técnica de la ULEAM, Extensión Chone, que permita fortalecer los mecanismos de acceso, y así optimizar la seguridad física y digital, y proteger de manera efectiva los recursos e información importante.

La necesidad de proteger información sensible, equipos tecnológicos y procesos operativos requiere la incorporación de herramientas que aseguren la identificación precisa y controlada de los usuarios. Por esta razón, surge la siguiente interrogante:

¿Mejorará la seguridad en el centro de vigilancia del área técnica de la Universidad Laica "Eloy Alfaro" de Manabí Extensión Chone mediante la implementación de un sistema de control de acceso biométrico?

1.4.1 Ubicación de la problemática

La presente problemática se sitúa en la ULEAM, extensión Chone, la cual se encuentra en la Avenida Eloy Alfaro, en el cantón Chone de la provincia de Manabí, Ecuador. Entre sus cuatro edificaciones se destaca, el bloque "B" específicamente en el área técnica donde operan los centros de control de vigilancia. Esta área cumple una función crítica en la supervisión y resguardo de las instalaciones universitarias, siendo este un punto estratégico para garantizar la seguridad tanto de los recursos institucionales como de la comunidad universitaria.

Actualmente los mecanismos de acceso a centros de control se basan en métodos básicos, como llaves físicas, y estas presentan limitaciones obvias en cuanto a verificación de identidad y protección frente a accesos no autorizados. Por ende, esta situación carece de una solución tecnológica avanzada que permita validar de forma confiable y automática la identidad de los usuarios que ingresan a zonas de seguridad donde el acceso es restringido.

Ante este contexto, surge la necesidad de fortalecer las medidas de control de acceso mediante la implementación de un sistema de autenticación biométrica. Este sistema permitiría una validación más precisa y segura, alineándose con las exigencias actuales en materia de seguridad institucional.

1.4.2 Problematización

La seguridad institucional se ha convertido en un aspecto importante dentro de los entornos universitarios, especialmente en áreas críticas como los centros de control de vigilancia. En la ULEAM extensión Chone, el acceso a zonas estratégicas se realiza actualmente mediante procedimientos convencionales, lo cual plantea limitaciones frente a los estándares modernos de seguridad. La falta de mecanismos robustos de autenticación, como los sistemas biométricos, impide garantizar con certeza que únicamente personal autorizado acceda a dichos espacios.

1.4.3 Génesis del problema

El origen del problema se encuentra en que se depende de métodos tradicionales de control de acceso, como llaves físicas, listas de ingreso manuales o tarjetas de identificación que pueden ser prestadas o extraviadas. Estos métodos, si bien han funcionado en el pasado, no responden adecuadamente a las exigencias actuales de seguridad ni ofrecen trazabilidad confiable de los accesos.

1.4.4 Estado actual del problema

Actualmente, el acceso al centro de control de vigilancia del área técnica de la ULEAM, extensión Chone, continúa haciéndose mediante mecanismos tradicionales. No hay un sistema automatizado ni biométrico que regule la entrada y salida del personal, lo cual impide llevar un registro exacto de los accesos y deja abierta la posibilidad de que personas no autorizadas ingresen a zonas de seguridad.

Además, no se tiene un sistema de respaldo de datos que garantice la integridad de los registros de ingreso, ni con protocolos modernos de verificación que minimicen el riesgo. Esto representa un desafío importante para la universidad, ya que compromete tanto la seguridad física como la protección de la información que allí se gestiona.

1.5 Objetivos

1.5.1 Objetivo general

Aplicar un sistema de control de acceso biométrico para el acceso al centro de vigilancia del área técnica de la Universidad Laica Eloy Alfaro de Manabí Extensión Chone.

1.5.2 Objetivos específicos

- Determinar el impacto de los sistemas biométricos en el fortalecimiento de la seguridad y la eficiencia operativa que ofrecen.
- Identificar las necesidades de seguridad y control de acceso actuales en el centro de vigilancia del área técnica de la Extensión Chone.
- Implementar un sistema de autenticación biométrica que se adapte a los requerimientos del área técnica.

1.6 Justificación

Al utilizar un control de acceso hace referencia a los métodos automáticos que analizan las características humanas con el único fin de identificar y autenticar a las personas para acceder a un lugar donde se guarde información de mucha importancia, y solo así se podrá ingresar si se cuenta con los mecanismos de seguridad como es la huella dactilar para obtener acceso a dicho departamento (Nieves Villamar, 2021).

Actualmente, la seguridad es fundamental dentro de cualquier institución, y más aún en áreas como los centros de control de vigilancia, donde se manejan equipos, información y recursos importantes. En la ULEAM extensión Chone, el acceso a estas áreas todavía se realiza de forma manual o sea de manera tradicional, esto representa ciertos riesgos, como el ingreso de personas no autorizadas o la falta de control sobre quién entra o sale.

Por esta razón, este proyecto busca proponer un sistema de autenticación biométrica que permita mejorar el acceso a esta área como lo es el centro de control de vigilancia, utilizando características únicas de cada persona, como la huella dactilar o el rostro. Esto

ayudaría a tener un mayor control y seguridad, ya que solo el personal autorizado podría ingresar.

También, este tipo de sistema no solo aporta seguridad, sino también organización, ya que dejaría un registro de los accesos y facilitaría el trabajo del personal de vigilancia. Esta propuesta también puede servir como base para futuras mejoras tecnológicas dentro de la universidad, demostrando que es posible implementar soluciones modernas que se adapten a las necesidades actuales.

Menciona Herrera, (2023) que “hoy en día se puede encontrar con sistemas básicos de automatización de puertas, estos son activados mediante un control remoto por radio frecuencia, es así como la delincuencia ha encontrado maneras para sustraer dicho mando remoto, el mismo que puede ser manipulado y utilizado de forma indebida sin ningún tipo de restricción”(p.13).

En sí este proyecto es interesante e importante ya que busca proteger mejor los espacios sensibles de la universidad y a la vez impulsar el uso de estas tecnologías enfocadas a la seguridad, y esto dentro del entorno académico de manera que facilite el acceso a personal autorizado al área de vigilancia.

1.7 Impactos esperados

1.7.1 Impacto tecnológico

La puesta en marcha de un sistema de reconocimiento biométrico es un progreso importante en la adopción de nuevas tecnologías en la universidad. Este proyecto facilita la incorporación de soluciones digitales que son más seguras y eficaces, sustituyendo métodos antiguos que ya no son útiles. También mejora la cultura tecnológica de la institución al incluir herramientas de identificación mejoradas que podrán actualizarse en el futuro. Este efecto también permite que otras secciones de la universidad piensen en usar sistemas parecidos, fomentando una evolución digital gradual en la institución.

1.7.2 Impacto Social

Desde la perspectiva social, el proyecto favorece la sensación de protección entre el personal, los alumnos y los visitantes de la universidad. Tener un sistema efectivo para controlar el acceso ayuda a crear un entorno más seguro y estructurado, donde todos sienten

que su información, incluso sus pertenencias están a salvo. Además, impulsa la responsabilidad personal, puesto que cada usuario tendrá una identificación única. También puede abrir nuevas posibilidades de aprendizaje para los estudiantes y técnicos interesados en entender este tipo de tecnología y cómo se utiliza en situaciones reales.

1.7.3 Impacto ecológico

Aunque la propuesta se basa principalmente en tecnología, también beneficia indirectamente al medio ambiente. Al manejar el acceso de forma automática y disminuir la necesidad de documentos impresos para el registro de acceso, se ayuda a usar menos materiales. Esto contribuye a minimizar el desperdicio y apoya hábitos más sostenibles en la universidad. Además, al eliminar los viajes innecesarios del personal para comprobar accesos o hacer informes a mano, se reduce el gasto de energía y tiempo, creando un espacio más eficiente.

CAPITULO II: MARCO TEÓRICO DE LA INVESTIGACIÓN

2.1 Sistema de autenticación biométrica

2.1.1 Concepto y fundamentos de la biometría

Según Santi Pereyra, (2018) La biometría humana actual se basa en un sistema de identificación que se nutre de indicadores estáticos, principalmente de datos biológicos estables (tales como características faciales, del iris, huellas digitales, mapeo vascular, etc.) y/o de patrones dinámicos, como ciertos datos del comportamiento de las personas (regularidades en la escritura y firma, la forma de caminar, etc.).

Por otro lado Valderrama, (2019) afirma que la autenticación biométrica consiste en la verificación de la identidad el usuario mediante el reconocimiento de características fisiológicas o de comportamiento únicas de un individuo como la fisonomía del rostro, patrón de la huella dactilar, reconocimiento de voz, retina, iris, entre otros. Para esto se utiliza un lector biométrico que captura el elemento biométrico para su posterior comparación con los previamente registrados.

Como lo menciona Rodríguez Pinto & Ortega Romero, (2017) en su estudio de “Pre- Factibilidad para un sistema de control de acceso peatonal en la Universidad Distrital Francisco José de Caldas”, los sistemas de control de acceso se han hecho muy populares en empresas e instituciones que venían utilizando los sistemas de control de accesos con personal, además, al ser su precio cada vez más asequible, también están siendo implantados en domicilios particulares y residencia.

Así mismo, Rangel Rivas, (2024) indica que la identificación de personas es sin duda el ámbito donde la aplicación de las huellas dactilares es más relevante. En criminalística y medicina forense, las huellas dactilares se consideran evidencia fundamental para identificar a las personas involucradas en hechos delictivos.

