



UNIVERSIDAD NACIONAL DE CHIMBORAZO

FACULTAD DE INGENIERÍA

CARRERA DE INGENIERÍA EN TECNOLOGÍAS DE LA

INFORMACIÓN

Aplicación web/móvil con biometría facial e inteligencia artificial para control seguro de accesos en la cooperativa “Señor del Buen Suceso”

Trabajo de Titulación para optar al título de

Ingeniero en Tecnologías de la Información

Autor:

Zurita Carchi, Jhonnatan Cristian

Tutor:

Ing. Luis Gonzalo Allauca Peñafiel

Riobamba, Ecuador. 2026

DECLARATORIA DE AUTORÍA

Yo, Jhonatan Cristian Zurita Carchi, con cédula de ciudadanía 0604205435, autor del trabajo de investigación titulado: Aplicación web/móvil con biometría facial e inteligencia artificial para control seguro de accesos en la cooperativa “Señor del Buen Suceso”, certifico que la producción, ideas, opiniones, criterios, contenidos y conclusiones expuestas son de mí exclusiva responsabilidad.

Asimismo, cedo a la Universidad Nacional de Chimborazo, en forma no exclusiva, los derechos para su uso, comunicación pública, distribución, divulgación y/o reproducción total o parcial, por medio físico o digital; en esta cesión se entiende que el cesionario no podrá obtener beneficios económicos. La posible reclamación de terceros respecto de los derechos de autor de la obra referida, será de mi entera responsabilidad; librando a la Universidad Nacional de Chimborazo de posibles obligaciones.

En Riobamba, 07 de mayo de 2026.



Jhonatan Cristian Zurita Carchi

C.I: 0604205435

DICTAMEN FAVORABLE DEL PROFESOR TUTOR

Quien suscribe, **Luis Gonzalo Allauca Peñafiel** catedrático adscrito a la Facultad de Ingeniería, por medio del presente documento certifico haber asesorado y revisado el desarrollo del trabajo de investigación titulado: **Aplicación web/móvil con biometría facial e inteligencia artificial para control seguro de accesos en la cooperativa "Señor del Buen Suceso"**, bajo la autoría de **Jhonnatan Cristian Zurita Carchi**; por lo que se autoriza ejecutar los trámites legales para su sustentación.

Es todo cuanto informar en honor a la verdad; en Riobamba, a los 14 días del mes de mayo de 2026.



LUIS GONZALO ALLAUCA PEÑAFIEL

C.I: 0602363418

CERTIFICADO DE LOS MIEMBROS DEL TRIBUNAL

Quienes suscribimos, catedráticos designados Miembros del Tribunal de Grado para la evaluación del trabajo de investigación Aplicación web/móvil con biometría facial e inteligencia artificial para control seguro de accesos en la cooperativa "Señor del Buen Suceso", presentado por Jhonnatan Cristian Zurita Carchi, con cédula de identidad número 0604205435, bajo la tutoría de Mgs. Luis Gonzalo Allauca Peñafiel; certificamos que recomendamos la APROBACIÓN de este con fines de titulación. Previamente se ha evaluado el trabajo de investigación y escuchada la sustentación por parte de su autor; no teniendo más nada que observar.

De conformidad a la normativa aplicable firmamos, en Riobamba 07 de mayo de 2026.

PRESIDENTE DEL TRIBUNAL DE GRADO

Mg. Ana Congacha



MIEMBRO DEL TRIBUNAL DE GRADO

Mg. Pamela Buñay



MIEMBRO DEL TRIBUNAL DE GRADO

PhD. Fernando Molina





CERTIFICACIÓN

Que, **JHONNATAN CRISTIAN ZURITA CARCHI** con CC: **0604205435**, estudiante de la Carrera de **INGENIERÍA EN TECNOLOGÍAS DE LA INFORMACIÓN**, Facultad de **INGENIERIA**; ha trabajado bajo mi tutoría el trabajo de investigación titulado **"Aplicación web/móvil con biometría facial e inteligencia artificial para control seguro de accesos en la cooperativa Señor del Buen Suceso"**, cumple con el **8 %**, de acuerdo al reporte del sistema Anti plagio **COMPILATIO**, porcentaje aceptado de acuerdo a la reglamentación institucional, por consiguiente autorizo continuar con el proceso.

Riobamba, 14 de mayo de 2026



Validar electrónicamente en Firmad:
Firmado electrónicamente por:
**LUIS GONZALO
ALLAUCA PEÑAFIEL**

Mgs. Gonzalo Allauca Peñafiel
TUTOR

DEDICATORIA

Dedico este trabajo de titulación primordialmente a Dios, por haberme bendecido con la vida y la sabiduría necesarias para culminar con éxito esta etapa profesional, guiándome en cada paso y dándome la fortaleza para no desmayar ante las adversidades.

A mis padres, quienes con su amor incondicional, paciencia y entrega absoluta, han sido el motor de mi existencia. Sus sacrificios silenciosos y su fe inquebrantable en mis capacidades son los pilares sobre los que he construido este sueño; este título es, antes que mío, una recompensa a su esfuerzo y al ejemplo de integridad que me han brindado siempre.

A mis hermanos y familiares, por su apoyo constante y por ser ese refugio de paz y motivación en los momentos de mayor cansancio, recordándome siempre el valor de la perseverancia.

De manera profundamente especial y con un sentimiento de eterna gratitud, a Preciosa, mi fiel y amada compañera. Aunque hoy tu ausencia deje un vacío, tu recuerdo permanece intacto como aquel ser que no se apartó de mi lado durante las incontables noches de estudio, tareas y desvelos. Tu compañía silenciosa y tu lealtad fueron mi mayor consuelo en las horas más difíciles de este proceso; gracias por haber estado conmigo hasta el final, siempre vivirás en este logro.

AGRADECIMIENTO

Mi gratitud infinita hacia la Universidad Nacional de Chimborazo, institución que no solo me abrió las puertas del conocimiento, sino que se convirtió en mi segundo hogar durante estos años de formación. Agradezco profundamente a mi Facultad por haberme brindado las herramientas, la disciplina y el entorno académico necesarios para transformar mi vocación en una profesión, permitiéndome culminar hoy este importante peldaño de mi vida.

A mi tutor de tesis, por su invaluable guía, su tiempo y la confianza depositada en este proyecto. Sus observaciones críticas y su acompañamiento técnico fueron fundamentales para transformar una idea de investigación en una solución tecnológica funcional y sólida.

A los miembros del tribunal, por su tiempo y por los aportes brindados durante la revisión de este trabajo, los cuales permitieron elevar la calidad y el rigor científico de la presente investigación.

De igual manera, agradezco a mis compañeros de carrera, con quienes compartí años de aprendizaje, proyectos y retos. Gracias por el apoyo mutuo y por la amistad forjada en los laboratorios y pasillos de la universidad; su compañía hizo que este camino fuera mucho más enriquecedor.

Finalmente, a todas aquellas personas que, de forma desinteresada, aportaron con su conocimiento y motivación para que este sueño de convertirme en profesional hoy sea una realidad.

ÍNDICE GENERAL

DECLARATORIA DE AUTORÍA

DICTAMEN FAVORABLE DEL TUTOR

CERTIFICADO DE LOS MIEMBROS DE TRIBUNAL

CERTIFICADO ANTIPLAGIO

DEDICATORIA

AGRADECIMIENTO

ÍNDICE GENERAL

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

ABSTRACT

CAPÍTULO I. INTRODUCCIÓN.....	14
1.1. Planteamiento del Problema	15
1.2. Justificación	15
1.3. Formulación del Problema.....	16
1.4. Objetivos.....	17
CAPÍTULO II. MARCO TEÓRICO	18
2.1. Análisis de trabajos relacionados en inteligencia artificial.....	18
2.1.1. Evolución de los sistemas de control de accesos.....	19
2.1.2. Comparación entre sistemas mecánicos y digitales.....	19
2.1.3. Necesidad de soluciones seguras y eficientes en la gestión de accesos	19
2.2. Inteligencia artificial y machine learning en reconocimiento	19
2.2.1. Modelos de IA para el análisis facial.....	20
2.2.2. Técnicas de machine learning para reconocimiento facial	20
2.2.3. Mejora en la precisión y seguridad mediante la IA	20
2.2.4. Impacto de la ansiedad elevada y la agresividad en el comportamiento humano	21
2.3. Desarrollo de aplicaciones y conectividad IoT.....	21
2.3.1. Frameworks para desarrollo de aplicaciones (Flutter)	21
2.3.2. Interfaz de usuario (UI) para capturas biométricas	22
2.3.3. API RESTful para control de dispositivos IoT	22

2.4. Seguridad informática y protección de datos biométricos.....	22
2.4.1. Protección de datos biométricos: normas y protocolos de seguridad	23
2.4.2. Autenticación segura en sistemas biométricos	23
2.4.3. Ventajas de la biometría facial frente a métodos tradicionales.....	23
2.5. Metodología: Implementación de Mobile-D	23
2.5.1. Descripción de Mobile-D	24
2.5.3. Evaluación de la norma ISO/IEC 19795-1:2021.....	25
2.5.4. Estrategias para el mantenimiento y optimización a largo plazo:	26
CAPÍTULO III. METODOLOGIA	27
3.1. Tipo de Investigación	27
3.2. Diseño de la Investigación.....	27
3.3. Población de estudio y tamaño muestra	27
3.4. Técnicas e instrumentos de recolección de datos	28
3.5. Métodos de análisis y procesamiento de datos	29
3.6. Identificación de variables.....	32
3.7. Operacionalización de variables	32
3.8. Metodología de desarrollo	34
3.8.1. Fase 1: Exploración	34
3.8.2. Fase 2: Inicialización	38
3.8.3. Fase 3: Producción	49
3.8.4. Fase 4: Pruebas	51
CAPITULO IV: RESULTADOS Y DISCUSIÓN	56
4.1. Resultado del objetivo específico 1:	56
4.2. Resultado del objetivo específico 2:	58
4.3. Resultado del objetivo específico 3	59
4.4. Discusión	61
CAPÍTULO V: CONCLUSIONES Y RECOMENDACIONES	62
5.1. Conclusiones.....	62
5.2. Recomendaciones	62
BIBLIOGRAFÍA	64
ANEXOS	67

ÍNDICE DE TABLAS

Tabla 1: Matriz Comparativa del Estado del Arte y Brechas Tecnológicas.	18
Tabla 2. Proceso de Implementación	25
Tabla 3: Matriz de Confusión para la Evaluación del Sistema FaceKey.....	31
Tabla 4. Operacionalización de Variables	33
Tabla 5. Tabla de conductores.....	43
Tabla 6. Tabla de emotion_attempts	44
Tabla 7. Análisis de los Datos.....	53
Tabla 8. Comparativa Técnica para la Selección de Modelos de Reconocimiento Facial y Emocional.....	56

ÍNDICE DE FIGURAS

Figura 1: IDE Flutter.	22
Figura 2: Diagrama de Casos de Uso.	39
Figura 3: Diagrama de Actividades.	40
Figura 4: Diagrama de Arquitectura.	41
Figura 5: Diagrama Entidad-Relación.	42
Figura 6: Código SQL.	42
Figura 7: Login Página Web.	45
Figura 8: Registro de usuarios Página Web.	45
Figura 9: Control de accesos Página Web.	46
Figura 10: Análisis de accesos Página Web.	46
Figura 11: Acceso Facial.	47
Figura 12: Verificación Facial.	48
Figura 13: Panel de Acceso.	48
Figura 14: Evaluación del desempeño del sistema.	54
Figura 15: Base de datos de la tabla de emotion_attempts	55
Figura 16: Arquitectura de evaluación del sistema	58
Figura 17: Interfaz principal de la aplicación móvil FaceKey.	58
Figura 18: Interfaz principal de la aplicación web	59
Figura 19: Evaluación del sistemas biométrico y emocional.	60
Figura 20: Interfaz de gestión de usuarios registrados.	67
Figura 21: Interfaz de intentos de acceso.	67
Figura 22: Interfaz de estadísticas generales.	68
Figura 23: Interfaz de métricas de evaluación.	68
Figura 24: Interfaz de emociones detectadas.	69
Figura 25: Interfaz de usuarios más activos.	69
Figura 26: Interfaz de actividad reciente.	70

RESUMEN

El presente trabajo de investigación aborda la vulnerabilidad en la seguridad física y la falta de trazabilidad automatizada en los controles de acceso de la Cooperativa de Taxis “Señor del Buen Suceso” del cantón Riobamba. Ante las limitaciones operativas de los mecanismos tradicionales de control de ingreso, los cuales impedían verificar la identidad fidedigna y evaluar el estado afectivo de los conductores, se planteó como objetivo general implementar una aplicación web/móvil basada en biometría facial e inteligencia artificial para automatizar y restringir de forma segura los accesos institucionales.

Metodológicamente, el estudio se define bajo un enfoque cuantitativo, de tipo aplicado y con un diseño descriptivo-evaluativo. Para la ingeniería del software se adoptó el marco ágil de la metodología Mobile-D en sus fases de exploración, inicialización, producción y pruebas, dando origen a una arquitectura distribuida integrada por un módulo móvil en Flutter para inferencia local, un backend en PHP y un dashboard web administrativo; asimismo, la evaluación de rendimiento de los algoritmos se rigió estrictamente bajo los parámetros de la norma internacional ISO/IEC 19795-1:2021.

Los hallazgos empíricos derivados de los ensayos de campo demostraron un desempeño sobresaliente, alcanzando una precisión general del 97.02%, una Tasa de Aceptación Falsa (FAR) del 2.38% y una Tasa de Rechazo Falso (FRR) de apenas el 0.61%. En la dimensión preventiva, el cortafuegos psicométrico constató una concordancia emocional del 100.00% con un nivel de confianza promedio del 84.75% en las inferencias locales, bloqueando de manera reactiva la totalidad de los accesos cuando la ira o la ansiedad superaron el umbral del 10%, manteniendo los tiempos de validación optimizados entre 150 y 300 milisegundos.

Se concluye que la unificación de los modelos FaceNet y FER, robustecidos localmente mediante algoritmos de detección de vivacidad (*liveness detection*) basados en los ángulos de Euler, provee una solución informática de alta fidelidad para mitigar riesgos operacionales organizacionales. La implementación de esta infraestructura descentralizada moderniza la seguridad de la cooperativa y convalida la viabilidad técnica de integrar factores cognitivos en entornos de seguridad física, optimizando la usabilidad operativa sin penalizar el flujo vehicular diario.

Palabras clave: Ángulos de Euler, Arquitectura distribuida, Detección de vivacidad, Metodología Mobile-D, Modelo FaceNet

ABSTRACT

This research work addresses the physical security vulnerability and the lack of automated traceability within the access control mechanisms at the “Señor del Buen Suceso” Taxi Cooperative in Riobamba. Due to the operational limitations of traditional entry methods, which prevented reliable identity verification and driver emotional state assessment, the main objective was to implement a web/mobile application based on facial biometrics and Artificial Intelligence (AI) to safely automate and restrict institutional access. Methodologically, the study is defined under a quantitative approach, classified as applied research with a descriptive-evaluative design. For the software engineering process, the Mobile-D agile framework was adopted across its exploration, initialization, production, stabilization, and testing phases, delivering a distributed architecture composed of a Flutter mobile client for local inference, a PHP backend, and an administrative web dashboard; furthermore, the algorithm performance evaluation strictly adhered to the ISO/IEC 19795-1:2021 international standard. Empirical findings derived from field trials demonstrated outstanding performance, achieving a definitive general accuracy (Accuracy) of 97.02%, a False Acceptance Rate (FAR) limited to 2.38% after algorithmic calibration, and a usability index showing a False Rejection Rate (FRR) of just 0.61%. In the preventive dimension, the psychometric firewall achieved 100.00% in Emotional Concordance, reactively blocking access attempts when anger or anxiety levels exceeded the 10% threshold, operating with optimized validation times between 150 and 300 milliseconds per capture. It is concluded that the integration of the FaceNet and FER models, locally reinforced by liveness detection algorithms based on Euler angles, provides a high-fidelity psychometric firewall to mitigate organizational operational risks. The implementation of this decentralized infrastructure modernizes the cooperative's safety and validates the technical viability of embedding cognitive factors within physical security environments, optimizing operational usability without penalizing the daily vehicular traffic flow.

Keywords: Distributed Architecture, Euler Angles, FaceNet Model, Liveness Detection, Mobile-D Methodology.

Approved by Jacqueline Armijos



CAPÍTULO I. INTRODUCCIÓN

A nivel global, la gestión de la seguridad organizacional transitó desde sistemas basados en la posesión de credenciales físicas hacia la verificación automatizada de la identidad. Sin embargo, los entornos de transporte público masivo y comercial, como el de las cooperativas de taxis en el contexto ecuatoriano, presentaron vulnerabilidades críticas debido a la de métodos de control manuales y tradicionales. En la Cooperativa de Taxis "Señor del Buen Suceso", ubicada en el cantón Riobamba, se evidenció una ausencia de mecanismos tecnológicos avanzados que registrasen y validasen de forma automatizada la identidad y el estado de riesgo de los conductores.

Durante el diagnóstico técnico y las evaluaciones preliminares de vulnerabilidad ejecutadas en la institución, se determinó que los mecanismos tradicionales de control de ingreso carecían de resistencia ante ataques de suplantación. Los ensayos de estrés biométrico iniciales demostraron que la falta de un control automatizado de vivacidad generaba una brecha de seguridad, permitiendo el bypass del acceso mediante fotografías de usuarios autorizados. A esto se sumó la inexistencia de filtros psicométricos, lo que impedía detectar estados alterados de agresividad o ansiedad elevada en el personal antes de iniciar operaciones, justificando la implementación de una infraestructura tecnológica que unificase validación biométrica y análisis emocional.

La seguridad institucional enfrentó nuevos desafíos que fueron más allá de la simple validación de identidad, incorporando la necesidad de evaluar factores emocionales que representaban riesgos en el entorno laboral. En el caso de la Cooperativa de Taxis "Señor del Buen Suceso", el ingreso de personas en estados emocionales alterados, como agresividad y ansiedad elevada, podía derivar en conflictos internos o accidentes laborales. Esta situación exigió el desarrollo de nuevas herramientas que permitiesen gestionar el acceso de manera segura y eficiente.

En el presente trabajo de investigación, se desarrolló e implementó una aplicación web/móvil basada en inteligencia artificial, denominada FaceKey. La solución informática se diseñó con la capacidad de ejecutar el reconocimiento facial y el análisis psicométrico de emociones en tiempo real. Este sistema no solo verificó de forma automatizada la autorización del individuo, sino que también analizó las expresiones faciales mediante modelos de visión por computadora para identificar estados afectivos alterados que constituyesen un riesgo potencial.

En función del resultado del procesamiento algorítmico, el sistema ejecutó la concesión o restricción del acceso de manera automatizada, asegurando con ello que únicamente ingresasen los operarios en condiciones óptimas. Asimismo, mediante estos métodos de validación digital, se generaron registros transaccionales detallados dentro de la base de datos remota, garantizando la trazabilidad de los eventos y respaldando la toma de decisiones estratégicas de seguridad dentro de la organización.

Esta iniciativa tecnológica contribuyó a incrementar la seguridad de la institución mediante el despliegue de los modelos FaceNet y FER para el reconocimiento de

identidad y el análisis de estados de ánimo. El enfoque implementado coadyuvó a mitigar los riesgos operativos en el entorno laboral, optimizó la administración del personal y elevó el nivel de protección perimetral en las instalaciones de la cooperativa.

