



UNIVERSIDAD TÉCNICA DE AMBATO

**FACULTAD DE INGENIERÍA EN SISTEMAS, ELECTRÓNICA E
INDUSTRIAL**

CARRERA DE SOFTWARE

Tema:

**SISTEMA DE RECONOCIMIENTO FACIAL PARA CONTROL DE
ACCESO CON DEEP LEARNING EN LA COOPERATIVA DE AHORRO Y
CRÉDITO SOL EN EL ÁREA DE CAJAS/BÓVEDA.**

Trabajo de titulación modalidad Proyecto de Investigación, presentado previo a la
obtención del título de Ingeniero de Software.

ÁREA: Gestión de Software

LÍNEA DE INVESTIGACIÓN: Software, Tecnologías de la Información y
Ciencia de Datos.

AUTOR: Santiago Estiven Yambay Miño

TUTOR: Ing. Julio Enrique Balarezo López, Mg.

Ambato - Ecuador

julio – 2026

APROBACIÓN DEL TUTOR

En calidad de tutor del trabajo de titulación con el tema: SISTEMA DE RECONOCIMIENTO FACIAL PARA CONTROL DE ACCESO CON DEEP LEARNING EN LA COOPERATIVA DE AHORRO Y CRÉDITO SOL EN EL ÁREA DE CAJAS/BÓVEDA, desarrollado bajo la modalidad Proyecto de Investigación por el señor Santiago Estiven Yambay Miño, estudiante de la Carrera de Software, de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial, de la Universidad Técnica de Ambato, me permito indicar que el estudiante ha sido tutorado durante todo el desarrollo del trabajo hasta su conclusión, de acuerdo a lo dispuesto en el Artículo 17 del Reglamento para la Titulación de Grado en la Universidad Técnica de Ambato y el numeral 6.3 del instructivo del reglamento referido.

Ambato, julio 2026.



Validar únicamente en FirmaEC.
Firmado electrónicamente por:
**JULIO ENRIQUE
BALAREZO LÓPEZ**

Ing. Julio Enrique Balarezo López, Mg.

TUTOR

AUTORÍA

El presente trabajo de titulación con el tema: SISTEMA DE RECONOCIMIENTO FACIAL PARA CONTROL DE ACCESO CON DEEP LEARNING EN LA COOPERATIVA DE AHORRO Y CRÉDITO SOL EN EL ÁREA DE CAJAS/BÓVEDA es absolutamente original, auténtico y personal y ha observado los preceptos establecidos en la Disposición General Quinta del Reglamento para la Titulación de Grado en la Universidad Técnica de Ambato. En tal virtud, el contenido, efectos legales y académicos que se desprenden del mismo son de exclusiva responsabilidad del autor.

Ambato, julio 2026.

**SANTIAGO
ESTIVEN
YAMBAY MINO**

Firmado digitalmente por SANTIAGO
ESTIVEN YAMBAY MINO
DN: cn=SANTIAGO ESTIVEN YAMBAY
MINO c=EC l=QUITO o=BANCO CENTRAL
DEL ECUADOR ou=ENTIDAD DE
CERTIFICACION DE
INFORMACION-ECIBCE
Motivo: Soy el autor de este documento
Ubicaci- n:
Fecha: 2026-06-22 12:17-05:00

Santiago Estiven Yambay Miño

C.C. 0650050594

AUTOR

DERECHOS DE AUTOR

Autorizo a la Universidad Técnica de Ambato para que reproduzca total o parcialmente este trabajo de titulación dentro de las regulaciones legales e institucionales correspondientes. Además, cedo todos mis derechos de autor a favor de la institución con el propósito de su difusión pública, por lo tanto, autorizo su publicación en el repositorio virtual institucional como un documento disponible para la lectura y uso con fines académicos e investigativos de acuerdo con la Disposición General Cuarta del Reglamento para la Titulación de Grado en la Universidad Técnica de Ambato.

Ambato, julio 2026.

**SANTIAGO
ESTIVEN
YAMBAY MINO**

Firmado digitalmente por SANTIAGO
ESTIVEN YAMBAY MINO
DN: cn=SANTIAGO ESTIVEN YAMBAY
MINO c=EC l=QUITO o=BANCO
CENTRAL DEL ECUADOR
ou=ENTIDAD DE CERTIFICACION DE
INFORMACION-ECIBCE
Motivo: Soy el autor de este documento
Ubicación:
Fecha: 2026-06-22 12:17-05:00

Santiago Estiven Yambay Miño

C.C. 0650050594

AUTOR

APROBACIÓN DEL TRIBUNAL DE GRADO

En calidad de par calificador del informe final del trabajo de titulación presentado por el señor Santiago Estiven Yambay Miño, estudiante de la Carrera de Software, de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial, bajo la Modalidad Proyecto de Investigación, titulado SISTEMA DE RECONOCIMIENTO FACIAL PARA CONTROL DE ACCESO CON DEEP LEARNING EN LA COOPERATIVA DE AHORRO Y CRÉDITO SOL EN EL ÁREA DE CAJAS/BÓVEDA, nos permitimos informar que el trabajo ha sido revisado y calificado de acuerdo al Artículo 19 del Reglamento para la Titulación de Grado en la Universidad Técnica de Ambato y el numeral 6.4 del instructivo del reglamento referido. Para cuya constancia suscribimos, conjuntamente con el señor Presidente del Tribunal.

Ambato, julio 2026.



Ing. Franklin Oswaldo Mayorga Mayorga, Mg.
PRESIDENTE DEL TRIBUNAL



Ing. Mg. Paulo César Torres Abril
PROFESOR CALIFICADOR



Ing. Mg. Santiago David Jara Moya
PROFESOR CALIFICADOR

DEDICATORIA

Dedico este trabajo, en primer lugar, a mi madre, quien estuvo conmigo durante todo este proceso desde que ingresé a la carrera. Gracias por nunca dejar de creer en mí, por brindarme tu amor incondicional y por apoyarme aun en los momentos más difíciles. Tu compañía, tus palabras y tu fortaleza fueron fundamentales para que pudiera seguir adelante y alcanzar esta meta.

De manera especial, dedico este logro a mi padre, quien con paciencia, amor y constancia me impulsó a continuar hasta alcanzar este momento, pese a todas las adversidades que se presentaron en el camino. Gracias por enseñarme que con esfuerzo, responsabilidad y perseverancia es posible superar los obstáculos y cumplir los objetivos propuestos.

A mis hermanas, por ser un apoyo incondicional, por el gran ejemplo que siempre me han dado y por acompañarme en cada una de mis decisiones con cariño y confianza. Su presencia en mi vida ha sido una motivación constante para seguir creciendo, aprendiendo y esforzándome cada día por ser mejor.

A toda mi familia, por sus consejos, su apoyo y su guía, los cuales me han ayudado a crecer como persona y me han motivado a continuar hasta el final.

Finalmente, dedico este trabajo a mi abuelito Guido, quien, aunque no estuvo conmigo de manera presencial, sé que me acompañó y me cuidó durante todos estos años. Su recuerdo fue una fuente de fuerza y aliento para culminar esta etapa tan importante de mi vida.

AGRADECIMIENTO

Agradezco profundamente a mis padres por su paciencia, comprensión y apoyo durante todo este proceso. Gracias por permitirme llegar a este momento a mi manera y a mi tiempo, sin dejar de creer en mí pese a los problemas y dificultades que se presentaron en el camino.

Agradezco al cuerpo docente y administrativo de la Universidad Técnica de Ambato por todos los conocimientos impartidos a lo largo de mi formación académica. Gracias por su guía, paciencia y compromiso durante todo el camino de la carrera, así como por el apoyo brindado para que pudiera llegar hasta este momento.

Agradezco de manera especial a los Ingenieros Julio Balarezo y Renato Urbina por el apoyo y la guía para poder culminar mi trabajo de la mejor manera con mucha paciencia y comprensión.

Agradezco a la Cooperativa de Ahorro y Crédito SOL por abrirme sus puertas y permitirme desarrollar mi trabajo de titulación dentro de la institución. Pese a las limitaciones e inconvenientes que surgieron durante el proceso, siempre existió la disposición de colaborar y brindar el apoyo necesario para alcanzar los objetivos propuestos. Su ayuda fue valiosa para la ejecución y culminación de este proyecto.

De manera especial, agradezco a Dios por darme la fuerza, la paciencia y la perseverancia necesarias para continuar en cada uno de los momentos críticos de este camino.

ÍNDICE GENERAL DE CONTENIDOS

PORTADA.....	i
APROBACIÓN DEL TUTOR.....	ii
AUTORÍA.....	iii
DERECHOS DE AUTOR	iv
APROBACIÓN DEL TRIBUNAL DE GRADO.....	v
DEDICATORIA.....	vi
AGRADECIMIENTO	vii
ÍNDICE GENERAL DE CONTENIDOS	1
ÍNDICE DE TABLAS.....	5
ÍNDICE DE FIGURAS.....	7
ÍNDICE DE ANEXOS	9
RESUMEN EJECUTIVO	10
ABSTRACT	11
CAPÍTULO I. MARCO TEÓRICO.....	12
1.1 Tema de investigación.....	12
1.1.1 Planteamiento del problema.....	12
1.2 Antecedentes investigativos	13
1.3 Fundamentación teórica	16

1.3.1 Seguridad en instituciones financieras	16
1.3.2 Sistemas biométricos.....	18
1.3.3 Reconocimiento facial.....	19
1.3.4 Machine Learning	21
1.3.5 Deep Learning.....	22
1.3.6 Redes neuronales convolucionales.....	24
1.3.7 Visión por computadora.....	25
1.3.8 Control de acceso	26
1.4 Objetivos	28
1.4.1 Objetivo general.....	28
1.4.2 Objetivos específicos	28
CAPÍTULO II. METODOLOGÍA.....	29
2.1 Materiales.....	29
2.2 Métodos.....	30
2.2.1 Modalidad de la investigación	30
2.2.2 Población y muestra	32
2.2.3 Recolección de información.....	32
2.2.4 Procesamiento y análisis de datos	49
CAPÍTULO III. RESULTADOS Y DISCUSIÓN.....	52
3.1 Situación actual del control de acceso en las áreas de cajas y bóveda.....	52
3.2 Limitaciones, riesgos y requerimientos del proceso actual.....	56

3.3 Diseño general del sistema propuesto con Deep Learning	60
3.3.1 Técnica de Machine Learning	62
3.3.2 Métricas de Validación	63
3.3.3 Selección del modelo	63
3.3.4 Preprocesamiento	66
3.3.5 Arquitectura funcional del sistema.....	68
3.3.6 Flujo operativo del sistema (pipeline).....	74
3.3.7 Matriz de confusión.....	75
3.3.8 Consideraciones técnicas del diseño	77
3.4 Diseño general del sistema propuesto con Aprendizaje supervisado.....	78
3.4.1 Técnica de Machine Learning	79
3.4.2 Métricas de Validación	80
3.4.3 Selección del modelo	81
3.4.4 Preprocesamiento	85
3.4.5 Arquitectura funcional del sistema.....	87
3.4.6 Flujo operativo del sistema (pipeline).....	90
3.4.7 Matriz de confusión.....	92
3.4.8 Consideraciones técnicas del diseño	94
3.5 Resultados	95
CAPÍTULO IV. CONCLUSIONES Y RECOMENDACIONES	98
4.1 Conclusiones	98

4.2 Recomendaciones.....	99
REFERENCIAS BIBLIOGRÁFICAS	101
ANEXOS	105

ÍNDICE DE TABLAS

Tabla 1. Comparación de modelos de Deep Learning aplicados a reconocimiento facial para control de acceso	14
Tabla 2. Definición de Muestra Cooperativa Sol.....	32
Tabla 3. Entrevista completa con el Gerente	33
Tabla 4. Entrevista con el Coordinador de TI.....	35
Tabla 5. Coeficiente alfa de Cronbach en la encuesta	37
Tabla 6. Criterios de la escala de consistencia del alfa de Cronbach.....	38
Tabla 7. Resultados pregunta 1	38
Tabla 8. Resultados pregunta 2	39
Tabla 9. Resultados pregunta 3	40
Tabla 10. Resultados pregunta 4	41
Tabla 11. Resultados pregunta 5	41
Tabla 12. Resultados pregunta 6	42
Tabla 13. Resultados pregunta 7	43
Tabla 14. Resultados pregunta 8	44
Tabla 15. Resultados pregunta 9	45
Tabla 16. Resultados pregunta 10	46
Tabla 17. Ficha de observación.....	47
Tabla 18. Matriz de riesgo BPMN de acceso actual a la Bóveda de la Cooperativa de Ahorro y Crédito SOL.....	56

Tabla 19. Requerimientos de la propuesta de solución.....	57
Tabla 20. Justificación de la Selección del Modelo con Deep Face	64
Tabla 21. Fragmentos del código del preprocesamiento de la imagen	67
Tabla 22. Parámetros de módulo de captura de imagen.....	68
Tabla 23. Condiciones utilizadas de validación y acceso	72
Tabla 24. Bitácora digital elaborada por el software	73
Tabla 25. Justificación del modelo de aprendizaje supervisado	81
Tabla 26. Fragmentos del código del preprocesamiento de la imagen	86
Tabla 27. Parámetros de módulo de captura de imagen.....	87
Tabla 28. Condiciones utilizadas de validación y acceso	89
Tabla 29. Bitácora digital elaborada por el software	90
Tabla 30. Comparativa técnica de los modelos evaluados.....	96
Tabla 31. Comparativa de métricas biométricas entre los modelos.....	96

ÍNDICE DE FIGURAS

Figura 1. Resultados pregunta 1	38
Figura 2. Resultados pregunta 2.....	39
Figura 3. Resultados pregunta 3.....	40
Figura 4. Resultados pregunta 4.....	41
Figura 5. Resultados pregunta 5.....	42
Figura 6. Resultados pregunta 6.....	43
Figura 7. Resultados pregunta 7.....	44
Figura 8. Resultados pregunta 8.....	45
Figura 9. Resultados pregunta 9.....	46
Figura 10. Resultados pregunta 10.....	47
Figura 11. Situación actual de acceso al sistema	53
Figura 12. Diagrama de la matriz de riesgos BPMN	55
Figura 13. Lógica de funcionamiento del programa con Deep learning.....	62
Figura 14. Código del reconocimiento facial con Deep Face	66
Figura 15. Identificación de rostro en el punto de acceso.....	70
Figura 16. Enfoque de procesamiento para control de acceso con reconocimiento facial	70
Figura 17. Carpeta donde se colocarán los rostros autorizados	71
Figura 18. Acceso permitido del usuario	72
Figura 19. Acceso denegado del usuario.....	72

Figura 20. Trazabilidad del programa en la consola de Python.....	74
Figura 21. Carpetas para realizar la matriz de confusión.....	76
Figura 22. Matriz de confusión modelo Deep Learning	76
Figura 23. Lógica de funcionamiento del programa con Aprendizaje supervisado...	79
Figura 24. Código de la captura de datos.....	84
Figura 25. Código del entrenamiento del modelo.....	84
Figura 26. Código del reconocimiento facial con Aprendizaje supervisado	85
Figura 27. Enfoque de procesamiento para control de acceso con Aprendizaje supervisado.....	92
Figura 28. Matriz de confusión modelo Machine Learning.....	93

ÍNDICE DE ANEXOS

Anexo A Matriz validación entrevista	105
Anexo B. Captura de carpeta de desarrollo	110
Anexo C. Código del aplicativo con Deep Learning	111
Anexo D. Código para la matriz de confusión del aplicativo de Deep Learning	114
Anexo E. Código de la captura de datos	117
Anexo F. Código del entrenamiento del modelo.....	118
Anexo G. Código del reconocimiento facial con Aprendizaje supervisado	119
Anexo H. Código para la matriz de confusión del aplicativo de Aprendizaje supervisado	122
Anexo I Validación cámara	124

RESUMEN EJECUTIVO

El control de paso a las áreas de cajas y bóveda de la Cooperativa de Ahorro y Crédito SOL presentaba vulnerabilidades de protección debido a la dependencia de bitácoras manuales, lo cual generaba riesgos de suplantación junto con errores de anotación y falta de trazabilidad, por consiguiente la finalidad principal de la investigación fue desarrollar un aplicativo automatizado de validación de entradas basado en reconocimiento facial utilizando redes neuronales convolucionales para resguardar las instalaciones, para lograrlo el estudio aplicó una metodología de campo y aplicada con enfoque mixto, empleando encuestas, entrevistas y fichas de observación dirigidas a una muestra de 12 empleados para diagnosticar la situación inicial, como resultado el aplicativo propuesto mitigó 4 riesgos de alta severidad y cumplió con 7 requerimientos operativos, además al comparar 2 modelos tecnológicos el programa de aprendizaje transferido con la librería Deep Face presentó mejor desempeño comparativo al clasificador de aprendizaje supervisado local, puesto que el sistema de inteligencia profunda utilizó 100 fotografías de referencia por empleado autorizado, alcanzando una exactitud del 98 por ciento, una precisión del 96.15 por ciento y una sensibilidad del 100 por ciento, mientras que el modelo local demandó 300 fotografías obteniendo apenas un 55 por ciento de exactitud con 89 falsos negativos, por lo tanto se concluyó que la implementación de redes neuronales eliminó la dependencia de registros físicos y automatizó la comprobación biométrica en tiempo real, proporcionando así una administración de accesos más segura y auditable para la institución financiera.

Palabras claves: Control de acceso, reconocimiento facial, redes neuronales convolucionales, seguridad institucional, Deep Face, Cooperativa de ahorro y crédito SOL.

ABSTRACT

Access control to the cash register and vault areas of Cooperativa de Ahorro y Crédito SOL presented security vulnerabilities due to the reliance on manual logs, which generated risks of identity impersonation, recording errors, and lack of traceability. Therefore, the main objective of this research was to develop an automated access validation application based on facial recognition using convolutional neural networks. The study applied a field and applied methodology with a mixed approach, using surveys, interviews, and observation sheets addressed to a sample of 12 employees in order to diagnose the initial situation. As a result, the proposed application mitigated four high-severity risks and fulfilled seven operational requirements. Furthermore, when comparing two technological models, the transfer learning program implemented with the DeepFace library showed better comparative performance than the local supervised learning classifier, since it used 100 reference photographs per authorized employee, achieving an accuracy of 98 percent, a precision of 96.15 percent, and a sensitivity of 100 percent. In contrast, the local model required 300 photographs and obtained 55 percent accuracy with 89 false negatives. Thus, it was concluded that the implementation of neural networks reduced dependence on physical records and automated biometric verification in real time, providing a more secure, traceable, and auditable access management process for the financial institution.

Keywords: Access control, facial recognition, convolutional neural networks, institutional security, Deep Face, Cooperativa de ahorro y crédito SOL.

CAPÍTULO I. MARCO TEÓRICO

1.1 Tema de investigación

Sistema de reconocimiento facial para control de acceso con deep learning en la Cooperativa de Ahorro y Crédito SOL en el área de cajas/bóveda.

1.1.1 Planteamiento del problema

La administración del ingreso hacia las zonas de alta sensibilidad representa una prioridad para las entidades financieras al momento de resguardar el dinero y los documentos almacenados en las bóvedas o ventanillas de atención, por consiguiente ante el incremento de las amenazas por fraudes o suplantaciones de identidad las corporaciones demandan mecanismos automatizados más certeros para proteger su patrimonio [1] , no obstante en la actualidad aún prevalecen prácticas convencionales que merman la agilidad operativa y la protección de los datos [2].

A nivel local el empleo de libretas físicas para vigilar el paso hacia los espacios restringidos prevalece como una costumbre habitual, ocasionando debilidades derivadas de las equivocaciones humanas junto con las omisiones y la carencia de una supervisión continua [2].

Específicamente en la Cooperativa de Ahorro y Crédito SOL de Riobamba el paso hacia la zona de cajeros y la bóveda se controla mediante un cuaderno de anotaciones manuales para registrar a las personas autorizadas, sin embargo los datos recolectados presentan inconsistencias al ser ilegibles o inexactos, disminuyendo así la trazabilidad y complicando la identificación exacta de los individuos que transitan por estas áreas [1], de igual manera la carencia de estandarización documental junto con la inexistencia de filtros de comprobación de identidad elevan el peligro de suplantaciones y entradas indebidas [3].

Por otra parte, la generación de reportes a partir de estas libretas se transforma en una tarea manual muy demorada y propensa a equivocaciones, limitando así la facultad de ejecutar auditorías exactas para mantener un rastreo fidedigno de los movimientos [2], provocando como resultado una disminución en la capacidad de administración

institucional que afecta directamente la toma de decisiones basada en información verídica [4].

Todas estas limitantes exponen la urgencia por incorporar herramientas tecnológicas capaces de automatizar la gestión de las entradas para perfeccionar la identificación de los trabajadores, garantizando de este modo la creación de bitácoras fiables y auditables al instante [5].

¿De qué manera un sistema automatizado puede optimizar la administración de los accesos y la creación de historiales verídicos en las zonas de cajas y bóveda de la Cooperativa de Ahorro y Crédito SOL?

1.2 Antecedentes investigativos

Diversos estudios han demostrado la eficacia del reconocimiento facial como método biométrico para el control de acceso en entornos de alta seguridad. Investigaciones recientes evidencian que los modelos sustentados en redes neuronales convolucionales superan a los métodos tradicionales de reconocimiento debido a su alta precisión y a su capacidad de aprendizaje automático [4].

González y Zhindón estructuraron modelos de identificación biométrica profunda, los cuales sirven como base operativa para diversas herramientas de protección, videovigilancia y comprobación de usuarios [4], por consiguiente en la región de América Latina se han desplegado plataformas informáticas similares dentro de centros de educación y corporaciones bancarias, logrando disminuir de manera exitosa los ingresos de personas no admitidas a las instalaciones [6].

Asimismo, Ibarreche, Martínez y Di Lorenzo analizaron el desempeño de modelos CNN frente a variaciones de iluminación, ángulos y expresiones faciales en entornos no controlados. Los autores concluyeron que los sistemas fundamentados en deep learning mantienen un rendimiento robusto, lo cual los convierte en una alternativa adecuada para aplicaciones de seguridad institucional [5].

Por su parte, Niola y Sanango realizaron un análisis comparativo entre métodos tradicionales y técnicas basadas en deep learning aplicadas al reconocimiento facial, determinando que las redes neuronales convolucionales presentan mayores tasas de

precisión, menor tasa de error y mejor capacidad de generalización en sistemas biométricos modernos [6].