Teniendo en cuenta lo dicho por el autor anteriormente mencionado, esta creciente adopción de sistemas de control de acceso evidencia una tendencia hacia la modernización. Esta evolución se debe, en su mayoría, a la accesibilidad económica de estas tecnologías lo cual a permitido apartarla en diferentes áreas. El paso de implementar un sistema de control no solo responde a una necesidad de eficiencia operativa, sino también a la búsqueda de

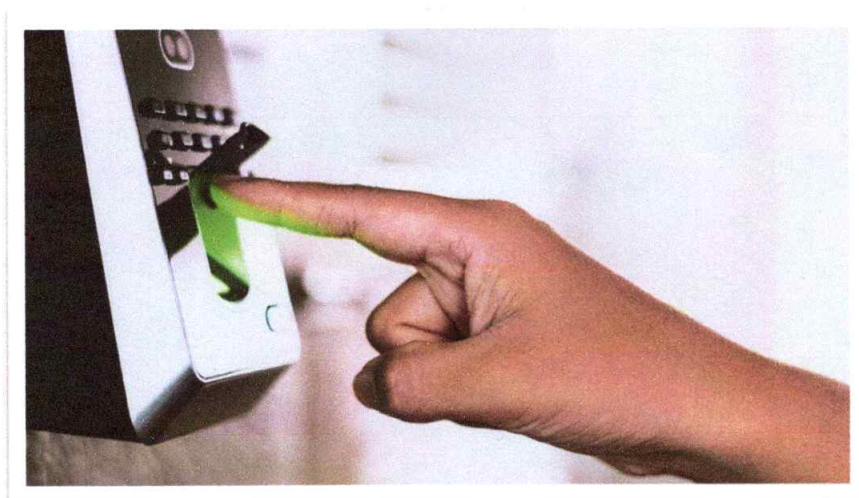
mayor fiabilidad y precisión en la identificación de las personas que acceden a un espacio en específico.

2.1.2 Tipos de sistemas biométricos.

Tal como menciona Meneses & Garcia, (2016) existen sistemas biométricos de carácter fisiológico y comportamental, para el campo que compete al proyecto se tratarán únicamente los que corresponden a los tipos de sistemas biométricos con carácter fisiológicos.

- **Reconocimiento de la huella dactilar:** Típicamente la huella dactilar de un individuo ha sido un patrón bastante bueno para determinar su identidad de forma inequívoca, ya que está aceptado que dos dedos nunca poseen huellas similares, ni siquiera entre gemelos o entre dedos de la misma persona. El uso de estos patrones fue uno de los primeros en establecerse como modelo de autenticación biométrica. Cuando un usuario desea autenticarse ante el sistema sitúa su dedo en un área determinada (área de lectura, no se necesita en ningún momento una impresión en tinta). En la siguiente figura se mostrará una imagen en la que se puede apreciar un dispositivo lector de huellas dactilares.

Figura 2. Lector de huellas dactilares

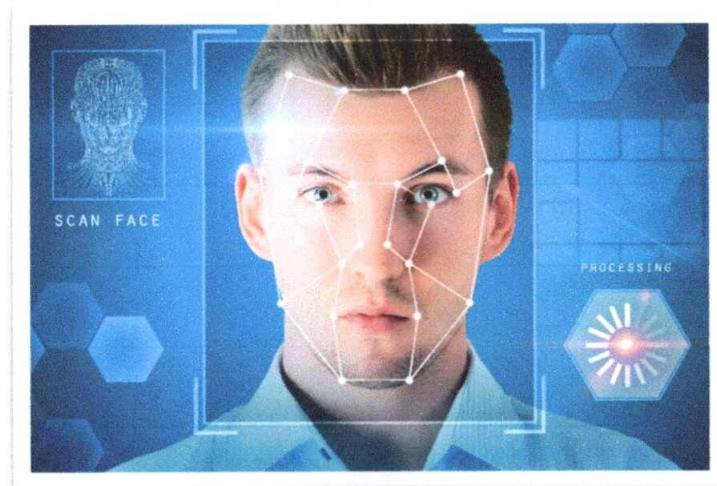


Nota. Imagen referencia a un lector de huellas dactilares. Tomado de ¿Fichar con huella dactilar es legal? [Imagen] Control Laboral, de 2023, <https://controllaboral.es/fichar-huella-dactilar-legal/>

- **Reconocimiento de la cara:** la biometría facial es una forma avanzada de identificación biométrica que utiliza características únicas del rostro para la autenticación de las personas. Su uso no es demasiado frecuente ya que los rasgos de la cara pueden verse afectados con el paso del tiempo, así como un cambio en el crecimiento de los bellos faciales puede influir a la hora de realizar la identificación. Sin embargo, en algunos casos al contar con patrones faciales puede llevarse a cabo la autenticación de una identidad.

A continuación, en la siguiente figura se muestra una referencia de cómo funcionan las tecnologías de reconocimiento facial, el sistema detecta y analiza rasgos del rostro (ojos, nariz, mandíbula, etc.)

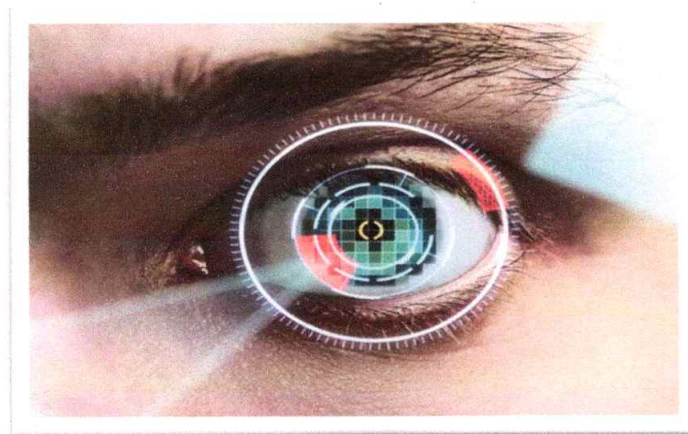
Figura 3. Biometría facial



Nota. Imagen referencia al funcionamiento de un sistema de biometría facial. Tomado de Biometría facial: ¿cómo funciona en la validación de identidad? [Imagen] Biometría facial, de 2024, <https://blog.truora.com/es/biometria-facial>

- **Reconocimiento de iris/retina:** Este sistema de autenticación es uno de los más usados ya que los patrones oculares cuentan con una probabilidad de coincidencia muy cercana a cero y a la hora de la muerte estos se degeneran rápidamente evitando así un fraude del patrón. A pesar de esto posee desventajas ya que al realizar la lectura con un láser es incómodo para el usuario y además si este usa lentes se verá afectado su patrón y no podrá realizarse la identificación.

Figura 4. Reconocimiento del iris



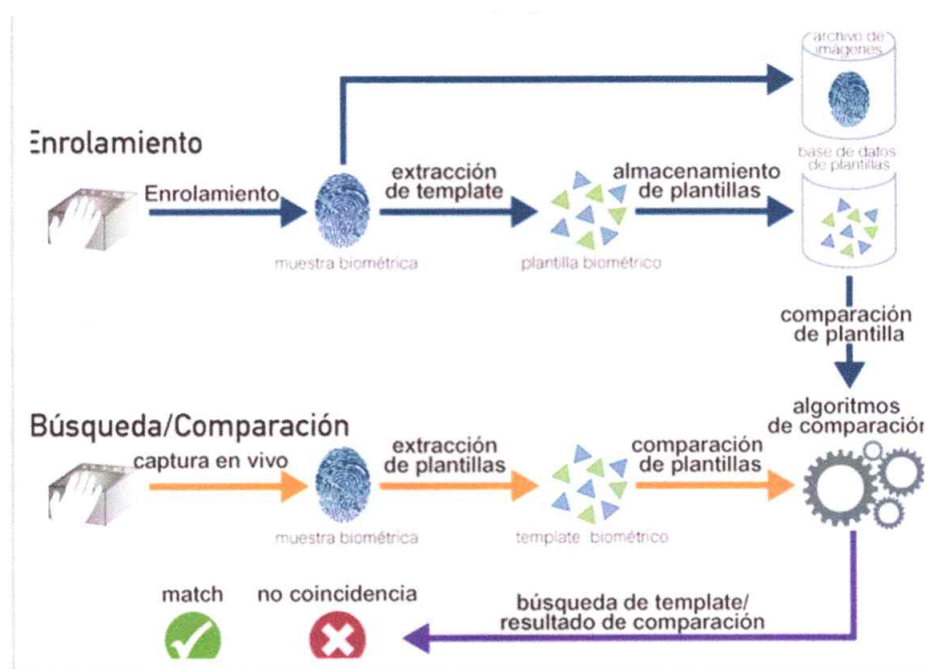
Nota. Imagen referencia al funcionamiento de un sistema de biometría de reconocimiento del iris. Tomado de EL BOLETIN: Reconocimiento del iris y la seguridad biométrica: ¿El sistema perfecto? [Imagen] EL BOLETIN, de 2021, <https://www.elboletin.com/reconocimiento-del-iris-y-la-seguridad-biometrica-el-sistema-perfecto/>

2.1.3 Funcionamiento técnico de un sistema biométrico.

Como mencionan los autores Murillo Quimiz & Delgado Pilligua, (2018) en su tesis, que los sistemas biométricos funcionan registrando imágenes a través de tomas de la huella digital. Cuando se toca el dispositivo, este envía la información de registro y recoge la muestra biométrica. Las huellas dactilares se almacenan en una base de datos y se guardan como plantillas.

Una vez que se obtiene la muestra, el sistema la evalúa con las distintas plantillas que están guardadas en la base de datos para hacer la comparación. Este procedimiento está completamente protegido por patente y se puede observar en la Figura 4, lo que significa que es confidencial y cada aparato tiene su propia forma única. Al comparar las minucias de la huella dactilar, con las plantillas guardadas si son las correctas entonces, da la autorización caso contrario esta no será aceptada debido a los cambios en las huellas dactilares.