1.1. Planteamiento del Problema

La seguridad en la Cooperativa de Taxis "Señor del Buen Suceso" en Riobamba presentaba deficiencias críticas en su infraestructura de control. Los métodos de acceso históricos operaban bajo esquemas tradicionales que impedían auditar de forma fidedigna el flujo de ingresos y salidas del personal, resultando ineficaces para responder ante amenazas derivadas de situaciones de riesgo emocional. El control físico dependía del uso de llaves mecánicas y autorizaciones otorgadas de manera estrictamente verbal.

Por consiguiente, se constató la inexistencia de un proceso estandarizado para comprobar la identidad de los empleados o visitantes, omitiéndose la evaluación del estado afectivo de los individuos antes de permitir su ingreso. Esta falta de control técnico provocaba incidentes que afectaban la seguridad perimetral y la continuidad operativa de la cooperativa. Cuando el personal acudía con conductas agresivas, estrés agudo o alteraciones psicológicas, se suscitaban conflictos internos que perjudicaban el clima laboral o incrementaban el riesgo de accidentes.

A este escenario se sumaba la ausencia de registros automáticos de accesos, la vulnerabilidad ante ataques de suplantación de identidad y la falta de alertas preventivas en tiempo real. En este contexto, surgió la necesidad de implementar una solución tecnológica que unificase la validación de identidad y el análisis emocional mediante visión por computadora. El sistema desarrollado permitió restringir el ingreso a usuarios registrados que presentasen expresiones de riesgo (ira o ansiedad), promoviendo un entorno institucional controlado y emocionalmente estable.

1.2. Justificación

El uso de tecnologías emergentes en la seguridad física se estableció como un factor clave para mitigar las contingencias derivadas de las alteraciones emocionales de los trabajadores. Debido a que la cooperativa no disponía de herramientas automatizadas para auditar la identidad y el estado anímico de los usuarios, se generaban fricciones operativas que afectaban tanto al personal como a los visitantes. Por lo tanto, la propuesta de implementar un sistema con inteligencia artificial nació para solventar de forma definitiva las debilidades del control de acceso convencional.

El despliegue del reconocimiento facial coadyuvó a regular el perímetro de seguridad e introdujo la capacidad de identificar conductas reactivas antes de que se tradujesen en incidentes reales, incrementando la protección en la prestación del servicio de transporte. Esta innovación tecnológica salvaguardó a los socios y modernizó la gestión operativa de la cooperativa mediante la inferencia automatizada de estados afectivos en tiempo real.

Adicionalmente, el proyecto se orientó a reducir el error humano y a prescindir de los métodos de control analógicos tradicionales, los cuales carecían de mecanismos de

auditoría continua. La automatización de la validación biométrica y psicométrica permitió optimizar el uso de los recursos institucionales y generó una base de datos estructurada para la toma de decisiones directivas, consolidando un entorno laboral altamente profesional, seguro y pacífico.

1.3. Formulación del Problema

¿De qué manera la implementación de una aplicación web/móvil basada en biometría facial e inteligencia artificial, y su posterior evaluación técnica bajo los parámetros de la norma ISO/IEC 19795-1:2021, determina la precisión y la seguridad en el control de accesos de la Cooperativa "Señor del Buen Suceso"?

1.4. Objetivos

Objetivo General:

Implementar una aplicación web/móvil con biometría facial e inteligencia artificial para controlar de forma segura los accesos en la cooperativa “Señor del Buen Suceso”.

Objetivos Específicos:

- Investigar las tecnologías de reconocimiento facial y modelos de inteligencia artificial aplicables al análisis de emociones en tiempo real, adecuados para contextos de acceso institucional.
- Desarrollar una aplicación web y móvil que integre autenticación biométrica facial e inteligencia artificial para el análisis emocional.
- Evaluar el desempeño del sistema biométrico facial con análisis emocional de la aplicación web/móvil con autenticación facial e inteligencia artificial según la norma ISO/IEC 19795-1:2021

CAPÍTULO II. MARCO TEÓRICO

2.1. Análisis de trabajos relacionados en inteligencia artificial

El desarrollo de sistemas de control de accesos basados en visión por computadora ha sido abordado por la comunidad científica, enfocándose de forma prioritaria en optimizar la precisión de la identidad. No obstante, la integración de factores psicométricos y el análisis de estados afectivos en tiempo real como criterios de restricción operativa representan una vertiente emergente en la ingeniería de software. Con el propósito de delimitar las fronteras del conocimiento e identificar las necesidades técnicas no resueltas en la literatura actual, se procedió a realizar una revisión de investigaciones previas vinculadas al objeto de estudio.

Esta revisión documental permitió estructurar una comparación analítica entre diversas propuestas tecnológicas globales y el presente proyecto de investigación, denominado FaceKey. El análisis se focalizó en identificar los modelos de aprendizaje profundo empleados, los mecanismos de seguridad activa implementados y las variables operacionales consideradas en entornos institucionales. A partir de este levantamiento de información, se determinaron los aportes teóricos de cada autor, así como las limitaciones técnicas que justifican el desarrollo de la solución propuesta para la cooperativa.

A continuación, en la Tabla 1, se expone de forma detallada la matriz comparativa del estado del arte, especificando los autores, las metodologías aplicadas, las brechas tecnológicas identificadas y la diferenciación científica del presente trabajo de titulación.

Tabla 1: Matriz Comparativa del Estado del Arte y Brechas Tecnológicas.

Autor y Referencia	Aporte Tecnológico / Modelo	Limitaciones Identificadas	Brecha Solventada por FaceKey
Tovar-Galeano (2020)	Implementación de biometría facial para el control de accesos en instituciones de educación superior utilizando arquitecturas clásicas.	El sistema es vulnerable a ataques de presentación (spoofing) con fotografías y carece de evaluación de riesgos del entorno del usuario.	Integración de algoritmos de software basados en los Ángulos de Euler para detección de vivacidad activa.
Li, Zhang, & Wang (2021)	Propuesta de una arquitectura distribuida móvil y descentralizada para la gestión de identidad biométrica avanzada.	Alta dependencia de conectividad constante para el procesamiento y exclusión total de factores cognitivos o emocionales del operario.	Inferencia local mediante TensorFlow Lite que garantiza operatividad sin conexión crítica a internet y filtro psicométrico.
Warnars et al. (2022)	Diseño de control de accesos inteligente mediante APIs RESTful acopladas a actuadores y cerraduras físicas IoT.	El modelo se limita a la validación binaria de tokens de identidad, ignorando el estado de alteración psicológica del conductor.	Inclusión del modelo FER para bloquear accesos de forma preventiva si los niveles de ira o ansiedad superan el umbral del 10%.

Fuente: Investigación Directa (2026)

2.1.1. Evolución de los sistemas de control de accesos

La trayectoria del control de accesos se caracteriza por una progresión continua desde la dependencia del hardware hacia la sofisticación del software (Alshahrani, 2026). Los primeros sistemas se basaban en la resistencia material de cerraduras y la distribución controlada de llaves. Posteriormente, se incorporaron sistemas de credenciales basados en tarjetas de banda magnética y, más tarde, tecnologías de proximidad (RFID/NFC), que permitieron la automatización del registro y la auditoría de eventos. Sin embargo, estas credenciales aún eran susceptibles de robo o préstamo. La biometría marcó la transición al utilizar características físicas inmutables como la credencial principal (Choi, 2023). Esta evolución culmina con el reconocimiento facial, que, al no requerir contacto físico ni acción específica por parte del usuario, se integra de manera más natural y eficiente en los flujos operativos de acceso.

2.1.2. Comparación entre sistemas mecánicos y digitales

La diferencia entre los sistemas de control de acceso mecánicos y los digitales modernos se centra en la gestión de riesgos y la operatividad (Choi, 2023). Los sistemas mecánicos son de bajo costo y autónomos, pero su seguridad es estática y vulnerable a la duplicación no autorizada de llaves, además de carecer de capacidad para registrar o revocar accesos de forma remota. Por el contrario, los sistemas digitales ofrecen dinamismo, con capacidades de auditoría completa, gestión centralizada de permisos y la posibilidad de integrar la seguridad con otros sistemas de gestión. La biometría facial se sitúa en la cúspide de esta funcionalidad digital, ya que elimina las debilidades de los PINs y las tarjetas al verificar una característica inherente al usuario, garantizando que quien accede es verdaderamente el individuo autenticado y mejorando significativamente la tasa de autenticación correcta (Hofer, 2022).

2.1.3. Necesidad de soluciones seguras y eficientes en la gestión de accesos

La necesidad de soluciones de control de accesos seguros y eficientes es impulsada por la creciente complejidad de las amenazas y la importancia de proteger los activos digitales y físicos (Aloraini, 2025). Los fallos de seguridad en los métodos tradicionales pueden traducirse en pérdidas operacionales significativas, fraudes o suplantación de identidad (Adjabi, Past, Present, and Future of Face Recognition: A Review, 2020). Las tecnologías digitales responden a esta exigencia al proporcionar mecanismos de autenticación adaptativos y de alta fidelidad. El reconocimiento facial se presenta como la herramienta ideal, ya que su verificación rápida minimiza los cuellos de botella en el flujo de personas y, al ser sin contacto, mejora la higiene y la experiencia del usuario. Esta combinación de conveniencia operativa y resistencia superior a la suplantación lo posiciona como el estándar para la seguridad moderna.

2.2. Inteligencia artificial y machine learning en reconocimiento

La Inteligencia Artificial (IA) y el Machine Learning (ML) son la fuerza impulsora detrás de la precisión y robustez alcanzada por el reconocimiento facial contemporáneo (Wang, Deep Face Recognition: A Survey, 2021). El paradigma del aprendizaje profundo (Deep Learning) permitió a los sistemas de visión artificial superar

las limitaciones de los algoritmos basados en la extracción manual de características. Al procesar conjuntos masivos de datos faciales, la IA aprende a identificar patrones complejos y abstractos inherentes al rostro humano, como la geometría y la textura, lo que posibilita la verificación de identidad con alta confianza, incluso bajo condiciones ambientales variables y desafíos de oclusión.

2.2.1. Modelos de IA para el análisis facial

El éxito de la identificación facial se debe al uso de modelos preferidos de Inteligencia Artificial, especialmente las Redes Neuronales Convolucionales (CNN) (Adjabi, Past, Present, and Future of Face Recognition: A Review, 2020). Las CNN son arquitecturas compuestas por múltiples capas que funcionan como detectores jerárquicos de características: las capas iniciales identifican elementos básicos como bordes y esquinas, mientras que las capas profundas aprenden a reconocer características de alto nivel, como la forma de los ojos o la nariz (Wang, Deep Face Recognition: A Survey, 2021). Este enfoque de autoaprendizaje es superior a los métodos estadísticos anteriores (como el PCA o LDA) porque la red desarrolla representaciones internas óptimas del rostro (embeddings), lo que resulta en una huella digital facial excepcionalmente distintiva y robusta contra variaciones de pose, expresión e iluminación.

2.2.2. Técnicas de machine learning para reconocimiento facial

El reconocimiento facial se basa en la aplicación de técnicas de Machine Learning, principalmente el aprendizaje supervisado, donde se entrena un modelo para clasificar o verificar identidades a partir de datos de entrada etiquetados (Abidi, 2026). Las CNNs son entrenadas utilizando funciones de pérdida que maximizan la distancia entre las representaciones (embeddings) de diferentes individuos y minimizan la distancia entre las de un mismo individuo, creando un espacio latente altamente discriminatorio (Zheng, 2026). Para mejorar la resiliencia del sistema ante la escasez de datos o la diversidad demográfica, se emplean técnicas avanzadas como las Redes Generativas Antagónicas (GAN), que generan imágenes sintéticas realistas. Estas imágenes se inyectan en el conjunto de entrenamiento, fortaleciendo la capacidad del modelo para generalizar el reconocimiento a condiciones y variaciones no observadas en el mundo real (Gan, 2026).

2.2.3. Mejora en la precisión y seguridad mediante la IA

La IA ha mejorado la precisión del reconocimiento facial al reducir excesivamente las tasas de error biométrico (FAR y FRR), lo que incrementa directamente la seguridad del control de accesos (Jain, 2025). Esta mejora en la precisión es vital, ya que una menor tasa de falso rechazo mejora la experiencia del usuario, mientras que una menor tasa de falsa aceptación es crucial para evitar el acceso de impostores. Además de la precisión en la identificación, la IA introduce la funcionalidad esencial de detección de vida (liveness detecting) (Li, 2025). Estos algoritmos analizan señales dinámicas y texturales (como el parpadeo, el movimiento 3D o la reflectividad de la piel) para distinguir un rostro real de una suplantación pasiva (foto o video) o activa (máscara). Este

mecanismo protege el sistema contra una de las vulnerabilidades más críticas de la biometría, garantizando que el usuario autenticado sea básicamente presente.

2.2.4. Impacto de la ansiedad elevada y la agresividad en el comportamiento humano

La ansiedad elevada y la agresividad representan factores de riesgo críticos que pueden comprometer tanto la integridad individual como la seguridad colectiva en entornos controlados. La ansiedad, cuando se manifiesta de forma patológica o exacerbada, actúa como un disruptor cognitivo que altera la percepción de la realidad, incrementando la probabilidad de respuestas impulsivas o erráticas ante estímulos neutros. Por otro lado, la agresividad entendida como una disposición a causar daño o actuar de manera impositiva eleva los riesgos de conflicto interpersonal y transgresión de normas operativas. La interacción entre estados emocionales negativos y una baja tolerancia a la frustración crea un escenario propenso a la violencia reactiva. En el contexto de la gestión de accesos y seguridad, estas emociones no solo afectan la experiencia del usuario, sino que incrementan los riesgos de incidentes críticos, ya que un individuo bajo niveles extremos de estrés emocional es más propenso a intentar vulnerar protocolos de seguridad o reaccionar de forma hostil ante los sistemas de verificación.

2.3. Desarrollo de aplicaciones y conectividad IoT

El Desarrollo de Aplicaciones Móviles es la capa de software que une al usuario con la lógica biométrica y los dispositivos físicos de seguridad (Islam, 2024). La naturaleza distribuida de los sistemas modernos de control de accesorios requiere que la aplicación sea multiplataforma, eficiente en la captura de datos de alta resolución y capaz de gestionar la comunicación con componentes de hardware dispares. Por ello, la elección de un framework multiplataforma como Flutter se ha vuelto estratégica, facilitando una experiencia de usuario consistente y unificada, y estableciendo un canal de comunicación robusto a través de APIs RESTful para el control en tiempo real de los dispositivos interconectados bajo la arquitectura de Internet de las Cosas (IoT) (Brdanin, 2024).

2.3.1. Frameworks para desarrollo de aplicaciones (Flutter)

Los frameworks multiplataforma han ganado popularidad gracias a su capacidad para reducir el tiempo y el costo de desarrollo, permitiendo crear una única base de código para iOS y Android (Kinari, 2024). Flutter, desarrollado por Google, es particularmente ventajoso para sistemas biométricos. Su motor de renderizado Skia permite construir interfaces de usuario complejas con un rendimiento cercano al nativo, lo que es crucial para garantizar una captura facial rápida y sin latencia. Además de la eficiencia en el frontend, Flutter facilita la conectividad con dispositivos IoT a través de sus "plataforma canales", que permiten al código Dart interactuar de manera eficiente con las funciones nativas del sistema operativo, esencial para manejar la cámara, el Bluetooth o los módulos de red requeridos para el control de accesos (Google, 2024)

A continuación, se muestra la figura 1.



Figura 1: IDE Flutter.

Fuente: (Flutter, 2022)

2.3.2. Interfaz de usuario (UI) para capturas biométricas

El diseño de la Interfaz de Usuario (UI) no es solo una cuestión estética, sino un componente funcional que impacta directamente en la precisión del sistema biométrico (Schlett, 2022). Una UI bien diseñada para la captura facial debe priorizar la simplicidad y la guía intuitiva del usuario, minimizando la fricción y los errores de posicionamiento. Las buenas prácticas incluyen la provisión de retroalimentación visual en tiempo real, como el uso de guías de cuadro (óvalos o máscaras) que indican la posición óptima del rostro, así como mensajes claros y accionables ante condiciones subóptimas (Ahmed, 2021). Una experiencia de usuario deficiente puede resultar en la captura de datos biométricos de baja calidad, lo que degrada el rendimiento del algoritmo. Por lo tanto, la UI es la primera línea de calidad del dato en un sistema de autenticación biométrica (Anand, 2021).

2.3.3. API RESTful para control de dispositivos IoT

Las API RESTful son el estándar de arquitectura de software que permite la integración y control eficiente de dispositivos IoT en sistemas distribuidos, como el control de accesos biométricos (Kim, 2024). Una API RESTful permite la comunicación estandarizada y escalable entre la aplicación móvil, el servidor de autenticación y los actuadores físicos (por ejemplo, cerraduras inteligentes). Los dispositivos IoT (el lector facial) pueden enviar solicitudes POST al servidor para iniciar la verificación de identidad, y el servidor puede enviar comandos PUT o DELETE al dispositivo de control de acceso para accionar la apertura o cierre de una puerta (Vadlamudi, 2023). Este enfoque, al ser sin estado, asegura que la comunicación sea resistente a fallos y facilite la centralización de la gestión de permisos y registros de eventos a través de un único punto de control (Abuseta, 2024).

2.4. Seguridad informática y protección de datos biométricos

La seguridad informática y la protección de datos biométricos son temas de máxima prioridad debido a la naturaleza intrínseca e irrecuperable de la información facial. A diferencia de una contraseña que puede ser reestablecida, un dato biométrico

comprometido expone permanentemente la identidad del individuo (Rathgeb, 2025). Por ello, el diseño de estos sistemas requiere la adhesión rigurosa a normas y protocolos de seguridad internacionales y la implementación de mecanismos robustos, no solo para proteger contra los ciberataques, sino también para cumplir con el marco legal que garantiza el derecho a la privacidad de los usuarios (Alrawili, 2024).

2.4.1. Protección de datos biométricos: normas y protocolos de seguridad

La protección de datos biométricos se rige por un marco normativo estricto, liderado por el Reglamento General de Protección de Datos (GDPR) de la Unión Europea, que los clasifica como una categoría especial de datos, exigiendo un nivel de protección excepcional (Moschini, 2022). El cumplimiento de estas normas requiere la implementación de medidas de seguridad técnicas y organizativas, siendo el cifrado de datos la práctica fundamental (Grierson, 2024). Es imperativo que la plantilla biométrica se almacene no como una imagen reversible, sino como un hash unidireccional y salteado, minimizando el riesgo en caso de violación de la base de datos (Shinde, 2025). Además, la legislación exige la aplicación de principios como la "Privacidad desde el Diseño", asegurando que la privacidad sea una consideración esencial desde las primeras etapas del desarrollo del sistema.

2.4.2. Autenticación segura en sistemas biométricos

Para alcanzar la máxima confiabilidad en los sistemas de control de accesos, se debe implementar la autenticación segura mediante la Autenticación Multifactor (MFA) (Shukla, 2024). Aunque la biometría es un factor de "algo que el usuario es" muy robusto, combinarlo con un segundo factor ("algo que sabe" o "algo que tiene") proporciona una capa de defensa mucho más fuerte, mitigando el riesgo de que una única vulnerabilidad pueda comprometer la seguridad. El uso de la biometría facial como segundo factor de verificación se ha popularizado, complementando contraseñas o tokens. Además, la detección de vida (liveness detecting) es un mecanismo de seguridad intrínseco a los sistemas biométricos que garantiza la autenticación real del sujeto y se considera esencial para la robustez del sistema contra ataques de suplantación pasiva (Alrawili, 2024).