Tabla 1. Comparación de modelos de Deep Learning aplicados a reconocimiento facial para control de acceso

Investigación	Modelo Aplicado	Contexto	Métricas Clave	Principales Hallazgos
[7]	YOLOv2	Reconocimiento facial en tiempo real para vigilancia.	mAP: 78,6%, FPS: 40.	Alta velocidad, apto para entornos con poca luz.
[8]	FastR-CNN	Reconocimiento facial Fast R-CNN en puntos de acceso controlados.	Precisión: 96,2%, Tiempo: 0,2 s por imagen.	Mayor precisión que YOLO, pero más lento.
[9]	CNN personalizada	Control de acceso CNN diseñado específicamente para instituciones educativas.	Precisión: 97,5%, Tasa de falsos positivos: 2,1%.	Eficaz en condiciones de control de iluminación.
[10]	FaceNet + SVM	Zona de seguridad FaceNet + SVM en empresas.	Precisión: 98,1%, Tasa de error: 1,5%.	Resulta indispensable estructurar colecciones de información completamente proporcionales para prevenir alteraciones estadísticas

				durante el procesamiento de los modelos.
[11]	CNN+LBPH	CNN + LBPH finanzas (bancos).	Precisión: 96,8 %, Tiempo de respuesta: 0,8 s.	Presenta una alta tolerancia matemática frente a los cambios de inclinación del rostro o las alteraciones gestuales del usuario.

En el ámbito institucional, Tovar y Martín desarrollaron un sistema de control de acceso mediante reconocimiento facial en una entidad bancaria, evidenciando una reducción significativa de accesos no autorizados y una mejora sustancial en el monitoreo del personal autorizado, fortaleciendo así los mecanismos de seguridad interna [7]. De forma similar, Cumbe y Potos implementaron un sistema biométrico facial en áreas restringidas de una empresa, destacando beneficios como la disminución de errores humanos, el incremento de la trazabilidad de ingresos y la automatización de los procesos de autorización [8].

Mite evaluó el desempeño de un sistema de reconocimiento facial basado en redes neuronales convolucionales en entornos financieros reales, obteniendo altos niveles de precisión y tiempos de respuesta adecuados para aplicaciones de control de acceso, lo cual confirma la viabilidad de este tipo de soluciones tecnológicas en el sector financiero [9].

Con respecto al apartado de seguridad, Oyaque analizó la detección temprana de eventos mediante el uso de visión artificial y Deep Learning. El autor concluyó que la dependencia humana constituye uno de los problemas más frecuentes en los sistemas

de seguridad, especialmente en videovigilancia, debido a la necesidad de mantener un monitoreo continuo. Por ello, el uso de métodos autónomos genera mayor confianza y automatiza el proceso de vigilancia [10].

1.3 Fundamentación teórica

1.3.1 Seguridad en instituciones financieras

La seguridad en instituciones financieras constituye uno de los elementos más importantes para garantizar la protección de activos económicos, información confidencial y operaciones institucionales [2]. Actualmente, bancos y cooperativas manejan diariamente grandes volúmenes de transacciones financieras, datos personales y registros digitales, por lo cual requieren mecanismos de protección capaces de minimizar riesgos asociados con robos, accesos indebidos y fraude electrónico. Diversos estudios de seguridad informática señalan que aproximadamente el 60% de incidentes relacionados con vulnerabilidades institucionales se encuentran asociados a errores humanos y deficiencias en controles manuales de supervisión, situación que evidencia la necesidad de implementar tecnologías automatizadas dentro de áreas críticas [9].

Los espacios protegidos como las ventanillas de atención, las bóvedas y las salas de vigilancia constituyen sectores de extrema vulnerabilidad porque albergan dinero en efectivo junto con documentación reservada y plataformas informáticas delicadas, por lo tanto el ingreso a estos recintos aún suele administrarse empleando libretas físicas, llaves tradicionales o tarjetas plásticas, herramientas que exponen deficiencias considerables vinculadas al extravío de los pases, la alteración de autorizaciones y la creación de historiales fragmentados, de acuerdo con las evaluaciones administrativas las metodologías no automatizadas llegan a elevar hasta un 45% las discordancias dentro de las bases de datos de visitas a causa de los descuidos o equivocaciones ocurridas durante el monitoreo a cargo del personal [9].

Desde un enfoque técnico, la seguridad financiera moderna se fundamenta en principios como autenticación, autorización, disponibilidad, confidencialidad y trazabilidad de la información. La autenticación corresponde al proceso de validar la identidad del usuario antes de permitir el acceso al sistema, mientras que la

autorización determina los privilegios disponibles para cada individuo dentro de la organización. Por otra parte, la trazabilidad permite generar logs digitales capaces de almacenar fecha, hora, usuario y eventos relacionados con los accesos realizados, facilitando posteriormente auditorías y procesos de control institucional [1].

Las infraestructuras de protección actuales integran herramientas de vanguardia tales como la supervisión visual computarizada, los detectores electrónicos, la vigilancia ininterrumpida y los aplicativos autónomos para administrar las entradas, por consiguiente estos recursos emplean dispositivos de captura IP junto con equipos de guardado de datos y modelos matemáticos capaces de identificar comportamientos inusuales o intrusiones, asimismo en los entornos de vigilancia analítica las plataformas logran evaluar flujos de grabación por encima de los 30 fotogramas por segundo, facilitando de este modo la ejecución de labores de observación permanente con un retraso mínimo y una elevada agilidad para reaccionar frente a cualquier eventualidad operativa [12].

Otro aspecto importante corresponde a la protección de información digital almacenada dentro de las bases de datos institucionales. Para garantizar la integridad y confidencialidad de los registros se emplean mecanismos de cifrado AES, protocolos seguros TLS/SSL y sistemas de autenticación multifactor. En aplicaciones biométricas, esta protección resulta aún más importante debido a que se almacenan características únicas de los usuarios, como patrones faciales y plantillas biométricas que requieren altos niveles de seguridad para evitar vulnerabilidades o filtraciones de información sensible [12].

Actualmente, las instituciones financieras han comenzado a incorporar tecnologías biométricas basadas en inteligencia artificial para fortalecer sus mecanismos de autenticación. Diversos estudios tecnológicos indican que más del 70% de entidades bancarias a nivel internacional utilizan algún tipo de validación biométrica en procesos de seguridad y autenticación digital. Estas soluciones permiten reducir tiempos de validación hasta en un 50%, mejorar la precisión de identificación y disminuir considerablemente los riesgos asociados con accesos indebidos dentro de áreas restringidas [13].

1.3.2 Sistemas biométricos

Los sistemas biométricos son tecnologías diseñadas para identificar o verificar la identidad de una persona mediante características físicas o conductuales únicas. Estos sistemas funcionan mediante procesos de captura, extracción y comparación de patrones biométricos que posteriormente son almacenados dentro de bases de datos digitales. La principal ventaja de la biometría radica en que las características humanas utilizadas poseen altos niveles de singularidad, dificultando procesos de falsificación o suplantación de identidad en comparación con métodos tradicionales como contraseñas o tarjetas de acceso [12].

Se encuentran disponibles diversas categorías de plataformas biométricas en función del rasgo físico evaluado durante la fase de verificación de identidad, sobresaliendo entre las alternativas más comunes el análisis del rostro junto con la lectura de huellas dactilares, el escaneo del iris o la retina, la identificación vocal y la medición geométrica de las manos, por consiguiente cada una de estas herramientas posee variados grados de exactitud y exigencia de procesamiento para los equipos informáticos, a modo de ilustración los lectores de iris logran superar el 99% de aciertos, en tanto que las arquitecturas actuales de evaluación facial estructuradas sobre aprendizaje profundo alcanzan cifras próximas al 97% o 98% bajo entornos regulados [14].

El funcionamiento técnico de un sistema biométrico comprende varias etapas fundamentales. Inicialmente se realiza la adquisición de datos mediante sensores, cámaras digitales o dispositivos especializados. Posteriormente, el sistema ejecuta procesos de preprocesamiento orientados a reducir ruido e inconsistencias dentro de la información capturada. Después de ello, se extraen características relevantes utilizando algoritmos matemáticos y se generan templates biométricos capaces de representar digitalmente la identidad del usuario [15].

Dentro de los aplicativos biométricos de última generación el desempeño se calcula habitualmente empleando parámetros estadísticos como la tasa de aceptación falsa (FAR) junto con la tasa de rechazo falso (FRR) y la tasa de error equivalente (EER), por consiguiente el indicador FAR establece la probabilidad de permitir el paso por equivocación a un sujeto sin permiso, en tanto que el parámetro FRR determina la

posibilidad de bloquear la entrada a un usuario verdadero, de este modo en los entornos de las entidades económicas se procura conservar los niveles de FAR por debajo del 1% para mitigar las brechas de seguridad asociadas a las intrusiones, de igual forma el coeficiente EER facilita la estimación del balance entre ambas medidas para dictaminar la certeza operativa global del programa informático desplegado [7].

Uno de los principales beneficios de los sistemas biométricos corresponde a la automatización de procesos de autenticación y monitoreo institucional. A diferencia de los métodos manuales, estas tecnologías permiten generar registros digitales automáticos de ingreso y salida, mejorando significativamente la trazabilidad y capacidad de auditoría. Además, la validación biométrica reduce riesgos asociados con pérdida de credenciales, intercambio de tarjetas o robo de contraseñas utilizadas en sistemas convencionales de acceso [14].

Dentro de las entidades económicas la validación biométrica se ha transformado en un recurso primordial para asegurar las zonas de alto riesgo como las ventanillas de atención y los recintos acorazados, por consiguiente los análisis informáticos de última generación exponen que el sector mundial de comprobación corporal conserva un ritmo de expansión por encima del 15% cada año a causa del aumento de implementaciones vinculadas con la protección corporativa y los servicios bancarios virtuales, de este modo la fusión de las mediciones físicas con la inteligencia artificial y el procesamiento visual computarizado ha facilitado la estructuración de programas informáticos mucho más veloces, exactos y amoldables a variados escenarios de trabajo [2].

1.3.3 Reconocimiento facial

El reconocimiento facial es una técnica biométrica basada en algoritmos de visión por computadora e inteligencia artificial, utilizada para identificar o verificar la identidad de una persona mediante el análisis de patrones únicos del rostro humano. Este proceso involucra varias etapas computacionales como adquisición de imagen, detección facial, alineación, extracción de características y clasificación biométrica. Su principal objetivo consiste en transformar imágenes faciales en representaciones matemáticas

conocidas como embeddings, las cuales pueden compararse posteriormente con registros almacenados dentro de una base de datos [16].

La operatividad de la identificación visual comienza a través de la obtención de fotografías empleando lentes RGB o equipos de monitoreo, posteriormente el programa lleva a cabo fases de preparación donde se ejecutan labores para equilibrar la luz junto con el ajuste de tamaño y la disminución de imperfecciones visuales además de la rectificación espacial de la captura, luego de esto los cálculos de rastreo ubican de manera autónoma la posición de la cara valiéndose de técnicas clásicas como Haar Cascade o esquemas actuales sustentados en redes neuronales convolucionales y estructuras YOLO [17].

Al haber localizado la cara el aplicativo obtiene marcas distintivas denominadas puntos de referencia anatómica, los cuales abarcan la ubicación de los ojos junto con la nariz y la mandíbula además de la boca y los bordes físicos, seguidamente estos datos se convierten en matrices numéricas de amplia dimensionalidad aptas para simbolizar de forma calculable la identidad biológica de la persona, por consiguiente para establecer igualdades la herramienta emplea parámetros estadísticos como la separación euclidiana y la semejanza del coseno, facilitando así el cotejo de la fisonomía captada frente a los archivos guardados con anterioridad [9].

Los sistemas modernos de reconocimiento facial basados en Deep Learning han alcanzado niveles de precisión superiores al 97% en datasets reconocidos como LFW (Labeled Faces in the Wild) y VGGFace2. Asimismo, modelos como FaceNet, DeepFace y ArcFace permiten generar embeddings altamente discriminativos incluso bajo condiciones variables de iluminación, postura o expresiones faciales. Gracias a estos avances, los sistemas actuales presentan valores FAR inferiores al 1%, reduciendo considerablemente riesgos de autenticación incorrecta dentro de aplicaciones de seguridad institucional [14].

Un factor adicional a considerar atañe a la velocidad de contestación del dispositivo biométrico, puesto que dentro de los aplicativos actuales para administrar entradas las fases de ubicación y reconocimiento del rostro logran procesarse en un lapso inferior a 2 segundos mediante el uso de procesadores gráficos y esquemas de cálculo perfeccionados, por consiguiente esta agilidad técnica facilita la puesta en marcha de

herramientas de vigilancia ininterrumpida sin perjudicar el ritmo de trabajo dentro de los recintos protegidos o las corporaciones de gran afluencia [2].

Actualmente, el reconocimiento facial tiene aplicaciones en banca, aeropuertos, control migratorio, videovigilancia inteligente y autenticación digital. Su integración con inteligencia artificial y aprendizaje profundo ha permitido automatizar procesos de identificación humana y fortalecer mecanismos de seguridad institucional. Sin embargo, todavía existen desafíos relacionados con oclusiones faciales, cambios extremos de iluminación y ataques de spoofing mediante fotografías o videos, por lo cual continúan desarrollándose técnicas más robustas de validación biométrica [7].

1.3.4 Machine Learning

El Machine Learning o aprendizaje automático constituye una rama de la inteligencia artificial enfocada en el desarrollo de algoritmos capaces de aprender patrones y realizar predicciones a partir de datos sin necesidad de programación explícita para cada tarea. Su funcionamiento se basa en modelos matemáticos y estadísticos que permiten identificar relaciones complejas dentro de grandes volúmenes de información. Actualmente, esta tecnología es ampliamente utilizada en aplicaciones relacionadas con reconocimiento de imágenes, procesamiento de lenguaje natural, sistemas predictivos y automatización inteligente [18].

Las metodologías de aprendizaje automático se categorizan en instrucción supervisada, no supervisada y por refuerzo, por consiguiente la modalidad supervisada emplea información marcada con anticipación para adiestrar a los esquemas matemáticos con el propósito de catalogar datos o formular pronósticos, en contraparte la técnica no supervisada opera sobre registros carentes de categorización persiguiendo el hallazgo de agrupaciones o regularidades invisibles dentro del material analizado, por último la variante de refuerzo faculta a un ente digital para adquirir destrezas a través del roce permanente con su medio exterior valiéndose de tácticas de gratificación y castigo [11].

El proceso de entrenamiento de modelos de aprendizaje automático comprende varias etapas técnicas como recolección de datos, preprocesamiento, extracción de características, entrenamiento, validación y pruebas. Durante el preprocesamiento se eliminan inconsistencias y se normalizan los datos para mejorar el rendimiento del

algoritmo. Posteriormente, el modelo ajusta sus parámetros internos mediante funciones de pérdida y algoritmos de optimización orientados a minimizar errores de clasificación [11].

Dentro de aplicaciones relacionadas con reconocimiento facial, Machine Learning permite construir modelos capaces de identificar patrones biométricos complejos mediante análisis matemático de imágenes digitales. Algoritmos como Support Vector Machine (SVM), K-Nearest Neighbors (KNN) y Random Forest fueron ampliamente utilizados en técnicas tradicionales de clasificación facial antes de la popularización del Deep Learning. Aunque estos métodos presentan buen rendimiento en ciertos escenarios, poseen limitaciones cuando trabajan con grandes volúmenes de datos o condiciones variables del entorno [19].

Un factor adicional a considerar dentro del aprendizaje automático atañe a los parámetros de evaluación empleados para comprobar el desempeño de las arquitecturas instruidas, por consiguiente entre las opciones más habituales se encuentran la exactitud junto con la precisión, la sensibilidad y la matriz de confusión, de este modo estas herramientas estadísticas facilitan el examen de la facultad de pronóstico del programa informático logrando detectar eventuales complicaciones por exceso de ajuste o déficit de adaptación a lo largo del proceso de asimilación de datos [20].

En el ámbito financiero, el Machine Learning ha permitido automatizar procesos de vigilancia, análisis de riesgo y autenticación biométrica. Los sistemas modernos pueden detectar comportamientos sospechosos, generar alertas en tiempo real y validar identidades mediante procesamiento inteligente de datos. Esto contribuye a mejorar la eficiencia operativa y fortalecer mecanismos de seguridad institucional dentro de áreas críticas como cajas y bóvedas [18].

1.3.5 Deep Learning

El Deep Learning es una subrama avanzada del Machine Learning que utiliza redes neuronales profundas para aprender representaciones complejas de los datos mediante múltiples capas de procesamiento. Estas arquitecturas computacionales permiten modelar patrones no lineales y realizar tareas de clasificación, reconocimiento y predicción con altos niveles de precisión. Debido a su capacidad de aprendizaje

automático, el Deep Learning ha revolucionado áreas como visión por computadora, reconocimiento facial, procesamiento de voz y análisis predictivo [18].

Las arquitecturas neuronales de gran profundidad se estructuran a partir de niveles de ingreso junto con estratos intermedios y fases de salida entrelazados a través de conexiones sinápticas, por consiguiente a lo largo del adiestramiento matemático la información recorre estas divisiones por medio de un mecanismo conocido como propagación frontal, posteriormente el programa computa el fallo de estimación empleando ecuaciones de pérdida para regular los valores numéricos internos gracias al algoritmo de propagación inversa acompañado de métodos de mejora operativa tales como Adam o el descenso de gradiente estocástico [12].

Uno de los elementos más importantes dentro del Deep Learning corresponde a las funciones de activación utilizadas para introducir no linealidad dentro de las redes neuronales. Entre las más utilizadas destacan ReLU, Sigmoid y Softmax. La función ReLU permite mejorar la velocidad de entrenamiento evitando problemas de gradientes desaparecidos, mientras que Softmax se utiliza comúnmente en tareas de clasificación multiclase para calcular probabilidades de pertenencia entre diferentes categorías [19].

Durante el entrenamiento de modelos profundos también es necesario considerar problemas relacionados con overfitting y underfitting. El overfitting ocurre cuando la red aprende excesivamente los datos de entrenamiento y pierde capacidad de generalización frente a nuevos ejemplos. Para reducir este problema se emplean técnicas como dropout, regularización L2 y data augmentation. Asimismo, parámetros como epochs, learning rate y batch size influyen directamente sobre el rendimiento final del modelo neuronal [14].

Dentro de la verificación visual el aprendizaje profundo ha logrado sobrepasar las restricciones habituales de las metodologías convencionales gracias a su aptitud para obtener de manera autónoma los rasgos distintivos de la cara humana, por consiguiente arquitecturas matemáticas como FaceNet y DeepFace consiguen construir vectores numéricos sumamente exactos aun frente a alteraciones complicadas de luminosidad junto con modificaciones de postura o cambios gestuales, elevando de esta forma la certeza operativa de las plataformas biométricas de última generación [21].

Actualmente, el entrenamiento de modelos Deep Learning requiere elevados recursos computacionales debido a la gran cantidad de operaciones matemáticas involucradas. Por esta razón, suelen utilizarse GPUs y librerías especializadas como TensorFlow, PyTorch y Keras que permiten acelerar el procesamiento de datos y optimizar el entrenamiento de redes neuronales profundas utilizadas en aplicaciones de inteligencia artificial y visión artificial [1].

1.3.6 Redes neuronales convolucionales

Las redes neuronales convolucionales son una arquitectura de red profunda especializada en el análisis de imágenes. Su funcionamiento se basa en capas de convolución, agrupamiento y clasificación, que permiten aprender rasgos jerárquicos desde características simples hasta patrones complejos [3], [6]. En sistemas de reconocimiento facial, las CNN son utilizadas para identificar rasgos distintivos del rostro de las personas, logrando un alto rendimiento en tareas de clasificación facial. Debido a su capacidad de aprendizaje y adaptación, constituyen una de las técnicas más empleadas en sistemas biométricos modernos [22].

Las CNN se inspiran en el funcionamiento del sistema visual humano, donde diferentes neuronas se encargan de detectar patrones específicos dentro de las imágenes. Estas redes procesan los datos mediante filtros matemáticos que permiten identificar bordes, formas, texturas y características relevantes para el reconocimiento de objetos o personas. Gracias a este mecanismo, las redes convolucionales pueden extraer automáticamente información importante sin necesidad de programación manual detallada [23].

Dentro de la arquitectura de una CNN existen diferentes tipos de capas que cumplen funciones específicas durante el procesamiento de imágenes. Las capas convolucionales se encargan de extraer características relevantes, mientras que las capas de agrupamiento o pooling reducen la dimensionalidad de la información para optimizar el rendimiento del sistema. Finalmente, las capas densas o fully connected realizan la clasificación final de los datos procesados [24].

Una de las principales ventajas de las redes neuronales convolucionales es su alta precisión en tareas relacionadas con visión artificial y reconocimiento facial. Estas

redes pueden aprender patrones complejos y adaptarse a diferentes condiciones del entorno, permitiendo identificar personas incluso cuando existen variaciones en la iluminación, expresiones faciales o posición del rostro. Debido a ello, las CNN han sido ampliamente implementadas en sistemas modernos de autenticación biométrica [25].

La implementación de redes neuronales convolucionales dentro de las plataformas de vigilancia corporativa ha facilitado la automatización de las tareas de reconocimiento, propiciando así una mayor certeza en los dispositivos de gestión de ingresos, por consiguiente en las entidades bancarias estos recursos tecnológicos simplifican la validación de los trabajadores autorizados, ayudando en la creación de historiales más exactos y protegidos, asimismo estos modelos de inteligencia artificial mantienen una progresión incesante gracias al progreso de la computación y a la mayor potencia de procesamiento actualmente disponible [26].

1.3.7 Visión por computadora

La visión por computadora constituye un área de la inteligencia artificial orientada a que los sistemas interpreten y procesen imágenes o videos de manera automatizada. En el contexto del reconocimiento facial, esta disciplina permite detectar rostros dentro de una imagen, procesarlos y extraer características útiles para su posterior identificación o verificación. Su incorporación dentro de sistemas de seguridad institucional aporta rapidez en el procesamiento, automatización de decisiones y capacidad de monitoreo en tiempo real, elementos clave para aplicaciones de control de acceso [27].

La visión artificial busca simular la capacidad humana de observar e interpretar el entorno mediante dispositivos electrónicos y algoritmos computacionales. Para lograrlo, los sistemas utilizan cámaras digitales y modelos matemáticos capaces de analizar imágenes, reconocer objetos y tomar decisiones automatizadas basadas en los datos obtenidos. Esta tecnología ha tenido un importante crecimiento debido al desarrollo de herramientas de inteligencia artificial y procesamiento digital de imágenes [28].

Dentro de los procesos de visión por computadora intervienen varias etapas fundamentales como adquisición de imágenes, preprocesamiento, segmentación, extracción de características y reconocimiento de patrones. Cada una de estas fases permite transformar imágenes capturadas en información útil para diferentes aplicaciones tecnológicas. En reconocimiento facial, estos procesos ayudan a identificar rostros humanos y diferenciarlos de otros elementos presentes en la escena.

La implementación de la visión artificial en los esquemas de protección ha facilitado la creación de dispositivos autónomos destinados a la vigilancia y al control inteligente, pues en la actualidad existen plataformas aptas para localizar comportamientos inusuales junto con la identificación de individuos autorizados y la emisión de avisos automáticos al instante, logrando de este modo elevar la eficacia de las labores de supervisión al disminuir la necesidad de una observación humana constante.