Figura 5. Arquitectura de un sistema biométrico



Nota. Imagen referencia al funcionamiento de un sistema biométrico. Aware: <https://www.aware.com/wp-content/uploads/2015/07/a-biometric-system.jpg>

2.1.3.1 Procesos de los Modelos de tecnologías biométricas

También el autor antes mencionado, en su tesis, menciona los siguientes procesos en cuanto al modelo de las tecnologías biométricas:

➤ Recopilación de datos.

Este proceso consiste en la captación inicial de los datos biométricos del usuario. Se da en la fase de entrada, donde el individuo busca acceder a un sistema controlado mediante tecnologías biométricas. Para lograr una correcta identificación, la información captada debe estar lo más estandarizada posible. Sin embargo, la calidad de esta fase no solo depende de los datos del usuario, sino también de las características técnicas del dispositivo utilizado, tales como la calibración, resolución, estabilidad y sensibilidad del sensor.

➤ **Transmisión de datos.**

Generalmente, la transmisión de los datos biométricos se realiza desde un punto distinto al lugar donde serán almacenados. Este tipo de información, como imágenes faciales, huellas digitales o registros de voz, tiende a ocupar gran cantidad de espacio. Para mitigar este problema, se emplean técnicas de compresión estándar o, en algunos casos, algoritmos especializados como la cuantificación escalar, permitiendo reducir el volumen sin comprometer la calidad necesaria para una identificación precisa.

➤ **Procesamiento de señales.**

Una vez que la información biométrica ha sido captada y transmitida, se procede a su procesamiento. Este se realiza mediante la conversión de las muestras en vectores de características (por ejemplo, en el caso de huellas o imágenes faciales), los cuales luego son organizados en matrices para facilitar su análisis y comparación en etapas posteriores.

➤ **Almacenamiento de información.**

Los datos biométricos procesados se almacenan en una base de datos central. Cuando un usuario es registrado en el sistema, su información queda guardada con el propósito de permitir futuras verificaciones. Posteriormente, cada intento de acceso será contrastado con esta base, donde se determinará si existe coincidencia suficiente para permitir la autenticación, como en el caso de las huellas dactilares.

➤ **Identificación.**

En esta fase, el sistema compara la muestra captada con los registros previos en la base de datos. El objetivo es determinar la identidad del usuario, evaluando similitudes que respondan a preguntas internas como: “¿Es usted Pedro?”. Si los datos coinciden, el acceso es autorizado; en caso contrario, se deniega automáticamente.

➤ **Verificación.**

Una vez identificado, el usuario puede ser verificado, es decir, se confirma que la identidad previamente establecida corresponde efectivamente con la muestra presentada. Este proceso suele realizarse mediante la comparación de datos binarios, utilizando secuencias codificadas en 0 y 1 para validar la autenticidad del acceso.

➤ **Toma de decisión.**

Este es el paso final en el modelo biométrico. Aquí, el sistema evalúa las comparaciones realizadas y toma una decisión sobre si autorizar o denegar el acceso. Si la muestra biométrica coincide adecuadamente con los registros, el sistema otorga la autorización correspondiente. De lo contrario, no se emite el código de validación y se bloquea el ingreso al sistema.

2.1.4 Ventajas y desventajas de la autenticación biométrica.

Cabe destacar que el avance de la tecnología y la necesidad de proteger datos sensibles han incrementado la importancia de la biometría en el ámbito de la seguridad. Su aplicación se ha extendido, pero a medida que se aplica en la vida cotidiana y en el entorno empresarial, surgen desafíos en términos de privacidad y seguridad. Por lo tanto, es fundamental evaluar las posibles vulnerabilidades en la autenticación biométrica (Cerna et al., 2023).

Entre las ventajas de implementar un sistema de autenticación biométrica se encuentran las siguientes:

- Elimina el uso de password vulnerable a olvido, divulgación, ingeniería social, robo, préstamo, ataques por fuerza bruta, etcétera.
- Dado que la huella digital es única intransferible no se desconfigura no es vulnerable a robo y difícilmente falsificada la tecnología permítela identificación del individuo de forma segura.
- Facilidad de uso.
- Alto nivel de confiabilidad.
- Reducción de hasta un 80% de las llamadas por problemas de uso y cambios de password dando como resultado un ahorro en cuanto a Recursos Humanos y así mismo, una elevación de la productividad.

Así mismo, existen ciertas desventajas al implementar un sistema de autenticación biométrica:

- Requiere de un costo inicial de implementación elevado debido a la adquisición de dispositivos, instalación y personal capacitado.

- Los sistemas biométricos requieren de un mantenimiento regular tanto en software para posibles actualizaciones como en la calibración del hardware.

2.1.5 Aplicaciones prácticas de la biometría en instituciones.

"Un ejemplo relevante sobre la implementación de biometría institucional es el estudio de Tamami González & Ortiz Minchala, (2024) En su investigación para la Universidad Técnica Estatal de Quevedo (UTEQ), las autoras proponen un sistema de seguridad telemático orientado al sector industrial que utiliza el reconocimiento facial para la autenticación, esto resulta aplicable en instituciones educativas que buscan controlar el acceso a lugares sensibles."

El sistema se basa en el uso de cámaras y software especializado que captura imágenes del rostro de los usuarios para permitir o denegar el acceso, lo cual garantiza un control más preciso y seguro que los métodos tradicionales como contraseñas o tarjetas magnéticas. Entre los beneficios identificados están la reducción de riesgos asociados a accesos no autorizados, el mejoramiento de la trazabilidad de entradas y salidas, y el fortalecimiento de la seguridad institucional. Además, el sistema fue desarrollado bajo estándares de eficiencia energética y con un enfoque económico accesible, lo que lo convierte en una alternativa viable para instituciones de diferente tamaño.

Este tipo de implementación evidencia cómo la biometría no solo mejora los niveles de seguridad, sino que también optimiza procesos internos en las organizaciones, permitiendo un monitoreo más eficiente del personal y reduciendo los márgenes de error de las personas en los registros de acceso.

Otro caso práctico que evidencia el uso institucional de la biometría se encuentra en la empresa Alignet S.A.C., donde se desarrolló un proyecto orientado a mejorar el proceso de autenticación de transacciones mediante tecnologías biométricas. Este estudio, realizado por Correa Cardenas & Panizo Pascual, (2020), aplicó la metodología Six Sigma para identificar fallas en el sistema de autenticación y propuso como solución la incorporación de biometría facial en las operaciones realizadas desde aplicaciones móviles.

La propuesta incluyó un rediseño del flujo de autenticación que integra una validación biométrica antes de confirmar transacciones digitales, especialmente en contextos financieros. Este enfoque no solo aumentó el porcentaje de autenticaciones exitosas, sino que

también redujo significativamente los intentos de fraude y mejoró la experiencia del usuario, permitiendo mayor agilidad y confianza en el uso del servicio.

El caso de Alignet S.A.C. demuestra que la biometría puede ser aplicada exitosamente en instituciones del sector privado con altos estándares de seguridad digital. Además, ofrece un modelo replicable en instituciones públicas y educativas que busquen fortalecer la verificación de identidad en entornos digitales.

Como último caso de aplicación práctica de la biometría, se presenta en la unidad educativa ITSI (Instituto Tecnológico Superior Informático) del Cantón Chone, con el proyecto titulado “Sistema biométrico para automatizar el registro de asistencia docente en la unidad educativa ITSI del cantón Chone” (Menéndez Chávez & Muñoz Loor, 2016).

El principal objetivo de aquel proyecto es la implementación de un sistema biométrico para los directivos de esta institución, ya que les permitirá llevar un mejor control del registro de asistencia para los docentes de la institución mencionada anteriormente, de esta manera generando automáticamente un reporte de las horas trabajadas.

Con la existencia de un dispositivo biométrico la institución tendrá una forma más segura de registrar la asistencia docente mediante la tecnología del reconocimiento facial, se ahorraría papel y el consumo de las impresoras, así como también se optimizaría el tiempo del encargado de llevar el registro de asistencia.

Es por este motivo que se implementa un sistema de seguridad más exacto y constante, el mismo que sea apto para reconocer, distinguir a los docentes de las demás personas, como padres de familia por ejemplo y de esta manera mejorar el sistema en cuanto a registrar la asistencia con el uso de un dispositivo biométrico.

2.2 Nivel de seguridad en el acceso al centro de control de vigilancia

2.2.1 Conceptualización de centros de controles de vigilancia

Pinargote Vines (2022) menciona qué los sistemas de seguridad son grupos de elementos instalados e intercomunicados entre sí que previenen, detectan o actúan ante intrusiones, intentos de robos y otros eventos”.

Por otro lado, SeguriTech (2022) menciona que son conocidos como Cuartos de Control o Control Rooms en otros países. Es en estos lugares, es en donde una serie de operadores capacitados, monitorean simultáneamente diversos puntos, con el fin de reaccionar de manera oportuna e inmediata ante cualquier alerta, emergencia o amenaza que ponga en riesgo la seguridad de la sociedad. Si bien dichos centros varían en cuanto a su estructura, todos comparten la misma misión: ser el primer escudo de seguridad

De esta manera se logra entender que un centro de vigilancia es una área o espacio donde se gestiona y/o supervisa la seguridad de un área en específico haciendo usos de sistemas tecnológicos. El objetivo principal de un centro de control de seguridad es supervisar y gestionar la seguridad de una organización, identificando y a la vez respondiendo ante incidentes y emergencias de manera eficiente mediante la instalación de cámaras de vigilancia en lugares estratégicos.

La implementación de un centro de control y monitoreo en el desarrollo de sistemas de vigilancia institucional se considera como un recurso efectivo para supervisar y administrar dispositivos de seguridad desde un punto estratégico. En la tesis sobre la Implementación de una central de control y monitoreo de cámaras de seguridad para la Facultad de Sistemas y Telecomunicaciones, el autor Cruz Vera (2021), explica que se habilitó una infraestructura de red y equipos de video vigilancia situados en lugares estratégicos, permitiendo la visualización en tiempo real desde una sala de control.