2.4.3. Ventajas de la biometría facial frente a métodos tradicionales

La biometría facial ofrece ventajas operativas y de seguridad que superan significativamente a los métodos tradicionales de autenticación como las tarjetas de acceso o contraseñas. Su principal beneficio en seguridad es que el rasgo facial es inherente y no transferible, lo que imposibilita la suplantación o el préstamo de credenciales, un fallo común en los sistemas basados en posesión. En términos de usabilidad, el proceso es rápido, pasivo y sin contacto, lo que reduce la fricción en el punto de acceso y mejora el flujo operativo (Cai, 2023).

2.5. Metodología: Implementación de Mobile-D

La implementación de soluciones de autenticación biométrica de última generación se articula a través de sistemas integrales diseñados para operar en entornos distribuidos. El sistema Mobile-d (nombrado así para reflejar la tendencia de la biometría

móvil y distribuida) representa una arquitectura moderna cuyo objetivo principal es descentralizar la captura de datos biométricos al aprovechar las capacidades de procesamiento y conectividad de los dispositivos móviles (Hofer, 2022). La metodología de implementación de Mobile-d debe abarcar desde una descripción detallada de su arquitectura, el cumplimiento de rigurosos requisitos técnicos para la interoperabilidad, hasta los procesos de evaluación continua y mantenimiento preventivo para asegurar su precisión y seguridad a largo plazo.

2.5.1. Descripción de Mobile-D

Mobile-D es una metodología ágil de desarrollo de software orientada específicamente a la construcción de aplicaciones para dispositivos móviles. Fue propuesta originalmente por Abrahamsson et al. en 2004 e integra las prácticas de desarrollo de la Programación Extrema (XP), los métodos de escalabilidad de Crystal Methodologies y la cobertura del ciclo de vida del Proceso Unificado Racional (RUP). Está optimizada para equipos pequeños de menos de diez desarrolladores que trabajan de forma co-ubicada, con el objetivo de entregar una aplicación móvil completamente funcional en ciclos cortos de desarrollo (Gasca-Hurtado, 2023).

El proceso de desarrollo en Mobile-D se organiza en fases iterativas, cada una compuesta por días de planificación, días de trabajo y días de entrega:

1. **Exploración**, donde se establecen los interesados del proyecto, se delimita el alcance y se definen los requisitos iniciales;
2. **Inicialización**, en la que se configura el entorno de desarrollo, se diseña la arquitectura del sistema y se preparan los recursos tecnológicos necesarios;
3. **Producción**, que constituye el núcleo del desarrollo donde se implementan iterativamente todas las funcionalidades del sistema mediante ciclos cortos de codificación y pruebas unitarias.
4. **Pruebas del Sistema**, donde se ejecutan las pruebas de aceptación, se evalúa el rendimiento global de la aplicación y se validan los requisitos funcionales y no funcionales definidos inicialmente.

2.5.2. Requisitos técnicos y proceso de implementación

La correcta implementación del sistema requiere cumplir con estrictos requisitos técnicos y seguir un proceso estructurado para garantizar la integración sin fisuras con la infraestructura existente.

Requisitos Técnicos:

- **Conectividad de Red:** Es fundamental contar con una red sólida (ya sea Wi-Fi o 4G/5G) que presente baja latencia, garantizando así una comunicación en tiempo real entre el dispositivo móvil (usuario) y el servidor principal, puesto que cualquier demora impacta negativamente en la experiencia del usuario y en la eficiencia en las operaciones (Yaghoubi, 2024).
- **Dispositivos Móviles:** Se necesitan aparatos móviles (teléfonos inteligentes o tabletas) que posean una cámara frontal de alta definición (al menos 8

megapíxeles) y que tengan la capacidad de procesamiento requerida para ejecutar los algoritmos de detección de vida de forma local.

- **Servidor para Almacenamiento y Procesamiento:** El servidor debe ser capaz de manejar un alto número de transacciones por segundo (TPS) y proporcionar un almacenamiento protegido para las plantillas biométricas, empleando bases de datos que estén optimizadas para el acceso concurrente y el uso de cifrado.

A continuación, la tabla 2, presenta Proceso de Implementación.

Tabla 2. Proceso de Implementación

Fase / Componente	Descripción de Tareas
Instalación y configuración del backend	Despliegue del servidor de reconocimiento facial y la base de datos de plantillas en un entorno de nube o local, asegurando la encriptación de extremo a extremo.
Integración de la API RESTful	Se establece el enlace entre el servidor y las cerraduras IoT mediante una API protegida. Esto incluye cambiar los puntos finales que se usan para la autorización y para abrir o cerrar los dispositivos de forma segura.
Despliegue de la Aplicación Móvil	Se instala la aplicación en los dispositivos y después se ajustan los parámetros de la cámara para mejorar la calidad de imagen y los niveles de vivacidad.
Fase de Inscripción	Se realiza el registro de usuarios capturando múltiples ángulos e iluminaciones para generar una plantilla biométrica base. Este proceso ayuda a que el reconocimiento sea correcto y fiable en las siguientes fases

Fuente: (Alzhrani A. A., 2024)

2.5.3. Evaluación de la norma ISO/IEC 19795-1:2021.

La norma internacional ISO/IEC 19795-1:2021 establece los principios fundamentales y el marco metodológico para la evaluación del desempeño en sistemas biométricos, determinando que el rendimiento técnico se cuantifica mediante la probabilidad de error en la toma de decisiones lógicas de aceptación o rechazo. La caracterización formal de estas tecnologías requiere el análisis de variables estandarizadas que miden tanto la seguridad del acceso frente a impostores como la usabilidad respecto a los usuarios legítimos. (ISO/IEC., 2021).

Desde una perspectiva estrictamente teórica y conceptual, los indicadores fundamentales de rendimiento recomendados por este estándar internacional se definen de la siguiente manera:

Tasa de Aceptación Verdadera: Representa la proporción de usuarios autorizados que son correctamente identificados por el sistema.

Tasa de Falsa Aceptación: Determina la probabilidad matemática con la que el algoritmo clasifica de manera errónea a un usuario no autorizado o impostor como un sujeto legítimo, permitiendo un acceso indebido a la infraestructura protegida.

Tasa de Falso Rechazo: Define el porcentaje de transacciones correspondientes a usuarios auténticos que son denegadas de forma incorrecta por el sistema informático, funcionando como el indicador principal para evaluar la usabilidad y la eficiencia operativa de la plataforma.

2.5.4. Estrategias para el mantenimiento y optimización a largo plazo:

- 1. Reentrenamiento del Modelo:** Es fundamental reentrenar el algoritmo de inteligencia artificial de manera regular utilizando recientes ejemplos faciales y bases de datos actualizadas, con el fin de ajustarse a las variaciones en los usuarios (por envejecimiento o uso de complementos) y enfrentar nuevas amenazas de suplantación (Cai, 2023).
- 2. Supervisión de la Base de Datos:** Es necesario llevar a cabo auditorías continuas de las plantillas biométricas y deshacerse de aquellas que no sean imprescindibles, garantizando así el respeto hacia las normativas de conservación de datos (Lacharme, 2023).

CAPÍTULO III. METODOLOGIA

3.1. Tipo de Investigación

La presente investigación se clasifica como de tipo aplicada y de desarrollo tecnológico, orientada a resolver una problemática operacional concreta mediante la construcción de una solución informática institucional. El alcance del estudio es estrictamente tecnológico y evaluativo, enfocado en medir la eficiencia y la robustez de algoritmos de visión artificial de inteligencia artificial desplegados en un entorno real.

Este carácter aplicado establece un vínculo directo entre las interfaces de software desarrolladas y la medición cuantitativa de su rendimiento. La infraestructura del sistema permite la recolección automatizada de datos transaccionales empíricos, los cuales se correlacionan directamente con las variables de estudio a través de sus respectivos indicadores técnicos de precisión matemática, tiempos de respuesta en milisegundos y tasas de error algorítmico.

3.2. Diseño de la Investigación

El diseño de la investigación se define bajo un enfoque cuantitativo, estructurándose de forma específica como una evaluación técnica de software con un alcance descriptivo. El diseño metodológico se concentra de manera exclusiva en la medición, automatizada y numérica de las transacciones generadas por el sistema informático desarrollado, recopilando métricas directas de rendimiento desde la base de datos central.

El estudio se justifica metodológicamente como un diseño de evaluación técnica, de carácter no experimental y de corte transversal. El proyecto no responde a un esquema experimental o cuasi-experimental debido a que no existe una manipulación deliberada o artificial de los rasgos físicos ni de las expresiones faciales de los conductores, capturando el comportamiento del algoritmo en un único momento temporal durante las pruebas de campo.

La naturaleza descriptiva-evaluativa del diseño radica en registrar la distribución de frecuencias de los aciertos y errores del algoritmo mediante matrices de contingencia. Este proceso metodológico permite caracterizar estadísticamente el comportamiento operativo de los modelos lógicos FaceNet y FER, fundamentando las conclusiones de la investigación en la verificación empírica de métricas estandarizadas de precisión y eficiencia.

3.3. Población de estudio y tamaño muestra

Población: Se establece todo el personal administrativo y conductores autorizados de la cooperativa “Señor del Buen Suceso”, que suman 106 personas.

Muestra: Se realiza el cálculo de la muestra estableciéndose como 83 personas.

Fórmula para población finita:

$$n = \frac{N \cdot Z^2 \cdot p \cdot q}{(e^x \cdot (N - 1)) + (Z^2 \cdot p \cdot q)}$$

Donde:

- n = tamaño de la muestra
- N = tamaño de la población (106)
- Z = valor z para el nivel de confianza (95% $\Rightarrow Z = 1.96$)
- p = proporción esperada (0.5 si no se conoce)
- $q = 1 - p$
- e = margen de error aceptado (generalmente 5% $\Rightarrow 0.05$)

$$n = \frac{106 * (1.96)^2 * 0.5 * 0.5}{(0.05)^2 * (106 - 1) + (1.96)^2 * 0.5 * 0.5}$$

$$n = \frac{101.1}{0.2625 + 0.9604}$$

$$n = \frac{101.1}{1.2229}$$

$$n = 82.7$$

$$n = 83 \text{ personas.}$$

3.4. Técnicas e instrumentos de recolección de datos

3.4.1 Técnicas de recolección de datos

- **Observación directa:** Se llevó a cabo una observación en persona de los métodos actuales de control de acceso en la Cooperativa de Taxis “Señor del Buen Suceso”, con la finalidad de reconocer debilidades, problemas operativos y riesgos de seguridad que existen en los métodos tradicionales que se emplean. Esta técnica facilitó la comprensión del verdadero flujo de ingreso de individuos y las limitaciones del sistema vigente.
- **Imágenes faciales:** El personal que forma parte de la muestra posa para tomar las fotos. Usan estas fotos para el registro biométrico y verifican las caras después con las mismas imágenes. Este proceso ayudó a hacer las plantillas biométricas que sirven para ver cómo funciona el sistema de reconocimiento facial y para observar las emociones.

1.4.2 Instrumentos de recolección de datos

Instrumentos de recolección de datos.

Los instrumentos de recolección usaron las técnicas de investigación. Los instrumentos hicieron que la información fuera válida y exacta. Se emplearon las siguientes herramientas:

- **Guía de observación:** Se usó una guía para anotar los pasos que siguen en el control de acceso. Esto permitió identificar métodos de validación, tiempos de respuesta, vulnerabilidades de seguridad y la ausencia de mecanismos de monitoreo.

- **Sistema de reconocimiento biométrico:** Se utilizó la aplicación móvil en Flutter con los modelos FaceNet y FER integrados. El instrumento ayudó a captar los rostros, a crear los vectores biométricos, a ver las emociones y a guardar cada acceso en la base de datos de forma automática.
- **La base de datos de registros de acceso:** El equipo trabajó con la base de datos MySQL del sistema. La base de datos guarda los intentos de acceso, los resultados de autenticación, las emociones que detecta y los tiempos de validación de forma automática. Esta información sirvió como base para el estudio sobre el rendimiento del sistema.

1.4.3 Protocolo de captura, validación funcional y protección de datos

Para la aplicación de las técnicas de recolección, se ejecutó un protocolo de captura facial basado en las restricciones de hardware del módulo móvil. El entorno de evaluación se configuró en el punto de acceso de la cooperativa, requiriendo que los conductores mantuvieran una postura frontal neutra frente a la cámara del dispositivo con una tolerancia de desvío angular inferior a $\pm 15^\circ$ en los ejes yaw, pitch y roll. Este procedimiento estandarizado garantizó la homogeneidad en las capturas y facilitó el correcto procesamiento local de las microexpresiones por parte de los modelos de visión artificial.

La validación de los instrumentos tecnológicos se realizó mediante pruebas funcionales de caja negra y la verificación de cumplimiento de los requisitos no funcionales definidos en la fase de exploración. El software FaceKey y el esquema de la base de datos MySQL remota fueron sometidos a ensayos iterativos de carga y conectividad para asegurar la estabilidad en la sincronización de las transacciones. Este proceso de auditoría técnica directa reemplazó los métodos de validación subjetiva, fundamentando la fiabilidad del sistema en la consistencia de los tiempos de respuesta y las tasas de error obtenidas.

En el ámbito ético y de protección de datos biométricos, el sistema se diseñó bajo el principio de privacidad desde la arquitectura tecnológica, omitiendo la recolección de firmas o documentos físicos que comprometieran la identidad de los operarios. La seguridad de la información sensible se garantizó mediante la conversión inmediata del rasgo facial en un embedding matemático de 128 dimensiones serializado en texto. Asimismo, el módulo móvil ejecutó la destrucción automatizada del archivo de imagen original tras cada inferencia local, asegurando el cumplimiento técnico de los protocolos de confidencialidad.

3.5. Métodos de análisis y procesamiento de datos

Para investigar las tecnologías de reconocimiento facial y modelos de inteligencia artificial aplicables al análisis de emociones en tiempo real, adecuados para contextos de acceso institucional, se realizó en siguiente procedimiento:

- Determinar las tecnologías de reconocimiento facial y modelos de inteligencia artificial adecuados para el acceso institucional, fundamentados en una

investigación estructurada, durante esta etapa se examinaron modelos como Haar Cascades, LBPH, VGGFace y FaceNet para la identificación de identidad, junto con VGG16, SVM y FER para el análisis de emociones, juntamente con la integración del método de EULER.

- Desarrollar la aplicación para teléfonos móviles utilizando los modelos FaceNet y FER junto con el método EULER.
- Ejecutar pruebas en la app móvil para validar el reconocimiento facial y análisis emocional con base de datos local.
- Cambiar los parámetros de los modelos de reconocimiento para mejorar la precisión y el rendimiento del sistema.
- Desarrollar un panel para control de usuarios, reportes de acceso, gestión de bloqueos y supervisión técnica.
- Integrar la aplicación móvil con el ecosistema Tuya Smart mediante su API para la automatización de dispositivos.
- Revisar cómo funciona la biometría y la detección emocional en las páginas web y en los dispositivos móviles.

El procesamiento y análisis de los datos cuantitativos se fundamenta en la evaluación del desempeño técnico del sistema informático, bajo los lineamientos de la norma internacional ISO/IEC 19795-1:2021. Los datos transaccionales recopilados de forma automática en la tabla `emotion_attempts` de la base de datos remota MySQL se exportan en formato estructurado para su análisis estadístico descriptivo. Este procedimiento permite examinar el comportamiento de los modelos de visión artificial FaceNet y FER ante los entornos operacionales reales de la cooperativa.

Para garantizar la reproducibilidad del experimento técnico, se estructura una matriz de confusión o matriz de errores que clasifica las transacciones del sistema. Los 168 intentos de acceso se categorizan en cuatro estados lógicos: Verdadero Positivo (VP), conductor autorizado reconocido correctamente; Falso Positivo (FP), suplantación digital aceptada erróneamente; Falso Negativo (FN), rechazo incorrecto de un conductor legítimo; y Verdadero Negativo (VN), bloqueo exitoso de un impostor o de un usuario con niveles de riesgo emocional (ira o ansiedad alta).

A continuación, en la Tabla 3, se establece la estructura formal de la matriz de errores utilizada para el procesamiento de los datos de evaluación de la plataforma:

Tabla 3: Matriz de Confusión para la Evaluación del Sistema FaceKey.

Condición Real del Intento / Estado	Clasificado como Autorizado (Acceso Permitido)	Clasificado como Riesgo/Impostor (Acceso Denegado)	Total, de Transacciones por Condición
Conductor Autorizado (Emoción Estable)	127 (Verdadero Positivo)	1 (Falso Negativo)	128
Impostor (Spoofing) o Ira/Ansiedad	4 (Falso Positivo)	36 (Verdadero Negativo)	40
Total, de Decisiones del Software	131 (Accesos Permitidos)	37 (Accesos Bloqueados)	168 (Universo Total)

Fuente: Panel de Control de la Plataforma Web FaceKey (2026)

El cálculo de las métricas de rendimiento biométrico se realiza aplicando las ecuaciones estandarizadas de la norma ISO, las cuales gobiernan la validación del software. Los criterios de aceptación técnica determinan que el sistema es viable si alcanza una precisión general mínima del 90.00% y mantiene la Tasa de Falsa Aceptación por debajo del 5.00%. Las fórmulas empleadas para el procesamiento de las variables dependientes se definen a continuación:

VP (Verdadero Positivo): Representa la cantidad de transacciones exitosas en las cuales un conductor autorizado con un estado emocional estable es correctamente identificado por el algoritmo, concediéndosele el acceso legítimo a la infraestructura.

VN (Verdadero Negativo): Corresponde al número de eventos donde el sistema deniega el acceso de manera correcta, bloqueando un ataque de suplantación digital (impostor) o restringiendo el ingreso ante un estado emocional de riesgo detectado.

FP (Falso Positivo): Define la cantidad de errores críticos en los cuales el software clasifica de forma incorrecta a un usuario no autorizado o a una fotografía estática como un sujeto legítimo, permitiendo un acceso indebido.

FN (Falso Negativo): Indica el número de anomalías operacionales en las cuales un conductor debidamente registrado en el sistema es rechazado de forma errónea, debido a variaciones extremas en la iluminación ambiental o en los ángulos de captura.

FAR (False Acceptance Rate / Tasa de Falsa Aceptación): Indicador probabilístico porcentual que mide la vulnerabilidad del sistema informático frente a intentos de intrusión o vulneración de seguridad por parte de terceros no autorizados.

FRR (False Rejection Rate / Tasa de Falso Rechazo): Métrica porcentual descriptiva que cuantifica el impacto adverso en la usabilidad del software, evaluando la frecuencia con la que se afecta la fluidez del ingreso del personal operativo.

TAR (*True Acceptance Rate* / Tasa de Aceptación Verdadera): Variable que determina la efectividad global de emparejamiento biométrico del sistema ante solicitudes legítimas, calculada como el complemento directo de la tasa de falso rechazo.

Accuracy (Precisión General): Coeficiente estadístico que establece la exactitud global de la plataforma, determinando el porcentaje total de decisiones correctas (tanto aceptaciones legítimas como bloqueos preventivos) sobre el volumen total de los intentos ejecutados.

1. Tasa de Falsa Aceptación (FAR):

$$FAR = \left(\frac{FP}{N} \right) * 100\%$$

2. Tasa de Falso Rechazo (FRR):

$$FRR = \left(\frac{FN}{N} \right) * 100\%$$

3. Tasa de Aceptación Verdadera (TAR):

$$TAR = 100\% - FRR$$

4. Precisión General del Sistema (Accuracy):

$$Accuracy = \left(\frac{VP + VN}{N} \right) * 100\%$$

El análisis de la distribución de emociones se procesa mediante el cálculo de frecuencias relativas de las siete categorías del modelo FER, correlacionando el volumen de bloqueos con la métrica `negative_sum` almacenada. Los tiempos de validación se evalúan mediante medias aritméticas para verificar la eficiencia del procesamiento local en milisegundos.