Dentro de las entidades económicas la visión artificial constituye un recurso de gran valor para robustecer la protección de los recintos protegidos y automatizar las gestiones de ingreso, por consiguiente la incorporación de lentes inteligentes junto con modelos de reconocimiento del rostro permite la elaboración de bitácoras fiables, ayudando a potenciar la facultad de monitoreo de la corporación, asimismo esta tecnología simplifica el despliegue de esquemas de seguridad actuales con una mayor exactitud y prontitud al momento de reconocer a los usuarios.

1.3.8 Control de acceso

El control de acceso es un mecanismo de seguridad que regula quién puede ingresar a un área o sistema específico. Su finalidad principal es proteger recursos físicos o digitales, restringiendo el acceso únicamente a personas autorizadas [1], [2]. En instituciones financieras, el control de acceso en áreas críticas como cajas y bóveda resulta indispensable para preservar la seguridad del personal, de los valores monetarios y de la información sensible. La integración de tecnologías biométricas en estos mecanismos incrementa los niveles de seguridad, reduce la probabilidad de suplantación de identidad y mejora la trazabilidad de los ingresos y salidas del personal autorizado [1].

Los sistemas de control de acceso pueden clasificarse en métodos manuales, electrónicos y biométricos. Los controles manuales generalmente utilizan registros escritos o supervisión humana para validar el ingreso de personas, mientras que los sistemas electrónicos emplean tarjetas magnéticas, códigos o dispositivos digitales.

De igual manera, las plataformas de verificación corporal emplean rasgos anatómicos distintivos tales como las huellas dactilares o la configuración del rostro para confirmar la identidad de los sujetos, por consiguiente uno de los mayores inconvenientes de las tácticas convencionales de gestión de ingresos reside en la sujeción a trámites manuales que suelen ocasionar equivocaciones junto con omisiones o el extravío de datos, dado que en diversas ocasiones los apuntes físicos exhiben discordancias que complican la comprobación precisa sobre qué individuos ingresaron a los sectores limitados, además la carencia de una supervisión autónoma aminora la facultad de actuar ante cualquier eventualidad que afecte la protección.

La integración de herramientas automatizadas facilita la optimización de los flujos de administración de entradas dentro de las organizaciones, pues los esquemas actuales logran producir bitácoras digitales al instante junto con la regulación automática de los accesos y el guardado de antecedentes para futuras revisiones de auditoría, beneficiando así el monitoreo institucional y perfeccionando el rastreo de las tareas ejecutadas por el personal avalado.

Dentro del ámbito de las entidades económicas la vigilancia de los ingresos representa un componente primordial para resguardar el patrimonio financiero y avalar la protección corporativa, por lo tanto la incorporación del reconocimiento facial junto con el aprendizaje profundo en estas arquitecturas permite robustecer las tácticas de validación y aminorar las debilidades vinculadas con los procedimientos de siempre, motivo por el cual los recursos biométricos configuran hoy en día una opción eficaz para automatizar la entrada hacia zonas de alta sensibilidad tales como las ventanillas de atención y los recintos acorazados.

1.4 Objetivos

1.4.1 Objetivo general

Desarrollar un sistema automatizado de control de acceso basado en reconocimiento facial utilizando redes neuronales convolucionales para el área de cajas y bóveda de la Cooperativa de Ahorro y Crédito SOL.

1.4.2 Objetivos específicos

- Analizar los procesos actuales de registro y control de acceso en las áreas críticas de cajas y bóveda de la Cooperativa de Ahorro y Crédito SOL, identificando sus limitaciones, riesgos y requerimientos para el diseño de una solución automatizada.
- Diseñar un modelo de reconocimiento facial basado en técnicas de aprendizaje automático para la identificación del personal autorizado de la Cooperativa de Ahorro y Crédito SOL.
- Evaluar el desempeño del sistema propuesto en términos de precisión, seguridad y eficiencia en el control de ingreso del personal.

CAPÍTULO II. METODOLOGÍA

2.1 Materiales

Para la recolección de información en la presente investigación se emplearon tres técnicas: la encuesta, la entrevista y la ficha de observación, con el propósito de obtener datos cuantitativos y cualitativos que permitan analizar los procesos actuales de control de acceso en las áreas críticas de cajas y bóveda de la Cooperativa de Ahorro y Crédito SOL.

La encuesta estructurada, compuesta por 10 preguntas cerradas, estuvo dirigida al personal autorizado que labora en las áreas de cajas y bóveda, así como al personal de seguridad. Esta técnica tuvo como finalidad identificar cómo se realizan actualmente los registros de ingreso y salida, evaluar el nivel de confiabilidad de los métodos utilizados (manuales o digitales) y detectar las principales falencias en el control de acceso, tales como errores en los registros, accesos no autorizados o demoras en los procesos. Además, permitió conocer la percepción del personal respecto a la necesidad de implementar un sistema automatizado basado en reconocimiento facial para mejorar la seguridad.

La entrevista, dirigida al administrador general o al encargado de la protección en la cooperativa, estuvo constituida por preguntas abiertas con la intención de examinar el desempeño del esquema vigente de administración de ingresos. Esta técnica posibilitó el reconocimiento de las amenazas vinculadas con las tácticas convencionales, además de avalar la factibilidad de desplegar una herramienta digital mediante el empleo de aprendizaje profundo, permitiendo obtener una perspectiva administrativa sobre la relevancia de robustecer las medidas de custodia en las zonas restringidas.

La entrevista fue validada mediante juicio de expertos, utilizando una matriz de validación del instrumento en la que se revisaron criterios de claridad, coherencia, pertinencia y relevancia de cada pregunta. Este proceso permitió comprobar que las interrogantes planteadas estaban correctamente formuladas y alineadas con los objetivos de la investigación, especialmente con el diagnóstico del proceso actual de control de acceso en las áreas de cajas y bóveda.

La ficha de observación, elaborada con el propósito de inspeccionar cómo se ejecutan cotidianamente las labores de vigilancia en las cajas y la bóveda, sirvió para constatar el empleo de bitácoras físicas junto con la inexistencia de filtros biométricos completos y la carencia de un rastreo continuo, por consiguiente, estos resultados posibilitaron el diagnóstico de las deficiencias presentes en la metodología actual para sustentar la urgencia de incorporar un programa autónomo de identificación de rostros.

2.2 Métodos

En la presente investigación se empleó una metodología con enfoque mixto para el análisis de la problemática identificada en el control de acceso a las áreas de cajas y bóveda de la Cooperativa de Ahorro y Crédito SOL. Se recopiló información mediante entrevistas y observación directa, lo que permitió comprender el funcionamiento actual de los procesos de control de acceso, identificar sus debilidades y analizar la percepción institucional sobre la necesidad de implementar un sistema automatizado. Desde el enfoque cuantitativo, se aplicaron encuestas al personal involucrado y se evaluó el desempeño del sistema propuesto mediante métricas objetivas como precisión, tasa de error y tiempo de respuesta.

Bajo esta perspectiva, la aplicación de un método mixto facilitó la obtención de una comprensión completa de la problemática estudiada, lo cual sirvió de base para justificar el análisis del estado actual del sistema y, al mismo tiempo, validar la propuesta tecnológica fundamentada en el reconocimiento facial y el aprendizaje profundo.

2.2.1 Modalidad de la investigación

El proyecto investigativo se enmarca en la modalidad de campo y aplicada, debido a que integra la recolección directa de información en el entorno real de la cooperativa y el desarrollo de una herramienta tecnológica, la cual será sometida a evaluación para determinar su funcionamiento y efectividad al momento de procesar los ingresos del personal.

Investigación de campo

El estudio se clasifica como investigación de campo al obtener datos directamente en las áreas de cajas y bóvedas de la Cooperativa de Ahorro y Crédito SOL, lugar donde se analizaron los procedimientos actuales de control de pasos, para lo cual se aplicaron encuestas a los empleados autorizados junto con entrevistas a los responsables institucionales y la observación directa de los movimientos diarios.

Esta aproximación permitió conocer la realidad operativa de la institución y detectar falencias en los mecanismos actuales de revisión, determinando así las necesidades específicas del entorno para recopilar datos valiosos, lo que facilitó el planteamiento de una solución tecnológica ajustada a los requerimientos verdaderos de la cooperativa financiera.

Investigación Aplicada

El estudio de tipo aplicado se enfoca en resolver de forma específica el inconveniente hallado por medio de la creación de un programa de identificación de rostros, dado que esta modalidad persigue obtener beneficios prácticos aplicables de manera inmediata en el escenario real, distanciándose de las indagaciones meramente conceptuales al proporcionar un instrumento funcional para optimizar la protección de los sectores delimitados.

Para la programación del aplicativo se utilizaron redes neuronales preentrenadas capaces de extraer las características faciales de los usuarios, este proceso incluyó etapas como la captura de video y la transformación a escala de grises para aislar el rostro humano, prosiguiendo con la comparación matemática de los vectores biométricos frente a las fotografías almacenadas en un directorio local.

Posteriormente la herramienta fue ejecutada en un entorno de pruebas para simular su funcionamiento bajo condiciones habituales de iluminación y movimiento, evaluando de esta manera su capacidad para identificar correctamente a los trabajadores autorizados, para lo cual se analizaron indicadores de rendimiento como la exactitud del sistema junto con los falsos positivos y el tiempo empleado en la verificación.

A partir de los resultados obtenidos se determinó la viabilidad del sistema informático como solución tecnológica para la cooperativa, analizando también su potencial de adaptación en otros entornos que requieran altos niveles de protección, esta modalidad

garantiza que la investigación no solo aporte al desarrollo tecnológico sino que entregue una solución aplicable al problema de los accesos manuales.

2.2.2 Población y muestra

El presente proyecto de investigación se enfoca en el personal operativo que posee acceso a las áreas de cajas y bóveda de la Cooperativa de Ahorro y Crédito SOL, constituyéndose como la población objetivo del estudio. En la Tabla 2 se detalla la caracterización de los diferentes actores institucionales con acceso a estas áreas, tomando en consideración la frecuencia de ingreso y la relevancia de cada rol dentro del flujo operativo que se desarrolla en la institución.

Tabla 2. Definición de Muestra Cooperativa Sol

Población	Nº de personas	Porcentaje %
Gerencia	1	8.33 %
Oficial de seguridad	1	8.33 %
Coordinador de TI	1	8.33 %
Cajero	4	33.33%
Servicio al cliente	2	16.67%
Guardia	2	16.67%
Coordinador de Operaciones	1	8.33 %
Total	12	100%

2.2.3 Recolección de información

La recolección de información en la presente investigación se realizó mediante la aplicación de tres técnicas: encuesta, entrevista y observación directa, dirigidas al personal que tiene acceso a las áreas de cajas y bóveda de la Cooperativa de Ahorro y Crédito SOL. Estas técnicas permitieron obtener información relevante sobre los procedimientos actuales de control de acceso, los niveles de seguridad existentes, las principales limitaciones del registro manual y la percepción del personal frente a la implementación de un sistema automatizado basado en reconocimiento facial.

El instrumento de encuesta se enfocó en el personal operativo y administrativo que utiliza dichas zonas, con el objetivo de obtener datos medibles sobre la recurrencia de entrada, los mecanismos de registro vigentes, el grado de fiabilidad de los métodos actuales, la incidencia de equivocaciones o disparidades y la disposición hacia la adopción de una alternativa tecnológica para robustecer la gestión de ingresos.

Por otro lado, la entrevista se destinó al personal directivo o encargado de la seguridad institucional, buscando recabar perspectivas más profundas acerca de las dificultades, los peligros actuales y la factibilidad de incorporar una solución biométrica. Finalmente, la guía de observación permitió constatar en el sitio la ejecución real de los protocolos de control de acceso.

a. Entrevistas

Tabla 3. Entrevista completa con el Gerente

Entrevistado		Gerente	
Fecha		02/06/2026	
No.	Pregunta	Respuesta	Observación/Análisis
1	Desde su perspectiva, ¿cómo evalúa el sistema actual de control de acceso en las áreas de cajas y bóveda?	Si bien el esquema vigente permite operar, este posee deficiencias considerables respecto a la administración y validación de accesos, ya que depende mayoritariamente de anotaciones escritas a mano y del monitoreo efectuado por los trabajadores.	Se observa una metodología convencional caracterizada por una escasa implementación de procesos autónomos y una elevada subordinación a la supervisión del personal.
2	¿Qué riesgos considera que existen actualmente en el control de acceso a estas áreas críticas?	Se identifican peligros relacionados con la usurpación de identidades, la captura errónea de datos, ingresos sin permiso y la carencia de supervisión inmediata.	Detecta las amenazas principales vinculadas directamente con las carencias del método de gestión manual.
3	¿Ha experimentado la institución situaciones de anomalía o eventos vinculados con el ingreso de personal sin permiso o errores en los procesos de bitácora?	Si bien no han ocurrido eventos de gravedad, se han detectado irregularidades en las bitácoras, tales como información parcial o imprecisiones en los registros temporales.	Ratifica la problemática central de la investigación, la cual radica en la falta de coherencia en los datos y la reducida capacidad de seguimiento.
4	¿Cuál es el grado de seguridad que usted atribuye a las herramientas empleadas en la actualidad, tales como el uso de llaves, carnets, o la	Estimo que el grado de seguridad es moderado, dado que tales métodos son susceptibles de ser comprometidos por equivocaciones involuntarias	Considero que el nivel de protección es intermedio, puesto que dichos mecanismos son propensos a verse afectados por fallos

	gestión de anotaciones, ya sean de índole manual o digital?	o por una utilización inadecuada.	del personal o por un empleo inapropiado.
5	¿Qué restricciones logra detectar respecto a los procedimientos vigentes de gestión de ingresos y el seguimiento de las actividades del personal?	La restricción más significativa radica en la escasa exactitud de los archivos, la complejidad para confirmar las identidades y la elaboración de informes mediante procedimientos manuales.	Subraya las deficiencias existentes en el seguimiento de actividades y en la creación de los informes correspondientes.
6	Desde una perspectiva corporativa, ¿cuál es el nivel de importancia que asigna a la optimización de los sistemas de protección en dichos espacios?	Se considera un asunto de suma relevancia, debido a que dichos espacios son fundamentales para el resguardo de activos financieros y de información confidencial.	Valida la importancia estratégica que tiene el proyecto para la institución.
7	¿Qué atributos debería reunir una plataforma óptima de gestión de ingresos para alinearse con los protocolos de seguridad requeridos por la institución?	El sistema requiere ser autónomo, fidedigno y operar de forma inmediata, incorporando además procesos de verificación de identidad y la creación automatizada de informes sujetos a auditoría.	Establece las especificaciones operativas esenciales para el desarrollo del sistema propuesto.
8	¿Cuál es su opinión sobre la implementación de tecnologías biométricas, específicamente el reconocimiento facial, para el control de acceso?	Considero que es una alternativa moderna y adecuada, ya que mejora la seguridad y reduce la intervención humana en los procesos.	Buena acogida hacia la implementación de soluciones biométricas.
9	¿Considera factible integrar una plataforma automatizada de identificación mediante rasgos faciales en la cooperativa? ¿Cuáles serían sus razones?	Es factible, siempre que se asegure la salvaguarda de la información, se garantice la exactitud de la herramienta y el costo se ajuste a las capacidades financieras de la entidad.	Presenta los criterios de factibilidad necesarios en los ámbitos legal, técnico y financiero.
10	¿Qué ventajas prevé alcanzar mediante la adopción de una solución automatizada para la gestión de accesos?	Un incremento en la seguridad, la disminución de fallos atribuidos al factor humano, un seguimiento exhaustivo y detallado, así como la creación ágil de informes.	Ventajas directamente vinculadas a los objetivos de el proyecto.
11	¿Qué factores (económicos, tecnológicos o humanos) podrían influir en la adopción de este tipo de solución?	Los recursos financieros asignados, la plataforma tecnológica instalada y la formación del equipo de trabajo.	Elementos determinantes para la puesta en marcha efectiva dentro del entorno operativo.
12	¿Qué sugerencias ofrecería para garantizar el despliegue adecuado y la durabilidad a largo plazo de la solución tecnológica?	Ejecutar una planificación rigurosa, instruir adecuadamente a los colaboradores, asegurar el mantenimiento constante y garantizar el acatamiento de las regulaciones sobre	Un desenlace táctico que garantiza la continuidad operativa y está estrictamente supeditado a los marcos de referencia de la gobernanza tecnológica.

		seguridad y privacidad de la información.	
--	--	---	--

Tabla 4. Entrevista con el Coordinador de TI

Entrevistado		Coordinador área TI	
Fecha		06/06/2026	
No.	Pregunta	Respuesta	Observación/Análisis
1	Desde su perspectiva, ¿cómo evalúa el sistema actual de control de acceso en las áreas de cajas y bóveda?	El sistema actual es básico y poco integrado. Se basa principalmente en registros manuales sin validación tecnológica, lo que limita su eficiencia.	Se evidencia ausencia de automatización e integración tecnológica.
2	¿Qué riesgos considera que existen actualmente en el control de acceso a estas áreas críticas?	Riesgos de suplantación de identidad, manipulación de registros, además de un seguimiento inconsistente para los informes mensuales del control del área. Igual al momento de hacer seguimientos hay que realizar más investigaciones y revisar varias cámaras en caso de que no existan registros lo cual hace que el seguimiento sea mucho más demorado	Riesgos asociados a sistemas no automatizados.
3	¿Se han presentado incidentes o irregularidades relacionadas con accesos no autorizados o fallas en el registro?	No incidentes críticos, pero sí inconsistencias frecuentes en los registros manuales, como datos incompletos o errores de digitación.	Confirma debilidad en calidad de datos.
4	¿Qué nivel de confiabilidad considera que tienen los métodos actuales (llaves, credenciales, registros manuales o digitales)?	El nivel de confiabilidad es medio-bajo, debido a la falta de mecanismos de validación automática y dependencia del factor humano.	Baja confiabilidad técnica del sistema actual.
5	¿Qué limitaciones identifica en los procesos actuales de control de acceso y trazabilidad del personal?	Falta de trazabilidad en tiempo real, dificultad para auditar registros, ausencia de integración con sistemas digitales y generación manual de reportes.	Identifica limitaciones técnicas clave para tu solución.
6	Desde el punto de vista institucional, ¿qué tan importante considera mejorar los mecanismos de seguridad en estas áreas?	Es crítico, especialmente por temas de cumplimiento normativo, auditorías y protección de activos institucionales.	Relaciona seguridad con cumplimiento y auditoría.
7	¿Qué características debería tener un sistema ideal de control de acceso para cumplir con los	Debe ser automatizado, integrado con otros sistemas, con autenticación biométrica, registro en	Define requisitos técnicos del sistema.

	estándares de seguridad de la cooperativa?	tiempo real, alta disponibilidad y almacenamiento seguro de datos.	
8	¿Cuál es su opinión sobre la implementación de tecnologías biométricas, específicamente el reconocimiento facial, para el control de acceso?	Es una solución adecuada, ya que permite autenticación rápida, precisa y sin contacto, además de mejorar la trazabilidad.	Validación técnica positiva.
9	¿Considera viable la implementación de un sistema automatizado basado en reconocimiento facial en la cooperativa? ¿Por qué?	Sí, es viable si se cuenta con la infraestructura adecuada, una correcta integración con sistemas existentes y se garantiza la seguridad de la información.	Introduce requisitos de infraestructura e integración.
10	¿Qué beneficios esperaría obtener con la implementación de un sistema de control de acceso automatizado?	Optimización en la exactitud de los registros, supervisión inmediata, mitigación de fallos operativos, procesos de auditoría eficaces y fortalecimiento integral de la seguridad.	Fortalecimiento de la integridad y exactitud en la gestión de datos, supervisión operativa inmediata, mitigación de riesgos por intervención humana, agilización de los procesos de auditoría y robustecimiento de los estándares de seguridad.
11	¿Qué factores (económicos, tecnológicos o humanos) podrían influir en la adopción de este tipo de solución?	Costos de implementación, capacidad de infraestructura (red, servidores), compatibilidad con sistemas existentes y resistencia al cambio del personal.	Factores críticos desde TI.
12	¿Qué recomendaciones daría para asegurar una correcta implementación y sostenibilidad del sistema en el tiempo?	Ejecutar pruebas de concepto, garantizar la capacidad de expansión del sistema, establecer protocolos de seguridad sólidos, instruir al capital humano y formalizar un programa de mantenimiento preventivo y correctivo de manera permanente.	Priorizar la ejecución de pruebas de concepto, asegurar la capacidad de expansión del sistema, establecer protocolos de seguridad sólidos, instruir al capital humano y formalizar un programa de mantenimiento preventivo y correctivo de manera permanente.

b) Encuestas

• Validación del instrumento (alfa de Cronbach)

Alfa de Cronbach en la encuesta dirigida al personal con acceso a las áreas de cajas y bóveda de la Cooperativa de Ahorro y Crédito SOL

El índice alfa de Cronbach representa un indicador de fiabilidad que permite valorar la coherencia interna entre los elementos que conforman un instrumento de evaluación o escala de medida.

Este coeficiente se emplea para verificar si los componentes del instrumento evalúan de forma homogénea una misma dimensión o variable. En la presente investigación, se aplicará el Alfa de Cronbach con el propósito de analizar la consistencia interna de los ítems cerrados del cuestionario de encuesta, especialmente aquellos relacionados con la percepción sobre el control de acceso actual, la confiabilidad del registro, la existencia de errores y la necesidad de implementar un sistema automatizado basado en reconocimiento facial esto correspondiendo a los siguientes cinco ítems de la encuesta: 1, 2, 3, 4 y 7.

$$\alpha = \frac{k}{k-1} \left(1 - \frac{\sum \sigma_i^2}{\sigma_{total}^2} \right)$$

Donde:

k = número de ítems en la escala.

$\sum \sigma_i^2$ = sumatoria de la varianza de los ítems.

σ_{total}^2 = varianza total del instrumento.

Los resultados serán tabulados en Excel, obteniendo los valores que se presentarán en la tabla correspondiente.

Tabla 5. Coeficiente alfa de Cronbach en la encuesta

Simbología	Valor
α	0.7
k	5
$\sum \sigma_i^2$	4.338
σ_{total}^2	9.724

El coeficiente obtenido fue de **0,7** tal como se muestra en la Tabla 5, el resultado muestra que el instrumento utilizado tiene un nivel aceptable de confiabilidad, según los criterios establecidos en la Tabla 6:

Tabla 6. Criterios de la escala de consistencia del alfa de Cronbach

Rango Interpretación	Rango Interpretación
0,9	Excelente
0,9 – 0,8	Buena
0,8 – 0,7	Aceptable
0,7 – 0,6	Cuestionable
0,6 – 0,5	Pobre
< 0,5	Inaceptable

- **Preguntas de la encuesta**

Pregunta 1 ¿Con qué frecuencia el personal entra y sale del área de cajas?