De acuerdo con Tasayco Coronado, Víctor Carlos (2023), La infraestructura de un centro de datos requiere una cuidadosa consideración de la seguridad de la infraestructura de TI. Esto puede incluir seguridad física para el edificio, como entrada de llave electrónica, video constante y vigilancia humana de las instalaciones, acceso cuidadosamente controlado al servidor y espacios de almacenamiento, etc. Esto garantiza que solo el personal autorizado

pueda acceder a la infraestructura de hardware del centro de datos y reduce la posibilidad de daños malintencionados o robo de datos.

la implementación de sistemas de video vigilancia con cámaras IP permite el monitoreo permanente de áreas críticas, el registro de evidencias y el fortalecimiento de la seguridad en instituciones educativas, de tal manera que contribuye a una gestión más eficiente de los centros de control de vigilancia (Arenas & Chan, 2017).

Podemos decir que un centro de control de vigilancia es un espacio físico y tecnológico destinado a la supervisión, gestión y respuesta ante eventos de seguridad, sea este en instituciones educativas, empresas públicas o privadas, y otras entidades. El funcionamiento de un centro de estos se basa en la integración de personal capacitado, dispositivos electrónicos, redes de comunicación y software especializado para que permita el monitoreo constante de las instalaciones.

En la tesis escrita por Yenitlfer del Carmen López Pardo, (2014) se mencionan aspectos de suma importancia en cuanto a la estructura y funcionamiento de un sistema de control biométrico utilizado en empresas de seguridad privada. En los aspectos que se describen en aquella tesis se encuentran:

- Contar con Hardware como lo son los sensores de huellas dactilares, Un Switch de Comunicaciones Administrable, y Un Servidor de almacenamiento en el cual está instalado el software de control que almacena la base de datos y manejo de reportes.
- En cuanto al software, existen diversas soluciones según el fabricante y el entorno de uso. Algunas opciones comerciales como ZKTeco, Suprema, entre otros ofrecen plataformas propietarias con interfaces gráficas amigables y funcionalidades avanzadas.

2.2.2 Tipos de centro de vigilancia

Por sus características, alcances, funciones y niveles de gobierno que operan a través de ellos, estos son los Centros de Control y Monitoreo más destacados en nuestro país:

- C2: Su nombre significa "Centro de Comando y Control" y son las unidades regionales que monitorean las grabaciones de vigilancia de diversas áreas

- C4: El Centro de Comando, Control, Comunicaciones y Cómputo es similar al C2. También funciona como estación de videovigilancia, pero integra tecnologías informáticas y la línea telefónica 911
- C5: El Centro de Comando, Control, Comunicaciones, Cómputo y Contacto Ciudadano integra todos los elementos de un C2 o un C4, pero además opera a escala nacional, estatal o municipal
- C5i: (Centro de Control, Comando, Comunicaciones, Cómputo, Contacto Ciudadano e Inteligencia)

2.2.3 Problemáticas comunes en los Centros de Vigilancia sin control biométrico

Como lo indica Gentile (2025), adoptar un sistema de acceso biométrico no solo es una medida tecnológica, sino una inversión estratégica que protege a las empresas de riesgos operativos y legales. Los métodos tradicionales, como tarjetas o registros manuales, pueden parecer suficientes, pero suelen ser altamente vulnerables al fraude y la falta de control.

De la misma manera, el autor antes mencionado describe que la ausencia de esta tecnología y cómo su implementación puede marcar la diferencia en cuanto a seguridad de alguna organización o entidad. A continuación, se detalla los principales problemas que se asocian a la falta de esta tecnología.

➤ Fraude en nóminas y pagos indebidos

El “marcado fantasma” es uno de los principales problemas en empresas sin sistemas biométricos, donde empleados ausentes o inexistentes son registrados como presentes. Esto genera pagos indebidos y eleva los costos operativos.

➤ Suplantación de identidad y acceso no autorizado

Los sistemas tradicionales como tarjetas o contraseñas son vulnerables a la suplantación de identidad. Esto permite que personas no autorizadas accedan a instalaciones restringidas, comprometiendo la seguridad de la empresa.

Por ejemplo, en una planta industrial, un contratista podría utilizar la tarjeta de un empleado registrado para trabajar sin estar autorizado. Este tipo de situaciones no solo comprometen la integridad de los procesos, sino que también pueden derivar en sanciones legales si se permite el acceso a personas no habilitadas para realizar ciertas tareas.

CAPITULO III: DISEÑO METODOLÓGICO

3.1 Tipo de investigación.

El tipo de investigación es aplicada, esto se debe a que busca implementar una solución tecnológica a una necesidad real en el contexto institucional como lo es en la ULEAM. Además, es de tipo cualitativo y descriptivo, debido a que se pretende comprender la situación actual del control de asistencia, la percepción de los usuarios frente a los sistemas tradicionales y las condiciones operativas que rodean la futura implementación del sistema biométrico.

3.2 Nivel de Investigación

El nivel de investigación que se optó es descriptivo. Este nivel permitirá detallar las características fundamentales de la falta de implementación de un control biométrico en el centro de vigilancia del área técnica, así como identificar las problemáticas más comunes en su operatividad. Este tipo de estudio busca observar y registrar el estado actual de los centros de vigilancia en cuanto a sus procedimientos de autenticación y control, permitiendo identificar problemáticas frecuentes

3.3 Enfoque de investigación

Se adoptará un enfoque cualitativo, debido a que el proyecto se centra en las experiencias, percepciones y/o problemáticas enfrentadas en el centro de vigilancia, ya que no dispone de un control de sistema biométrico. Además, nos permitirá interpretar, desde la perspectiva de las personas autorizadas, las debilidades y riesgos del modelo actual de acceso, mediante entrevistas a responsables de seguridad y observación directa de los procedimientos.

3.4 Métodos de investigación.

Se utilizará el método científico, el método experimental y bibliográfico.

El método científico se entiende como un procedimiento general que se aplica a todo el ciclo de la investigación, no solo en etapas aisladas como la medición o el análisis, sino desde el planteamiento del problema hasta la validación de las hipótesis. Según se expone, especializarse únicamente en una técnica o etapa no otorga una visión completa de este método; por el contrario, lo ideal es abordar una investigación desde sus inicios, comprendiendo las preguntas que la originan y todo el proceso que conlleva. Solo así se

puede captar la estructura metódica integral que sustenta a toda práctica científica (Bunge 2017).

El método científico permitirá seguir una secuencia lógica (observación del problema, formulación de hipótesis, diseño de solución, prueba e interpretación de resultados), por otro lado, el método experimental permitirá validar el sistema implementado, verificando su funcionamiento y su impacto en el control de acceso.

3.5 Fuentes de datos.

3.5.1 Fuentes primarias

- Entrevistas a responsables de seguridad y administración institucional.
- Observación directa de los accesos actuales.

3.5.2 Fuentes secundarias

- Tesis y artículos científicos sobre sistemas biométricos, centros de vigilancia y control de acceso.
- Manuales técnicos de dispositivos biométricos y software relacionados.
- Normativas institucionales de seguridad y control.

3.6 Estrategia operacional para la recolección de datos.

Se aplicará una estrategia basada en tres fases:

- Diagnóstico inicial: se plantea realizar una observación del entorno, entrevistas con el personal, análisis documental.
- Levantamiento de requerimientos y preparación de entrevista para conocer la percepción sobre la seguridad actual y la viabilidad del sistema biométrico.
- Implementación del prototipo y validación experimental del funcionamiento del sistema con usuarios autorizados.

3.6.1 Técnicas y herramientas

Para la recolección de datos se emplearán técnicas cualitativas que permitan diagnosticar la situación actual, definir los requerimientos y validar el funcionamiento del sistema a implementar. Las herramientas específicas serán:

- Entrevistas semiestructuradas: realizadas al encargado del laboratorio en el que se encuentra el centro de vigilancia y a la coordinadora de carrera, con el fin de obtener información detallada sobre las necesidades operativas de este centro y validar requerimientos funcionales.
- Observación directa: para identificar las condiciones físicas y los flujos de entrada actuales en el área de vigilancia, así como los posibles puntos vulnerables.
- Software de grabación: Para registrar entrevistas y garantizar la fidelidad de los datos obtenidos.

3.6.2 Instrumentos de la Investigación.

- Ficha de observación: Diseñada para registrar flujos de trabajo, tiempos y errores en los procesos actuales.
- Guion de entrevistas: Una guía con preguntas clave para profundizar en las necesidades y problemas de la institución.

3.7 Descripción de la población y Diseño de la muestra

La población está constituida por el personal administrativo y técnico del área, entre los cuales se escogió una muestra por conveniencia a dos personas. Aquellos escogidos son quienes participan directamente en la gestión y control de acceso al centro de vigilancia, cabe resaltar que es importante recopilar información sobre el ingreso de personal e identificar irregularidades o acceso no debidos a esta zona privada del área técnica.

3.8 Análisis y presentación de los resultados

3.8.1 Análisis de la ficha de observación aplicada

La ficha de observación que fue aplicada en el centro de control de vigilancia de la ULEAM extensión Chone tuvo como objetivo evaluar la situación actual del control de acceso y proponer mejoras para la implementación de un sistema biométrico basado en huellas dactilares. A continuación, se detallan los hallazgos de la observación y su análisis.

1. ¿El proceso de control de accesos actual es eficiente?

- **Observación:** No es eficiente, ya que se necesita solicitar presencialmente una autorización previa.
- **Análisis:** El proceso no se considera eficiente ya que, si alguien necesita ingresar, este debe primeramente solicitar permiso o contar con llaves para abrir la puerta.

2. ¿Existen debilidades en la verificación de identidad del personal?

- **Observación:** Se conoce al personal autorizado.
- **Análisis:** Como tal no existen debilidades al conocer el personal autorizado, esto debido a que el encargado conoce el personal que puede solicitar ingresar.