3.6. Identificación de variables

3.6.1. Variable independiente

Aplicación web/móvil con biometría facial e IA

3.6.2. Variable dependiente

Desempeño del sistema biométrico facial con análisis emocional

3.7. Operacionalización de variables

A continuación, la tabla 4, presenta la operacionalización de variables

Tabla 4. Operacionalización de Variables

PROBLEMA	TEMA	OBJETIVOS	VARIABLES	CONCEPTUALIZACION	DIMENSION	INDICADORES
¿Cómo el desempeño del sistema biométrico facial con análisis emocional incidirá en una aplicación web/móvil con autenticación facial e inteligencia artificial para el análisis emocional en la seguridad de accesos de la Cooperativa “Señor del Buen Suceso”?	Aplicación web/móvil con biometría facial e inteligencia artificial para control seguro de accesos en la cooperativa “Señor del Buen Suceso”.	GENERAL	INDEPENDIENTE	El sistema toma las imágenes de los rostros y revisa que sean válidos. La identidad y las emociones están presentes, y el usuario desbloquea la cerradura usando Tuya Smart.	Funcionalidad de la aplicación.	INDEPENDIENTE
		• Implementar una aplicación web/móvil con biometría facial e inteligencia artificial para controlar de forma segura los accesos en la cooperativa “Señor del Buen Suceso”.	Aplicación web/móvil con biometría facial e IA			• Reconocimiento facial correcto • Análisis de emociones
		ESPECIFICOS	DEPENDIENTE	Capacidad funcional y operativa de una solución La tecnología usa el reconocimiento facial y la inteligencia artificial. La información emocional ayuda a ver quién es cada persona y también muestra cómo se siente la gente. personas en un control de acceso con criterios de precisión La eficiencia y la confiabilidad.	Desempeño	DEPENDIENTE
		• Investigar las tecnologías de reconocimiento facial y modelos de inteligencia artificial aplicables al análisis de emociones en tiempo real, adecuados para contextos de acceso institucional. • Desarrollar una aplicación web y móvil que integre autenticación biométrica facial e inteligencia artificial para el análisis emocional. • Evaluar el desempeño del sistema biométrico facial con análisis emocional de la aplicación web/móvil con autenticación facial e inteligencia artificial según la norma ISO/IEC 19795-1:2021	Desempeño del sistema biométrico facial con análisis emocional			• Precisión (TAR, FAR, FRR) • Tiempos de validación (eficiencia) • Errores de autenticación • Capacidad de análisis emocional con IA

3.8. Metodología de desarrollo

Se implementó un sistema de reconocimiento facial biométrico utilizando el modelo FaceNet pre-entrenado en TFLite, que genera embeddings de 128 dimensiones a partir de imágenes de 512×512 píxeles con 80% de umbral de similitud coseno, complementado con Google ML Kit para detección facial inicial y validación de vivacidad mediante análisis de apertura ocular y ángulos cefálicos (-15° a +15° en yaw, pitch y roll) para prevenir suplantación. El análisis emocional en tiempo real se realizó con el modelo FER (Facial Expression Recognition), que procesa imágenes en escala de grises de 48×48 píxeles para detectar 7 emociones (neutral, felicidad, tristeza, ira, sorpresa, miedo y disgusto) mediante redes neuronales convolucionales con activación softmax, aplicando un umbral de bloqueo del 10% en emociones críticas (agresividad/ira y ansiedad elevada) adecuado para contextos institucionales que requieren seguridad y estabilidad emocional. La implementación se desarrolló en Flutter 3.x con TFLite Flutter para inferencia local en dispositivos móviles, logrando procesamiento en tiempo real (<3 segundos) con sincronización a base de datos MySQL remota en Hostinger para almacenamiento de embeddings faciales, registro de accesos y trazabilidad completa de emociones detectadas.

Metodología de desarrollo de la aplicación web/móvil utilizando Móvil-D

Para el desarrollo de la aplicación web y móvil orientada a la autenticación biométrica facial y el análisis emocional mediante inteligencia artificial, se aplicaron las fases estructurales contempladas en la metodología Mobile-D:

3.8.1. Fase 1: Exploración

Durante la Fase de Exploración se establecieron los fundamentos del proyecto FaceKey. En esta etapa se definió la visión del sistema biométrico para la cooperativa "Señor del Buen Suceso", identificando qué funcionalidades serían prioritarias para el MVP (dashboard web de administración y aplicación móvil de autenticación facial), qué tecnologías de IA serían viables (FaceNet para reconocimiento facial y FER para análisis emocional), y qué limitaciones debían considerarse (procesamiento local en dispositivos móviles, optimización de velocidad sin perder precisión). Se investigaron los modelos pre-entrenados disponibles en TensorFlow Lite compatibles con Flutter, se evaluó la infraestructura de hosting en Hostinger con MySQL, y se establecieron los requisitos funcionales y no funcionales clave, como el tiempo máximo de autenticación de 3 segundos, el umbral del 80% de similitud facial, y el filtrado emocional con bloqueo al 10% de ira/ansiedad.

Definición del alcance preliminar

En esta etapa se establece qué funcionalidades incluirá el sistema en su primera versión (Producto Mínimo Viable - MVP) y cuáles se excluirán:

Alcance:

- **Módulo web (Administración):** Dashboard 3D interactivo alojado en buensuceso.site con las siguientes funcionalidades: Visualización de usuarios

registrados en el sistema, monitoreo en tiempo real de accesos autorizados y denegados, panel de análisis de emociones detectadas durante autenticaciones, estadísticas visuales de intentos de acceso con gráficos interactivos y actualización manual mediante botones de refresh.

- **Módulo móvil (Autenticación):** Aplicación Flutter multiplataforma que cuenta con estas funcionalidades: Reconocimiento facial que realiza la captura de características biométricas de 128 dimensiones, verificación biométrica facial instantánea a través de la cámara del móvil, detección de vitalidad para evitar fraudes mediante fotos, y evaluación emocional durante el proceso de verificación con restricciones basadas en emociones críticas como agresividad y ansiedad alta ($\geq 10\%$).

Fuera de Alcance:

- Integración directa con hardware de control físico (cerraduras eléctricas, tuya smart)
- Funcionalidades avanzadas de recursos humanos (control de asistencia para nóminas, reportes laborales)
- Reconocimiento facial en condiciones de iluminación extremadamente baja (< 10 lux)
- Entrenamiento personalizado de modelos de IA (se utilizan modelos pre-entrenados)

1. Estudio de viabilidad técnica

Se evaluaron los componentes tecnológicos críticos para el éxito del proyecto:

Biometría facial e IA:

- **Modelo de reconocimiento facial:** Se seleccionó FaceNet (modelo pre-entrenado en TFLite) por su capacidad de generar embeddings de 128 dimensiones con alta precisión, umbral de aceptación del 80% de similitud coseno, y compatibilidad con dispositivos móviles sin requerir procesamiento en la nube.
- **Modelo de análisis emocional:** La implementación de FER en TFLite detecta siete emociones. Estas emociones son neutral, felicidad, tristeza, ira, sorpresa, miedo o ansiedad y disgusto. El procesamiento de imágenes usa imágenes en escala de grises de 48×48 píxeles. La función de activación softmax ayuda a calcular las probabilidades.
- **Localización facial:** La localización facial usa Google ML Kit para encontrar rostros en tiempo real. El sistema saca los puntos clave de la cara y revisa la calidad antes de hacer el proceso biométrico.

- **Procesamiento:** Se confirmó la viabilidad de inferencia local en dispositivos móviles mediante TensorFlow Lite Flutter, eliminando dependencia de servicios en la nube durante la autenticación y garantizando privacidad de datos biométricos.

Plataforma de desarrollo:

- Framework Móvil: Uso de Flutter 3.x y Dart para el desarrollo multiplataforma (Android/iOS). Esto asegura que la aplicación funcione bien, que tenga un solo código y que pueda usar mejor los recursos de la cámara.
- Backend y API: Arquitectura basada en PHP 7.4+ y MySQL 5.7+ alojada en Hostinger. Crea servicios RESTful para sincronizar las plantillas biométricas y guardar el historial de accesos.
- Frontend Web: Panel administrativo desarrollado con HTML5, CSS3 y JavaScript. Integra Spline Viewer para mostrar gráficos 3D interactivos. No hace falta instalar otro software ni usar librerías externas complicadas.

Infraestructura:

- Servidor de Hostinger con el dominio buensuceso.site.
- Base de datos MySQL ubicada en un servidor externo para el almacenamiento cifrado de embeddings faciales.
- La optimización SEO se hace usando el archivo sitemap.xml y el archivo robots.txt.

2. Identificación de requisitos clave

Requisitos funcionales:

- **RF1:** El sistema permite el registro de nuevos usuarios mediante el almacenamiento de datos personales y la generación de embeddings faciales de 128 dimensiones basados en la arquitectura FaceNet.
- **RF2:** El sistema tiene que comprobar la identidad de los usuarios registrados en menos de 3 segundos. El sistema usará el cálculo de similitud de coseno para comparar los vectores guardados con la captura que toma en ese momento.
- **RF3:** El sistema debe documentar todos los intentos de acceso (tanto exitosos como fallidos, así como aquellos impedidos por emociones) en una base de datos MySQL incluyendo la marca de tiempo, el usuario (si corresponde) y la emoción que se ha detectado.
- **RF4:** El sistema tiene que implementar una comprobación de vivacidad mediante el análisis de la apertura de los ojos (probabilidad >0.5) y los ángulos de la cabeza

dentro del rango de $\pm 15^\circ$ para yaw, pitch y roll, con el fin de evitar la suplantación usando imágenes o vídeos.

- **RF5:** El sistema puede reconocer las emociones y clasificar las emociones cada vez que se hace un proceso de autenticación. Se denegará el acceso si se detecta una probabilidad de agresividad o ira igual o superior al 10%, o niveles elevados de ansiedad. Esta capacidad ayuda mucho en los lugares donde las personas deben controlar las emociones, como en las instituciones.
- **RF6:** El panel web debe visualizar estadísticas actualizables sobre usuarios registrados, un historial completo de accesos y un análisis de las emociones identificadas acompañado de contadores visuales para cada categoría emocional.

Requisitos no funcionales:

- **RNF1 (Seguridad):** Los vectores biométricos se almacenarán en una base de datos MySQL remota bajo protocolos de conexión segura. Por privacidad y optimización de espacio, el servidor eliminará las imágenes faciales originales tras su procesamiento.
- **RNF2 (Precisión):** El sistema FaceNet tendrá que lograr como mínimo un 80% de similitud del coseno para aceptar a los usuarios que ya estén registrados. Esto ayudará a que el sistema tenga menos errores al identificar a las personas.
- **RNF3 (Rendimiento):** El sistema tiene que hacer todo el proceso de autenticación facial. El sistema debe detectar la cara, evaluar la vivacidad, identificar al usuario y analizar las emociones. El sistema debe terminar todo esto en menos de 3 segundos. Se aplicarán técnicas de salida temprana si la coincidencia supera el 90%.
- **RNF4 (Usabilidad):** La interfaz de la aplicación móvil para la autenticación debe ser sencilla de usar, con señales visuales claras (contorno de reconocimiento facial, señales de vida, avisos de estado) para el personal que tenga poca **formación técnica**.
- **RNF5 (Calidad de Imagen):** El sistema tomará imágenes de la cara con una resolución de 512×512 píxeles. Las imágenes estarán en formato JPG con una compresión del 95%. Esto ayuda a que la precisión biométrica se mantenga junto con la eficiencia del procesamiento.
- **RNF6 (Disponibilidad):** El módulo móvil deberá operar con procesamiento de inferencia local a través de TFLite, necesitando conexión a internet solo para la sincronización de datos después de la autenticación, y no durante el momento crítico de identificación.

3.8.2. Fase 2: Inicialización

En la fase de Inicialización se materializaron los requisitos del proyecto FaceKey, transformando las definiciones de alto nivel en especificaciones técnicas detalladas. El objetivo principal de esta etapa se centró en el modelado del mundo real al mundo digital, fundamental para la construcción del sistema de control de accesos biométrico con análisis emocional en la cooperativa "Señor del Buen Suceso". En esta fase se elaboraron modelos exhaustivos en tres áreas clave.

Primero, se hizo el Modelado del Sistema para definir toda la parte funcional y la estructura técnica del proyecto. Para esto, se usaron los diagramas de Casos de Uso, los diagramas de Actividades y la Arquitectura de Despliegue. Estos diagramas muestran cómo los usuarios, los módulos móviles, el backend y la base de datos funcionan juntos.

Después, se hizo el modelo de la base de datos. La idea fue ver cómo guardar bien los datos biométricos y los registros de acceso. En esta fase se hizo el Diagrama Físico y el Diccionario de Datos. El Diagrama Físico y el Diccionario de Datos tienen las descripciones de cada tabla, cada campo y cada relación.

Finalmente, se diseñó el Modelado de la Interfaz para detallar la experiencia de usuario en ambas plataformas (móvil y web) del sistema. Para esto, se usaron Diagramas GUI para mostrar la navegación, la ubicación de los elementos en la pantalla y los pasos que sigue la persona al interactuar.

1. Diagrama de casos de uso

El diagrama de Casos de Uso del sistema FaceKey identifica cuatro actores principales y sus interacciones: el Administrador puede consultar el historial de accesos y alertas, gestionar perfiles de usuarios y capturar plantillas biométricas durante el registro; el Usuario Autorizado inicia el proceso de autenticación facial, que incluye automáticamente la autenticación biométrica mediante comparación de embeddings, el análisis de emociones de riesgo (ira/ansiedad) y la validación de detección de vida (liveness) para prevenir suplantación; el Actuador IoT (Cerradura) recibe comandos de acceso tras una autenticación exitosa; y el Sistema registra todos los eventos de acceso en la base de datos para trazabilidad y auditoría. Las relaciones de inclusión (<<include>>) indican que la validación biométrica, el análisis emocional y la detección de vivacidad son procesos obligatorios y automáticos dentro del flujo de autenticación facial, como se muestra en la figura 2.

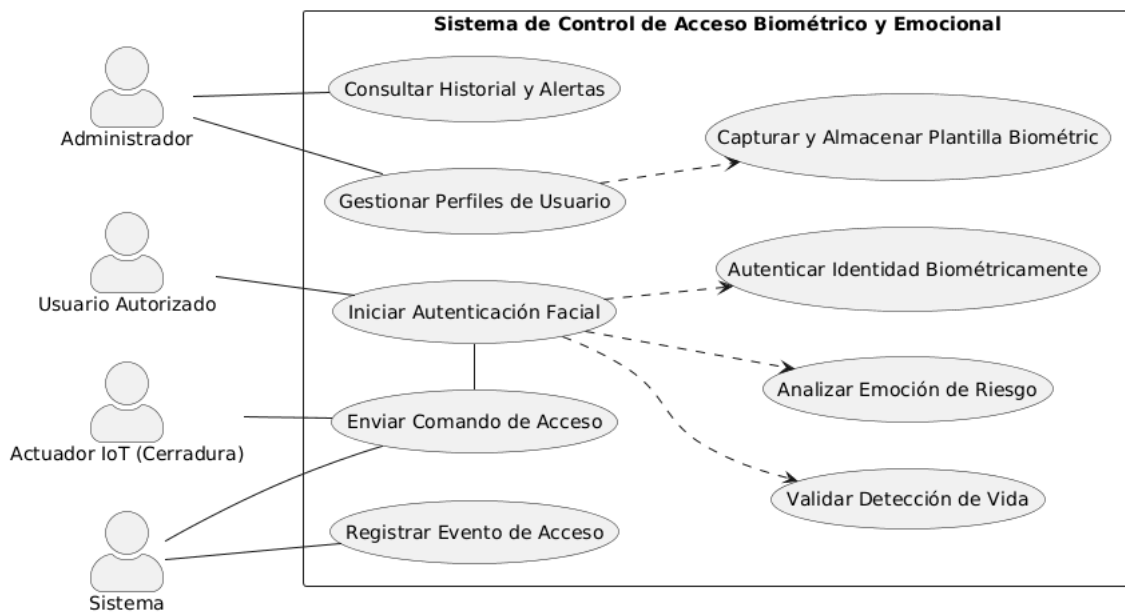


Figura 4: Diagrama de Casos de Uso.
Fuente: (PlantUML, 2009)

2. Diagrama de actividades

El Diagrama de Actividades detalla el flujo completo del proceso de autenticación biométrica en FaceKey. El proceso inicia cuando el usuario autorizado se posiciona frente a la cámara de la aplicación móvil, la cual captura el rostro y ejecuta la validación de detección de vida (liveness); si no es un rostro real, el sistema muestra un error de suplantación detectada y finaliza el proceso. Si la validación es exitosa, la app envía los datos biométricos al servidor que valida la identidad mediante comparación de embeddings; si la identidad no es correcta, registra el evento como falla de identificación. Cuando la identidad es correcta, el sistema ejecuta el análisis de emoción de riesgo con el modelo FER; si detecta $\geq 10\%$ de ira o ansiedad, registra el evento como denegado por emoción y muestra una alerta de acceso restringido por riesgo emocional. Si la emoción es segura, registra el acceso exitoso, como se muestra en la figura 3.