Tabla 7. Resultados pregunta 1

Indicador	Frecuencia	Porcentaje
Nunca	0	0%
Ocasionalmente	3	25%
Frecuentemente	7	58%
Siempre	2	17%

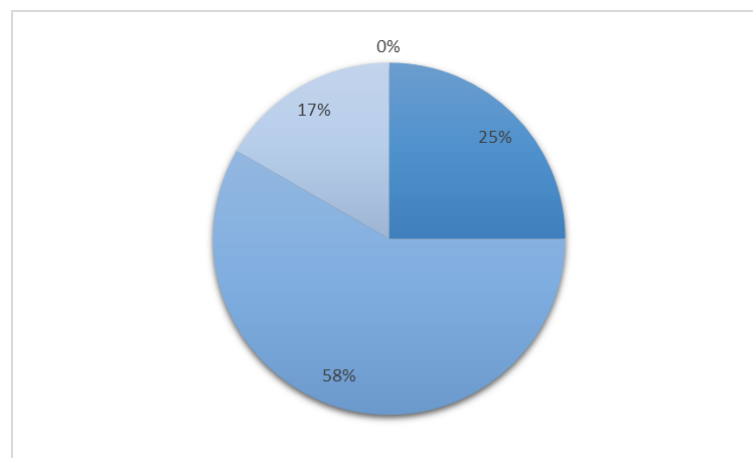


Figura 1. Resultados pregunta 1

Análisis e Interpretación de resultados

Los resultados muestran que la mayor parte de los encuestados, correspondiente al 58.33%, considera que el personal entra y sale frecuentemente del área de cajas, mientras que un 16.67% señala que esto ocurre siempre. Asimismo, el 25% indica que este ingreso y salida se da ocasionalmente, y ningún encuestado manifestó que nunca ocurra. Estos datos evidencian que existe una circulación constante de personal en un área sensible dentro de la institución. En ese sentido, la información obtenida permite inferir que los controles de permanencia y acceso no serían lo suficientemente restrictivos, lo que podría representar una debilidad en el manejo y resguardo de este espacio.

Pregunta 2 ¿Con qué frecuencia el personal entra y sale del área de bóveda?

Tabla 8. Resultados pregunta 2

Indicador	Frecuencia	Porcentaje
Nunca	0	0%
Ocasionalmente	8	67%
Frecuentemente	3	25%
Siempre	1	8%

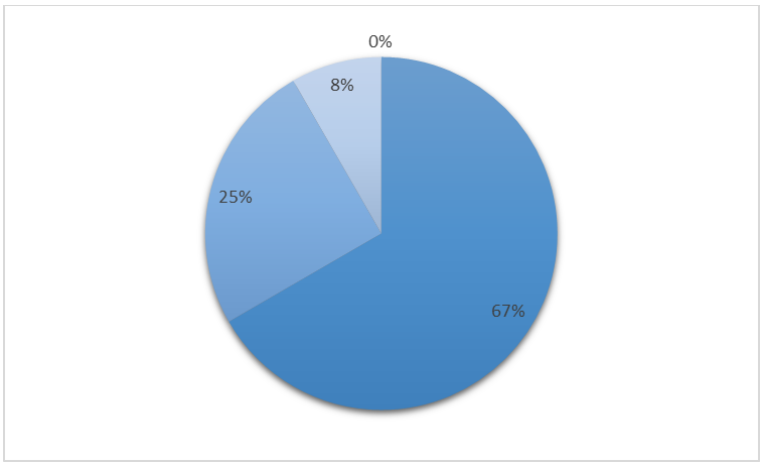


Figura 2. Resultados pregunta 2

Análisis e Interpretación de resultados

Los resultados reflejan que, para la mayoría de los encuestados, el ingreso y salida del personal en el área de bóveda ocurre ocasionalmente, con un 66.67%, mientras que el 25% considera que sucede frecuentemente y el 8.33% manifiesta que siempre ocurre.

La ausencia de respuestas en la categoría «nunca» revela que, si bien el flujo de colaboradores no es constante, ocurre con la suficiente periodicidad en un entorno altamente crítico. Esta distribución sugiere que el acceso a la bóveda carece de restricciones absolutas, lo que denota una permisividad que compromete la rigurosidad en la gestión de entradas y salidas del personal.

Pregunta 3 ¿Con qué frecuencia registra su ingreso o salida del área de cajas?

Tabla 9. Resultados pregunta 3

Indicador	Frecuencia	Porcentaje
Nunca	2	17%
Ocasionalmente	7	58%
Frecuentemente	1	8%
Siempre	2	17%

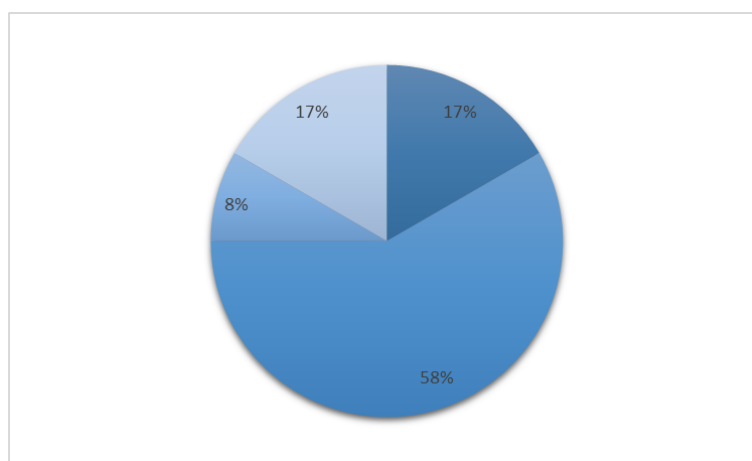


Figura 3. Resultados pregunta 3

Análisis e Interpretación de resultados

Los resultados muestran que el 58.33% de los encuestados registra su ingreso o salida del área de cajas de manera ocasional, mientras que el 16.67% señala que nunca lo hace y el mismo porcentaje indica que siempre realiza este registro. Por su parte, apenas el 8.33% manifestó que lo hace frecuentemente. Esta distribución evidencia que el registro de entradas y salidas en el área de cajas no se realiza de manera constante por parte de la mayoría del personal. En ese sentido, los datos reflejan que este control presenta un cumplimiento irregular, lo que permite identificar una debilidad en la constancia con que se documenta el acceso a esta área.

Pregunta 4 ¿Con qué frecuencia registra su ingreso o salida del área de bóveda?

Tabla 10. Resultados pregunta 4

Indicador	Frecuencia	Porcentaje
Nunca	1	8%
Ocasionalmente	2	17%
Frecuentemente	5	42%
Siempre	4	33%

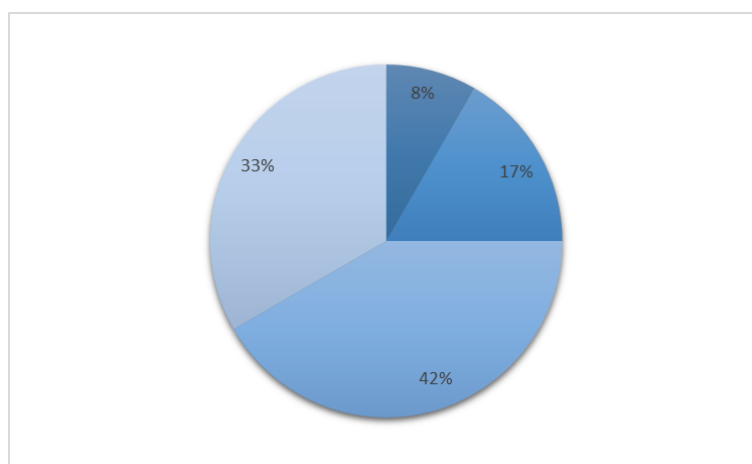


Figura 4. Resultados pregunta 4

Análisis e Interpretación de resultados

Los resultados evidencian que el 41.67% de los encuestados registra su ingreso o salida del área de bóveda frecuentemente, mientras que el 33.33% señala que siempre lo hace. Por su parte, el 16.67% indicó que realiza este registro ocasionalmente y el 8.33% manifestó que nunca lo efectúa. Esta distribución permite interpretar que, en comparación con otras áreas, en la bóveda existe una mayor regularidad en el registro de accesos. No obstante, la presencia de respuestas que indican un cumplimiento ocasional o inexistente demuestra que este control no se aplica de forma totalmente uniforme entre todo el personal.

Pregunta 5 ¿Cómo se realiza el registro de entrada y salida de cajas actualmente?

Tabla 11. Resultados pregunta 5

Indicador	Frecuencia	Porcentaje
Manual (hojas y cuadernos)	5	42%
Digital (Excel o archivo digital)	0	0%
Mixto (manual o digital)	7	58%
No se realiza un registro	0	0%

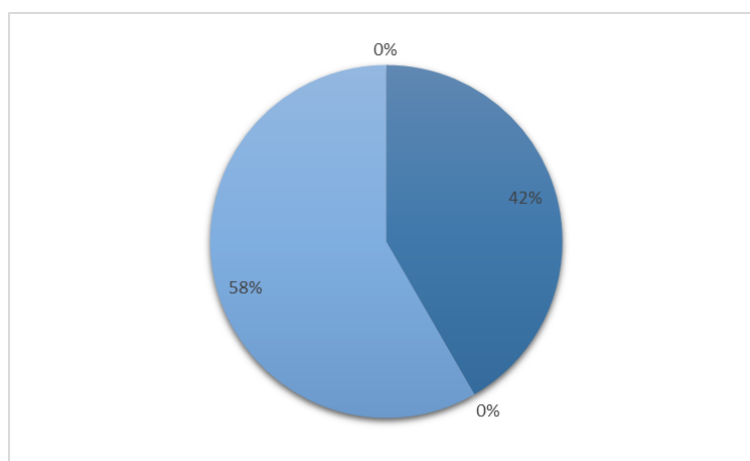


Figura 5. Resultados pregunta 5

Análisis e Interpretación de resultados

Los resultados muestran que el 58.33% de los encuestados señala que el registro de entrada y salida de cajas se realiza de forma mixta, combinando medios manuales y digitales, mientras que el 41.67% indica que este proceso se lleva únicamente de manera manual, mediante hojas o cuadernos. Ningún encuestado manifestó que el registro se efectúe exclusivamente de forma digital, ni que no se realice. Esta distribución evidencia que predomina el uso de mecanismos tradicionales y parcialmente apoyados en recursos digitales. En ese sentido, los datos reflejan que no existe una estandarización total en la forma de registrar los accesos al área de cajas, lo que demuestra diferencias en la gestión y control de esta información.

Pregunta 6 ¿Qué tan confiable considera el método actual de registro de entrada y salida de cajas y bóveda?

Tabla 12. Resultados pregunta 6

Indicador	Frecuencia	Porcentaje
Nada confiable	5	42%
Medianamente confiable	5	42%
Confiable	1	8 %
Muy confiable	1	8%

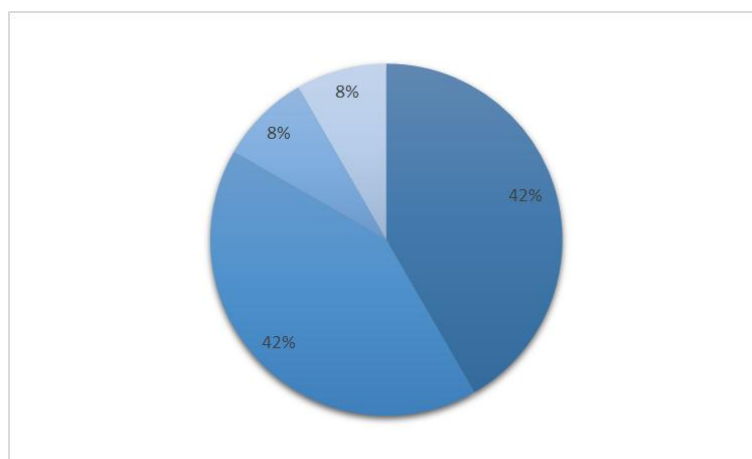


Figura 6. Resultados pregunta 6

Análisis e Interpretación de resultados

Los resultados reflejan que el 41.67% de los encuestados considera que el método actual de registro de entrada y salida de cajas y bóveda es nada confiable, mientras que otro 41.67% lo califica como medianamente confiable. En menor proporción, el 8.33% lo percibe como confiable y el mismo porcentaje como muy confiable. Esta distribución evidencia que predomina una percepción poco favorable respecto a la confiabilidad del mecanismo utilizado. En ese sentido, los datos permiten interpretar que el método actual no genera un nivel sólido de confianza entre la mayoría del personal, lo que demuestra limitaciones en la percepción de seguridad y consistencia del registro aplicado.

Pregunta 7 ¿Con qué frecuencia se presentan errores o inconsistencias en los registros actuales?

Tabla 13. Resultados pregunta 7

Indicador	Frecuencia	Porcentaje
-----------	------------	------------

Nunca	0	0%
Ocasionalmente	1	8%
Frecuentemente	3	25%
Siempre	8	67%

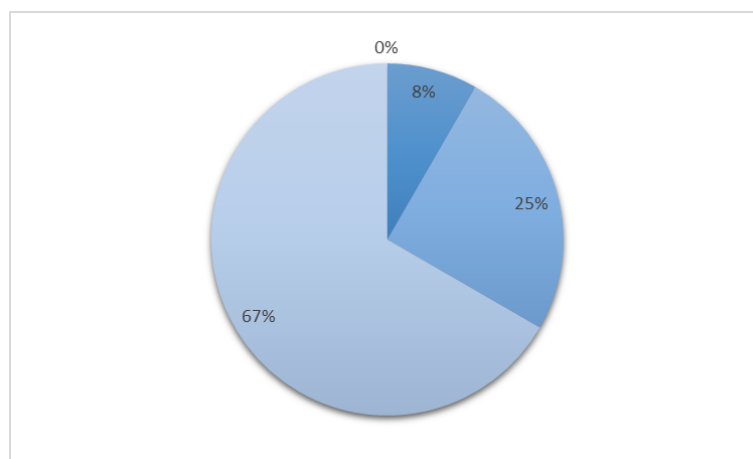


Figura 7. Resultados pregunta 7

Análisis e Interpretación de resultados

Los resultados muestran que el 66.67% de los encuestados afirma que los errores o inconsistencias en los registros actuales se presentan siempre, mientras que el 25% indica que ocurren frecuentemente. Por su parte, el 8.33% señala que estas situaciones se presentan ocasionalmente y ningún encuestado manifestó que nunca ocurran. Esta distribución evidencia una alta recurrencia de fallas dentro del proceso de registro. En ese sentido, los datos reflejan que los registros actuales presentan deficiencias de consistencia y precisión, lo que demuestra que su manejo no se desarrolla de manera totalmente confiable ni uniforme.

Pregunta 8 ¿Qué vulnerabilidades o amenazas detecta usted con mayor periodicidad al gestionar los accesos y egresos en las áreas de cajas o bóvedas?

Tabla 14. Resultados pregunta 8

Indicador	Frecuencia	Porcentaje
Descuadre de caja	2	17%
Accesos no autorizados	4	33%

Errores en el registro manual	5	42%
Demora en los procesos	1	8 %

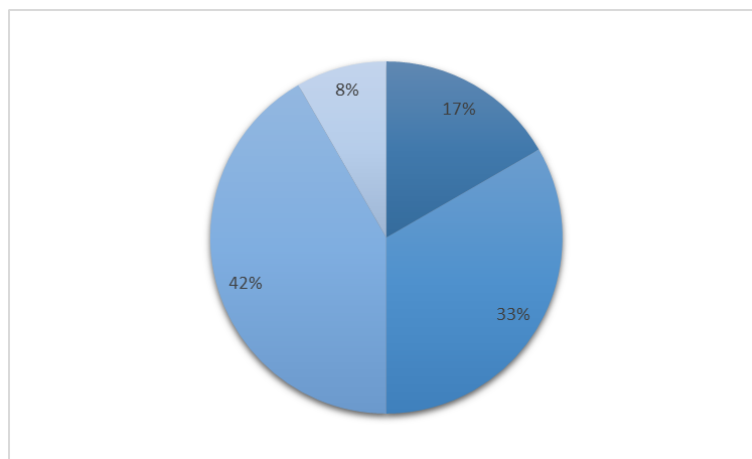


Figura 8. Resultados pregunta 8

Análisis e Interpretación de resultados

Los resultados evidencian que el riesgo identificado con mayor frecuencia en el control de ingreso y salida de cajas o bóveda corresponde a los errores en el registro manual, con un 41.67%, seguido de los accesos no autorizados, con el 33.33%. En menor proporción, el 16.67% de los encuestados señala el descuadre de caja y el 8.33% la demora en los procesos. Esta distribución permite interpretar que las principales preocupaciones del personal se concentran en fallas asociadas al registro y al control de accesos. En ese sentido, los datos reflejan que existen debilidades percibidas tanto en la exactitud del registro como en la seguridad del control de ingreso y salida en estas áreas.

Pregunta 9 ¿Considera que un registro automático mejoraría el control de ingreso y salida del personal?

Tabla 15. Resultados pregunta 9

Indicador	Frecuencia	Porcentaje
En desacuerdo	0	0%
Neutral	3	25%

De acuerdo	5	43 %
Muy de acuerdo	4	33%

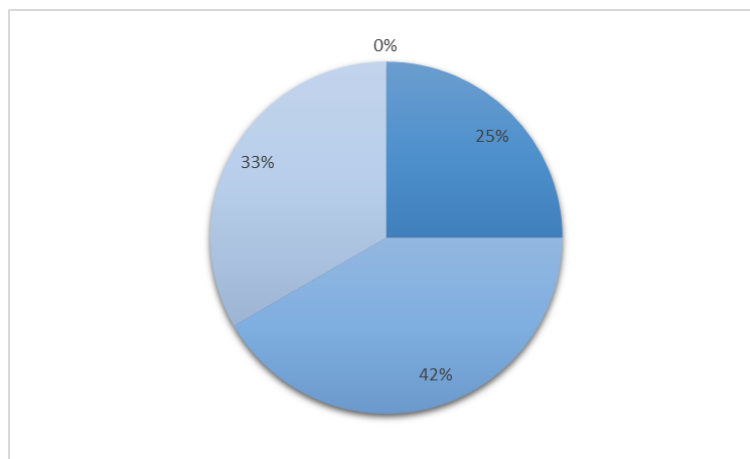


Figura 9. Resultados pregunta 9

Análisis e Interpretación de resultados

Los resultados muestran que el 41.67% de los encuestados está de acuerdo en que un registro automático mejoraría el control de ingreso y salida de personas, mientras que el 33.33% se encuentra muy de acuerdo. Por su parte, el 25% mantiene una posición neutral y ningún encuestado manifestó estar en desacuerdo. Esta distribución evidencia una percepción mayoritariamente favorable hacia la implementación de un registro automático. En ese sentido, los datos reflejan que la mayoría del personal asocia este tipo de mecanismo con una mejora en el control, lo que demuestra un nivel importante de aceptación frente a su posible utilidad dentro del proceso.

Pregunta 10 ¿Qué beneficio considera más importante que debería ofrecer un registro automático a las áreas?

Tabla 16. Resultados pregunta 10

Indicador	Frecuencia	Porcentaje
Mayor seguridad en la salida/ingreso	4	33%
Ahorro de tiempo en los registros	1	8%

Reducción de errores humanos	5	42%
Acceso a la información sin inconsistencias	2	17%

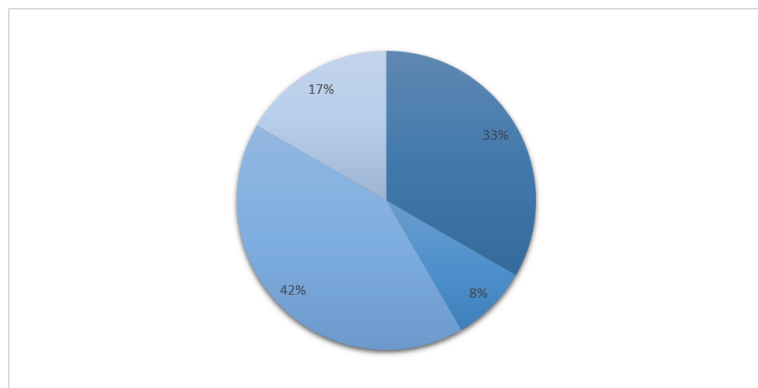


Figura 10. Resultados pregunta 10

Análisis e Interpretación de resultados

Los resultados evidencian que el beneficio considerado más importante de un registro automático es la reducción de errores humanos, con un 41.67%, seguido de una mayor seguridad en la salida e ingreso, con el 33.33%. En menor proporción, el 16.67% de los encuestados destaca el acceso a la información sin inconsistencias y el 8.33% señala el ahorro de tiempo en los registros. Esta distribución permite interpretar que las principales expectativas del personal se concentran en la precisión y la seguridad del proceso. En ese sentido, los datos reflejan que existe una mayor preocupación por minimizar fallas operativas antes que por la rapidez del registro.

c. Fichas de observación

Tabla 17. Ficha de observación

Fecha: 04/04/2026							
Hora de inicio: 8:00 am							
Hora de fin: 11:30 am							
Ubicación: Agencia Riobamba							
Aspectos a observar	Indicador	1	2	3	4	5	Comentario

Procedimiento de control	Existe un protocolo formal para el control de acceso a cajas y bóveda.		x			Se pregunta al encargado de cajas o guardia, pero si es urgente el cajero permite el paso sin más.
Involucramiento de los colaboradores.	El personal con facultades autorizadas interviene de manera proactiva en los procesos de validación de identidad.			x		El procedimiento actual presenta una debilidad en el protocolo de verificación, ya que, si bien se cuestiona el motivo del ingreso, la validación se limita a una consulta superficial sin profundizar en los detalles ni requerir una confirmación jerárquica adicional o una segunda autorización formal.
Bitácora y seguimiento de operaciones.	Documentación y monitoreo de los movimientos de entrada y salida mediante la identificación nominal de cada usuario.			x		En varias ocasiones las personas que ingresaban de manera rápida dejaban solo escribiendo el ingreso y no la salida y la persona dentro se encargaba de eso, pero eso produce una inconsistencia o en casos pude observar que no se firmaba o firmaba de manera incorrecta
Uso de tecnología	Se utilizan herramientas tecnológicas para el control de acceso.		x			Pude presenciar que se acabaron los registros en la libreta y ese momento lo llenaban en un archivo Excel lo cual representa muchos factores poco convenientes en muchos aspectos.
Seguridad en el acceso	Se aplican medidas de		x			Solo se pide que no se ingrese con teléfonos, pero en los casos sin mucho

	seguridad en puntos críticos.						control no se cumplía o en casos se dejaba la puerta abierta.
Control de registro	Se valida el ingreso y la salida del personal por algún encargado una vez fuera la persona.			x			Lo vi en el comportamiento de una persona que veía si el registro estaba bien o si lo llenaban mal se pedía que lo vuelvan a llenar, pero la otra persona encargada no lo tenía presente.
Monitoreo en tiempo real	Existe supervisión en tiempo real de los accesos.		x				El registro se lo llevan al finalizar la jornada, pero como tal no existe un control o un encargado en específico debido a las personas que están allí.
Respaldo de información	Los registros de acceso se almacenan de forma segura.				x		Lo guardan en una carpeta aparte, posteriormente se lo llevan al área de operaciones

Criterio:

- 1= Muy bajo
- 2= Bajo
- 3= Moderado
- 4= Alto
- 5= Muy Alto

2.2.4 Procesamiento y análisis de datos

En función de lo recolectado y siguiendo los lineamientos de cada uno de los métodos de obtención de información se puede evidenciar varias conclusiones significativas

que respaldan la necesidad de implementar un método de control de ingreso en cajas y bóveda de la Cooperativa de Ahorro y Crédito SOL Ltda.