3. ¿Se detectan ingresos no autorizados o intentos de suplantación?

- **Observación:** No existen antecedentes relacionados a este caso.
- **Análisis:** No es común que se den estos casos, sin embargo, aplicar un sistema de seguridad biométrica no solo previene casos así, sino que también agiliza el ingreso.

4. ¿El flujo de acceso al centro de vigilancia es rápido y ordenado?

- **Observación:** Se debe solicitar permiso lo cual conlleva tiempo.
- **Análisis:** Además de que se debe solicitar permiso para acceder, también el ingreso es limitado o sea que no pueden estar muchas personas dentro del centro de control de vigilancia.

5. ¿Se utilizan herramientas tecnológicas en el proceso actual?

- **Observación:** No se dispone de herramientas tecnológicas para el acceso al centro de vigilancia.

- **Análisis:** La manera en que se maneja el ingreso es a través de llaves físicas, esto retrasa y no permite llevar un registro automatizado.

6. ¿Se evidencian errores frecuentes en el registro manual de accesos?

- **Observación:** No se evidencian de errores frecuentes.
- **Análisis:** No se evidencian errores, sin embargo, la recolección de firmas de los ingresos al laboratorio donde se ubica el centro de control de vigilancia puede darse que alguien no registre su ingreso.

7. ¿El personal administrativo requiere capacitación en nuevas tecnologías?

- **Observación:** Todo el personal administrativo cuenta con conocimientos sobre nuevas tecnologías.
- **Análisis:** Por lo general el personal del administrativo del área técnica ya conoce sobre nuevas tecnologías, así como lo son los dispositivos biométricos por tal manera la capacitación no sería compleja.

8. ¿El personal de seguridad cumple con los protocolos establecidos?

- **Observación:** Se registra el ingreso al laboratorio.
- **Análisis:** El personal de seguridad si cumple con los protocolos establecidos.

3.8.2 Análisis de los resultados de la entrevista.

La entrevista aplicada al personal previamente seleccionado del área técnica permitió identificar elementos clave sobre la gestión actual del acceso al centro de control de vigilancia del bloque B. Estos resultados muestran que el ingreso se administra mediante solicitudes y autorizaciones previas, sin embargo, este proceso depende en gran medida del personal de turno. Esta dependencia genera variabilidad en el control, ya que la supervisión no siempre se realiza con el mismo nivel de rigurosidad y por lo tanto acceso actual carece de mecanismos tecnológicos que permitan validar la identidad real de los usuarios, dando paso a procedimientos manuales que son probables a errores y a posibles fallas en la verificación de quienes ingresan.

Uno de los puntos con más relevancia identificados es la presencia de problemáticas relacionadas con la falta de un registro preciso y automatizado de los ingresos. Según los entrevistados, existen horarios en los que no se cuenta con un registro exacto, lo que aumenta la vulnerabilidad del área. Además, debido a que el centro de vigilancia se encuentra dentro de un laboratorio, detectar ingresos no autorizados resulta complejo, ya que comparten el mismo espacio físico. Esto indica una necesidad urgente de fortalecer los mecanismos de control interno y determinar con mayor claridad los accesos al centro.

Los entrevistados también mencionaron que la seguridad actual no es completamente suficiente, ya que la falta de tecnología dificulta la verificación del personal que ingresa y limita el rastreo de los eventos ocurridos. En si la percepción sobre la implementación de un sistema biométrico es positiva, se considera que dicho sistema tendría un impacto favorable al mejorar la precisión en la identificación, reducir el riesgo de accesos indebidos y fortalecer la seguridad institucional. A esto se suma que la mayoría del personal cuenta con conocimientos previos sobre biometría, lo que facilitaría la implementación del sistema sin mayores dificultades.

3.8.3 Presentación y descripción de los resultados obtenidos

La recolección de datos se realizó mediante dos instrumentos cualitativos, una entrevista semiestructurada dirigida a una pequeña parte del personal del área técnica y una ficha de observación aplicada directamente en el centro de control de vigilancia del bloque B. Ambos instrumentos permitieron obtener una visión completa del funcionamiento actual del control de acceso, así como de las dinámicas internas y debilidades del sistema vigente. La entrevista aportó información desde la perspectiva de la experiencia del personal, mientras que la observación permitió contrastar dichos testimonios con la realidad operativa del lugar. La complementariedad entre ambas fuentes posibilitó identificar patrones que coinciden, detalles críticos y áreas que requieren intervención para mejorar la seguridad institucional.

CAPITULO IV: EJECUCIÓN DEL PROYECTO

4.1 Descripción del proyecto

Este proyecto propone la implementación de un sistema de seguridad actualizado, esto con dispositivos de biométricos que ayuden a facilitar el acceso haciéndolo más rápido y efectivo. Se propone utilizar un dispositivo biométrico basado en huellas digitales para manejar el control de acceso al área de vigilancia del área técnica de la ULEAM Extensión Chone.

El sistema biométrico permitirá gestionar el ingreso sea del personal docente o técnico, y este almacenará los registros de ingresos en una base de datos centralizada, este control contribuiría a reducir el riesgo de accesos no autorizados, pérdida de información y manipulaciones no debidas de externos. Cabe mencionar que el uso de tecnología biométrica en el área técnica refuerza el uso de recursos tecnológicos.

4.2 Determinación de recursos

4.2.1 Recursos Humanos.

El desarrollo e implementación del sistema requiere la participación de un equipo que contribuya en distintas fases del proyecto. A continuación, se detallan los roles:

Tabla 1: Recursos humanos

Recurso	Descripción
Estudiantes desarrolladores	Encargados del diseño, programación e integración del sistema biométrico, así como del levantamiento de información y pruebas de funcionamiento.
Docente asesor	Brinda acompañamiento académico y técnico durante el desarrollo del proyecto, velando por el cumplimiento de los objetivos y la calidad metodológica.
Responsable del Área	Colaborador institucional que facilita el acceso al centro de vigilancia, participa en la validación del sistema y proporciona información sobre el entorno de trabajo.
Personal de vigilancia	Usuarios directos del sistema; aportan con su experiencia en los accesos actuales y participan en las pruebas del prototipo.

Nota. Recursos Humanos a tener en cuenta para desarrollo del proyecto. [Tabla] Autores del proyecto, 2025

4.2.2 Recursos tecnológicos.

Para garantizar un desarrollo y funcionamiento adecuado del sistema de autenticación biométrica por huella digital, se requiere el siguiente equipamiento y software:

Tabla 2: Recursos Tecnológicos

Recurso	Descripción
Sensor biométrico ZKTeco	Lector de huellas digitales, modelo como ZKTeco Ma300 o similar.
Laptop o PC de desarrollo	Con procesador i5 o superior, 8GB de RAM, para programación e integración.
Base de datos local	Sistema de almacenamiento de registros y datos de usuarios.
Cableado y conectividad	Cables USB, energía y red para conexión del lector biométrico.
Fuente de alimentación	Estabilizador o UPS para asegurar el funcionamiento continuo.
Monitor	Para visualizar registros de acceso en el centro de control.

Nota. Recursos tecnológicos a tener en cuenta para desarrollo del proyecto. [Tabla] Autores del proyecto, 2025

4.2.3 Recursos económicos.

A continuación, se presenta una estimación del presupuesto necesario para ejecutar el proyecto, considerando recursos tecnológicos, materiales y apoyo logístico:

Tabla 3: Recursos económicos

Ítem	Cantidad	Costo unitario aprox. (USD)	Subtotal (USD)
Sensor biométrico ZKTeco ZK4500	2	\$85.00	\$370.00
Laptop	1	\$500.00	\$500.00
Material impreso (encuestas, informes)	-	\$15.00	\$15.00
Fuente de poder / Estabilizador	1	\$30.00	\$30.00
Cables y conectores	Varios	\$10.00	\$10.00
Total estimado			\$925.00

Nota. Recursos económicos a tener en cuenta para desarrollo del proyecto. [Tabla] Autores del proyecto, 2025.

4.3 Etapas de ejecución del proyecto

4.3.1 Fase I: Planificación

Esta primera fase del proyecto constituye el punto de partida, la cual es fundamental para la implementación del sistema de autenticación biométrica en el centro de vigilancia del área técnica de la ULEAM, Ext. Chone. En esta etapa se llevará un diagnóstico de las condiciones actuales de acceso y control en el área, de tal manera que se identifique limitaciones de los métodos de acceso tradicional y la necesidad de aplicar una solución tecnológica basada en sensores biométricos.

Se tendrán en cuenta los objetivos específicos y los lineamientos que permitan la correcta instalación y el funcionamiento del sistema biométrico, se va a seleccionar la tecnología a usar, siendo dispositivos de huellas dactilares de marca ZKTeco seleccionados por su precisión y compatibilidad con sistemas de gestión como ZKAccess. También se

planifican los recursos a necesarios, de tal forma que se garantice la disponibilidad de los elementos requeridos para la ejecución del proyecto.

4.3.2 Fase II: Diseño del sistema

En esta fase se establecen los aspectos técnicos y estructurales necesarios para la correcta implementación del sistema de autenticación biométrica mediante huellas dactilares en el Centro de Vigilancia del Área Técnica de la ULEAM, Extensión Chone. El objetivo principal es definir de manera clara y detallada la arquitectura del sistema, la ubicación física de los dispositivos, los flujos de información y las políticas de acceso que garantizarán la seguridad de los espacios controlados.