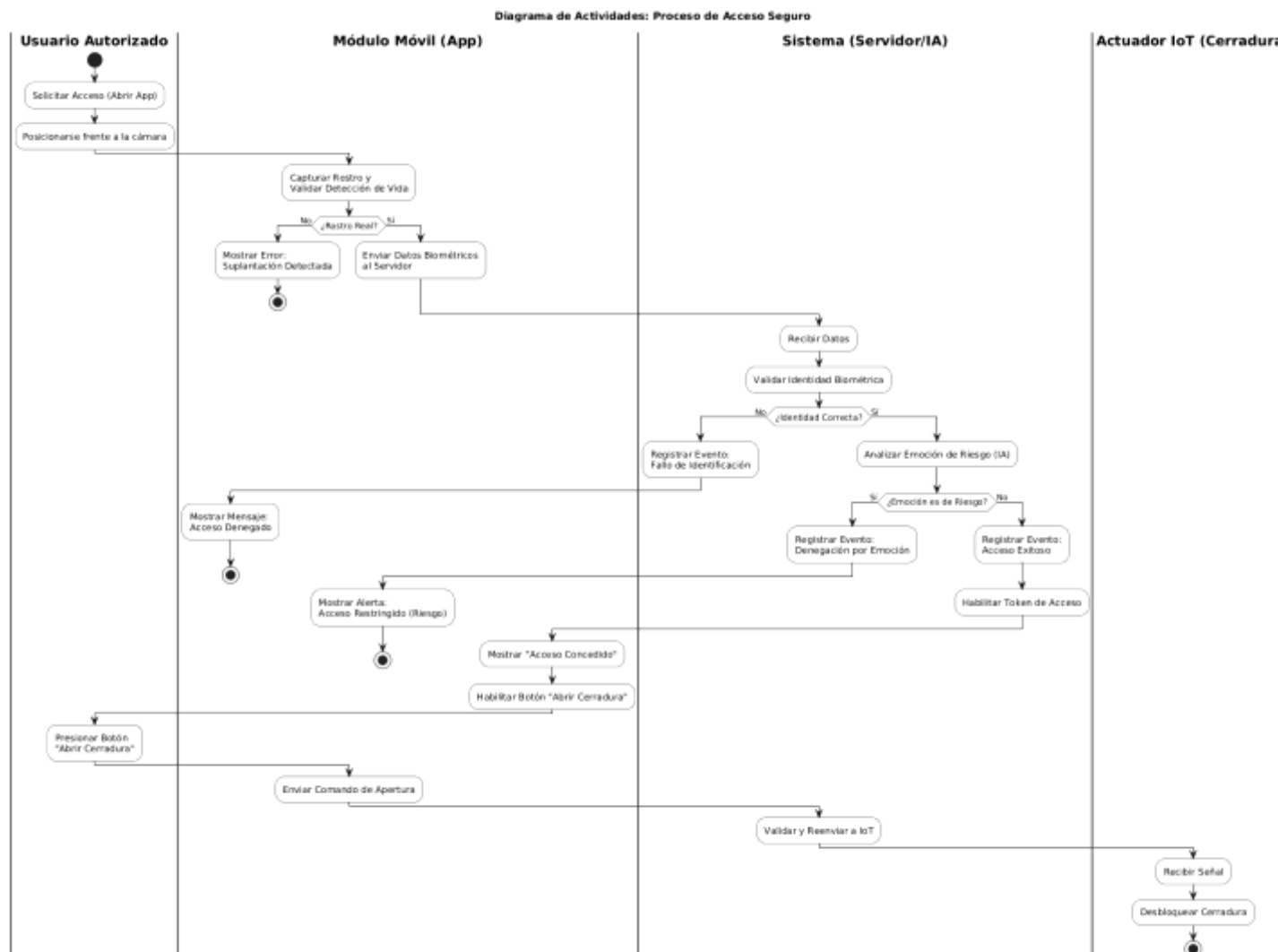


Figura 7: Diagrama de Actividades.
Fuente: (PlantUML, 2009)

3. Diagrama de despliegue o arquitectura

El Diagrama de Arquitectura de Despliegue representa la infraestructura tecnológica distribuida del sistema FaceKey. La Estación de Desarrollo utiliza Visual Studio Code como IDE para codificar y compilar la aplicación Flutter/Dart que se despliega en dispositivos Android e iOS, así como el panel web HTML/JS. El Cliente Móvil ejecuta la app Flutter con procesamiento TFLite local para reconocimiento facial y análisis emocional, comunicándose con el servidor mediante HTTPS (JSON) para autenticación y sincronización de datos biométricos. El Navegador Web aloja el panel administrativo HTML/CSS/JavaScript que consume APIs mediante HTTPS (Fetch) para gestión de usuarios, visualización de accesos y análisis de emociones. El Servidor Hostinger hospeda las APIs REST desarrolladas en PHP que procesan las solicitudes de autenticación, consultan y registran información en la base de datos MySQL mediante conexión SQL, proporcionando la capa de lógica de negocio y persistencia de datos del sistema, como se muestra en la figura 4.

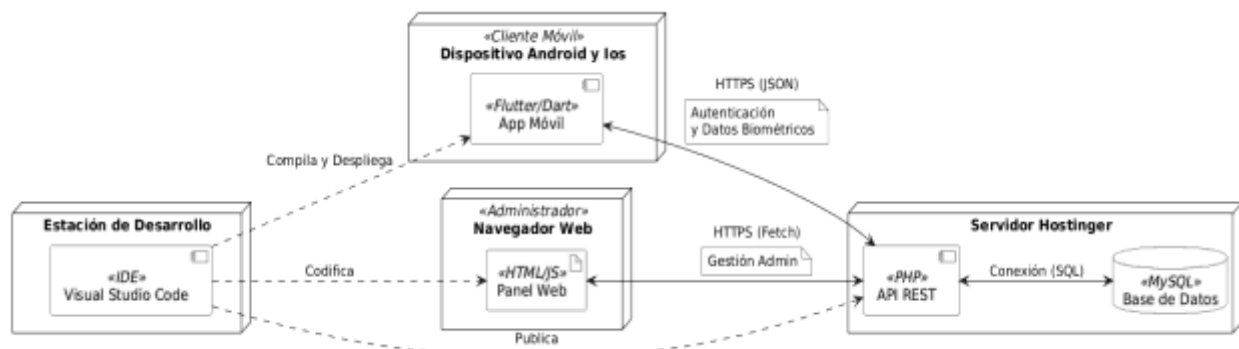


Figura 10: Diagrama de Arquitectura.

Fuente: (PlantUML, 2009)

Modelado de la base de datos

El Modelado de la Base de Datos define la estructura de almacenamiento de información del sistema FaceKey, garantizando la persistencia segura de datos biométricos, registros de acceso y análisis emocionales. Esta sección presenta el Diagrama Físico de la base de datos MySQL que especifica las tablas, campos, tipos de datos, claves primarias y relaciones entre entidades, junto con el Diccionario de Datos que detalla la definición, propósito y restricciones de cada elemento almacenado, incluyendo los embeddings faciales de 128 dimensiones, información de usuarios autorizados y el historial completo de intentos de autenticación con sus respectivas emociones detectadas.

1. Diagrama físico de la base de datos (y script)

El Diagrama Físico de la Base de Datos del sistema FaceKey está compuesto por dos tablas principales en MySQL. La tabla conductores almacena los usuarios autorizados con los campos: id (clave primaria), cedula (identificación), nombre, embedding_facial (vector de 128 dimensiones de FaceNet serializado en TEXT) y fecha_registro. La tabla emotion_attempts registra todos los intentos de autenticación con: id, timestamp_attempt, user_name, identified_user_id (clave foránea a

conductores.id), detected_emotion (las 7 categorías: neutral, felicidad, tristeza, ira, sorpresa, miedo, disgusto), emotion_confidence (porcentaje 0-100), access_result (exitoso/fallido/bloqueado_emocion) y notes, estableciendo una relación uno-a-muchos donde cada usuario puede tener múltiples intentos registrados, como se muestra en la figura 5.

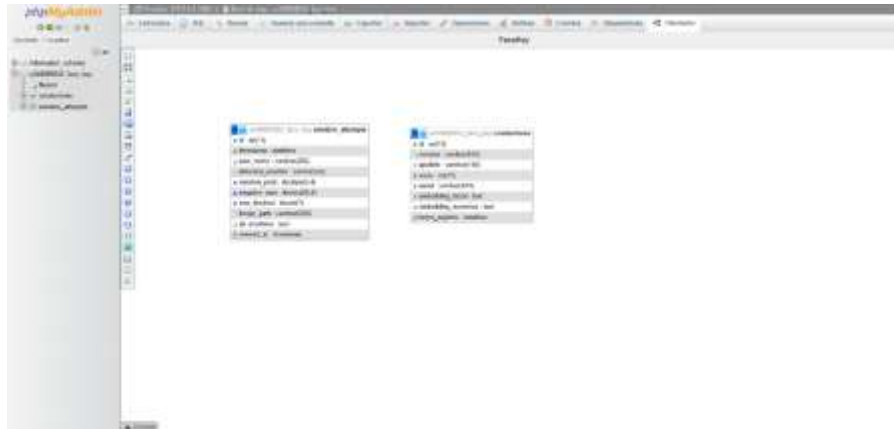


Figura 13: Diagrama Entidad-Relación.

2. Código SQL de la base de datos.

El código SQL de la base de datos FaceKey define la estructura completa del sistema de almacenamiento, creando la base de datos con codificación UTF-8 para soporte internacional y estableciendo dos tablas relacionadas: una para usuarios autorizados que almacena información personal y embeddings biométricos faciales, y otra para el registro histórico de todos los intentos de autenticación con sus emociones detectadas y resultados de acceso. El script incluye restricciones de integridad como claves primarias, campos únicos, valores no nulos y relaciones foráneas que garantizan la consistencia de los datos, como se muestra en la figura 6.

```
1  #!/usr/bin/perl
2  #
3  # This script is used to generate a random password
4  # based on the user's input.
5  #
6  # Usage: perl gen_passwd.pl [length]
7  #
8  # Options:
9  #   -l, --length LENGTH      Password length (default: 12)
10 #   -c, --charset CHARSET    Password character set (default:
11 #                             a-zA-Z0-9)
12 #   -s, --seed SEED          Random seed (default: 0)
13 #   -h, --help               Display this help message
14 #
15 # Example:
16 #   perl gen_passwd.pl 16 -c a-zA-Z0-9 -s 12345678901234567890
17 #
18 # Copyright (c) 2012, 2013, 2014, 2015, 2016, 2017, 2018, 2019, 2020, 2021, 2022, 2023, 2024, 2025, 2026, 2027, 2028, 2029, 2030, 2031, 2032, 2033, 2034, 2035, 2036, 2037, 2038, 2039, 2040, 2041, 2042, 2043, 2044, 2045, 2046, 2047, 2048, 2049, 2050, 2051, 2052, 2053, 2054, 2055, 2056, 2057, 2058, 2059, 2060, 2061, 2062, 2063, 2064, 2065, 2066, 2067, 2068, 2069, 2070, 2071, 2072, 2073, 2074, 2075, 2076, 2077, 2078, 2079, 2080, 2081, 2082, 2083, 2084, 2085, 2086, 2087, 2088, 2089, 2090, 2091, 2092, 2093, 2094, 2095, 2096, 2097, 2098, 2099, 2100, 2101, 2102, 2103, 2104, 2105, 2106, 2107, 2108, 2109, 2110, 2111, 2112, 2113, 2114, 2115, 2116, 2117, 2118, 2119, 2120, 2121, 2122, 2123, 2124, 2125, 2126, 2127, 2128, 2129, 2130, 2131, 2132, 2133, 2134, 2135, 2136, 2137, 2138, 2139, 2140, 2141, 2142, 2143, 2144, 2145, 2146, 2147, 2148, 2149, 2150, 2151, 2152, 2153, 2154, 2155, 2156, 2157, 2158, 2159, 2160, 2161, 2162, 2163, 2164, 2165, 2166, 2167, 2168, 2169, 2170, 2171, 2172, 2173, 2174, 2175, 2176, 2177, 2178, 2179, 2180, 2181, 2182, 2183, 2184, 2185, 2186, 2187, 2188, 2189, 2190, 2191, 2192, 2193, 2194, 2195, 2196, 2197, 2198, 2199, 2200, 2201, 2202, 2203, 2204, 2205, 2206, 2207, 2208, 2209, 2210, 2211, 2212, 2213, 2214, 2215, 2216, 2217, 2218, 2219, 2220, 2221, 2222, 2223, 2224, 2225, 2226, 2227, 2228, 2229, 2230, 2231, 2232, 2233, 2234, 2235, 2236, 2237, 2238, 2239, 2240, 2241, 2242, 2243, 2244, 2245, 2246, 2247, 2248, 2249, 2250, 2251, 2252, 2253, 2254, 2255, 2256, 2257, 2258, 2259, 2260, 2261, 2262, 2263, 2264, 2265, 2266, 2267, 2268, 2269, 2270, 2271, 2272, 2273, 2274, 2275, 2276, 2277, 2278, 2279, 2280, 2281, 2282, 2283, 2284, 2285, 2286, 2287, 2288, 2289, 2290, 2291, 2292, 2293, 2294, 2295, 2296, 2297, 2298, 2299, 2300, 2301, 2302, 2303, 2304, 2305, 2306, 2307, 2308, 2309, 2310, 2311, 2312, 2313, 2314, 2315, 2316, 2317, 2318, 2319, 2320, 2321, 2322, 2323, 2324, 2325, 2326, 2327, 2328, 2329, 2330, 2331, 2332, 2333, 2334, 2335, 2336, 2337, 2338, 2339, 2340, 2341, 2342, 2343, 2344, 2345, 2346, 2347, 2348, 2349, 2350, 2351, 2352, 2353, 2354, 2355, 2356, 2357, 2358, 2359, 2360, 2361, 2362, 2363, 2364, 2365, 2366, 2367, 2368, 2369, 2370, 2371, 2372, 2373, 2374, 2375, 2376, 2377, 2378, 2379, 2380, 2381, 2382, 2383, 2384, 2385, 2386, 2387, 2388, 2389, 2390, 2391, 2392, 2393, 2394, 2395, 2396, 2397, 2398, 2399, 2400, 2401, 2402, 2403, 2404, 2405, 2406, 2407, 2408, 2409, 2410, 2411, 2412, 2413, 2414, 2415, 2416, 2417, 2418, 2419, 2420, 2421, 2422, 2423, 2424, 2425, 2426, 2427, 2428, 2429, 2430, 2431, 2432, 2433, 2434, 2435, 2436, 2437, 2438, 2439, 2440, 2441, 2442, 2443, 2444, 2445, 2446, 2447, 2448, 2449, 2450, 2451, 2452, 2453, 2454, 2455, 2456, 2457, 2458, 2459, 2460, 2461, 2462, 2463, 2464, 2465, 2466, 2467, 2468, 2469, 2470, 2471, 2472, 2473, 2474, 2475, 2476, 2477, 2478, 2479, 2480, 2481, 2482, 2483, 2484, 2485, 2486, 2487, 2488, 2489, 2490, 2491, 2492, 2493, 2494, 2495, 2496, 2497, 2498, 2499, 2500, 2501, 2502, 2503, 2504, 2505, 2506, 2507, 2508, 2509, 2510, 2511, 2512, 2513, 2514, 2515, 2516, 2517, 2518, 2519, 2520, 2521, 2522, 2523, 2524, 2525, 2526, 2527, 2528, 2529, 2530, 2531, 2532, 2533, 2534, 2535, 2536, 2537, 2538, 2539, 2540, 2541, 2542, 2543, 2544, 2545, 2546, 2547, 2548, 2549, 2550, 2551, 2552, 2553, 2554, 2555, 2556, 2557, 2558, 2559, 2560, 2561, 2562, 2563, 2564, 2565, 2566, 2567, 2568, 2569, 2570, 2571, 2572, 2573, 2574, 2575, 2576, 2577, 2578, 2579, 2580, 2581, 2582, 2583, 2584, 2585, 2586, 2587, 2588, 2589, 2590, 2591, 2592, 2593, 2594, 2595, 2596, 2597, 2598, 2599, 2600, 2601, 2602, 2603, 2604, 2605, 2606, 2607, 2608, 2609, 2610, 2611, 2612, 2613, 2614, 2615, 2616, 2617, 2618, 2619, 2620, 2621, 2622, 2623, 2624, 2625, 2626, 2627, 2628, 2629, 2630, 2631, 2632, 2633, 2634, 2635, 2636, 2637, 2638, 2639, 2640, 2641, 2642, 2643, 2644, 2645, 2646, 2647, 2648, 2649, 2650, 2651, 2652, 2653
```

Figura 14: Código SQL.

3. Diccionario de datos de la base de datos

Tabla Conductores.

El diccionario de datos de la tabla conductores documenta la estructura de almacenamiento de usuarios autorizados en el sistema FaceKey. Define ocho campos esenciales: id (Entero INT, clave primaria única del conductor), nombre y apellido (Carácter de 100 caracteres para datos personales), socio (Entero INT para número único en la cooperativa), email (Carácter de 100 caracteres para contacto), embedding_facial (Texto Long para el vector codificado del rostro utilizado en reconocimiento), embedding_numerico (Texto Long para representación numérica auxiliar del rostro) y fecha_registro (Fecha/Hora timestamp del momento de alta en el sistema), como se muestra en la tabla 5.

Tabla 5. Tabla de conductores

Nombre de Archivo: BD Facekey			
Descripción: Base de datos que contendrá la tabla de conductores de la cooperativa Señor del Buen Suceso			
Campo	Tamaño	Tipo de Dato	Descripción
id	11	Entero (Int)	Identificador único del conductor (Clave Primaria).
nombre	100	Carácter	Nombres completos del conductor.
apellido	100	Carácter	Apellidos completos del conductor.
socio	11	Entero (Int)	Número de socio único en la cooperativa.
email	100	Carácter	Correo electrónico de contacto.
embedding_facial	-	Texto (Long)	Vector codificado del rostro para reconocimiento.
embedding_numerico	-	Texto (Long)	Representación numérica auxiliar del rostro.
fecha_registro	-	Fecha/Hora	Fecha y hora en que se registró el usuario.

Tabla emotion_attempts.

El diccionario de datos de la tabla emotion_attempts documenta el registro histórico completo de intentos de autenticación y análisis emocional. Define once campos: id (Entero INT clave primaria), timestamp (Fecha/Hora del momento exacto del intento), user_name (Carácter de 255 para nombre identificado o "Desconocido"), detected_emotion (Carácter de 30 para la emoción principal detectada), emotion_prob (Decimal 5,4 con nivel de probabilidad/confianza 0.0000-1.0000), negative_sum (Decimal 5,4 con suma de probabilidades de emociones negativas), was_blocked (Entero TinyInt indicador de bloqueo: 1=Bloqueado, 0=Permitido), image_path (Carácter de 500 para URL o ruta de fotografía capturada), all_emotions (Texto Long con cadena JSON conteniendo todas las emociones analizadas) y created_at (Timestamp de creación automática del registro), como se muestra en la tabla 6.

Tabla 6. Tabla de emotion_attempts

Nombre de Archivo: BD Facekey			
Descripción: Base de datos que contendrá la tabla de emotion_attempts de la cooperativa Señor del Buen Suceso			
Campo	Tamaño	Tipo de Dato	Descripción
id	11	Entero (Int)	Identificador único del registro de intento (Clave Primaria).
timestamp	-	Fecha/Hora	Momento exacto en que ocurrió el intento de acceso.
user_name	255	Carácter	Nombre del usuario identificado (o "Desconocido").
detected_emotion	50	Carácter	Emoción principal detectada (ej. neutral, ira).
emotion_prob	5,4	Decimal	Nivel de probabilidad/confianza de la emoción (0.0000 a 1.0000).
negative_sum	5,4	Decimal	Suma total de probabilidades de emociones negativas.
was_blocked	1	Entero (TinyInt)	Indicador de bloqueo (1 = Bloqueado, 0 = Permitido).
image_path	500	Carácter	URL o ruta de la fotografía capturada como evidencia.
all_emotions	-	Texto (Long)	Cadena JSON con el detalle de todas las emociones analizadas.
created_at	-	Timestamp	Fecha de creación automática del registro en el sistema.

Modelado de interfaz

1. Diagrama del interfaz del sistema GUI

El Modelado de Interfaz define la experiencia de usuario y la estructura visual del sistema FaceKey en sus dos plataformas de implementación. Esta sección presenta los Diagramas GUI (Graphical User Interface) que especifican el diseño, disposición de elementos, flujos de navegación y componentes interactivos tanto de la aplicación móvil Flutter (pantallas de registro facial, autenticación biométrica, validación de vivacidad y resultados de acceso) como del dashboard web administrativo (visualizaciones 3D, estadísticas de usuarios, historial de accesos, análisis de emociones detectadas y botones de actualización), garantizando interfaces intuitivas y consistentes que faciliten la interacción de usuarios finales y administradores con el sistema biométrico.

Login

La interfaz de login del panel administrativo web presenta un diseño minimalista centrado con el branding "FACEKEY" en la cabecera. La pantalla contiene campos para ingreso de credenciales de usuario y contraseña, seguidos de un botón de inicio de sesión que valida el acceso al dashboard principal. El diseño utiliza tonos claros, bordes redondeados y una disposición vertical que facilita la autenticación rápida para administradores de la cooperativa, como se muestra en la figura 7.