- Se evidencia una circulación constante de personal en áreas sensibles de la institución. En el área de cajas, el 58% de los encuestados indicó que el personal entra y sale frecuentemente, mientras que el 17% señaló que esto ocurre siempre; por su parte, en el área de bóveda, aunque el 67% manifestó que el movimiento ocurre ocasionalmente, un 25% afirmó que se presenta frecuentemente y un 8% siempre. Estos resultados demuestran que se trata de espacios con tránsito real de personal, por lo que requieren mecanismos de control estrictos, permanentes y confiables. Este hallazgo se refuerza con el ítem 6 de la encuesta, en el que se recoge la percepción del personal respecto a la importancia de fortalecer el control, así como con los resultados de las entrevistas a Gerencia y al área de TI, desde donde se reconoce que las áreas de cajas y bóveda son espacios de alta sensibilidad y, por tanto, demandan un control más riguroso.
- La ficha de observación permitió corroborar estas debilidades desde la práctica institucional. Conforme a la escala establecida, el procedimiento de control obtuvo una valoración baja (2/5) además del comentario de la pregunta 2 de la entrevista con el coordinador de TI, debido a que, aunque existe una referencia informal para controlar el ingreso, en la práctica el acceso depende del encargado de cajas o del guardia, e incluso, cuando la situación se considera urgente, el cajero permite el paso sin una validación más rigurosa. Esto evidencia la inexistencia de un protocolo formal plenamente estructurado y aplicado de manera uniforme. Lo que desemboca no solo en inconsistencias en informes de registro sino en no poder evidenciar en papel incidentes y tener que recurrir a cámaras o métodos más lentos para sustentar los incidentes.
- En cuanto a la gestión de registros y la trazabilidad, la ficha de observación obtuvo una calificación intermedia (3/5). En coherencia, más del 67% de los encuestados reportó inconsistencias en la información. Esto refleja que, por la premura, el personal a menudo registra únicamente el ingreso, trasladando la responsabilidad del egreso a terceros, además de detectarse firmas faltantes o erróneas. En conjunto, estos factores impiden asegurar una trazabilidad íntegra, aumentando el

riesgo de errores documentales y limitando la eficacia de las auditorías institucionales.

- La entrevista bajo los dos entes aplicados exactamente en la pregunta 4 evidencia que la percepción de los controles tradicionales no están orientados en mejoras actuales debido a que tanto la experiencia actual es muy tediosa y no genera resultados como se puede evidenciar de manera paralela en la pregunta 9 de la encuesta aplicada donde se pregunta si considera que un registro automático ayudaría de manera significativa donde 42% de los encuestados está de acuerdo y 33% de los encuestados está muy de acuerdo.
- En conjunto, los hallazgos obtenidos permiten establecer que la problemática central no se limita únicamente a la existencia de un control manual, sino a la baja estandarización del procedimiento, la escasa confiabilidad del registro, la limitada validación de identidad, la ausencia de monitoreo permanente y la débil integración tecnológica. Esta situación reduce la capacidad institucional para prevenir accesos indebidos, garantizar trazabilidad completa y disponer de información precisa para procesos de supervisión y auditoría. Tomando en cuenta lo dicho, respuestas obtenidas tanto por entes de control como personal que participa en el flujo el usar un modelo de reconocimiento facial propuesto tanto en la encuesta como en las entrevistas a percepción de los encuestados y entrevistados lo ven como una alternativa viable en función de las necesidades y problemas.

CAPÍTULO III. RESULTADOS Y DISCUSIÓN

3.1 Situación actual del control de acceso en las áreas de cajas y bóveda

Las áreas de cajas y bóveda de la Cooperativa de Ahorro y Crédito SOL constituyen espacios críticos dentro de la institución, debido a que en ellas se manipulan valores monetarios, documentación sensible y recursos que requieren un control estricto de ingreso. Por esta razón, el acceso a estas áreas no puede ser tratado como un proceso operativo común, sino como una actividad directamente relacionada con la seguridad física, la trazabilidad institucional y la protección de activos.

El acceso a dichas áreas está resguardado por un sistema de autenticación biométrica situado en la entrada. Esta tecnología restringe el ingreso exclusivo a un personal selecto —específicamente cajeras, el responsable de seguridad física y el gerente—, quienes cuentan con autorización previa fundamentada en la naturaleza de sus cargos y la recurrencia operativa requerida para operar en los espacios de manejo de efectivo y bóvedas. Pese a que existe un control biométrico este no genera una trazabilidad digital completa.

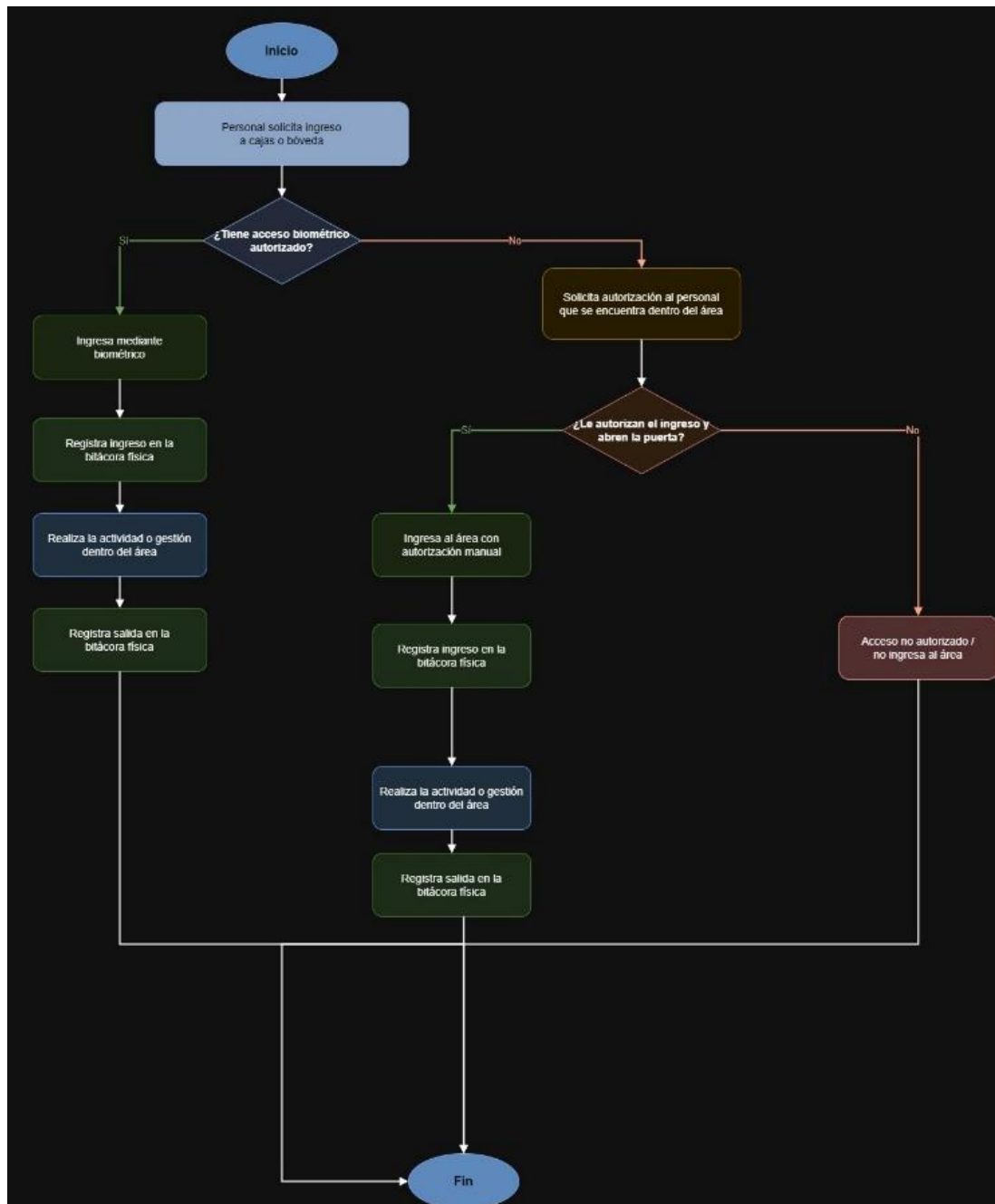


Figura 11. Situación actual de acceso al sistema

Sin embargo, existen casos en los que otras personas también requieren ingresar a estas áreas, ya sea por actividades de supervisión, soporte, mantenimiento, auditoría interna u otros procesos administrativos. En estos casos, el ingreso no se realiza de forma autónoma mediante el sistema biométrico, sino que depende de la autorización de una persona responsable que permita el acceso y abra la puerta. Una vez dentro del área

restringida, la persona debe registrar su ingreso en una bitácora física, donde se deja constancia de la visita o actividad realizada.

El protocolo vigente integra la autenticación biométrica con un registro físico posterior al acceso. Si bien este modelo aporta un control parcial, presenta fallas significativas, sobre todo cuando la entrada está sujeta a validaciones verbales o manuales, supeditando la trazabilidad a la exactitud y oportunidad del llenado de la bitácora.

Adicionalmente, el uso de registros físicos entorpece la consulta histórica, al exigir una revisión manual que impide la generación ágil de informes, el análisis de patrones de comportamiento y la auditoría inmediata de los movimientos en zonas de alta criticidad, como cajas y bóvedas. Esta ineficiencia evidencia una clara oportunidad para optimizar la precisión y la capacidad de verificación de los controles.

Ante este panorama, surge la necesidad de implementar una solución automatizada que valide identidades, registre cada evento y provea datos estructurados para el monitoreo de seguridad. Bajo este enfoque, el reconocimiento facial se presenta como una alternativa tecnológica idónea para robustecer el control actual, minimizando la dependencia de procesos manuales y garantizando una trazabilidad integral.

La matriz de riesgos estructurada a partir del diagrama de la Figura 12 expone las grandes vulnerabilidades del acceso manual a la bóveda, iniciando con la solicitud de autorización donde existe un peligro crítico de ingeniería social por la dependencia de la decisión humana, lo cual podría provocar un ingreso indebido con probabilidad alta, además cuando el encargado abre la puerta se presenta un riesgo alto por posible colusión, esto se debe directamente a la carencia de un protocolo digital o de un doble factor para validar la verdadera identidad.

Continuando con el flujo del proceso se nota que la escritura en la bitácora física acarrea un peligro alto de falsificación de información, ya que al ser un método manual propicia la alteración de la información, lo cual compromete la integridad de las auditorías subsiguientes y, en última instancia, el mayor peligro radica en la falta de trazabilidad cuando se omite por completo el registro de la visita, esto genera un riesgo crítico de pérdida de control sobre el área, haciendo imposible rastrear a los verdaderos responsables al presentarse un incidente dentro de las instalaciones.

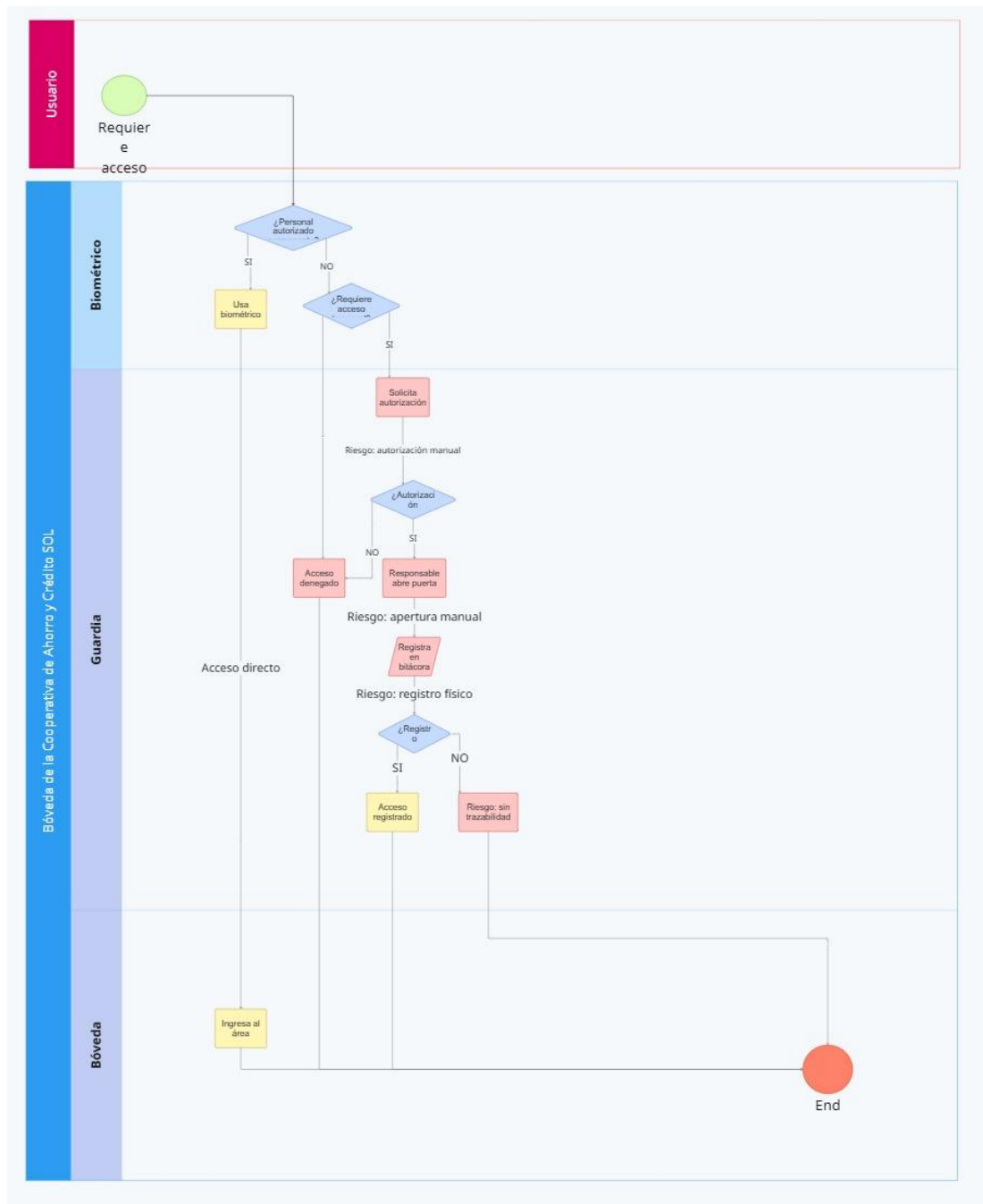


Figura 12. Diagrama de la matriz de riesgos BPMN

Tabla 18. Matriz de riesgo BPMN de acceso actual a la Bóveda de la Cooperativa de Ahorro y Crédito SOL

Actividad / Nodo BPMN	Riesgo Identificado	Causa Raíz	Impacto	Probabilidad	Nivel de Riesgo
Solicita autorización	Ingeniería Social / Acceso no autorizado	Dependencia de la validación verbal o humana.	Muy Alto (Acceso indebido a la bóveda)	Alta	Crítico
Responsable abre puerta	Error humano / Colusión	Falta de protocolo de validación digital o de doble factor.	Alto (Vulneración de la seguridad física)	Media	Alto
Registra en bitácora	Falsificación o error en el registro	Proceso manual y sin integridad de datos (es fácil escribir información falsa).	Medio (Falla en la auditoría)	Alta	Alto
Riesgo: sin trazabilidad	Pérdida total de control	Omisión del registro (la decisión de no registrar termina en el fin del proceso sin control).	Crítico (Imposibilidad de auditar un incidente)	Media	Crítico

3.2 Limitaciones, riesgos y requerimientos del proceso actual

A partir del análisis del proceso actual de ingreso a las áreas de cajas y bóveda, se evidencia que la Cooperativa de Ahorro y Crédito SOL cuenta con un mecanismo de control basado en autenticación biométrica para el personal autorizado. Sin embargo, cuando el ingreso corresponde a personas que no tienen acceso directo mediante el proceso se fundamenta en una validación biométrica complementada por una autorización interna y el asiento de los movimientos en una bitácora física.

La bitácora utilizada actualmente permite registrar información básica del ingreso, como el nombre de la persona, departamento, tema u objetivo de la visita, hora de

ingreso, hora de salida, firma y observaciones. Este formato permite dejar una constancia general de quién ingresó y con qué finalidad.

El registro manual depende totalmente del cumplimiento de quien anota los datos y de quien supervisa su veracidad, pues la intervención directa del personal genera fallas si la persona omite detalles, escribe información errónea o dilata el momento del llenado, lo cual perjudica el seguimiento de los ingresos en espacios donde se gestionan recursos de valor y resulta en una vulnerabilidad de seguridad al impedir la verificación clara de la identidad, el tiempo exacto y la validez del permiso de acceso.

La imposibilidad de efectuar consultas ágiles o automatizadas sobre los ingresos pasados constituye un problema añadido, ya que la necesidad de revisar físicamente la bitácora para buscar datos previos, detectar tendencias, confirmar jornadas laborales o preparar informes genera demoras, propicia interpretaciones equivocadas y complica la obtención de pruebas cuando ocurren auditorías, anomalías internas o inspecciones de seguridad.

Este modelo carece de mecanismos para capturar por cuenta propia los intentos de ingreso sin éxito, puesto que no deja constancia documental de las personas ajenas al área o de situaciones de suplantación, lo cual obstaculiza las labores de prevención al impedir la identificación de comportamientos anómalos previo a la materialización de algún suceso negativo.

El esquema vigente arrastra peligros vinculados a la autorización hecha por personas, a la carencia de respaldos digitales, a la frecuente falta de registros y a la complejidad para auditar los ingresos al momento de suceder, de modo que, pese al uso de dispositivos biométricos para el personal habilitado, el procedimiento manual requiere ser sustituido por una herramienta técnica que agrupe la identificación, el asiento de datos y la creación de reportes.

Por esta razón, se establecen los siguientes requerimientos para el diseño de la solución propuesta:

Tabla 19. Requerimientos de la propuesta de solución

Tipo de requerimiento	Descripción
Identificación del personal	El mecanismo técnico requiere la detección biométrica de los rostros de los trabajadores permitidos como paso previo indispensable para conceder el ingreso o generar el asiento de entrada, ya que esta validación garantiza que únicamente los individuos debidamente acreditados tengan acceso a las instalaciones, pues el sistema compara los rasgos físicos con una base de datos preexistente y asegura que la identidad coincida con los permisos asignados, además de evitar la suplantación de personas al automatizar el proceso de verificación sin depender de la voluntad humana.
Registro automático	Cada intento de entrada exige el almacenamiento inmediato y desatendido de los datos, pues el dispositivo debe archivar la fecha exacta, la hora precisa, la identidad del trabajador reconocido y el desenlace de la operación, lo cual permite generar un historial ordenado que facilita la revisión posterior de los movimientos, ya que esta metodología elimina la brecha de información causada por la omisión voluntaria o involuntaria de los registros, además de otorgar una fuente de consulta veraz para aclarar cualquier eventualidad, supervisar la puntualidad del personal o auditar los flujos de trabajo en el área resguardada.
Control de accesos no autorizados	La herramienta debe catalogar y clasificar los ingresos según su desenlace, pues el equipo tiene la tarea de separar los eventos permitidos de aquellos rechazados, lo cual permite distinguir con claridad los patrones de comportamiento diario, ya que el desglose entre quién logra entrar y quién es bloqueado ayuda a detectar posibles amenazas o riesgos sin esperar a que ocurra algún daño, además de proporcionar una base de datos organizada para comparar los intentos legítimos frente a las tentativas de intrusión, pues esta distinción aporta una visión clara sobre el estado de la seguridad en el área, permitiendo

	tomar medidas de protección más efectivas según la frecuencia de los ingresos rechazados.
Trazabilidad	Los registros deben guardarse en un repositorio digital centralizado que organice toda la actividad, pues esta disposición permite ejecutar búsquedas veloces, realizar comprobaciones detalladas para auditorías y mantener una vigilancia constante sobre el historial de los movimientos, ya que la digitalización de los datos elimina la fragmentación propia del papel, facilita la extracción de informes precisos en cualquier momento y permite que los responsables tengan a mano una fuente de información segura para identificar irregularidades, analizar comportamientos a través del tiempo y asegurar la integridad de los recursos bajo protección.
Reportes	La herramienta debe posibilitar la creación de hojas de cálculo con el historial de los movimientos, pues esta función permite exportar los datos recopilados hacia formatos de uso común para facilitar la lectura, el procesamiento de las cifras y la creación de reportes detallados sobre la actividad del personal, ya que la capacidad de transformar los registros digitales en archivos manejables otorga libertad a los supervisores para organizar la información según sus necesidades específicas, realizar cálculos de tiempo, crear tablas comparativas de accesos y presentar la documentación necesaria ante cualquier proceso de control, pues esto simplifica el manejo administrativo y mejora la claridad con la que se presentan los resultados obtenidos diariamente.
Seguridad	El mecanismo debe desplazar la anotación física para disminuir la vulnerabilidad ante errores o descuido humano, pues al instaurar un entorno digital se garantiza que cada interacción quede grabada mediante procesos técnicos automatizados, ya que el paso hacia un formato electrónico otorga validez probatoria a las operaciones de ingreso, elimina el riesgo de omisión por parte del personal y crea un respaldo permanente

	que sirve para certificar la veracidad de los hechos sin los inconvenientes de la bitácora tradicional, además de dotar a la organización de un control más firme al asegurar que toda acción sea capturada de forma inmediata, inalterable y auditable.
Eficiencia	La verificación de la identidad debe ejecutarse con prontitud para evitar contratiempos que entorpezcan el flujo de trabajo cotidiano de los empleados, pues el sistema ha de procesar los datos biométricos de manera instantánea y desatendida, ya que esta agilidad permite que el personal acceda a su lugar de labor sin esperas innecesarias ni obstáculos que alteren la continuidad de sus tareas, pues la eficiencia en la respuesta técnica asegura que la protección del área y la productividad del grupo avancen al mismo tiempo, sin que las medidas de seguridad se conviertan en una carga operativa para quienes tienen el permiso de ingresar.

La propuesta consiste en la creación de un modelo práctico que utiliza la identificación de rostros mediante una lente encargada de obtener la imagen, un equipo central para guardar los datos y un programa instalado en la computadora creado con el lenguaje Python, pues esta herramienta tiene el propósito de sumar capacidades al mecanismo biométrico ya instalado, organizar por sí mismo el historial de ingresos y elevar el nivel de vigilancia en los espacios de mayor riesgo dentro de la entidad, ya que el uso de estas tecnologías asegura que la gestión de los accesos pase de una tarea física a una tarea digital, garantizando así una supervisión más precisa, una respuesta técnica veloz y un control sobre los recursos de la cooperativa mucho más sólido al eliminar los vacíos que el procedimiento manual dejaba anteriormente.