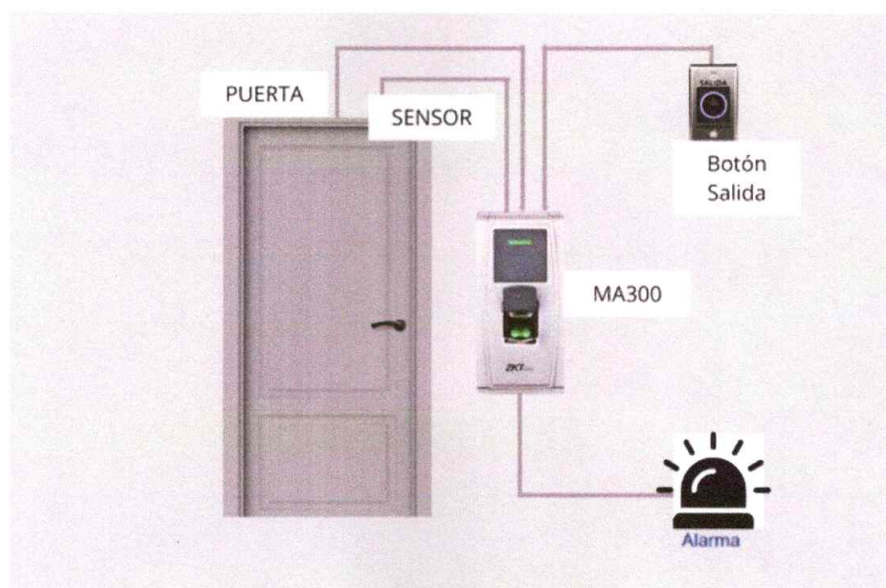
4.3.2.1 Ubicación física de los dispositivos.

En cuanto a la ubicación física de los equipos biométricos, se establece que el sistema contará con dos dispositivos ZKTeco estratégicamente instalados dentro del área técnica. Uno de ellos se colocará en la puerta principal de ingreso al laboratorio de base de datos, punto donde acceden los docentes y personal autorizado. Esta ubicación permite controlar el acceso general al área, garantizando que solo usuarios previamente registrados puedan ingresar a las instalaciones donde se manejan equipos y recursos académicos.

El segundo dispositivo se instalará en la puerta de acceso a la zona de vigilancia, área que se encuentra dentro del laboratorio de base de datos, esta zona contiene equipamiento sensible, sistemas de monitoreo y recursos institucionales de suma importancia, por lo que requiere un nivel de seguridad adicional. Al ubicar un dispositivo biométrico en este punto, se crea un doble filtro de seguridad, asegurando que únicamente el personal técnico autorizado pueda acceder al centro de vigilancia y realizar actividades relacionadas con monitoreo, control y gestión de la información.

En la figura a continuación se muestra una referencia al diseño de como quedaría el dispositivo MA300 en una de las puertas.

Figura 6. Diseño del sistema.

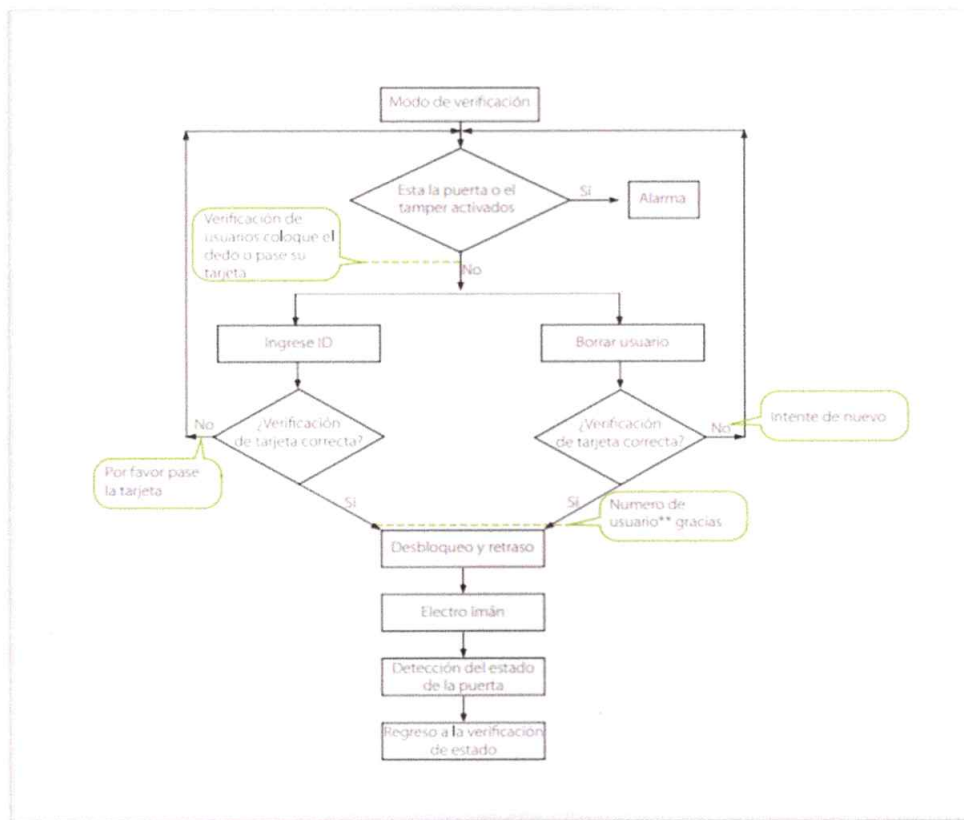


Nota. Imagen referencia al flujo de la verificación de usuario. Tomado de «MA300», (2025)

4.3.2.2 Flujos de información.

Posteriormente a la selección de la ubicación para los dispositivos se establece el flujo de control de acceso, el cual inicia con la verificación biométrica mediante huella dactilar. El usuario coloca su dedo en el sensor ZKTeco, y el dispositivo captura y compara la lectura con los registros previamente almacenados en la base de datos del sistema. Si la coincidencia es válida, se autoriza el acceso físico o en caso contrario, se genera un evento de rechazo que queda registrado en el historial del sistema como medida de seguridad.

Figura 7. Tabla de verificación de usuario.



Nota. Imagen referencia al flujo de la verificación de usuario. Tomado de «MA300», (2025)

4.3.2.3 Integración con la aplicación ZKAccess.

Posteriormente, se emplea la integración con la aplicación ZKAccess, esta es la plataforma oficial para la administración del dispositivo biométrico. Esta integración permitirá registrar usuarios, cargar plantillas de huella, asignar permisos, generar reportes de accesos y monitorear en tiempo real los eventos del sensor.

En la siguiente figura (figura 8) se demuestra la interfaz en el panel de agregación de usuarios, en este se deberá registrar el personal al mismo o importarlo desde otro software o documento al sistema. Desde este mismo panel se deberá agregar la huella digital de las personas que requieren tener accesos en este caso a la zona de vigilancia.

Figura 8. Interfaz agregar usuarios ZKAccess

The screenshot shows the 'Agregar' (Add) user interface in the ZKAccess software. The interface is in Spanish and features a sidebar on the left with options like 'Personal', 'Departamentos', 'Usuarios', and 'Registro de tarjetas'. The main area contains a form with the following fields: 'ID de usuario', 'Nombre', 'Apellido', 'Género' (set to 'Masculino'), 'Contraseña', 'Email', 'Departamento', 'Company Name', 'Número de tarjeta', 'Tel. móvil', 'Fecha de Empleo' (set to '06/12/2025'), 'Fecha de Nacimiento' (set to '05/12/2025'), 'Privilegio', and 'Usuario'. There are also buttons for 'Registrar huellas' (with a 'Sensor de huellas USB' option), 'Examinar', 'Capturar', 'Guardar y continuar', 'OK', and 'Cancelar'. A placeholder image for a fingerprint sensor is shown on the right with the text 'Tamaño óptimo 120 x 140 píxeles'.

Nota. Imagen referencia agregar usuarios mediante el software de ZKAccess. autores del proyecto (2025)

4.3.2.4 Agregar dispositivo.

La agregación del dispositivo biométrico ZKTeco MA300 al sistema ZKAccess 3.5, puede realizarse mediante comunicación TCP/IP o RS-485, según la infraestructura disponible. En el caso de TCP/IP, el dispositivo se conecta a la red local mediante un cable Ethernet, asignándole una dirección IP válida y accesible desde el equipo donde se encuentra instalado el software. Este método permite una comunicación estable y en tiempo real, esto facilita la sincronización de usuarios, huellas, horarios y registros de acceso, además de ser el más recomendado para entornos con red estructurada.

Figura 9. Agregación de dispositivo biométrico por TCP/IP

The screenshot shows the 'Dispositivo' (Device) tab in the ZKAccess software. The table below lists the devices:

Dispositivo	Numero de serie	Comunicac.	Dirección IP	Puerto	RS485	Habill.	Usuarios	Huellas	Venias	Releves	Palm Quan	Modelo	Firmware	Area
PP	AKGU205240118	TCP/IP	192.168.1.201				198	0	0	0	0	MA300	Ver 6.62 Dec 7 2015	Area Name

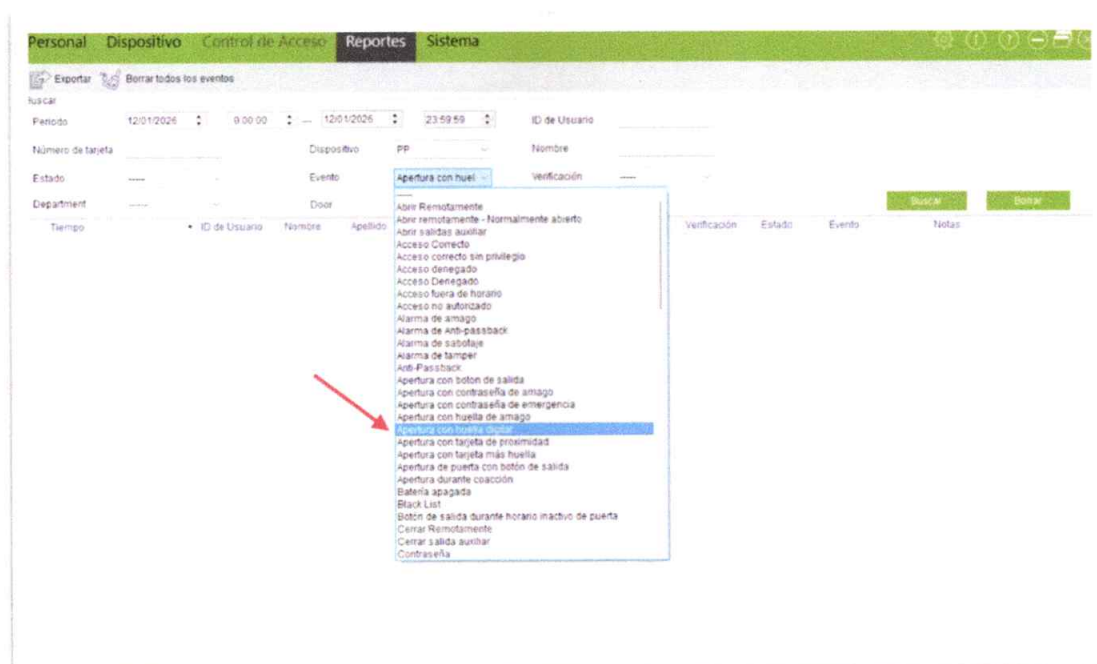
Red arrows in the image point to the 'Comunicac.' and 'Dirección IP' columns of the highlighted device row.