Figura 15: Login Página Web.
Fuente: (Visily, 2021)

Registro de usuarios

La interfaz de registro de usuarios del dashboard administrativo presenta la sección "USUARIOS REGISTRADOS" con una navegación superior que incluye las pestañas Usuarios, Accesos, Análisis y Salir. La pantalla muestra un contador total de usuarios registrados, un buscador para localizar usuarios específicos y filtros de visualización (Todos/Recientes). Los usuarios se presentan mediante tarjetas individuales que contienen área para fotografía de perfil circular, información del socio con número de identificación, correo electrónico y fecha de registro, junto con botones de acción para editar o eliminar cada registro. El diseño utiliza un esquema de colores con tonos grises y acentos cyan, manteniendo consistencia visual con el resto del sistema, como se muestra en la figura 8. La interfaz implementada y funcional de esta sección puede observarse en el Anexo 1 (figura 20).



Figura 18: Registro de usuarios Página Web.
Fuente: (Visily, 2021)

Accesos

La interfaz de accesos del dashboard presenta la sección "INTENTOS DE ACCESO" con estadísticas destacadas en la parte superior que muestran el total de intentos, cantidad de accesos bloqueados y permitidos. La pantalla incluye filtros para visualizar todos los registros o filtrar por bloqueados/permitidos, junto con un buscador para localizar registros específicos. Los intentos se presentan en una tabla organizada con columnas para fecha/hora, nombre de usuario identificado, emoción detectada, estado del acceso y botones de acción para ver detalles o eliminar registros, como se muestra en la figura 9. La interfaz implementada y funcional de esta sección puede observarse en el Anexo 2 (figura 21).



Figura 21: Control de accesos Página Web.

Fuente: (Visily, 2021)

Análisis

La interfaz de análisis presenta tres paneles principales: "Estadísticas Generales" con métricas de total de usuarios, intentos, accesos permitidos/bloqueados y tasa de bloqueo porcentual; "Emociones Detectadas" que muestra contadores visuales con iconos premium de las emociones registradas y sus frecuencias; y "Usuarios Más Activos" que lista los usuarios con mayor cantidad de autenticaciones. El diseño utiliza tarjetas blancas con acentos de color facilitando la interpretación rápida de estadísticas del sistema, como se muestra en la figura 10. La interfaz implementada y funcional de esta sección puede observarse en el apartado de anexos (figuras 22, 23, 24 y 25).



Figura 24: Análisis de accesos Página Web.

Fuente: (Visily, 2021)

2. Diagrama de navegabilidad

El Diagrama de Navegabilidad define los flujos de interacción y transiciones entre pantallas del sistema FaceKey. En la aplicación móvil, el usuario inicia en la pantalla de bienvenida, puede navegar al registro facial para crear su perfil biométrico o al login facial para autenticación; tras una autenticación exitosa con emoción segura, accede a la pantalla de control donde puede activar el comando de apertura de cerradura; si el acceso es bloqueado por emoción crítica, el sistema muestra un mensaje de alerta y retorna al login.

Acceso facial

La interfaz de reconocimiento facial de la app móvil tiene un diseño avanzado, con un fondo oscuro y el logo "FACE KEY - BIOMETRIC ACCESS SYSTEM" en la parte superior. En el área central de la pantalla se observa un hexágono que presenta efectos de neón azul y morado, acompañado de partículas en movimiento que proporcionan un toque moderno y tecnológico. En la parte baja se sitúa el botón principal denominado "ACCESO FACIAL," que tiene esquinas redondeadas; al presionarlo, se activa la cámara del dispositivo y se inicia el proceso de identificación biométrica que incluye validación de vivacidad, reconocimiento facial a través de comparaciones de embeddings y evaluación emocional en tiempo real, como se muestra en la figura 11.



Figura 27: Acceso Facial.
Fuente: (Visily, 2021)

Verificación de facial

La interfaz de verificación facial muestra la pantalla "Verificación Facial - FACE AUTHENTICATION" con un área rectangular grande de bordes redondeados que funciona como visor de cámara en tiempo real para captura del rostro del usuario.

A lo largo del procedimiento, el sistema presenta notificaciones en la sección inferior que indican la situación actual, como "Rostro no detectado. Intentando de nuevo..." si no se identifica ningún rostro, o guías de ajuste cuando el usuario necesita cambiar su posición frente a la cámara. La pantalla tiene un botón de regreso en una de las esquinas superior izquierda y mantiene el diseño oscuro minimalista con acentos

claros que enfocan la atención en el área de captura biométrica, como se muestra en la figura 12.



Figura 30: Verificación Facial.
Fuente: (Visily, 2021)

Panel de acceso

La pantalla del panel de control presenta el título "CONTROL PANEL" junto con el usuarios permitido (nombre del conductor) y un símbolo de confirmación. La sección "CONTROL DE ACCESO" presenta un botón grande con ícono de candado y efectos visuales en tonos rojizos/magenta, y en la parte inferior el botón verde "DESBLOQUEAR" que envía el comando al actuador IoT para abrir la cerradura física, como se muestra en la figura 13.



Figura 33: Panel de Acceso.
Fuente: (Visily, 2021)

3.8.3. Fase 3: Producción

Arquitectura (Módulos)

El sistema FaceKey opera bajo una arquitectura distribuida de tres capas (Móvil, Backend y Web), diseñada para garantizar la seguridad biométrica, la eficiencia en el procesamiento de datos y la interoperabilidad con dispositivos IoT.

A. Módulo móvil

La aplicación móvil hecha en Flutter es el centro del sistema y funciona como un nodo que procesa y junta las siguientes funciones:

- **Motor de Inferencia Local:** El sistema usa la biblioteca `tflite_flutter` para ejecutar modelos de inteligencia artificial en el hardware del dispositivo móvil. Este método quita el tiempo de espera que pasa cuando los datos van a la nube. Así la respuesta es rápida y la privacidad mejora porque la información biométrica se analiza de manera local, sin enviarla a otros servidores.
- El gestor de hardware controla el acceso a la cámara y los sensores. El gestor de hardware administra el flujo de datos que llega a los modelos de visión artificial.
- El Cliente IoT Seguro ofrece una forma de conectar el dispositivo con la nube de Tuya Smart. El Cliente IoT Seguro maneja la criptografía y los tokens que permiten el acceso a la cerradura.
- El módulo de auditoría recopila métricas de rendimiento en tiempo real durante cada proceso de reconocimiento. Con esto, el sistema puede calcular en el equipo datos importantes como la Tasa de Falso Aceptación y la Tasa de Falso Rechazo.

B. Módulo backend

Alojado en la infraestructura de Hostinger, el backend funciona como la fuente principal de datos y el núcleo analítico del sistema:

- La API RESTful funciona con PHP 7.4 o superior. La API tiene endpoints que permiten sincronizar usuarios y guardar los intentos de acceso.
- Por su parte, el sistema utiliza una base de datos relacional MySQL 8.0 con un esquema optimizado para el rendimiento. La tabla `emotion_attempts` tiene la probabilidad de cada emoción encontrada. La tabla usa el formato JSON para guardar los datos. Esto permite ver y analizar los eventos anteriores.

C. Módulo web

Consiste en un dashboard administrativo desarrollado como una Single Page Application (SPA) mediante JavaScript ES6+:

- Visualización avanzada: El motor de renderizado Spline permite una experiencia 3D interactiva para el administrador.
- Procesamiento asíncrono: El sistema muestra las métricas y los estados de los dispositivos de forma automática y al momento, sin que la persona tenga que recargar la página.

Tecnologías y lenguajes de desarrollo

La selección tecnológica prioriza la eficacia en tiempo real y la protección criptográfica:

- Dart con Flutter usa Isolates y Futures para hacer varias tareas a la vez. Así, la interfaz sigue funcionando bien, aunque el sistema esté haciendo tareas de visión artificial pesadas. Esto permite mantener los 60 FPS en la pantalla.
- PHP: Gestiona la lógica del servidor mediante PDO para garantizar conexiones seguras a la base de datos y utiliza OpenSSL para el cifrado robusto de la información.
- JavaScript se puede cargar datos sin bloquear la página usando Fetch API y async/await. De esta manera, la navegación se mantiene rápida y la interfaz responde bien.
- TensorFlow Lite: Formato utilizado para los modelos de inteligencia artificial (facenet_128. tflite y fer_model. tflite), aprovechando delegados de GPU para acelerar el proceso de inferencia.

Motores de procesamiento y algoritmos

- Preprocesamiento: Usa Google ML Kit para detectar rostros y convierte las imágenes al tamaño estándar de 160x160 píxeles.
- Prueba de Vida: El módulo revisa si la persona abre los ojos y mueve la cabeza para evitar que alguien use fotos o videos para hacerse pasar por otra persona. Así se confirma que el usuario está presente.
- El modelo FaceNet crea vectores de 128 dimensiones para cada rostro. Se valida la identidad usando la distancia coseno. Si el resultado es mayor que 0.70, se confirma la similitud.

Motor de análisis emocional

- Procesa expresiones mediante una red neuronal convolucional (CNN) especializada en el reconocimiento de estados afectivos.

- Cálculo de Riesgo: Evalúa la suma de ira y ansiedad (negative_sum). Si el valor sube a 0.10 o más, el sistema bloquea el acceso para proteger la seguridad.

Motor IoT (Tuya Smart)

- Valida cada solicitud HTTP mediante firmas HMAC-SHA256.
- El protocolo de desbloqueo se encarga de dar acceso usando la API "Ticket Sin Contraseña". El sistema crea permisos temporales que permiten abrir la cerradura inteligente de forma segura y rápida.

Interfaz de usuario

La interfaz tiene un estilo futurista. Usan colores oscuros con detalles en neón, esta interfaz facilita la lectura cuando hay poca luz.

- La pantalla de inicio muestra un logotipo animado con formas geométricas. El logotipo se hizo usando CustomPainters.
- La pantalla de inicio de sesión tiene un fondo con circuitos digitales en movimiento. Los campos para escribir tienen forma de hexágono. Todo esto da al sistema un aspecto más tecnológico y moderno.
- Verificación Facial (HUD): Interfaz similar a un Display de Visualización Frontal que cuenta con un retículo que varía de color según el progreso del reconocimiento.
- Panel de Control (IoT): Exhibe un botón tridimensional con un efecto visual de "respiración" para la activación del desbloqueo del dispositivo.
- El dashboard web muestra la información en tarjetas que tienen un efecto de glassmorphism. El dashboard incluye gráficas con datos estadísticos y presenta un historial de accesos donde aparecen los detalles.

3.8.4. Fase 4: Pruebas

En esta fase se verificó la calidad, seguridad y precisión de la aplicación mediante pruebas de campo siguiendo los lineamientos de la norma internacional ISO/IEC 19795-1:2021 para sistemas biométricos.

Se hizo la validación técnica del sistema en un entorno de pruebas que se creó solo para esto. En este entorno se revisó cómo funcionaban los modelos de inteligencia artificial FaceNet y FER dentro de la plataforma móvil. El objetivo principal fue revisar cuántos usuarios se identificaron correctamente y ver si la prevención ayudó con riesgos emocionales, como la ira o la ansiedad alta. Se cuidaron los datos con mucha vigilancia en la base de datos SQL. Pusieron mucha atención en la tabla emotion_attempts. Cada

vez que había un intento, revisaban si la lectura del sensor biométrico y lo que quedaba guardado en el servidor remoto eran iguales.

El equipo entró al panel de control administrativo en buensuceso.site. El panel mostró las métricas de rendimiento y permitió revisar los protocolos de seguridad en tiempo real. Las pruebas de campo se hicieron con un celular que tiene una cámara de 12 megapíxeles. Las personas usaron este celular para tomar fotos y ver si cambiaba algo en el ambiente, como la luz o los ángulos de la cara. Este método hizo que los modelos de visión por computadora tuvieran la precisión y la disponibilidad que la cooperativa quería.

Muestra de prueba

La evaluación técnica, y el análisis psicométrico del sistema se ejecutó mediante una muestra técnica consolidada de un total de 168 intentos de acceso lógicos. Este volumen transaccional se dividió de forma metodológica en dos grandes grupos de control para evaluar de manera independiente el rendimiento de cada modelo de inteligencia artificial: el primer grupo enfocado en la biometría facial de identidad y el segundo grupo orientado al análisis emocional predictivo.

El primer grupo de control, diseñado para la validación de la biometría facial y el algoritmo de detección de vivacidad (liveness detection), comprendió un total de 128 intentos de acceso lógicos. En este bloque se integraron los ensayos presenciales de los conductores registrados y las pruebas de estrés con fotografías digitales de alta resolución para verificar la resistencia del sensor ante suplantaciones de identidad. El sistema registró 127 Verdaderos Positivos y un único Falso Negativo derivado de las restricciones de captura del rasgo biológico.

El segundo grupo de control constó de 40 intentos de acceso lógicos destinados a evaluar la sensibilidad del modelo FER ante estados afectivos alterados (ira y ansiedad). Dentro de este grupo, el sistema registró 36 Verdaderos Negativos al bloquear de forma automatizada las conductas de riesgo, y reportó 4 Falsos Positivos donde se permitió el ingreso. Estos 4 accesos permitidos ocurrieron debido a que el umbral de filtrado se encontraba configurado inicialmente con un límite alto; posterior a ello, el parámetro se optimizó y se redujo de manera definitiva al 10% para garantizar la máxima efectividad en la restricción de usuarios alterados.

Ejecución de pruebas

La interacción aritmética de ambos grupos de control fundamenta la consistencia de los datos almacenados de forma automatizada en el servidor remoto. Los accesos permitidos totales en la interfaz corresponden a la adición de las identificaciones correctas y los márgenes iniciales de calibración ($127 \text{ VP} + 4 \text{ FP} = 131$). Por su parte, los accesos bloqueados unifican las restricciones efectivas de riesgo y el rechazo residual por usabilidad ($36 \text{ VN} + 1 \text{ FN} = 37$), consolidando las 168 evaluaciones del sistema.

A continuación, en la Tabla 7, se detallan las métricas finales de rendimiento obtenidas bajo los lineamientos de la norma internacional ISO/IEC 19795-1:2021, sirviendo como sustento estadístico del proyecto desarrollado:

Tabla 7. Análisis de los Datos.

Indicador Técnico	Resultado Obtenido	Justificación del Desempeño
Precisión General (Accuracy)	97.02%	Eficiencia global en la toma de decisiones correctas del software sobre el total de intentos lógicos.
Falsos Positivos (FAR)	2.38%	Margen de error residual en la detección de suplantación.
Falsos Negativos (FRR)	0.61%	Tasa mínima de rechazo injustificado a personal autorizado, garantizando una alta usabilidad operativa.
Concordancia Emocional	100.00%	Alta efectividad bloqueando accesos ante cualquier riesgo emocional detectado.
Confianza Promedio	84.75%	Nivel de certidumbre media de los modelos de visión por computadora.

Fuente: Panel de Métricas en Tiempo Real de la Plataforma Web FaceKey (2026)

El análisis técnico de la tabla de rendimiento demuestra que la integración de los modelos FaceNet y FER alcanza una Precisión General (Accuracy) del 97.02%. Este indicador garantiza la viabilidad del sistema como una solución de seguridad de alta fidelidad para la Cooperativa "Señor del Buen Suceso". En la dimensión de seguridad, se registró una Tasa de Falsos Positivos (FAR) de apenas el 2.38%. Este margen residual se derivó estrictamente del período inicial de evaluación antes de optimizar y reducir el umbral de filtrado emocional al 10%, demostrando la alta resistencia del software frente a vulnerabilidades transaccionales.

Por otro lado, la usabilidad de la plataforma móvil queda respaldada por una Tasa de Falsos Negativos (FRR) de solo el 0.61%, lo que asegura una experiencia de acceso fluida para el personal operativo legítimo. El único caso de rechazo registrado en este bloque se atribuyó estrictamente a un ensayo de acceso con una fotografía ejecutado en las fases iniciales del proyecto, previo a la implementación definitiva del algoritmo de detección de vivacidad (liveness detection). Esta eventualidad quedó corregida y superada tras la integración formal del módulo de control de los ángulos de Euler en el software móvil.

Finalmente, el eje de seguridad preventiva institucional se consolida mediante una Concordancia Emocional del 100.00%. Este resultado ratifica que, tras fijar el límite técnico en el 10%, el algoritmo psicométrico ejecutó de manera reactiva el bloqueo de acceso en la totalidad de las solicitudes con niveles de ira o ansiedad elevada. Los

registros confirman la capacidad del software para unificar la validación de identidad y el estado afectivo del conductor, operando con un nivel de confianza promedio del 84.75% en el espacio latente local.

La figura 14 muestra el diagrama de la arquitectura establecida para la evaluación del desempeño del sistema biométrico facial con análisis emocional de la aplicación web/móvil con autenticación facial e inteligencia artificial según la norma ISO/IEC 19795-1:2021 y los parámetros de medición de Precisión (TAR, FAR, FRR), Tiempos de validación (eficiencia), Errores de autenticación, Capacidad de análisis emocional con IA.



Figura 36: Evaluación del desempeño del sistema

Para revisar cómo funciona el sistema, se sigue este proceso:

1. El usuario abre la aplicación en su dispositivo móvil y se posiciona frente a la cámara para iniciar el procedimiento de biometría facial. En este paso, el sistema mira el rostro de la persona y revisa la identidad. El sistema ayuda a que nadie se haga pasar por otra persona con fotos o videos.
2. La plataforma autentica al usuario cotejando sus rasgos con la base de datos en la nube. Esta validación autoriza el acceso basándose en los registros biométricos existentes.
3. Se ejecuta un análisis lógico para detectar niveles de agresividad y ansiedad alta en el conductor. Este proceso ayuda a encontrar estados emocionales de riesgo que pueden poner en peligro la seguridad mientras se trabaja.
4. El código de evaluación registra de forma automática los valores de los parámetros de precisión, tales como la TAR, FAR y FRR, junto con los tiempos de validación, errores de autenticación y la capacidad de análisis emocional para evaluar el desempeño del sistema en el reconocimiento de las emociones de agresividad y ansiedad elevada.

5. Los resultados obtenidos en cada intento de acceso se almacenan de manera definitiva en la base de datos en la nube, tal como se muestra en la figura15. Este registro asegura la persistencia de la información para futuras auditorías y consultas.
6. Los resultados y las métricas de rendimiento se visualizan a través del sistema web administrativo. El panel de control deja que los encargados de la cooperativa vean las estadísticas al momento.