3.3 Diseño general del sistema propuesto con Deep Learning

El sistema informático fue concebido como una solución de control de acceso automatizado para las áreas protegidas de cajas y bóvedas de la Cooperativa de Ahorro y Crédito SOL, integrando técnicas de visión artificial junto con el procesamiento digital de imágenes para identificar a los empleados, desde un punto de vista operativo

la arquitectura del programa permite capturar el rostro del usuario en la puerta de ingreso, procesando esta información visual mediante un modelo preentrenado para comparar la identidad con el directorio local de fotografías, culminando con el registro del suceso en un archivo de texto para facilitar la revisión administrativa.

La arquitectura de la herramienta tecnológica se estructuró mediante una organización por módulos independientes para delimitar las tareas de adquisición de video y el tratamiento de los datos, logrando de esta manera una gestión eficiente sobre los procesos de validación biométrica y el almacenamiento seguro de las transacciones diarias, esto permite que el mantenimiento futuro del código fuente se realice con mayor facilidad sin alterar el funcionamiento general, garantizando así que cada bloque de programación ejecute una instrucción específica dentro del flujo de seguridad diseñado para la institución financiera.

Para estructurar la herramienta bajo los parámetros del aprendizaje automático se definió una tubería de procesamiento que detalla el ciclo de los datos dentro del aplicativo, iniciando con la extracción continua de los fotogramas en vivo para aplicar un preprocesamiento que convierte los píxeles a una escala de grises, logrando así aislar la zona exacta de la cara antes de enviarla a la red neuronal convolucional para la ejecución de este modelo permite la valoración objetiva de cada situación, de manera que la puesta en marcha definitiva logra automatizar la elección sobre el ingreso de los trabajadores, pues el sistema procesa los permisos mediante reglas preestablecidas que eliminan la intervención manual, lo cual otorga una mayor fluidez a la operación al decidir al instante quién cuenta con la habilitación necesaria para acceder, además de asegurar que los criterios de seguridad se apliquen sin excepciones ni posibles errores de juicio, pues al delegar esta acción en una herramienta técnica se garantiza que las normas de la cooperativa se cumplan de forma estricta y constante en cada punto de control.

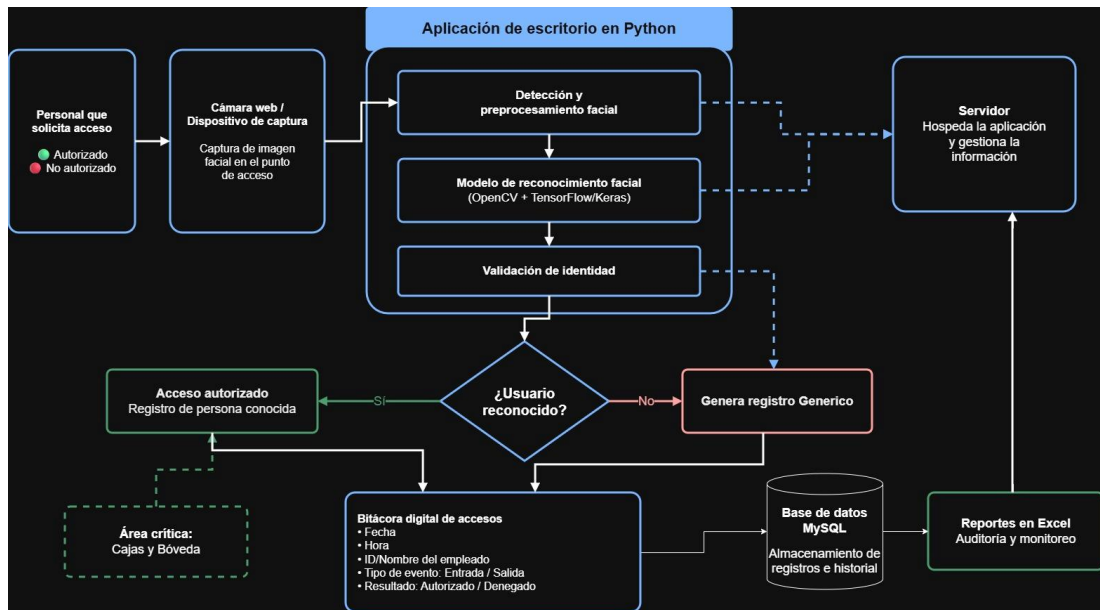


Figura 13. Lógica de funcionamiento del programa con Deep learning

3.3.1 Técnica de Machine Learning

El desarrollo de este sistema de control de acceso se fundamenta en un enfoque híbrido de Aprendizaje Supervisado que combina la Visión Artificial tradicional con el Aprendizaje Profundo (Deep Learning). Operativamente, el modelo se divide en dos etapas:

- 1) Fase de Detección (Localización espacial): Se emplea una técnica clásica de Machine Learning basada en el Algoritmo de Viola-Jones mediante Clasificadores en Cascada (Haar Cascades). Esta técnica escanea los fotogramas en escala de grises buscando patrones de contraste rápido (como la zona oscura de los ojos frente a las mejillas) para localizar las coordenadas exactas del rostro en tiempo real.
- 2) La etapa inicial emplea el aprendizaje transferido para validar la identidad sin incurrir en gastos informáticos elevados, ya que se aprovecha una red neuronal convolucional previamente adiestrada, como la arquitectura VGG-Face disponible en el marco de trabajo DeepFace, pues este modelo dispone de la facultad de obtener rasgos faciales complejos al haber procesado una enorme cantidad de muestras visuales previamente.

Dentro de las instalaciones, la herramienta emplea un modelo de aprendizaje supervisado mediante la técnica de comparación única, pues el sistema transforma el rostro detectado en un vector numérico de varias dimensiones y establece la diferencia respecto a una sola imagen de prueba guardada en el archivo, permitiendo que la máquina determine si el ingreso debe ser aprobado o rechazado según la proximidad entre ambos datos, logrando así una distinción clara y directa para el control del acceso.

3.3.2 Métricas de Validación

Para asegurar la fiabilidad y protección del programa en un espacio de alto riesgo como el área de cajas y bóveda de la institución financiera, el funcionamiento del algoritmo debe medirse utilizando métricas específicas de clasificación biométrica. Por consiguiente, se seleccionó la exactitud (Accuracy) junto con la matriz de confusión como los parámetros de evaluación principales para este desarrollo.

El parámetro de exactitud permite evaluar la tasa global de aciertos del motor de inteligencia artificial, al considerar tanto los ingresos concedidos correctamente a los empleados permitidos como los bloqueos ejecutados eficazmente ante individuos no reconocidos, de manera que la medición arroja un valor numérico directo que permite conocer la eficacia de la red neuronal para diferenciar con precisión los rostros capturados por el dispositivo visual, pues esta métrica sirve para comprobar si el modelo matemático cumple con las metas de seguridad establecidas al discriminar adecuadamente entre quien tiene permiso y quien debe ser excluido del área.

Por otro lado, la matriz de confusión se emplea para desglosar detalladamente los resultados obtenidos por el modelo de seguridad durante las pruebas controladas. Esta herramienta permite clasificar cada intento de acceso en verdaderos positivos, verdaderos negativos, falsos positivos y falsos negativos según corresponda a la realidad. Esto permite visualizar gráficamente si el aplicativo confunde las identidades o si mantiene una precisión inalterable al momento de autorizar a los empleados de la cooperativa.

3.3.3 Selección del modelo

La selección de la arquitectura VGG-Face combinada con los algoritmos de Haar Cascades se apoya en varios motivos técnicos que garantizan la viabilidad del

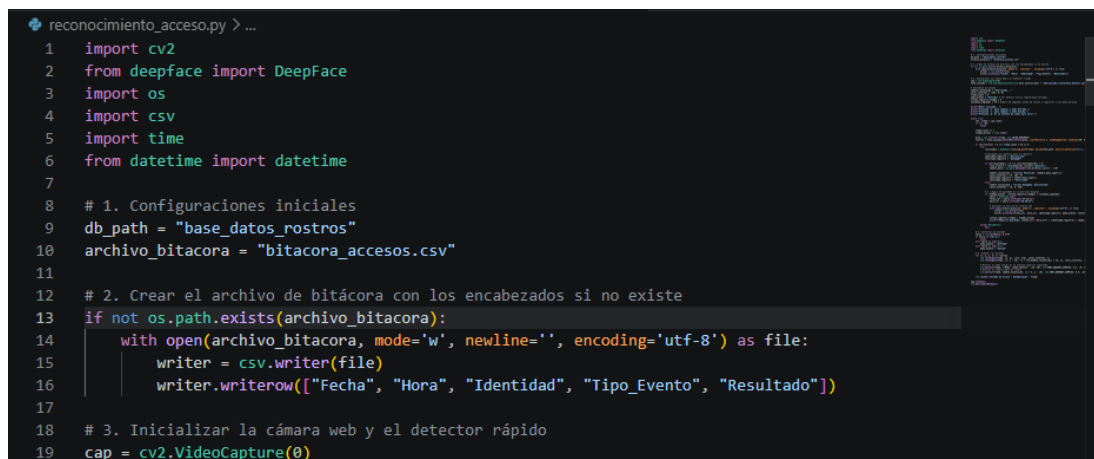
proyecto, por consiguiente en la Tabla 20 se detallan los factores determinantes para esta decisión tecnológica, abarcando la capacidad del modelo para reconocer identidades utilizando una sola imagen de referencia junto a su alta tolerancia frente a los cambios de iluminación o postura del empleado, consiguiendo de esta manera un equilibrio adecuado entre la exactitud biométrica y el procesamiento del equipo informático sin requerir servidores especializados.

Tabla 20. Justificación de la Selección del Modelo con Deep Face

Criterio de Selección	Justificación Técnica	Beneficio Operativo en la Cooperativa
Transfer Learning y One-Shot Learning	Uso de la arquitectura preentrenada VGG-Face que hereda la capacidad de extraer características profundas tras haber sido entrenada con millones de imágenes.	Permite autenticar al personal utilizando una única fotografía de referencia en la base de datos, eliminando la necesidad de entrenar la red desde cero o requerir hardware masivo.
Robustez frente a Variaciones	Las redes neuronales convolucionales poseen una alta resistencia frente a deformaciones en la ubicación de los elementos visuales y a cambios complejos en la intensidad de los puntos que forman la imagen, pues esta capacidad les permite identificar rasgos faciales sin importar que el rostro presente giros, cambios en la iluminación o variaciones en la postura ante la cámara, ya que el diseño de estas arquitecturas logra filtrar las características esenciales de la figura humana pese a las alteraciones en la disposición de los datos visuales, garantizando así que el proceso de comparación sea estable ante el movimiento natural	El modelo conserva un nivel elevado de eficacia ante los diversos cambios del entorno donde se ubican las cajas o la bóveda, pues la tecnología procesa adecuadamente tanto las modificaciones en la claridad del ambiente como el paso del tiempo en las facciones de las personas o las distintas posturas del rostro frente al lente, ya que la arquitectura de la red reconoce los patrones básicos que definen la identidad sin verse afectada por los giros de cabeza, el envejecimiento natural o la falta de luz uniforme, lo cual asegura que el control de acceso funcione de manera estable en condiciones reales de trabajo y garantice la seguridad del

Criterio de Selección	Justificación Técnica	Beneficio Operativo en la Cooperativa
	de las personas al acercarse al punto de acceso.	área sin interrupciones causadas por factores externos.
Equilibrio Precisión/Rendimiento	La arquitectura propone un modelo combinado que delega la búsqueda inicial de rostros al algoritmo ligero denominado Haar Cascades, mientras que la autenticación mediante la red neuronal ocurre únicamente en momentos específicos al procesar uno de cada treinta cuadros, lo cual permite que el equipo dedique menos potencia computacional a la tarea de rastreo constante y deje la carga de procesamiento pesada solo para la etapa de verificación, consiguiendo así que el sistema funcione con rapidez y eficiencia sin calentar el procesador ni desperdiciar recursos, logrando un equilibrio entre una vigilancia atenta del entorno y una validación de identidad técnica, precisa y veloz para el personal.	Esta estrategia de diseño impide que la transmisión de video se trabe por exceso de trabajo en el procesador, pues la carga computacional disminuye al optimizar las tareas, lo que permite que el programa funcione de forma continua y sin demoras en los equipos estándar que ya utiliza la cooperativa sin necesidad de adquirir servidores con capacidades técnicas de alto costo, ya que la gestión inteligente de los cuadros de imagen asegura una ejecución veloz y estable, permitiendo que la seguridad opere con fluidez en tiempo real sobre la infraestructura tecnológica existente.

Para detallar la construcción interna de la herramienta tecnológica a continuación se expone una captura directa del código fuente estructurado en el lenguaje Python, dentro de este bloque de programación se organizan las instrucciones necesarias para inicializar la transmisión de video y cargar el clasificador matemático, permitiendo entrelazar la lectura de los fotogramas con el motor de inteligencia artificial para ejecutar la comparación de las características físicas, logrando de esta manera un procesamiento continuo que administra los accesos de los empleados hacia las zonas protegidas de la cooperativa.



```

reconocimiento_acceso.py > ...
1  import cv2
2  from deepface import DeepFace
3  import os
4  import csv
5  import time
6  from datetime import datetime
7
8  # 1. Configuraciones iniciales
9  db_path = "base_datos_rostros"
10 archivo_bitacora = "bitacora_accesos.csv"
11
12 # 2. Crear el archivo de bitácora con los encabezados si no existe
13 if not os.path.exists(archivo_bitacora):
14     with open(archivo_bitacora, mode='w', newline='', encoding='utf-8') as file:
15         writer = csv.writer(file)
16         writer.writerow(["Fecha", "Hora", "Identidad", "Tipo_Evento", "Resultado"])
17
18 # 3. Inicializar la cámara web y el detector rápido
19 cap = cv2.VideoCapture(0)

```

Figura 14. Código del reconocimiento facial con Deep Face

3.3.4 Preprocesamiento

El sistema ejecuta una fase de preprocesamiento sobre el flujo de video en tiempo real para optimizar los datos capturados y reducir la carga computacional. Este proceso se divide en las siguientes etapas:

- 1) **Conversión de Espacio de Color:** Los fotogramas capturados inicialmente en formato BGR (Blue, Green, Red) son convertidos a escala de grises. Esta reducción de dimensionalidad elimina la información de color innecesaria, acelerando significativamente el algoritmo de detección espacial.
- 2) **Detección y Extracción de la Región de Interés (ROI):** Emplea clasificadores en cascada de Haar para explorar el cuadro de video en tonos grises, de manera que el programa localiza las coordenadas precisas del rostro y procede a recortar únicamente esa porción para descartar cualquier elemento extraño del entorno, pues esta acción garantiza que la red trabaje solo con la información necesaria.
- 3) **Normalización y Alineación Facial:** La plataforma DeepFace ejecuta un proceso de limpieza adicional que ajusta la posición de puntos específicos como los ojos y la boca, además de ajustar el tamaño de la imagen hasta coincidir con las medidas que la arquitectura de la red neuronal necesita, pues al estandarizar los valores de los píxeles se asegura que los cálculos matemáticos ocurran bajo condiciones estables, garantizando así una lectura uniforme durante la fase de reconocimiento.

El preprocesamiento de la imagen se ejecuta en el bucle principal del sistema, procesando el flujo de video en tiempo real antes de realizar la inferencia en el modelo de Deep Learning. A continuación, se presenta el fragmento de código responsable de esta fase:

Tabla 21. Fragmentos del código del preprocesamiento de la imagen

1. Captura del fotograma en bruto (formato BGR por defecto en OpenCV)
<code>ret, frame = cap.read()</code>
2. Conversión a escala de grises (Reducción de dimensionalidad)
<code>gray = cv2.cvtColor(frame, cv2.COLOR_BGR2GRAY)</code>
3. Detección espacial del rostro (Localización de la Región de Interés - ROI)
<code>rostros = face_cascade.detectMultiScale(gray, scaleFactor=1.1, minNeighbors=5, minSize=(50, 50))</code>
4. Inferencia y Preprocesamiento Profundo (Alineación y Normalización interna)
<pre># Se ejecuta 1 vez cada 30 fotogramas para no saturar el procesador if len(rostros) > 0 and frame_count % 30 == 0: resultados = DeepFace.find(img_path=frame, db_path=db_path, enforce_detection=False, silent=True)</pre>

La instrucción `cv2.cvtColor` transforma la información visual desde el esquema de tres colores a una representación en tonos grises, de manera que esta modificación disminuye notablemente el tamaño de los datos del cuadro para permitir que el análisis matemático del sistema trabaje con mayor velocidad, pues procesar una sola capa simplifica las operaciones necesarias para rastrear el rostro.

La función `detectMultiScale` utiliza el mecanismo de Haar Cascades sobre la imagen ya procesada, donde la configuración de parámetros específicos actúa como un filtro que descarta elementos innecesarios, asegurando que el sistema únicamente identifique y aisle aquellas áreas que coinciden con la geometría de una cara humana, siempre que cumplan con la medida mínima de cincuenta por cincuenta píxeles, evitando así falsas detecciones provenientes del fondo o de objetos ajenos.

Finalmente, el método DeepFace.find realiza la predicción definitiva mediante un proceso interno que toma el cuadro original y detecta la posición de los ojos y la boca para alinear el rostro de manera frontal, pues ajusta el tamaño al formato que demanda la estructura VGG-Face y estandariza los valores de cada punto de luz, logrando así que el vector biométrico resultante sea preciso para comparar la identidad con la base de datos, garantizando una validación coherente antes de emitir cualquier resultado.

3.3.5 Arquitectura funcional del sistema

La arquitectura global del sistema se organiza a través de cinco componentes vinculados entre sí, de modo que el movimiento de los datos mantiene una secuencia lógica y ordenada, pues el diseño asegura que cada paso desde la captura visual hasta la entrega del resultado final ocurra bajo un esquema de trabajo estructurado, permitiendo que la información fluya sin interrupciones entre las distintas etapas de procesamiento, garantizando así que la verificación de la identidad sea un proceso coherente, ininterrumpido y eficiente para las necesidades operativas de la cooperativa. Iniciando con la captura de video en tiempo real mediante las funciones de OpenCV, para luego avanzar hacia el análisis de los rostros empleando la librería DeepFace, prosiguiendo con la verificación de la identidad para conceder o negar el ingreso, culminando con el almacenamiento de estos sucesos y la gestión administrativa de los registros, asegurando así un desempeño óptimo durante las validaciones.

a. Módulo de captura de imagen

El primer bloque comprende el módulo de captura, integrado por una cámara web o un aparato encargado de obtener la imagen instalado en la entrada de los espacios restringidos, pues su labor consiste en registrar en el momento preciso el rostro de quien pide el acceso, asegurando una nitidez adecuada para los pasos siguientes, ya que este elemento funciona como el punto de contacto físico entre el usuario y la plataforma, razón por la cual su emplazamiento, su capacidad de resolución y su firmeza determinan en gran medida la eficacia del reconocimiento facial.

Tabla 22. Parámetros de módulo de captura de imagen

Parámetro	Descripción
Marca	SINOVISION
Modelo	MFPT20
Clasificación de resistencia al agua	IP66
Movimiento	PTZ
Control	App, PC, remoto
Conectividad	IP, LAN, Wi-Fi
Resolución	2MP
Distancia focal de lente	3.6 mm
Sensor de imagen	1/2.7" BSI Sensor
Resolución de video	Full HD
Compresión de video	H265
Tipo de almacenamiento	Micro-SD, nube, NVR
Capacidad de almacenamiento	64GB
Alimentación	12 V
Consumo	2.1W
Asistentes virtuales compatibles	Alexa, Google Assistant, Siri

b. Módulo de procesamiento e identificación facial

Una vez capturada la imagen del usuario en el punto de acceso como se puede observar en la Figura 15, esta es enviada a la aplicación de escritorio desarrollada en Python 3.11.9, garantizando de esta manera la compatibilidad absoluta con las librerías matemáticas donde se ejecuta el procesamiento facial inicial, este módulo comprende las etapas de detección de rostro, además del preprocesamiento de la imagen y la generación de la región de interés conocida como ROI facial.

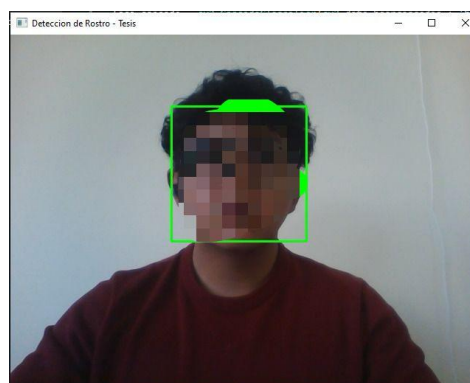


Figura 15. Identificación de rostro en el punto de acceso

La Figura 16 detalla el funcionamiento en tiempo real de la herramienta de seguridad ejecutada desde la computadora, allí el algoritmo detecta el rostro del individuo para luego examinar la carpeta de archivos buscando la coincidencia matemática exacta, además dentro de la pantalla interactiva se visualiza el texto de acceso permitido confirmando así la validación biométrica del empleado, asimismo en la esquina superior se aprecia la configuración manual para registrar el paso alternando entre entradas y salidas, consolidando finalmente un historial ordenado de los movimientos y logrando una demostración visual del código operando con éxito.

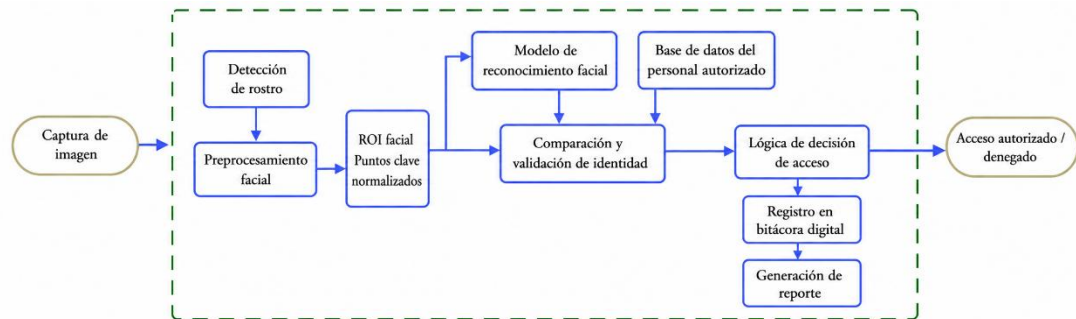


Figura 16. Enfoque de procesamiento para control de acceso con reconocimiento facial

En la etapa de detección el sistema localiza automáticamente el rostro dentro del fotograma capturado por la cámara web, esta fase permite descartar cuadros de video que no contienen un rostro válido para agilizar el proceso de reconocimiento, posteriormente en la etapa de preprocesamiento se aplican operaciones como la conversión a escala de grises y el recorte de la región facial, con el propósito de reducir variaciones provocadas por la iluminación o la distancia.

Como resultado de este procesamiento matemático se obtiene una ROI facial normalizada, la cual representa la matriz exacta de píxeles que será analizada por el modelo de inteligencia artificial de DeepFace, en esta etapa también se consideran puntos de referencia faciales para alinear la imagen, logrando así mejorar la consistencia de entrada al modelo especialmente cuando existen pequeñas variaciones en la posición del usuario frente a la cámara.