Nota. Imagen referencia a agregar dispositivo. autores del proyecto (2025)

4.3.2.5 Reportes

Cada que un usuario valida su identidad utilizando su huella dactilar, el dispositivo almacena automáticamente información como la fecha, hora, identificación del usuario, método de verificación y el estado de la apertura de la puerta. Estos datos son sincronizados con el software, donde pueden ser organizados y filtrados para generar reportes por usuario, rango de fechas, dispositivo o área específica.

Figura 10. Generación de reportes de aperturas por huella dactilar.



Nota. Imagen referencia a generación de reportes de aperturas por huella digital. autores del proyecto (2025)

4.3.3 Fase III: Instalación e implementación

Se procede a la instalación física y puesta en marcha del sistema biométrico, siguiendo los lineamientos establecidos en la planificación y el diseño técnico previamente aprobados. El objetivo principal es realizar la integración efectiva de los dispositivos de huella dactilar ZKTeco con el entorno físico y tecnológico del Centro de Vigilancia del Área Técnica de la ULEAM Extensión Chone, garantizando un funcionamiento estable, seguro y confiable del sistema de control de acceso.

El proceso inicia con la instalación de los equipos biométricos en los puntos estratégicos definidos durante el diseño, considerando factores como accesibilidad, seguridad eléctrica y visibilidad. Posteriormente, se efectúa la configuración del software ZKAccess,

que permite registrar, administrar y controlar el acceso de los usuarios autorizados. En esta etapa se lleva a cabo la carga inicial de datos en la base de datos del sistema, registrando la información del personal técnico y administrativo del área, junto con sus respectivas huellas digitales.

Luego, se realiza la sincronización entre los dispositivos biométricos y el sistema de gestión, verificando la correcta comunicación y transmisión de datos. También se efectúan pruebas iniciales de lectura y reconocimiento de huellas para asegurar la precisión del sistema y ajustar los parámetros de sensibilidad y respuesta, también se comprueba la generación automática de reportes de entrada y salida, y su almacenamiento correcto en el servidor o equipo de control.

Durante esta fase se brinda asistencia técnica al personal de vigilancia encargado de operar el sistema, explicando los procedimientos de registro de nuevos usuarios, verificación manual y control de incidencias. Finalmente, se documenta el proceso de instalación y configuración mediante informes técnicos, registros fotográficos y reportes de validación, asegurando que el sistema cumpla con los requerimientos funcionales definidos. Esta fase culmina con la puesta en funcionamiento oficial del sistema biométrico, marcando el inicio de su operación en condiciones reales dentro del centro de vigilancia.

4.3.4 Fase IV: Pruebas del sistema

Se inicia a evaluar el desempeño, la precisión y la estabilidad del sistema de autenticación biométrica luego de su instalación. El objetivo principal es verificar que todos los componentes (hardware, software, sensores y base de datos) funcionen correctamente y cumplan con los requerimientos de acceso seguro establecidos en el diseño del sistema. Esto se realiza a través de pruebas controladas que permiten identificar fallos, inconsistencias o retrasos en la autenticación. Las pruebas incluyen:

➤ Pruebas funcionales

Se evalúa el funcionamiento básico del dispositivo MA300 y del software ZKAccess, comprobando la correcta lectura de huellas, tiempos de respuesta, apertura del acceso y registro automático en la base de datos.

➤ Pruebas de rendimiento

Se toman los tiempos de procesamiento en horas de mayor concurrencia, garantizando que la lectura biométrica no genere cuellos de botella o demoras en el acceso del personal.

➤ **Pruebas de seguridad**

Se simulan intentos de acceso no autorizados utilizando huellas no registradas, variaciones en las colocaciones del dedo o intentos repetidos, evaluando la capacidad del sistema para detectarlos y generar alertas.

➤ **Pruebas de falla y recuperación**

Se desconecta temporalmente la red, se reinicia el dispositivo y se simulan cortes eléctricos breves para validar los protocolos de respaldo, reconexión y sincronización automática de datos una vez restablecido el servicio.

Una vez finalizadas las pruebas, se elabora un informe con los resultados obtenidos, las incidencias detectadas y las acciones correctivas aplicadas. Esta fase concluye únicamente cuando el sistema demuestra un funcionamiento estable, preciso y continuo.

4.3.5 Fase V: Mantenimiento y monitoreo

Esta fase representa la etapa final del proyecto y se centra en garantizar una correcta operatividad del sistema biométrico en el Centro de Vigilancia, asegurando que se mantenga funcional, actualizado y seguro a lo largo del tiempo, permitiendo prevenir fallos, optimizar procesos y garantizar la confiabilidad de los registros de acceso.

El mantenimiento comprende tanto actividades preventivas como correctivas. En cuanto al mantenimiento preventivo, se ejecutan revisiones periódicas del lector biométrico MA300, incluyendo la limpieza y revisión física del sensor. También se consideran tareas de actualización de firmware y revisión constante de la integridad de la base de datos.

En el caso del mantenimiento correctivo, se actúa cuando se presentan fallos en el funcionamiento, ya sea por problemas de lectura, errores de comunicación con el sistema ZKAccess o daños físicos en el dispositivo. Esto implica realizar ajustes técnicos, reemplazos de componentes, reconfiguraciones o restauraciones del sistema cuando sea necesario.

El monitoreo continuo es otro componente fundamental de esta fase. A través del software ZKAccess se supervisan en tiempo real los registros de acceso, los intentos fallidos,

las alertas generadas por eventos sospechosos y la actividad de los usuarios dentro del sistema.

Dentro del proceso de monitoreo también se incluye la actualización constante de los usuarios registrados. Cada cambio de personal técnico o administrativo requiere retirar o agregar registros biométricos, lo cual asegura que la base de datos se mantenga actualizada y evita accesos indebidos por parte de usuarios inactivos.

Esta fase culmina con evaluaciones periódicas del desempeño general del sistema, considerando aspectos como la confiabilidad de las autenticaciones, la rapidez en la verificación y la efectividad en la reducción de accesos no autorizados. Con estos resultados se identifican posibles mejoras futuras o ampliaciones del sistema, asegurando su adecuado funcionamiento a largo plazo.

CAPITULO V: CONCLUSIONES Y RECOMENDACIONES

5.1 Conclusiones

La aplicación de un sistema de acceso biométrico mediante huella dactilar en el centro de vigilancia del área técnica de la ULEAM Extensión Chone, representa una solución efectiva para fortalecer la seguridad institucional, al permitir un control preciso, confiable y automatizado del ingreso del personal autorizado.

La investigación realizada permitió evidenciar que el sistema biométrico tiene un impacto positivo en el fortalecimiento de la seguridad, ya que elimina la dependencia de métodos tradicionales y poco fiables como llaves. Por otro lado, también facilita la generación de reportes de ingresos con todos los datos de personas autorizadas.

El sistema de autenticación biométrica implementado se adapta adecuadamente a los requerimientos del área técnica, integrándose de manera eficiente con el entorno físico y operativo, y permitiendo la generación de reportes que aportan valor a los procesos de control, auditoría y toma de decisiones institucionales.

5.2 Recomendaciones

Se recomienda a la ULEAM Extensión Chone mantener el sistema de autenticación biométrica como sistema de seguridad principal para el control de acceso al centro de vigilancia del área técnica, debido a los beneficios evidenciados en el control de acceso.

Con la necesidad de garantizar la continuidad operativa del sistema, se sugiere implementar sistemas de respaldo eléctrico como unidades UPS para que permitan el correcto funcionamiento del sistema biométrico ante posibles cortes de energía, también es recomendable realizar capacitaciones continuas al personal administrativo encargado del sistema, para asegurar una operación eficiente y autónoma del sistema.

También es aconsejable realizar mantenimientos preventivos a los dispositivos biométricos, con el fin de minimizar errores operativos, mejorar la gestión de usuarios y aprovechar de manera eficiente los reportes generados por el sistema. Además, se recomienda evaluar en el futuro la ampliación del sistema biométrico a otras áreas estratégicas de la institución, con el objetivo de reforzar la seguridad integral de las instalaciones.