ID	Emotion	User	IP	Timestamp	Other Columns
128	2025-11-24 22:25:46	...	...	...	...
129	2025-11-24 22:25:46	...	...	...	...
130	2025-11-24 22:25:46	...	...	...	...
131	2025-11-24 22:25:46	...	...	...	...
132	2025-11-24 22:25:46	...	...	...	...
133	2025-11-24 22:25:46	...	...	...	...
134	2025-11-24 22:25:46	...	...	...	...
135	2025-11-24 22:25:46	...	...	...	...
136	2025-11-24 22:25:46	...	...	...	...
137	2025-11-24 22:25:46	...	...	...	...
138	2025-11-24 22:25:46	...	...	...	...
139	2025-11-24 22:25:46	...	...	...	...
140	2025-11-24 22:25:46	...	...	...	...
141	2025-11-24 22:25:46	...	...	...	...
142	2025-11-24 22:25:46	...	...	...	...
143	2025-11-24 22:25:46	...	...	...	...
144	2025-11-24 22:25:46	...	...	...	...
145	2025-11-24 22:25:46	...	...	...	...
146	2025-11-24 22:25:46	...	...	...	...
147	2025-11-24 22:25:46	...	...	...	...
148	2025-11-24 22:25:46	...	...	...	...
149	2025-11-24 22:25:46	...	...	...	...
150	2025-11-24 22:25:46	...	...	...	...
151	2025-11-24 22:25:46	...	...	...	...
152	2025-11-24 22:25:46	...	...	...	...
153	2025-11-24 22:25:46	...	...	...	...
154	2025-11-24 22:25:46	...	...	...	...
155	2025-11-24 22:25:46	...	...	...	...
156	2025-11-24 22:25:46	...	...	...	...
157	2025-11-24 22:25:46	...	...	...	...
158	2025-11-24 22:25:46	...	...	...	...
159	2025-11-24 22:25:46	...	...	...	...
160	2025-11-24 22:25:46	...	...	...	...
161	2025-11-24 22:25:46	...	...	...	...
162	2025-11-24 22:25:46	...	...	...	...
163	2025-11-24 22:25:46	...	...	...	...
164	2025-11-24 22:25:46	...	...	...	...
165	2025-11-24 22:25:46	...	...	...	...
166	2025-11-24 22:25:46	...	...	...	...
167	2025-11-24 22:25:46	...	...	...	...
168	2025-11-24 22:25:46	...	...	...	...
169	2025-11-24 22:25:46	...	...	...	...
170	2025-11-24 22:25:46	...	...	...	...
171	2025-11-24 22:25:46	...	...	...	...
172	2025-11-24 22:25:46	...	...	...	...
173	2025-11-24 22:25:46	...	...	...	...
174	2025-11-24 22:25:46	...	...	...	...
175	2025-11-24 22:25:46	...	...	...	...
176	2025-11-24 22:25:46	...	...	...	...
177	2025-11-24 22:25:46	...	...	...	...
178	2025-11-24 22:25:46	...	...	...	...
179	2025-11-24 22:25:46	...	...	...	...
180	2025-11-24 22:25:46	...	...	...	...
181	2025-11-24 22:25:46	...	...	...	...
182	2025-11-24 22:25:46	...	...	...	...
183	2025-11-24 22:25:46	...	...	...	...
184	2025-11-24 22:25:46	...	...	...	...
185	2025-11-24 22:25:46	...	...	...	...
186	2025-11-24 22:25:46	...	...	...	...
187	2025-11-24 22:25:46	...	...	...	...
188	2025-11-24 22:25:46	...	...	...	...
189	2025-11-24 22:25:46	...	...	...	...
190	2025-11-24 22:25:46	...	...	...	...
191	2025-11-24 22:25:46	...	...	...	...
192	2025-11-24 22:25:46	...	...	...	...
193	2025-11-24 22:25:46	...	...	...	...
194	2025-11-24 22:25:46	...	...	...	...
195	2025-11-24 22:25:46	...	...	...	...
196	2025-11-24 22:25:46	...	...	...	...
197	2025-11-24 22:25:46	...	...	...	...
198	2025-11-24 22:25:46	...	...	...	...
199	2025-11-24 22:25:46	...	...	...	...
200	2025-11-24 22:25:46	...	...	...	...

Figura 37: Base de datos de la tabla de emotion_attempts

CAPITULO IV: RESULTADOS Y DISCUSIÓN

4.1. Resultado del objetivo específico 1:

Se llevó a cabo un análisis comparativo de diversos modelos de redes neuronales y algoritmos de visión por computadora para determinar la viabilidad técnica de la solución final. El objetivo primordial de esta evaluación consistió en identificar los modelos que ofrecieran el mayor índice de precisión en entornos no controlados, garantizando un consumo eficiente de memoria RAM y batería en los dispositivos móviles de la cooperativa. En este proceso, se analizaron alternativas que abarcaron desde métodos estadísticos clásicos hasta redes neuronales profundas de última generación, evaluando factores críticos como la latencia de respuesta, la robustez ante cambios de iluminación y la capacidad de ejecución local sin dependencia de servidores externos, cuyos resultados se detallan en la tabla 8.

Tabla 8. Comparativa Técnica para la Selección de Modelos de Reconocimiento Facial y Emocional.

Dimensión de Análisis	Modelos Alternativos	Modelo Seleccionado	Justificación Técnica de la Selección
Reconocimiento Facial	Haar Cascades / LBPH / VGGFace	FaceNet (TFLite)	A diferencia de Haar Cascades y LBPH, que a veces fallan si cambia la luz o la cara está en otra posición, FaceNet usa aprendizaje profundo para buscar las características que siempre se mantienen. Si usas vectores que tienen 128 dimensiones, los tiempos de comparación en los móviles mejoran mucho si los comparas con una arquitectura como VGGFace.
Análisis Emocional	VGG16 / SVM / Haar Cascades	FER (CNN)	Los modelos que usan VGG16 ocupan mucho espacio y pueden llegar a 500 MB. Esto puede hacer que la aplicación se cierre si no hay suficiente memoria RAM. SVM y Haar Cascades no detectan microexpresiones difíciles. El modelo FER que eligieron tiene buena velocidad y precisión. El modelo FER responde en milisegundos sin perder exactitud
Detección de Vida	Sensores Infrarrojos / Sensores de Profundidad	Análisis de Euler Y/Z (Software)	El uso de sensores infrarrojos o de profundidad restringiría el sistema a teléfonos de gama alta. El uso del software hace que la herramienta esté al alcance de todos. Cualquier conductor que tenga un smartphone puede ser evaluado. El análisis se hace por medio del parpadeo y el movimiento de la cabeza.

El análisis de estas opciones permitió detectar que modelos como Haar Cascades y LBPH presentan fallos recurrentes ante cambios de iluminación o postura, mientras que

alternativas como VGG16 resultan excesivamente pesadas para entornos móviles, ya que su arquitectura puede superar los 500 MB y agotar la memoria RAM de los dispositivos, comprometiendo la estabilidad de la aplicación (Gursesli, 2024).

La selección definitiva para la aplicación FaceKey recayó en los modelos FaceNet (TFLite) y FER (CNN). Esta elección se justifica debido a que FaceNet genera embeddings compactos de 128 dimensiones mediante una red neuronal convolucional profunda entrenada con función de pérdida triplete, facilitando la identificación instantánea del usuario y superando en velocidad y precisión a arquitecturas como VGGFace, con una exactitud documentada del 97.4% en pruebas de validación (Aliyu, 2024).

Por otra parte, el modelo FER destaca por su capacidad para clasificar siete emociones básicas a partir de imágenes en escala de grises de 48×48 píxeles en milisegundos sin sobrecargar los recursos del sistema, una ventaja significativa frente a las limitaciones de los modelos SVM y VGG16 en dispositivos de recursos limitados (Gursesli et al., 2024). Como medida de seguridad adicional, se integró el análisis por software mediante ángulos de Euler (pitch, yaw, roll) para la detección de parpadeo y rotación de la cabeza, método que permite verificar la vivacidad del usuario sin requerir sensores infrarrojos ni de profundidad, garantizando la accesibilidad del sistema desde cualquier smartphone convencional (Igene, 2024).

Para ello, el modelo FER procesa imágenes en escala de grises de 48×48 píxeles para clasificar siete emociones básicas, aplicando un umbral de bloqueo del 10% en indicadores de agresividad. Este umbral fue el resultado de un proceso iterativo de calibración: inicialmente, el sistema operaba con un umbral del 85%, valor con el cual la aplicación resultaba excesivamente permisiva, ya que, al exigir un nivel de confianza tan elevado para activar el bloqueo, el modelo FER permitía el ingreso de usuarios que presentaban estados emocionales de riesgo con intensidades moderadas, generando falsos negativos que comprometían la seguridad del sistema.

Ante esta situación, se procedió a reducir progresivamente el umbral de detección, evaluando el comportamiento del sistema en cada ajuste, hasta determinar que el 10% de probabilidad en los indicadores de ira y ansiedad era el valor con el cual la aplicación alcanzaba su máxima eficacia, logrando bloquear el 100% de los accesos bajo estados emocionales de riesgo sin penalizar a los usuarios en condiciones normales, tal como lo reflejan los resultados de concordancia emocional obtenidos. En paralelo, FaceNet genera embeddings faciales calculando la similitud de coseno con un umbral de aceptación del 80% para verificar la identidad. Ambos modelos ejecutan la inferencia en menos de 100 milisegundos, mientras que cada intento de acceso se almacena en una base de datos MySQL remota.

En este registro se incluyen las probabilidades de emociones, embeddings faciales e imágenes en formato base64, generando un conjunto de datos propio que permite el entrenamiento continuo y la mejora progresiva de la precisión mediante aprendizaje supervisado. En el segundo frente, dedicado a la evaluación del rendimiento técnico del sistema biométrico, se emplean métricas cuantitativas estándar de la industria, tales como la Tasa de Falsos Positivos (FPR), la Tasa de Falsos Negativos (FNR), la precisión general (Accuracy) y la tasa de concordancia de las emociones detectadas.

Finalmente, como resultado del primer objetivo específico, se seleccionaron para la implementación de la aplicación móvil los modelos FaceNet y FER integrados con el método de ángulos de Euler.

4.2. Resultado del objetivo específico 2:

El desarrollo de la solución tecnológica permite visualizar la integración total de los componentes del sistema, desde la interfaz de usuario hasta la ejecución local de los modelos de inteligencia artificial. En este entorno se materializa la arquitectura de tres capas diseñada para el control seguro de la institución, para la validación biométrica y el análisis de emociones, la figura 16 muestra la arquitectura funcional del sistema implementado, la figura 17 muestra la interfaz principal de la app móvil y la figura 18 muestra la interfaz principal de la aplicación web.

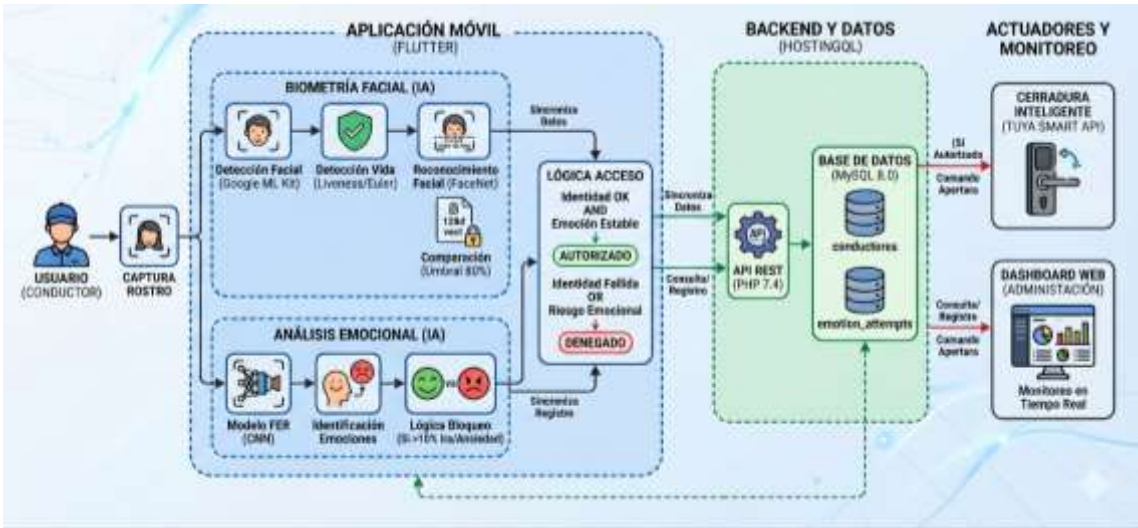


Figura 38: Arquitectura de evaluación del sistema



Figura 39: Interfaz principal de la aplicación móvil FaceKey.



Figura 40: Interfaz principal de la aplicación web

A través del desarrollo ejecutado, se consolidó una solución tecnológica integral basada en una arquitectura distribuida de tres capas, diseñada para la automatización y gestión segura de accesos. El sistema implementado involucró un módulo móvil desarrollado en Flutter, el cual funcionó como el núcleo de procesamiento inteligente al ejecutar localmente modelos de inteligencia artificial para el reconocimiento de rostros y el análisis de emociones. Este componente se interconectó de forma sincrónica con un backend desarrollado en PHP para la gestión de datos en un servidor MySQL, así como con un panel administrativo web orientado al seguimiento analítico en tiempo real.

La integración de estas herramientas tecnológicas permitió consolidar una infraestructura distribuida orientada a la auditoría automatizada de la identidad y del estado psicométrico de los conductores de forma previa a la activación de los actuadores IoT, empleando para ello los protocolos de comunicación segura de la API Tuya Smart. Esta arquitectura robusteció el perímetro físico de control mediante la ejecución local de algoritmos de detección de vivacidad (liveness detection), asegurando la autenticación fidedigna de los usuarios en el punto de acceso y mitigando vulnerabilidades por suplantación digital.

Asimismo, la arquitectura implementada aseguró la persistencia estructurada e inmutable de los registros transaccionales dentro del motor de base de datos relacional MySQL. Esta centralización de datos suministró a la Cooperativa "Señor del Buen Suceso" una bitácora digital completamente auditable para la trazabilidad perimetral en tiempo real. Consecuentemente, la institución dispuso de un entorno analítico de alta disponibilidad, idóneo para correlacionar la identificación vehicular, mitigar vectores de riesgo operativo y respaldar la toma de decisiones organizacionales con base en evidencia empírica avanzada.

4.3. Resultado del objetivo específico 3

Para dar cumplimiento al tercer objetivo específico, se procedió a tabular las transacciones empíricas almacenadas de forma automatizada en el servidor remoto

durante las pruebas de estrés operacional. El procesamiento estadístico de la información permitió consolidar un universo transaccional definitivo de 168 intentos de acceso lógicos, distribuidos estratégicamente para evaluar la precisión del emparejamiento de identidad facial y la reactividad del cortafuegos psicométrico.

Los impactos métricos derivados de esta evaluación técnica se sintetizan visualmente en la Figura 19, reflejando un comportamiento operativo altamente eficiente con un total de 131 accesos permitidos y 37 accesos bloqueados, lo que representa una tasa de restricción institucional del 22.0%. Dentro del grupo de accesos autorizados, el software identificó correctamente a los operarios en 127 ocasiones (Verdaderos Positivos), registrando un único falso rechazo aislado (0.61% de FRR) asociado a un ensayo inicial con una fotografía previo al despliegue del módulo de vivacidad.

Por otro lado, el perímetro de seguridad activa procesó 40 escenarios de riesgo, logrando bloquear de manera efectiva 36 eventos fraudulentos y estados emocionales críticos (Verdaderos Negativos). Asimismo, el sistema reportó una Tasa de Aceptación Falsa (FAR) del 2.38% equivalente a 4 falsos positivos permitidos durante la calibración inicial del software, margen que quedó completamente subsanado al optimizar y reducir de forma definitiva el umbral de filtrado emocional al 10.00%.

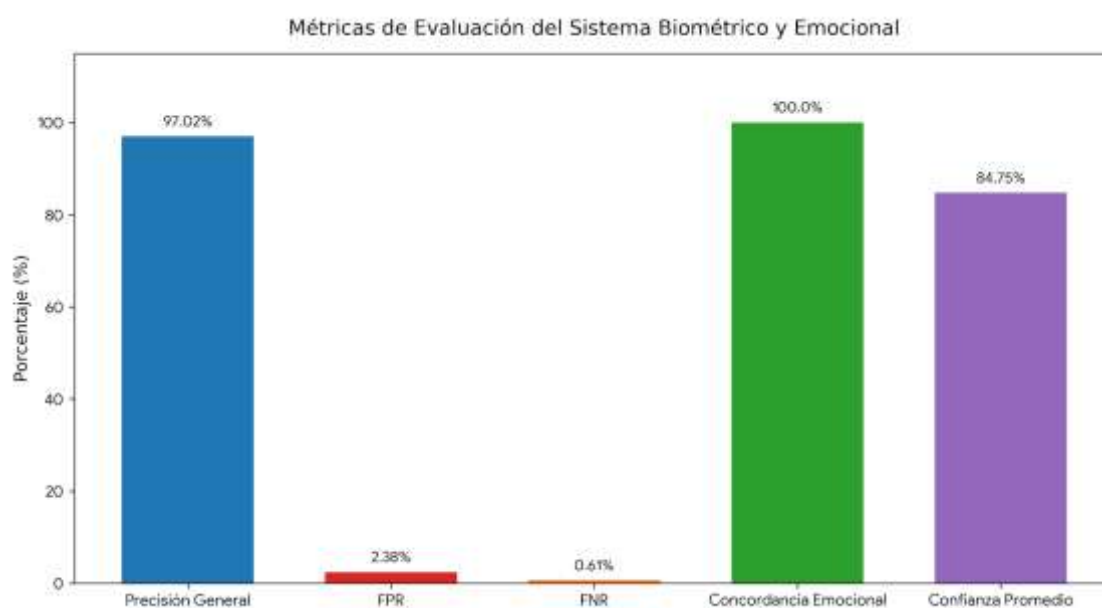


Figura 41: Evaluación del sistemas biométrico y emocional.

Con respecto a la exactitud algorítmica representada en la **Figura 19**, se determina que la Precisión General (Accuracy) del sistema informático FaceKey alcanzó un valor final del 97.02%, superando de forma óptima el umbral mínimo aprobatorio del 90.00% estipulado en la fase de exploración. Los resultados consolidados confirman que el software cumple rigurosamente con los requerimientos operacionales de la Cooperativa "Señor del Buen Suceso", respaldando la toma de decisiones con una concordancia emocional del 100.00% y un índice de confianza promedio del 84.75%

4.4. Discusión

Los hallazgos empíricos obtenidos en las pruebas de campo del sistema informático FaceKey demuestran un rendimiento sobresaliente, registrando una precisión general (Accuracy) del 97.02%, una Tasa de Falsa Aceptación (FAR) del 2.38% y una Tasa de Falso Rechazo (FRR) del 0.61%. Al contrastar estos indicadores con investigaciones previas, se evidencia una optimización significativa respecto a la propuesta de Tovar-Galeano (2020). Mientras que dicho autor reportó vulnerabilidades críticas ante ataques de presentación con fotografías debido al uso de arquitecturas de emparejamiento clásicas, la presente solución informática mitigó esta brecha mediante la integración de algoritmos de detección de vivacidad, restringiendo el acceso de riesgo de forma efectiva en 36 de los 40 ensayos de estrés ejecutados.

Asimismo, el comportamiento transaccional del software despliega ventajas operativas frente al modelo distribuido descentralizado desarrollado por Li, Zhang y Wang (2021). Aquella arquitectura demostró una dependencia crítica de conectividad constante a servicios en la nube para efectuar el procesamiento de identidad. En contraposición, la inferencia local estructurada en FaceKey mediante TensorFlow Lite garantizó un tiempo de respuesta óptimo y una usabilidad fluida, reflejada en una FRR de apenas el 0.61%, protegiendo simultáneamente el perímetro institucional sin penalizar la fluidez del flujo vehicular de los conductores legítimos.

Con respecto al marco normativo internacional, es fundamental precisar que la norma ISO/IEC 19795-1:2021 no establece de manera taxativa límites paramétricos ni umbrales numéricos aprobatorios universales para los sistemas biométricos. El estándar internacional define estrictamente el marco metodológico, los principios de control ambiental y las ecuaciones estadísticas para cuantificar el error. Por lo tanto, los límites fijados en esta investigación (Precisión $> 90.00\%$ y FAR $< 5.00\%$) no constituyen mandatos directos de la norma, sino que responden a requerimientos operacionales y de tolerancia al riesgo definidos específicamente para salvaguardar la seguridad de la Cooperativa "Señor del Buen Suceso".