El modelo de reconocimiento facial profundo recibe la imagen procesada y genera una representación vectorial asociada al usuario capturado, esta salida numérica no constituye por sí sola una autorización directa de acceso a las áreas restringidas, sino que es enviada al módulo de comparación y validación de identidad, donde se contrasta asincrónicamente con la información almacenada en la base de datos del personal autorizado como podemos observar la carpeta “base_datos_rostros” en la Figura 17.

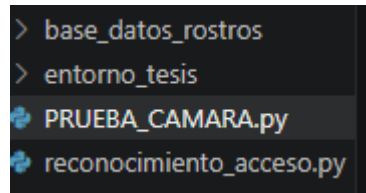


Figura 17. Carpeta donde se colocarán los rostros autorizados

c. Módulo de validación de identidad y decisión de acceso

El módulo de validación de identidad y decisión de acceso conforma el núcleo lógico del programa elaborado, debido a que convierte el resultado del reconocimiento facial en una decisión operativa directa para autorizar o denegar el ingreso a las áreas de cajas y bóveda, este bloque recibe como entrada el fotograma procesado junto con la predicción generada por el motor de inteligencia artificial, comparando estos datos con el repositorio local de fotografías del personal.

El proceso inicia con la comparación matemática entre el rostro capturado en vivo y los vectores almacenados en el archivo de representaciones neuronales de la computadora, para ello el algoritmo verifica asincrónicamente si el usuario cuenta con una imagen válida dentro de la carpeta de la base de datos, evaluando las similitudes de los rasgos faciales para aceptar la coincidencia y descartando aquellas capturas que corresponden a personas ajenas a la cooperativa.

La lógica de decisión del código fue definida considerando los escenarios que pueden presentarse durante el monitoreo de la cámara web, cuando el rostro es detectado correctamente y el sistema encuentra una similitud exacta se extrae el nombre del empleado para generar un aviso de acceso permitido como se puede apreciar en la Figura 18.

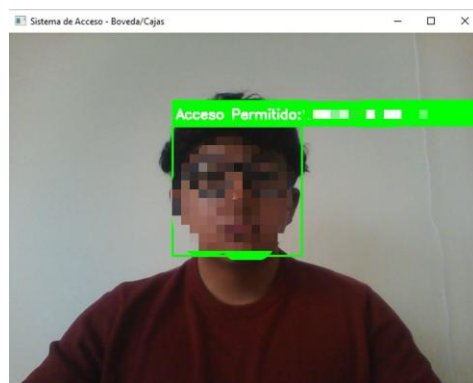


Figura 18. Acceso permitido del usuario

Por el contrario, si el individuo es desconocido se emite una alerta visual de color rojo para denegar de inmediato el paso hacia la zona de seguridad esto se puede observar en la Figura 19.



Figura 19. Acceso denegado del usuario

Mediante la arquitectura programada en Python la herramienta ejecuta esta validación biométrica tomando únicamente un cuadro por cada treinta capturas de video, esta estrategia matemática garantiza que la interfaz interactiva mantenga una fluidez constante sin congelar el equipo durante las comprobaciones, a continuación, la Tabla 23 resume las condiciones exactas utilizadas en el script para gestionar las autorizaciones de las personas.

Tabla 23. Condiciones utilizadas de validación y acceso

Condición evaluada por el algoritmo	Acción ejecutada por el sistema	Resultado visual
-------------------------------------	---------------------------------	------------------

Rostro detectado en el fotograma y empleado reconocido mediante coincidencia en el directorio local	Se extrae el nombre del archivo y se autoriza la identidad del usuario	Acceso Permitido (Recuadro Verde)
Rostro detectado en pantalla, pero la persona no cuenta con una imagen en la base de datos	Se rechaza la solicitud al no encontrar coincidencias matemáticas válidas	Acceso Denegado (Recuadro Rojo)
No se detecta ningún rostro dentro de los parámetros de tamaño mínimo del clasificador	El motor de inteligencia artificial omite el análisis para no saturar la memoria	Analizando... (Recuadro Azul)

d. Módulo de bitácora digital de accesos

Independientemente del resultado de la comprobación biométrica el sistema genera un archivo de texto en formato de valores separados por comas para guardar cada suceso, esta bitácora digital almacena los datos necesarios para el monitoreo del acceso incluyendo la fecha, la hora exacta, el nombre del empleado cuando existe una coincidencia, la modalidad de paso y la resolución del intento, además el programa cuenta con un temporizador de diez segundos entre cada captura para evitar la duplicación de anotaciones de una misma persona como se puede apreciar en la Tabla 24.

Tabla 24. Bitácora digital elaborada por el software

Fecha	Hora	Identidad	Tipo_Evento	Resultado
08/05/2026	16:29:52	USUARIO_1	Entrada	Autorizado
08/05/2026	16:30:01	Desconocido	Entrada	Denegado
08/05/2026	16:30:12	Desconocido	Entrada	Denegado
08/05/2026	16:30:24	USUARIO_1	Entrada	Autorizado
08/05/2026	16:30:35	USUARIO_1	Salida	Autorizado
08/05/2026	16:30:46	Desconocido	Salida	Denegado
08/05/2026	16:30:57	Desconocido	Entrada	Denegado
08/05/2026	16:31:07	Desconocido	Entrada	Denegado
08/05/2026	16:31:19	USUARIO_1	Entrada	Autorizado
08/05/2026	16:31:30	USUARIO_1	Entrada	Autorizado
08/05/2026	16:31:40	USUARIO_1	Salida	Autorizado

Para registrar la modalidad de paso el operador puede alternar manualmente entre la entrada y la salida presionando teclas específicas en la computadora, esta funcionalidad permite mantener un orden sobre el movimiento del personal dentro de las áreas de protección de la cooperativa, de este modo se supera en gran medida el esquema tradicional basado en libretas físicas, facilitando enormemente la búsqueda de la información y agilizando las revisiones de los horarios de los trabajadores mediante herramientas de ofimática de uso común. El registro de entradas/salidas también se ve reflejado en la consola de respuesta de Python como se puede observar en la Figura 20.

Registro guardado: 2026-05-11 10:19:05		Desconocido		Entrada		Denegado
Registro guardado: 2026-05-11 10:19:08		USUARIO_1		Entrada		Autorizado
Registro guardado: 2026-05-11 10:19:18		Desconocido		Entrada		Denegado
Registro guardado: 2026-05-11 10:19:30		USUARIO_1		Salida		Autorizado
Registro guardado: 2026-05-11 10:19:42		Desconocido		Salida		Denegado

Figura 20. Trazabilidad del programa en la consola de Python

3.3.6 Flujo operativo del sistema (pipeline)

El flujo operativo de la herramienta tecnológica inicia con las configuraciones el segundo bloque abarca los pasos previos dentro del entorno virtual, mediante los cuales se determina la dirección específica donde se encuentran guardados los archivos en la computadora, pues esta configuración garantiza que el programa localice sin errores tanto la base de datos de imágenes como los recursos necesarios para el funcionamiento del código, ya que establecer esta ruta de acceso permite que el sistema opere con orden al leer la información almacenada en el disco local y asegura que el enlace entre la interfaz lógica y los archivos físicos sea totalmente preciso para evitar fallos de lectura durante la ejecución del proceso que contiene las fotografías de los usuarios autorizados y se prepara el archivo de texto para la bitácora, seguidamente el algoritmo enciende la cámara web para capturar el video en tiempo real, habilitando al mismo tiempo el clasificador rápido encargado de escanear los fotogramas para localizar los rostros de las personas que transitan por el área de cajas.

Una vez que el video fluye continuamente el sistema transforma cada imagen a una escala monocromática para agilizar el procesamiento matemático, mediante esta técnica el clasificador logra enmarcar la cara del empleado para aislar sus rasgos

físicos del fondo, posteriormente el código aplica una validación asíncrona tomando únicamente un cuadro por cada treinta capturas, enviando esta selección específica al motor de inteligencia artificial de DeepFace para comparar el rostro en vivo con las imágenes almacenadas en la computadora.

Con el resultado de esta comparación biométrica el aplicativo toma una decisión operativa directa sobre el intento de acceso, si el trabajador es reconocido exitosamente se extrae su nombre y se muestra una autorización visual de color verde, por el contrario, si la persona es desconocida el sistema deniega el paso inmediatamente con una alerta visual de color rojo, procediendo en ambos escenarios a guardar la fecha y la modalidad de movimiento dentro del archivo de valores separados por comas.

Para finalizar este ciclo continuo el programa cuenta con un temporizador de diez segundos que evita la creación de registros duplicados para una misma persona, además la interfaz permite al operador alternar manualmente entre las modalidades de entrada y salida utilizando el teclado del equipo informático, dibujando todas estas interacciones directamente sobre la ventana de video para ofrecer una retroalimentación visual clara y logrando así una administración automatizada de la seguridad de la cooperativa financiera.

3.3.7 Matriz de confusión

Para validar la exactitud del algoritmo de clasificación biométrica se construyó un directorio de pruebas controlado, presentado en el Anexo C, con imágenes estáticas organizadas en carpetas separadas. Para el registro biométrico de los usuarios autorizados se consideraron 100 fotografías de referencia por empleado, con el propósito de disponer de una base facial más representativa frente a variaciones de iluminación, ángulo y expresión. Posteriormente, para la evaluación del rendimiento, se agruparon imágenes correspondientes a usuarios autorizados y personas no autorizadas, permitiendo comparar la identidad real de cada fotografía con la predicción emitida por el programa. Este proceso se realizó mediante la librería matemática scikit-learn, obteniendo una evaluación directa del rendimiento del modelo sin depender de la cámara web en tiempo real.

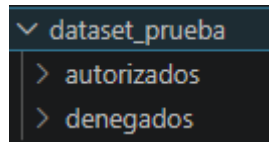


Figura 21. Carpetas para realizar la matriz de confusión

Los resultados de esta prueba de escritorio se organizaron dentro de una matriz de confusión para detallar los aciertos y las equivocaciones del aplicativo, en el cuadrante de los verdaderos positivos el programa logró identificar y conceder el paso correctamente a las 100 imágenes del usuario autorizado, asimismo en el cuadrante de los verdaderos negativos la herramienta bloqueó con éxito a 96 fotografías de personas ajenas a la institución financiera, garantizando de esta manera un nivel de protección alto frente a los intrusos como podemos observar en la Figura 22.

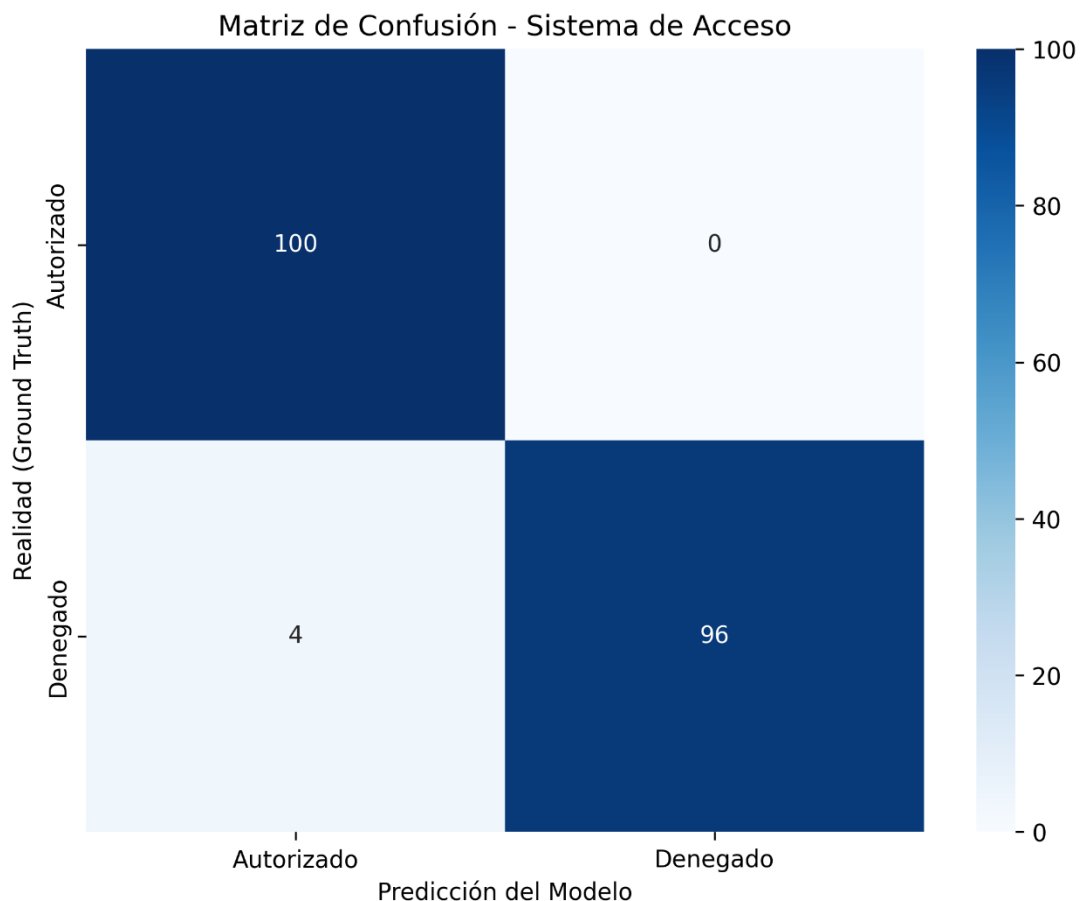


Figura 22. Matriz de confusión modelo Deep Learning

Exactitud

$$Exactitud = \frac{VP + VN}{VP + VN + FP + FN} = \frac{100 + 96}{200} = 98\%$$

Precisión

$$Precisión = \frac{VP}{VP + FP} = \frac{100}{100 + 4} = 96.15\%$$

Sensibilidad

$$Sensibilidad = \frac{VP}{VP + FN} = \frac{100}{100 + 0} = 100\%$$

En cuanto a los fallos del software, la evaluación contabilizó cero falsos negativos, lo cual evidencia que el sistema no denegó el acceso al empleado autorizado durante el entorno de prueba. Por otro lado, se registraron cuatro falsos positivos, correspondientes a autorizaciones incorrectas hacia personas no autorizadas. Estos resultados muestran una ligera tendencia permisiva del algoritmo, por lo que el umbral de confianza podría ajustarse para fortalecer la restricción de acceso en las áreas de cajas y bóveda, considerando que dicho ajuste podría requerir más de un intento de validación frente a la cámara.

3.3.8 Consideraciones técnicas del diseño

El diseño del programa responde a criterios de utilidad y adaptabilidad operativa, en términos de utilidad la arquitectura elaborada en Python permite ejecutar el proceso completo de reconocimiento biométrico junto con el registro de los movimientos dentro de una sola interfaz interactiva, en cuanto a la escalabilidad la estructura del código facilita incorporar a futuro nuevas fotografías de usuarios o puntos de control adicionales sin alterar el funcionamiento del aplicativo.

Finalmente, en relación con la trazabilidad del sistema la conservación de todos los sucesos se realiza mediante un archivo de texto con valores separados por comas, por consiguiente, este método de almacenamiento ligero permite reconstruir el historial exacto de las entradas o salidas del personal, facilitando así la emisión rápida de reportes en hojas de cálculo para respaldar las labores de auditoría por parte de los administradores de la institución financiera.

3.4 Diseño general del sistema propuesto con Aprendizaje supervisado

El diagrama de la Figura 23 ilustra la arquitectura principal del sistema de reconocimiento facial en Python comenzando con las entradas de datos, primero se activa la captura en tiempo real mediante la cámara web mientras se cargan los modelos de entrenamiento y los archivos locales, la fase inicial se encarga de preparar el motor de predicción LBPH junto al clasificador en cascada para validar la existencia del archivo CSV, de esta manera si la bitácora digital no existe el programa la genera con las columnas necesarias para almacenar las fechas y los eventos, este paso preparatorio asegura que todas las dependencias técnicas estén correctamente configuradas antes de iniciar el procesamiento ininterrumpido de las imágenes capturadas.

El núcleo del programa consiste en un bucle continuo que toma cada fotograma del video para convertirlo a escala de grises, luego se utiliza la detección de rostros para ubicar y redimensionar la cara antes de enviarla al modelo de predicción LBPH, en esta etapa ocurre la validación central donde el sistema evalúa el nivel de confianza matemático generado por el algoritmo, por lo tanto si el valor numérico es menor a 70 el rostro se considera una coincidencia válida aprobando el acceso, por el contrario si la cifra supera este límite el programa rechaza la identificación marcando a la persona como un sujeto desconocido, toda esta evaluación lógica ocurre en fracciones de segundo para mantener la fluidez del video en vivo.

Después de la validación la ejecución se divide hacia la actualización visual y el almacenamiento estructurado de la información, el sistema verifica mediante una condición matemática si han pasado 10 segundos desde el último registro para escribir en la bitácora CSV, al mismo tiempo el código dibuja sobre el fotograma un cuadro delimitador y un texto dinámico que muestran el estado de la autorización, además el flujo monitorea continuamente las pulsaciones del teclado para permitir al administrador alternar rápidamente entre los modos de entrada y salida, finalmente la imagen procesada con la interfaz superpuesta se proyecta en la pantalla del usuario mediante una ventana emergente, culminando el ciclo al presionar la tecla designada para liberar ordenadamente los recursos de la cámara.

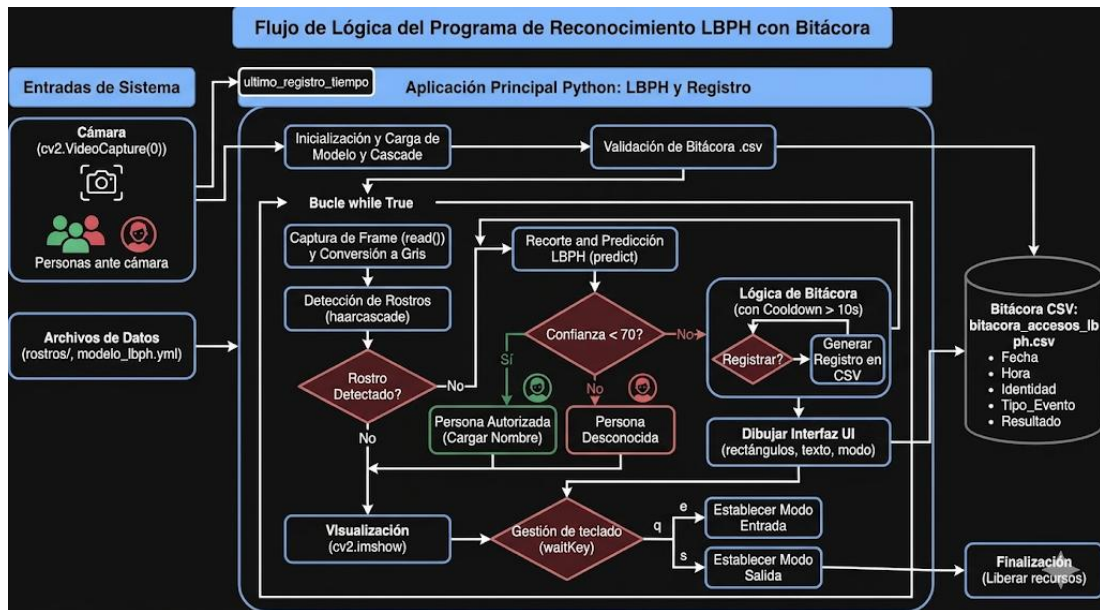


Figura 23. Lógica de funcionamiento del programa con Aprendizaje supervisado

3.4.1 Técnica de Machine Learning

El desarrollo de este sistema informático de control de acceso se fundamenta en un modelo estructurado de aprendizaje automático supervisado, operativamente el software ejecuta una tubería de procesamiento que emplea técnicas clásicas de visión artificial para analizar los datos biométricos, dividiendo su funcionamiento en 3 etapas principales para garantizar la protección de las instalaciones.

- 1) Fase de detección espacial: El programa utiliza un algoritmo basado en los clasificadores en cascada de Haar, esta técnica matemática escanea continuamente los fotogramas en escala de grises buscando variaciones de contraste para ubicar el rostro humano, logrando así recortar la matriz de píxeles exacta en tiempo real para su posterior análisis.
- 2) Fase de extracción y entrenamiento: Para la asimilación de las identidades se aplica el algoritmo de histogramas de patrones binarios locales conocido como LBPH, este método evalúa la textura de la cara comparando cada píxel con sus vecinos para construir un modelo descriptivo único, asimilando así las 300 fotografías capturadas previamente para cada empleado.
- 3) Fase de reconocimiento en vivo: El sistema captura un nuevo rostro mediante la cámara para calcular su histograma y medir la distancia matemática frente

al archivo guardado, de esta manera si el valor de confianza numérico resulta menor a 70 se aprueba la coincidencia, logrando así diferenciar a los trabajadores de las personas ajenas a la institución.

A nivel operativo el aplicativo funciona bajo un paradigma de aprendizaje automático supervisado, el algoritmo procesa la imagen en vivo para calcular su nivel de similitud contra las etiquetas numéricas generadas durante el entrenamiento, clasificando finalmente el intento de paso en 2 categorías exactas correspondientes a un acceso autorizado o denegado.

3.4.2 Métricas de Validación

Para evaluar el desempeño del clasificador biométrico se implementaron métricas de validación estructuradas a partir de una matriz de confusión compuesta por 4 cuadrantes, esta herramienta estadística permite desglosar los aciertos y las equivocaciones del algoritmo LBPH frente a un grupo de imágenes de prueba, facilitando así la medición exacta de la capacidad predictiva del modelo matemático. El sistema trasciende la inspección ocular directa para generar métricas precisas sobre la operatividad del programa de vigilancia, ya que la transformación de imágenes en valores cuantificables permite un control técnico basado en hechos concretos, pues al prescindir de la valoración humana y sustituirla por cálculos matemáticos se logra una medición veraz del rendimiento, asegurando que la gestión del software se sustente en datos que facilitan la toma de decisiones, el ajuste de parámetros y la verificación del cumplimiento de los protocolos de seguridad establecidos.

La métrica principal extraída de esta matriz es la exactitud del sistema para procesar los ingresos diarios, este parámetro matemático se calcula sumando los verdaderos positivos con los verdaderos negativos para luego dividir esa cifra entre el total de las validaciones, por consiguiente este valor numérico representa la proporción global de las decisiones correctas emitidas por la red de aprendizaje automático, permitiendo establecer un porcentaje claro sobre el nivel de protección que el aplicativo ofrece para las instalaciones financieras.