BIBLIOGRAFÍA

- Arenas, B., & Chan, H. (2017). *Implementación de sistema de video cámaras IP como medio de seguridad para el Tecnológico de Álvaro Obregón.*
- Bunge, M. A. (2017). El planteamiento científico. *Revista Cubana de Salud Pública*, 43, 470-498.
- Cerna, J. J. V., Quincho, L. M. S., & Santos, A. C. M. de los. (2023). La vulnerabilidad de las tecnologías biométricas en la autenticación. *ingeniería investiga*, 5.
<https://doi.org/10.47796/ing.v5i0.866>
- Correa Cardenas, C. J., & Panizo Pascual, M. del P. (2020). *Mejora en el proceso de autenticación utilizando la metodología Six Sigma en la empresa Alignet S.A.C.*
<https://repositorio.ulima.edu.pe/handle/20.500.12724/12777>
- Cruz Vera, I. I. (2021). *Implementación de una central de control y monitoreo de cámaras de seguridad para la Facultad de Sistemas y Telecomunicaciones.*
<https://repositorio.upse.edu.ec/handle/46000/5783>
- Gentile, S. (2025, enero 7). *Sistema de acceso biométrico: Las consecuencias de no aplicarlo.* <https://blog.rekonpeople.com/sistema-de-acceso-biometrico-las-consecuencias-de-no-aplicarlo>
- Herrera, S. M. C. (2023). *desarrollo de un sistema de seguridad en apertura de portones de garaje automáticos mediante datos biométricos e iot.*
- MA300. (2025, noviembre 4). *ZKTeco Latinoamerica.*
<https://zktecolatinoamerica.com/producto/ma300/>
- Menéndez Chávez, H. M., & Muñoz Loor, C. L. (2016). *Sistema biométrico para automatizar el registro de asistencia docente en la unidad educativa ITSI del cantón*

Chone [bachelorThesis, Calceta: Espam].

<http://repositorio.espm.edu.ec/handle/42000/318>

Meneses, A. J. B., & Garcia, C. G. V. (2016). *diseño e implementación de un prototipo para el control de acceso en la sede de ingeniería de la universidad distrital francisco José de caldas mediante el uso de torniquetes controlados por carnet con tecnología nfc y lector biométrico de huella dactilar*.

Murillo Quimiz & Delgado Pilligua. (2018). *implementación de sistema de seguridad biométrico para control de acceso zkteco tf1700 mediante huella dactilar para el laboratorio de telecomunicaciones en la carrera de ingeniería en computación y redes de la Universidad Estatal del sur de Manabí*. [bachelorThesis, JIPIJAPA-UNESUM]. <http://repositorio.unesum.edu.ec/handle/53000/1473>

Nieves Villamar, K. X. (2021). *“reestructuración de un sistema biométrico para fortalecer la seguridad y control de acceso en el decanato de la facultad de ciencias técnicas”*.
<https://repositorio.unesum.edu.ec/bitstream/53000/3039/1/NIEVES%20VILLAMAR%20KLEVER%20XAVIER.pdf>

Pinargote Vences, G. J. (2022). *diseño de un sistema de control de acceso con supervisión remota y video vigilancia para el centro de estudio de biotecnología de la universidad estatal del sur de manabí* [bachelorThesis, Jijipijapa.UNESUM].
<http://repositorio.unesum.edu.ec/handle/53000/3555>

Quintanilla Mendoza, G. (2020). Legislación, riesgos y retos de los sistemas biométricos. *Revista chilena de derecho y tecnología*, 9(1), 63-91. <https://doi.org/10.5354/0719-2584.2020.53965>

Rangel Rivas, Y. M. (2024). *Sistema biométrico: Reconocimiento por huella dactilar uno de los menos vulnerables*. <https://dspace.tdea.edu.co/handle/tdea/6833>

- Rodriguez Pinto, C. A., & Ortega Romero, R. (2017). *Estudio de Pre-Factibilidad para un Sistema de Control de Acceso Peatonal en la Universidad Distrital Francisco José de Caldas*. <https://repository.udistrital.edu.co/items/cbcb23ca-9497-4aaf-9b01-b8d1f2e7d6fb>
- Santi Pereyra, S. E. (2018). Biometría y vigilancia social en Sudamérica: Argentina como laboratorio regional de control migratorio. *Revista mexicana de ciencias políticas y sociales*, 63(232), 247-268.
<https://doi.org/10.22201/fcpys.2448492xe.2018.232.56580>
- SeguriTech. (2022, diciembre 30). *Centros de Control y Monitoreo, ¿cuál es su función? -...*
<https://seguritech.com/post/centros-de-control-y-monitoreo-cual-es-su-funcion>
- Tamami González, G. A., & Ortiz Minchala, A. L. (2024). *Sistema de seguridad telemático aplicado al sector industrial para la autenticación de reconocimiento de IMAGEN*.
<https://repositorio.uteq.edu.ec/handle/43000/7248>
- Tasayco Coronado, Víctor Carlos. (2023). *Implementación de una data center del Centro de Monitoreo y Video Vigilancia de una Municipalidad* [Facultad de Ingeniería y Negocios]. <https://repositorio.uwiener.edu.pe/server/api/core/bitstreams/9855e31c-4c92-4116-8d44-1a8b74bf8750/content>
- Valderrama, A. J. P. (2019). *esquema de autenticación mediante códigos qr para ingreso a instalaciones restringidas*.
- Yenitlfer del Carmen López Pardo. (2014). *análisis de inversión para la implantación de un sistema de control biométrico de rondas para las empresas de vigilancia privada*. [Universidad Militar Nueva Granada].
<https://repository.umng.edu.co/server/api/core/bitstreams/98844983-9fa8-4a98-95c2-e5c7a79252e5/content>

ANEXOS

Anexo Nr1. Guion para entrevista



UNIVERSIDAD LAICA “ELOY ALFARO” DE MANABÍ

Unidad académica: Extensión Chone

Carrera: Tecnología de la Información

Instrumento: Guion para entrevista

Objetivo: Obtener información sobre la gestión actual del acceso al centro de control de vigilancia, identificando debilidades, riesgos y expectativas en torno a la implementación de un sistema de autenticación biométrica.

Investigador: López Moreira Joel José y Cedeño Moreira Jhon Erick

Fecha: 21/10/2025

Ubicación: ULEAM Extensión Chone

Instrucciones: De acuerdo con el siguiente guion, responda bajo su experiencia en la institución. Sus respuestas serán utilizadas únicamente con fines investigativos.

1. ¿Como se maneja el acceso al centro de control de vigilancia del área técnica del bloque b?

El manejo del acceso se controla a través de una solicitud y autorización previa. Solo el personal autorizado puede ingresar, pero la supervisión a veces es básica y depende del personal de turno.

2. ¿Cuáles son las principales problemáticas detectadas en la gestión de acceso?

Algunas problemáticas surgen con el registro y control de ingreso, ya que no se tiene un control exacto en ciertos horarios, y ausencia de un sistema que identifique realmente a cada persona, lo que puede generar posibles vulnerabilidades.

**3. ¿Considera que el control de acceso actual garantiza seguridad suficiente?
¿Por qué?**

No completamente. Aunque se tienen controles, la falta de tecnología de control de acceso y los registros manuales facilitan el acceso no autorizado y dificultan el seguimiento preciso de ingresos y salidas.

4. ¿Existen incidentes frecuentes relacionados con el ingreso no autorizado al centro de vigilancia del área técnica del bloque b?

Como es un laboratorio y dentro del mismo está el centro de vigilancia, es bastante complejo detectar ingresos no autorizados al mismo.

5. ¿El personal que puede acceder al centro de control de vigilancia cuenta con conocimientos de tecnología biométrica?

En su gran mayoría si conoce sobre tecnología biométrica, lo que facilitaría la implementación de estos sistemas.

6. ¿Qué impacto cree que tendría la implementación de un sistema de autenticación biométrica en la seguridad institucional?

Un impacto positivo, ya que aumentaría la precisión en la identificación, minimizaría riesgos de infracciones, y mejoraría el control del acceso.

7. ¿Qué aspectos considera fundamentales en un sistema biométrico para que sea confiable y efectivo?

Este debe ser preciso, rápido, con alta seguridad de datos, fácil de usar y que permita registros viables para verificar accesos.

8. ¿Cómo evalúa la confidencialidad y seguridad de los datos en un sistema de control biométrico?

Que los datos estén seguros, que cuente con accesos restringidos y protocolos claros para proteger la privacidad y evitar filtraciones.

Anexo Nr2. Ficha de observación



UNIVERSIDAD LAICA “ELOY ALFARO” DE MANABÍ

Unidad académica: Extensión Chone

Carrera: Tecnología de la Información

Instrumento: Ficha de observación

Objetivo: Identificar problemáticas y deficiencias en los procedimientos actuales de control de accesos al centro de vigilancia, con el fin de fundamentar la propuesta de un sistema de autenticación biométrica.

Investigador: López Moreira Joel José y Cedeño Moreira Jhon Erick

Fecha: 21/10/2025

Ubicación: ULEAM, Extensión Chone

Número	Descripción	Si	No	Observaciones
1	¿El proceso de control de accesos actual es eficiente?		X	No es eficiente, ya que se necesita solicitar presencialmente el ingreso.
2	¿Existen debilidades en la verificación de identidad del personal?		X	Se conoce al personal autorizado.
3	¿Se detectan ingresos no autorizados o intentos de suplantación?		X	No existen antecedentes relacionados a este caso.

4	¿El flujo de acceso al centro de vigilancia es rápido y ordenado?		X	Se debe solicitar permiso.
5	¿Se utilizan herramientas tecnológicas en el proceso actual?		X	N/A
6	¿Se evidencian errores frecuentes en el registro manual de accesos?		X	No se evidencian de errores frecuentes.
8	¿El personal administrativo requiere capacitación en nuevas tecnologías?		X	Todo el personal administrativo cuenta con conocimientos sobre nuevas tecnologías.
9	¿El personal de seguridad cumple con los protocolos establecidos?	X		Se registra el ingreso al laboratorio.

Anexo Nr3. Aplicación de instrumentos