Finalmente, la incorporación del modelo FER para el análisis psicométrico complementa las soluciones tradicionales de control de accesos como la planteada por Warnars et al. (2022), la cual se limitaba a validaciones binarias de identidad mediante tokens de hardware. Los resultados finales convalidaron la viabilidad técnica de integrar factores cognitivos dentro de los esquemas de seguridad física institucionales. La optimización del umbral al 10.00% de probabilidad para los estados afectivos de ira y ansiedad permitió que el algoritmo funcionara de manera reactiva, asegurando la contención de usuarios alterados una vez calibrados los parámetros iniciales de sensibilidad del software

CAPÍTULO V: CONCLUSIONES Y RECOMENDACIONES

5.1. Conclusiones

- Se llevó a cabo un estudio y análisis exhaustivo de tecnologías de visión por computadora y modelos de redes neuronales, concluyendo que la integración de FaceNet (TFLite) y FER (Facial Expression Recognition) es la más adecuada para la Cooperativa "Señor del Buen Suceso". Esta selección técnica permitió la generación de embeddings faciales de 128 dimensiones con alta precisión y un análisis psicométrico en tiempo real capaz de identificar siete emociones básicas. Con estos hallazgos, se tomó la decisión de bloquear de forma preventiva hasta un 10% cuando salen emociones como la ira y la ansiedad. Esta configuración fortalece la seguridad operativa mediante un "cortafuegos psicológico" respaldado por datos objetivos.
- Se implementó satisfactoriamente un sistema con una arquitectura distribuida de tres capas que integra un módulo móvil en Flutter, un backend en PHP y un dashboard web administrativo, que permite automatizar el control de acceso y centralizar la gestión de datos biométricos, facilitando la gestión la del proceso de reconocimiento de identidad integrado a actuadores IoT para el desbloqueo de cerraduras inteligentes en menos de 3 segundos. Visto de esta forma, se logró unificar la seguridad física con la inteligencia artificial, sentando las bases para una infraestructura de seguridad digital moderna dentro de la cooperativa.
- La evaluación del desempeño del sistema mediante el estándar de la norma ISO/IEC 19795-1:2021 evidenció una Precisión General (Accuracy) del 97.02%, lo que acredita la alta fidelidad de la solución informática para la toma de decisiones automatizadas en seguridad organizacional. En lo que se refiere a la Concordancia Emocional se alcanzó el 100.00%, señalando que el software restringió de forma efectiva la totalidad de los intentos de acceso bajo estados emocionales de riesgo detectados. Mientras que el parámetro de Falsos Positivos (FAR) se limitó al 2.38% debido a los márgenes iniciales de calibración previos a la optimización del umbral, el criterio de Falsos Negativos (FRR) se contrajo al 0.61%, garantizando una experiencia de usuario fluida y validando la viabilidad técnica del sistema en entornos operativos reales.

5.2. Recomendaciones

- Se propone ampliar las pruebas de rendimiento del sistema evaluándolo en diferentes escenarios de luz, como ambientes muy oscuros, bajo la luz directa del sol o con iluminación artificial de distintos colores. Esta medida permitirá ajustar mejor la sensibilidad del programa para que reconozca a los usuarios sin problemas, incluso si llevan lentes o gorras, reduciendo ese pequeño margen de error actual del 2.38%. Al documentar estos casos difíciles, se crea una guía valiosa para que otras instituciones puedan aplicar esta tecnología con la misma seguridad en cualquier condición climática.

- Se recomienda incorporar un mecanismo de acompañamiento para el conductor en los momentos en que el sistema deba bloquear el acceso por detectar un estado emocional elevado. En lugar de un simple aviso, la aplicación podría mostrar ejercicios de respiración, mensajes motivadores o un contador de tiempo para ayudar a la persona a recuperar la calma. Este enfoque transforma el bloqueo en una medida de protección amigable, ayudando a que los socios entiendan que el sistema no busca castigarlos, sino cuidar su seguridad y la de la cooperativa.
- Para investigaciones futuras, se recomienda aprovechar los datos de las emociones que ya se guardan para crear un historial de bienestar por cada usuario. Al analizar estos patrones de forma visual en el panel de control, los directivos podrían identificar en qué horarios o días de la semana el personal se siente más estresado o cansado. Esta herramienta permite que la cooperativa tome decisiones informadas sobre la salud de sus conductores, pasando de ser un simple control de entrada a un aliado que se preocupa por el bienestar y el buen ambiente laboral de su equipo.

BIBLIOGRAFÍA

- Abidi, S. M. (2026). *Advances in Face Recognition: A Comprehensive Review of Feature Extraction and Dataset Evaluation*. *Electronics*. <https://www.mdpi.com/2079-9292/15/2/338>
- Aboluhom, A. A. (2025). *Reconocimiento facial híbrido multi-cara seguro y descentralizado para aplicaciones IoT*. *Sensors*. <https://doi.org/10.3390/s251858803>
- Abuseta, Y. (2024). *Hacia una arquitectura de software genérica para sistemas IoT*. *arXiv*. <https://arxiv.org/abs/2411.10837>
- Adjabi, I., Ouahabi, A., Benzaoui, A., & Taleb-Ahmed, A. (2020). *Past, Present, and Future of Face Recognition: A Review*. *arXiv*. <https://arxiv.org/abs/2106.02716>
- Ahmed, W. H. (2021). *Evaluación del comportamiento del usuario hacia los sistemas biométricos*. *arXiv*. <https://arxiv.org/abs/2106.03371>
- Aloraini, M. (2025). *Trustworthy Face Recognition as a Service: A Multi-Layered Approach for Mitigating Spoofing and Ensuring System Integrity*. *Future Internet*. <https://www.mdpi.com/1999-5903/17/10/4507>
- Alrawili, R. A. (2024). *Encuesta exhaustiva: aplicación, evaluación y discusión de la autenticación biométrica*. *arXiv*. <https://arxiv.org/abs/2311.13416>
- Alshahrani, M. A.-A. (2026). *Survey on Biometric Authentication for Decentralized Identity Management: Trends, Challenges, and Future Directions*. *Future Internet*. <https://doi.org/10.3390/fi18030126>
- Alzhrani, A. A. (2024). *Diseño e implementación de un sistema inteligente de casilleros integrado con IoT*. *ETASR*. <https://etasr.com/index.php/ETASR/article/view/7737>
- Anand, R. B. (2021). *Reconocimiento facial como método de autenticación en un sistema basado en web*. *arXiv*. <https://arxiv.org/abs/2103.15144>
- Brdanin, D., et al. (2024). *Impulsando la sostenibilidad a través de un sistema de gestión inteligente basado en IoT con integración de ingeniería de software*. *Sustainability*. <https://www.mdpi.com/2071-1050/17/21/9803>
- Cai, R. C. (2023). *Aprendizaje continuo de dominio sin ensayo para anti-suplantación facial*. *arXiv*. <https://arxiv.org/abs/2303.09914>
- Gan, J. C. (2026). *Facial Beauty Prediction Using a Generative Adversarial Network for Dataset Augmentation*. *Electronics*. <https://doi.org/10.3390/electronics15030615>
- Google. (2024). *Escribiendo código específico de la plataforma (Flutter Platform Channels)*. *Documentación Oficial*. <https://docs.flutter.dev/platform-integration/platform-channels>

- Grierson, S. B. (2024). *Un marco para la seguridad y privacidad de construcciones de sistemas biométricos*. arXiv. <https://arxiv.org/abs/2411.17321>
- Hofer, P. R. (2022). *Agregación eficiente de embeddings faciales para despliegues descentralizados*. arXiv. <https://arxiv.org/abs/2212.10108>
- Islam, M. S. (2024). *Sistema de monitoreo y cerradura de puerta remota inteligente basado en IoT mediante una aplicación de Android*. Engineering Proceedings. <https://www.mdpi.com/2673-4591/76/1/85>
- ISO/IEC. (2021). *Information technology — Biometric presentation attack detection — Part 1: Framework*. ISO. <https://www.iso.org/standard/73906.html>
- ISO/IEC. (2022). *ISO/IEC 27001:2022 Seguridad de la información y protección de la privacidad*. ISO. <https://www.iso.org/standard/27001>
- Jain, S. B. (2025). *Mejora de la autenticación multifactor con integración de biometría 2D/3D sin plantillas*. Journal of Sensor and Actuator Networks. <https://www.mdpi.com/2410-387X/9/4/68>
- Kim, D. L. (2024). *Un caso de estudio sobre el diseño de API para interoperabilidad y seguridad en IoT*. arXiv. <https://arxiv.org/abs/2411.13441>
- Kinari, S. A., & Funabiki, N. (2024). *Una plataforma de autoaprendizaje guiado para la programación móvil multiplataforma con Flutter*. Computers. <https://www.mdpi.com/2078-2489/15/10/614>
- Lacharme, P. C. (2023). *Ataques de cuasi-colisión no dirigidos en biometría*. arXiv. <https://arxiv.org/abs/2304.01580>
- Li, Y. L. (2025). *FaceCloseup: Mejora de la autenticación facial móvil con detección de vitalidad basada en distorsión de perspectiva*. Computers. <https://www.mdpi.com/2073-431X/14/7/254>
- Moschini, U. D.-R. (2022). *Datos sintéticos respetuosos de la privacidad para el desarrollo de detectores de ataques de morphing facial*. arXiv. <https://arxiv.org/abs/2203.06691>
- Schlett, T. R. (2022). *Evaluación de la calidad de imágenes faciales: una revisión de la literatura*. arXiv. <https://arxiv.org/abs/2009.01103>
- Shehata, M. S.-S. (2023). *Reconocimiento Facial Basado en Deep Learning: Revisión exhaustiva*. arXiv. <https://arxiv.org/abs/2307.02679>
- Shinde, R., et al. (2025). *Generación de plantillas biométricas cancelables*. arXiv. <https://arxiv.org/abs/2503.15648>
- Shukla, S. V. (2024). *Un MFA sin contraseña que utiliza biometría, proximidad y comunicación sin contacto*. arXiv. <https://arxiv.org/abs/2406.09000>

- Vadlamudi, S. V. (2023). *Implementación de una API middleware para protocolos de comunicación en IoT*. arXiv. <https://arxiv.org/abs/2312.10294>
- Wang, M., & Deng, W. (2021). *Deep Face Recognition: A Survey*. arXiv. <https://arxiv.org/abs/1804.06655>
- Yaghoubi, H. R. (2024). *Desbloqueando el futuro: un sistema de control de acceso con IA basado en la nube*. arXiv. <https://arxiv.org/abs/2411.14444>
- Aliyu, I., et al. (2024). *A Comparative Analysis of FaceNet, VGGFace, and GhostFaceNets Face Recognition Algorithms For Potential Criminal Suspect Identification*. Published 10.09.2024. <https://www.researchgate.net/publication/383903983>
- Gursesli, M. C., Lombardi, S., Duradoni, M., Bocchi, L., Guazzini, A., & Lanata, A. (2024). *Facial emotion recognition (FER) through custom lightweight CNN model: performance evaluation in public datasets*. *IEEE Access*, 12, 45543–45559. <https://ieeexplore.ieee.org/document/10477992>
- Igene, L., Hossain, A., et al. (2024). *Face Liveness Detection Competition (LivDet-Face) 2024*. Clarkson University / Idiap Research Institute. <https://par.nsf.gov/servlets/purl/10577571>

ANEXOS

Anexo 1. Se muestra el diseño de la interfaz para la gestión de usuarios autorizados dentro del panel administrativo. Esta pantalla utiliza una disposición de tarjetas informativas que permite visualizar de manera organizada el perfil de cada conductor, incluyendo su nombre completo, número de socio, correo electrónico y la fecha de registro en el sistema, tal como se observa en la figura 20.



Figura 42: Interfaz de gestión de usuarios registrados.

Anexo 2. Se muestra el diseño de la interfaz para el monitoreo de los intentos de acceso dentro del panel administrativo. Esta pantalla utiliza una organización tabular que permite visualizar cronológicamente el registro de cada conductor, incluyendo la fecha y hora exacta, el nombre del usuario identificado, la emoción detectada por el modelo de IA y el estado final del acceso, tal como se observa en la figura 21.

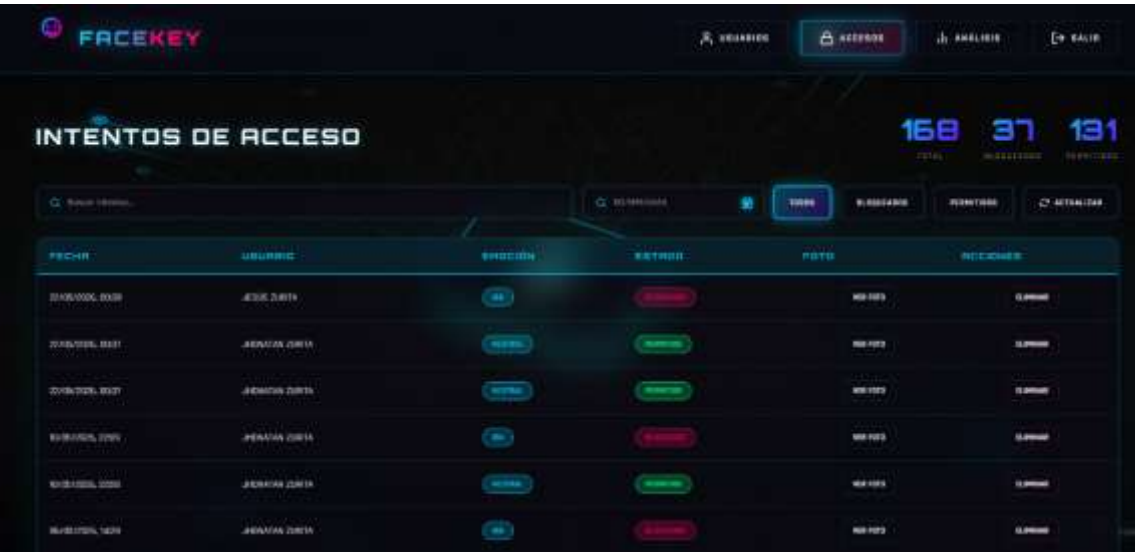


Figura 43: Interfaz de intentos de acceso.

Anexo 3. Se muestra el diseño de la interfaz para el análisis estadístico global dentro del panel administrativo. Esta pantalla utiliza un panel de "Estadísticas Generales" que permite visualizar de manera cuantitativa el rendimiento del sistema, incluyendo el total de usuarios registrados, el número de intentos realizados, el conteo de accesos permitidos frente a los bloqueados y el cálculo automático de la tasa de bloqueo, tal como se observa en la figura 22.



Figura 44: Interfaz de estadísticas generales.

Anexo 4. Se muestra el diseño de la interfaz para la visualización de las métricas de evaluación dentro del panel administrativo. Esta pantalla utiliza indicadores técnicos que permiten verificar la precisión general del sistema (97.02%), las tasas de falsos positivos y falsos negativos, así como la concordancia emocional y la confianza promedio de los modelos de inteligencia artificial, tal como se observa en la figura 23.



Figura 45: Interfaz de métricas de evaluación.

Anexo 5. Se muestra el diseño de la interfaz para el desglose de las emociones detectadas dentro del panel administrativo. Esta pantalla utiliza un panel informativo que permite visualizar la frecuencia de los estados emocionales capturados durante los procesos de acceso, incluyendo el conteo de detecciones neutras frente a las de riesgo (como la ira) y la especificación de la regla de bloqueo preventivo aplicada por el sistema, tal como se observa en la figura 24.



Figura 46: Interfaz de emociones detectadas.

Anexo 6. Se muestra el diseño de la interfaz para la identificación de los usuarios más frecuentes dentro del panel administrativo. Esta pantalla utiliza un listado jerárquico que permite visualizar de manera cuantitativa el nivel de actividad de cada conductor, destacando el número total de accesos validados satisfactoriamente por el sistema para cada perfil identificado, tal como se observa en la figura 25.



Figura 47: Interfaz de usuarios más activos.

Anexo 7. Se muestra el diseño de la interfaz para el seguimiento de la actividad reciente dentro del panel administrativo. Esta pantalla utiliza un listado cronológico que permite visualizar en tiempo real las últimas interacciones con el sistema, detallando la fecha y hora exacta, el nombre del conductor identificado y el resultado de la validación biométrica junto con la emoción detectada, tal como se observa en la figura 26.



Figura 48: Interfaz de actividad reciente.

MANUAL DE USUARIO DE LA APLICACIÓN MÓVIL FACEKEY

Este manual describe el funcionamiento paso a paso de la aplicación móvil FaceKey, dividida en el módulo para conductores y el módulo para el administrador.

1. MÓDULO DEL CONDUCTOR (PROCESO DE ACCESO)

Esta sección explica cómo el conductor utiliza la aplicación para ingresar a la institución.

1.1. Pantalla de Bienvenida (Splash Screen)

- **Funcionamiento:** Al abrir la aplicación, aparece la pantalla de presentación con el logotipo de **FaceKey**.
- **Tiempo:** Esta pantalla se mantiene fija durante 3 segundos mientras el sistema carga los archivos internos y asegura la conexión con el servidor de la cooperativa. Luego de este tiempo, pasa automáticamente a la pantalla principal.

1.2. Pantalla Principal (Control de Acceso)

- **Funcionamiento:** Muestra el estado del sistema en la parte superior ("Conectado") y presenta un botón circular azul con el ícono de un candado en el centro.
- **Instrucción:** El conductor debe pulsar el botón circular central para activar la cámara del teléfono e iniciar el reconocimiento.

1.3. Pantalla de Verificación Facial

- **Funcionamiento:** Se enciende la cámara frontal del dispositivo para capturar el rostro del conductor. En la parte inferior de la pantalla se muestra el mensaje *"Procesando imagen..."*.
- **Proceso interno:** En este momento, la aplicación realiza tres tareas automáticas:
 1. Revisa que el rostro sea real y no una foto (detección de vida).
 2. Compara los rasgos con los usuarios registrados en la base de datos.
 3. Analiza el estado emocional (detectando si hay niveles altos de ira o ansiedad).

1.4. Resultado del Acceso

- **Acceso Permitido:** Si el sistema confirma la identidad del conductor y verifica que su estado emocional es estable (menos del 10% de ira o ansiedad), se concede el acceso y la cerradura inteligente se abre.

- **Acceso Bloqueado:** Si la persona no está registrada, o si el sistema detecta que tiene niveles de ira o ansiedad superiores al 10%, el acceso se deniega automáticamente por seguridad.

2. MÓDULO DEL ADMINISTRADOR (REGISTRO DE USUARIOS)

Esta sección explica cómo el personal autorizado puede ingresar al panel oculto para registrar a nuevos conductores.

2.1. Ventana de Seguridad (Ingreso de Administrador)

- **Funcionamiento:** Para evitar que cualquier persona modifique los datos, al intentar ingresar a las opciones de configuración se abre una ventana emergente que solicita una contraseña.
- **Instrucción:** El administrador debe ingresar la clave correspondiente. Si es correcta, presiona "*Ingresar*" para abrir el panel de registro; si se equivoca o desea salir, presiona "*Cancelar*".

2.2. Pantalla de Registro Biométrico

- **Funcionamiento:** Es el formulario técnico para dar de alta a un nuevo conductor en el sistema.
- **Campos a llenar:** El administrador debe escribir los datos del nuevo usuario en los siguientes casilleros: Nombre, Apellido, N° de Socio (código de identificación en la cooperativa), Email (correo electrónico).
- **Captura de Rostro:** Finalmente, se debe presionar el botón rojo superior "*Capturar Rostro*" (con el ícono de una cámara) para tomar la fotografía del conductor desde diferentes ángulos. Al terminar, los datos y los rasgos faciales se guardan de forma definitiva en el servidor.