Adicionalmente se evalúa la precisión del modelo para medir su efectividad al momento de conceder los accesos hacia la bóveda, esta métrica resulta de dividir los aciertos positivos entre el total de las autorizaciones otorgadas incluyendo los falsos

positivos, por lo tanto este cálculo es indispensable en el área de cajas un resultado equivocado de aprobación supone el ingreso sin trabas de una persona ajena, pues la falla permite que alguien no autorizado pase al espacio protegido, lo cual obliga al motor de inteligencia artificial a conservar un nivel de exigencia elevado para reducir las vulnerabilidades en la entrada mediante la revisión minuciosa de los rasgos, ya que cualquier error de cálculo tiene repercusiones directas en la protección de los bienes y recursos, pues la eficacia del programa depende de su capacidad para distinguir con total exactitud cada rostro, manteniendo así un control constante que impida el acceso de quienes no forman parte del personal habilitado.

Finalmente la sensibilidad complementa el análisis estadístico del aplicativo para medir los problemas de acceso del personal autorizado, este indicador cuantifica la habilidad del programa para identificar a los trabajadores registrados penalizando los falsos negativos donde el sistema rechaza a una persona conocida, aunque una sensibilidad baja genera cierta fricción operativa al solicitar 2 o más intentos frente a la cámara, este comportamiento restrictivo es preferible para mantener resguardada la cooperativa frente a condiciones variables de iluminación.

3.4.3 Selección del modelo

La selección de la arquitectura matemática basada en histogramas de patrones binarios combinada con los algoritmos de Haar Cascades se apoya en varios motivos técnicos que garantizan la viabilidad del proyecto, por consiguiente en la Tabla 25 se detallan los factores para esta decisión tecnológica, abarcando la capacidad del modelo para asimilar 300 fotografías por empleado durante el entrenamiento local junto a su tolerancia frente a los cambios de iluminación, consiguiendo de esta manera un equilibrio adecuado entre la exactitud biométrica y el procesamiento del equipo informático sin requerir servidores externos.

Tabla 25. Justificación del modelo de aprendizaje supervisado

Criterio de Selección	Justificación Técnica	Beneficio Operativo en la Cooperativa
Eficiencia de Entrenamiento Local	Uso del algoritmo de histogramas de patrones binarios locales que permite procesar y	La plataforma permite incorporar a cada colaborador mediante la obtención directa de

Criterio de Selección	Justificación Técnica	Beneficio Operativo en la Cooperativa
	asimilar rápidamente cientos de imágenes directamente en el procesador.	trescientas imágenes, las cuales sirven para configurar un modelo de reconocimiento a la medida sin necesidad de recurrir a equipos con tarjetas gráficas de alta potencia, pues la cantidad de muestras garantiza que la red neuronal aprenda los rasgos distintivos del usuario con una variedad suficiente de ángulos y expresiones, logrando así una alta precisión en la identificación posterior, además de asegurar que la cooperativa pueda gestionar su base de datos de manera autónoma en el hardware disponible, eliminando costos adicionales de infraestructura técnica mientras mantiene una capacidad de respuesta óptima para los fines de vigilancia requeridos.
Tolerancia a la Iluminación	El método matemático evalúa la textura comparando cada píxel con sus 8 vecinos para ignorar las alteraciones globales de luz sobre el rostro humano.	El sistema conserva una tasa de aciertos elevada aun cuando las condiciones lumínicas en los espacios de cajas o bóvedas fluctúan, pues el modelo compensa de forma autónoma la presencia de sombras pronunciadas o el resplandor de la iluminación eléctrica, ya que la arquitectura de la red extrae los rasgos invariantes del rostro sin importar la intensidad de la luz que incida sobre la piel, logrando así que el reconocimiento mantenga

Criterio de Selección	Justificación Técnica	Beneficio Operativo en la Cooperativa
		su fiabilidad sin requerir cambios en la configuración física del sitio, pues la capacidad de adaptarse a estos cambios permite que la protección del área sea constante y libre de errores causados por el entorno lumínico.
Equilibrio de Rendimiento	La propuesta incorpora un esquema de trabajo organizado donde la búsqueda constante de rostros en el espacio recae en el clasificador Haar Cascades, debido a que este algoritmo consume pocos recursos computacionales al realizar su labor, mientras que el cálculo biométrico se reserva para la red neuronal, la cual actúa solo cuando el primer bloque detecta una posible presencia, logrando así que la capacidad del procesador se utilice únicamente en el momento preciso de la validación, garantizando que el sistema opere con agilidad, mantenga un flujo de video sin interrupciones y asegure una autenticación de alta precisión mediante la matriz matemática en cada acceso detectado.	Esta estrategia impide que la transmisión visual se bloquee debido a una saturación en las capacidades del procesador, pues al distribuir las tareas se reduce el esfuerzo técnico requerido, lo cual permite que el programa trabaje de manera constante y sin pausas en los equipos comunes con los que ya cuenta la entidad, evitando así la adquisición de servidores especializados, pues el manejo inteligente de los datos asegura que la operatividad fluya con naturalidad, manteniendo la seguridad del área en todo momento mediante una ejecución eficiente que aprovecha al máximo el hardware existente.

```

1  import cv2
2  import os
3
4  nombre = "Santiago"
5  ruta_datos = "data_rostros"
6  ruta_persona = os.path.join(ruta_datos, nombre)
7
8  if not os.path.exists(ruta_persona):
9      os.makedirs(ruta_persona)
10
11  cap = cv2.VideoCapture(0)
12  face_cascade = cv2.CascadeClassifier(cv2.data.haarcascades + 'haarcascade_frontalface_default.xml')
13  count = 0
14
15  while True:
16      ret, frame = cap.read()
17      if not ret: break
18      gray = cv2.cvtColor(frame, cv2.COLOR_BGR2GRAY)
19      rostros = face_cascade.detectMultiScale(gray, 1.1, 5)

```

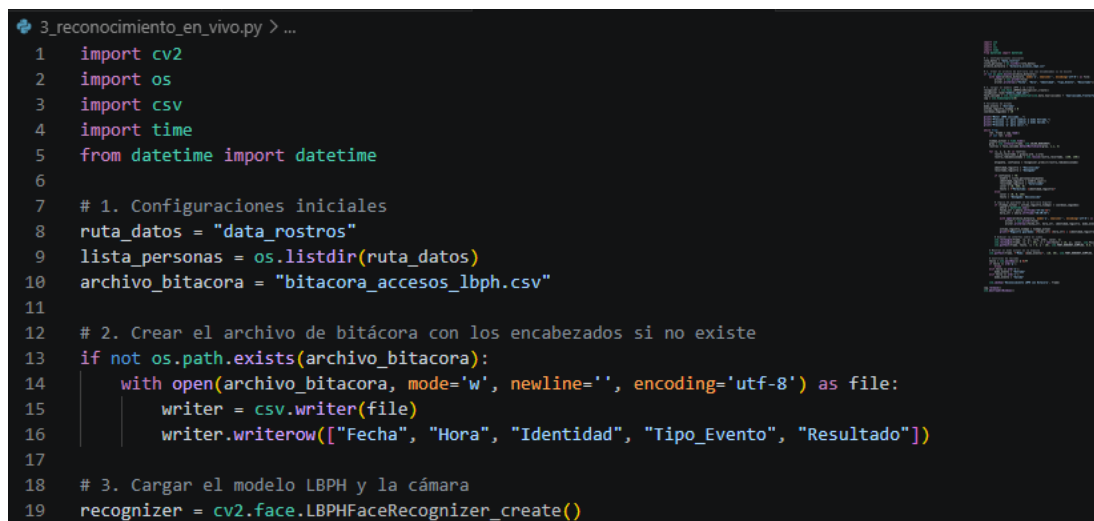
Figura 24. Código de la captura de datos

```

1  import cv2
2  import os
3  import numpy as np
4
5  ruta_datos = "data_rostros"
6  lista_personas = os.listdir(ruta_datos)
7  etiquetas = []
8  datos_rostros = []
9  etiqueta_actual = 0
10
11  for persona in lista_personas:
12      ruta_persona = os.path.join(ruta_datos, persona)
13      for archivo in os.listdir(ruta_persona):
14          ruta_imagen = os.path.join(ruta_persona, archivo)
15          imagen = cv2.imread(ruta_imagen, 0)
16          datos_rostros.append(imagen)
17          etiquetas.append(etiqueta_actual)
18      etiqueta_actual += 1
19

```

Figura 25. Código del entrenamiento del modelo



```

3_reconocimiento_en_vivo.py > ...
1  import cv2
2  import os
3  import csv
4  import time
5  from datetime import datetime
6
7  # 1. Configuraciones iniciales
8  ruta_datos = "data_rostros"
9  lista_personas = os.listdir(ruta_datos)
10 archivo_bitacora = "bitacora_accesos_lbph.csv"
11
12 # 2. Crear el archivo de bitácora con los encabezados si no existe
13 if not os.path.exists(archivo_bitacora):
14     with open(archivo_bitacora, mode='w', newline='', encoding='utf-8') as file:
15         writer = csv.writer(file)
16         writer.writerow(["Fecha", "Hora", "Identidad", "Tipo_Evento", "Resultado"])
17
18 # 3. Cargar el modelo LBPH y la cámara
19 recognizer = cv2.face.LBPHFaceRecognizer_create()

```

Figura 26. Código del reconocimiento facial con Aprendizaje supervisado

3.4.4 Preprocesamiento

El sistema ejecuta una fase de preprocesamiento estructurada tanto en la captura de datos como en el flujo de video en tiempo real para optimizar la información y reducir la carga computacional, este proceso se divide en 3 etapas fundamentales que preparan las imágenes para el clasificador.

- 1) Conversión de espacio de color: Los fotogramas capturados inicialmente en formato tridimensional son convertidos a escala de grises, esta reducción elimina la información de color innecesaria acelerando significativamente el algoritmo de detección espacial y facilitando el análisis de texturas para el modelo matemático.
- 2) Detección y extracción de la región de interés: Utilizando los clasificadores en cascada de Haar el sistema escanea el fotograma en escala de grises para identificar las coordenadas espaciales del rostro, esto permite aislar la región facial descartando por completo el fondo y el ruido visual del entorno operativo.
- 3) Redimensionamiento geométrico: Una vez identificada el área facial el aplicativo recorta la imagen original y la escala a una proporción exacta de 150x150 píxeles, logrando de esta manera estandarizar todas las fotografías para asegurar que el motor de inferencia procese matrices idénticas durante el entrenamiento y la validación en vivo.

El preprocesamiento de la imagen se ejecuta dentro del bucle principal de los programas capturando el flujo de video en tiempo real para limpiar los datos antes de guardarlos o analizarlos, a continuación, se presenta el fragmento de código responsable de ejecutar esta fase preparatoria.

Tabla 26. Fragmentos del código del preprocesamiento de la imagen

Etapas del procesamiento	Fragmento de código en Python
1. Captura del fotograma en bruto mediante la cámara web	<code>ret, frame = cap.read()</code>
2. Conversión a escala de grises para reducción de dimensionalidad	<code>gray = cv2.cvtColor(frame, cv2.COLOR_BGR2GRAY)</code>
3. Detección espacial del rostro para localizar la región de interés	<code>rostros = face_cascade.detectMultiScale(gray, 1.1, 5)</code>
4. Recorte de la matriz y redimensionamiento estandarizado	<code>rostro_recortado = gray[y:y+h, x:x+w] rostro_redimensionado = cv2.resize(rostro_recortado, (150, 150))</code>

(cv2.cvtColor): Ejecuta la transformación del espacio tridimensional a una matriz bidimensional en escala de grises, reduciendo drásticamente el peso del fotograma y facilitando un rastreo matemático más ágil para la posterior extracción de las características faciales.

(detectMultiScale): El procedimiento aplica el algoritmo de Haar Cascades sobre la captura en tonos grises mediante una configuración de escala de 1.1 y cinco vecinos, de modo que estos valores actúan como mecanismos de filtrado para el ruido visual, asegurando que el software delimite únicamente los espacios que coincidan con la forma de un rostro humano, pues la escala controla el tamaño de la búsqueda entre cada iteración mientras el parámetro de vecinos exige un número mínimo de coincidencias para aceptar la detección, permitiendo descartar elementos del entorno que no guardan relación con la anatomía facial y garantizando que el sistema identifique únicamente objetivos válidos para el procesamiento posterior.

(cv2.resize): Representa la fase final del preprocesamiento donde el rostro es recortado desde el cuadro original utilizando sus coordenadas de ubicación, para luego ajustar su tamaño a 150 píxeles de alto por 150 píxeles de ancho, La estandarización de la imagen asegura que el modelo procese datos visuales totalmente uniformes, ya que el

preprocesamiento alinea los rasgos clave y ajusta el tamaño de la captura a las dimensiones requeridas por la red, permitiendo que la información esté preparada para la confrontación matemática, lo cual elimina cualquier disparidad causada por variaciones en la distancia, el ángulo o el encuadre de la persona, pues al alimentar la red con datos normalizados se garantiza una ejecución estable, precisa y libre de errores en la comparación biométrica, facilitando que el resultado final sea certero al contrastar al usuario con la base de datos almacenada.

3.4.5 Arquitectura funcional del sistema

La estructura general del sistema se compone de 4 bloques interconectados para mantener el orden del flujo de información, iniciando con la captura de video en tiempo real mediante las funciones de OpenCV para registrar 300 fotografías por empleado, para luego avanzar hacia el entrenamiento del modelo empleando el algoritmo LBPH, prosiguiendo con la verificación de la identidad en vivo para conceder o negar el ingreso, culminando con el almacenamiento de estos sucesos y la gestión administrativa de los registros para asegurar un desempeño óptimo durante las validaciones.

a. Módulo de captura de imagen y recolección de datos

El primer bloque corresponde al módulo de captura constituido por una cámara web o dispositivo de adquisición de imagen ubicado en el punto de acceso a las áreas restringidas, su función consiste en capturar en tiempo real el rostro de la persona para guardar un conjunto de 300 imágenes, garantizando una calidad visual suficiente para su posterior entrenamiento, este componente representa la interfaz física entre el usuario y el sistema por lo que su correcta ubicación y resolución influyen directamente en el rendimiento del reconocimiento facial.

Tabla 27. Parámetros de módulo de captura de imagen

Parámetro	Descripción
Marca	SINOVISION
Modelo	MFPT20
Clasificación de resistencia al agua	IP66
Movimiento	PTZ

Parámetro	Descripción
Control	App, PC, remoto
Conectividad	IP, LAN, Wi-Fi
Resolución	2MP
Distancia focal de lente	3.6 mm
Sensor de imagen	1/2.7" BSI Sensor
Resolución de video	Full HD
Compresión de video	H265
Tipo de almacenamiento	Micro-SD, nube, NVR
Capacidad de almacenamiento	64GB
Alimentación	12 V
Consumo	2.1W
Asistentes virtuales compatibles	Alexa, Google Assistant, Siri

b. Módulo de procesamiento y entrenamiento del modelo

Una vez capturadas las imágenes del usuario en el punto de acceso estas son procesadas por el segundo bloque del sistema desarrollado en Python, garantizando de esta manera la compatibilidad absoluta con las librerías matemáticas donde se ejecuta el entrenamiento facial inicial, este módulo comprende las etapas de detección de rostro además del preprocesamiento de la imagen para aislar la zona facial y redimensionarla a 150 píxeles, posteriormente el algoritmo extrae las características de todas las fotografías para entrenar la matriz matemática LBPH, consolidando finalmente el conocimiento adquirido en un archivo local con extensión YML que servirá como base para las comparaciones biométricas futuras.

c. Módulo de validación de identidad y decisión de acceso

El módulo de validación de identidad y decisión de acceso conforma el núcleo lógico del programa de reconocimiento en vivo debido a que convierte el resultado matemático en una decisión operativa directa para autorizar o denegar el ingreso a las áreas de cajas y bóveda, este bloque recibe como entrada el fotograma procesado junto con el nivel de confianza generado por el motor LBPH al comparar la cara capturada con el modelo previamente entrenado, para cumplir con este propósito, el algoritmo

realiza una verificación asincrónica comparando la distancia numérica obtenida en la comparación biométrica; si este valor resulta inferior a 70, el sistema interpreta que existe una coincidencia suficiente entre los rasgos faciales del usuario capturado y la fotografía de referencia, validando así la identidad. Este umbral de 70 actúa como el filtro decisivo de seguridad: un valor menor a este límite indica una alta probabilidad de correspondencia, permitiendo el acceso, mientras que un valor superior sugiere una diferencia demasiado amplia para considerarse como el mismo individuo, disparando el protocolo de denegación de ingreso para aceptar la coincidencia y descartando aquellas capturas que superan este límite marcándolas como personas ajenas a la cooperativa, la lógica de decisión del código fue definida considerando los escenarios que pueden presentarse durante el monitoreo de la cámara web, cuando el rostro es detectado correctamente y el sistema encuentra una similitud válida se extrae el nombre de la etiqueta para generar un aviso de acceso permitido de color verde, por el contrario si el individuo es desconocido se emite una alerta visual de color rojo para denegar de inmediato el paso hacia la zona de seguridad.

Tabla 28. Condiciones utilizadas de validación y acceso

Condición evaluada por el algoritmo	Acción ejecutada por el sistema	Resultado visual
Rostro detectado en el fotograma y confianza matemática menor a 70 al comparar con el modelo LBPH	Se extrae el nombre de la etiqueta numérica asociada y se autoriza la identidad del usuario	Acceso Permitido (Recuadro Verde)
Rostro detectado en pantalla pero el valor numérico de confianza es superior a 70	Se rechaza la solicitud al no encontrar coincidencias matemáticas válidas	Acceso Denegado (Recuadro Rojo)

d. Módulo de bitácora digital de accesos

Independientemente del resultado de la comprobación biométrica el sistema genera un archivo de texto en formato de valores separados por comas para guardar cada suceso, esta bitácora digital almacena los datos necesarios para el monitoreo del acceso incluyendo la fecha y la hora exacta junto con el nombre del empleado cuando existe una coincidencia, además el programa cuenta con un temporizador de 10 segundos entre cada captura para evitar la duplicación de anotaciones de una misma persona,

para registrar la modalidad de paso el operador puede alternar manualmente entre la entrada y la salida presionando teclas específicas en la computadora, esta funcionalidad permite mantener un orden sobre el movimiento del personal dentro de las áreas de protección de la cooperativa superando en gran medida el esquema tradicional basado en libretas físicas, facilitando enormemente la búsqueda de la información y agilizando las revisiones de los horarios de los trabajadores mediante herramientas de ofimática de uso común.

Tabla 29. Bitácora digital elaborada por el software

Fecha	Hora	Identidad	Tipo_Evento	Resultado
08/05/2026	16:29:52	USUARIO_1	Entrada	Autorizado
08/05/2026	16:30:01	Desconocido	Entrada	Denegado
08/05/2026	16:30:12	Desconocido	Entrada	Denegado
08/05/2026	16:30:24	USUARIO_1	Entrada	Autorizado
08/05/2026	16:30:35	USUARIO_1	Salida	Autorizado
08/05/2026	16:30:46	Desconocido	Salida	Denegado

3.4.6 Flujo operativo del sistema (pipeline)

1) Fase de Adquisición de Datos

Objetivo: Crear el *Dataset* (conjunto de datos) crudo.

- **Entrada:** Video en vivo desde la cámara web.
- **Procesamiento:** Convierte los fotogramas a escala de grises.
 - Usa el algoritmo Haar Cascade para encontrar la coordenada exacta del rostro.
 - Recorta solo esa región (elimina el fondo y otros elementos no relevantes de la imagen).
 - Estandariza el tamaño a 150x150 píxeles.
- **Salida:** Una carpeta (data_rostros/Santiago) poblada con 300 imágenes estandarizadas y listas para ser analizadas.

2) Fase de Entrenamiento / Aprendizaje

Objetivo: Extraer patrones matemáticos y generar el centro del sistema.

- **Entrada:** Las 300 imágenes generadas en la Fase 1, junto con el nombre de la carpeta que actúa como etiqueta (ID = 0, Nombre = Santiago).
- **Procesamiento:** El código recorre la carpeta e inyecta las fotos en dos listas (datos_rostros y etiquetas).
 - El algoritmo LBPH analiza las 300 fotos, buscando los patrones geométricos y de textura que definen el rostro del usuario, ignorando las variaciones leves de luz o ángulo.
- **Salida:** Un archivo binario comprimido llamado modelo_lbph.yml. Este archivo es el modelo entrenado de Inteligencia Artificial empaquetado; ya no contiene fotos, solo los cálculos matemáticos del rostro del usuario.

3) Fase de Inferencia y Despliegue

Objetivo: Poner el modelo en producción para tomar decisiones en el mundo real.

- **Entrada:** Video en vivo (cámara) + el archivo modelo_lbph.yml (creado en la Fase 2) + el archivo Haar Cascade.
- **Procesamiento:**
 - Detecta y recorta el rostro en vivo exactamente igual que en la Fase 1 (150x150).
 - Le pasa ese recorte al modelo LBPH para que haga la Inferencia (predicción).
 - Compara el resultado matemático con el umbral de seguridad de seguridad (Confianza < 70).
 - Aplica lógica de negocio: maneja el delay de 10 segundos para no saturar los registros.
- **Salida:** * **Visual:** Interfaz gráfica con recuadros verdes (Autorizado) o rojos (Denegado).

- **Datos:** Un archivo de texto bitacora_accesos_lbph.csv que actúa como base de datos histórica de los eventos.

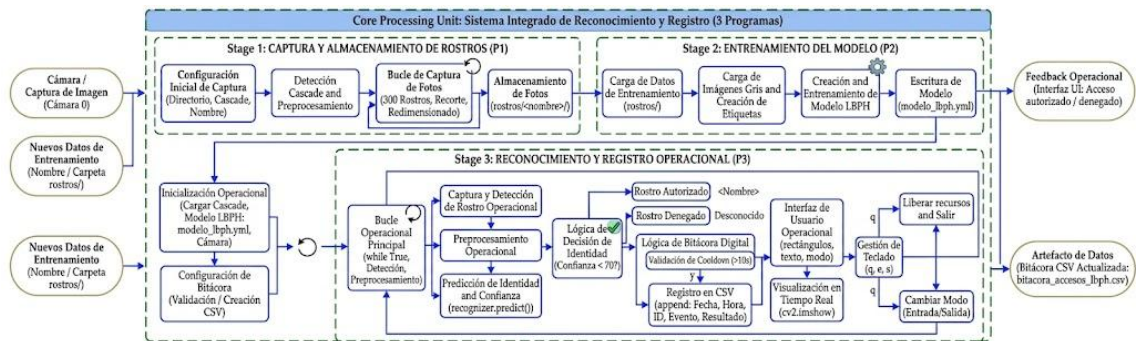


Figura 27. Enfoque de procesamiento para control de acceso con Aprendizaje supervisado

3.4.7 Matriz de confusión

Para validar la exactitud del algoritmo de clasificación biométrica se construyó un directorio de pruebas controlado, presentado en el Anexo G, con imágenes estáticas organizadas en carpetas separadas. Para el registro biométrico de los usuarios autorizados se consideraron 100 fotografías de referencia por empleado, con el propósito de disponer de una base facial más representativa frente a variaciones de iluminación, ángulo y expresión. Posteriormente, para la evaluación del rendimiento, se agruparon imágenes correspondientes a usuarios autorizados y personas no autorizadas, permitiendo comparar la identidad real de cada fotografía con la predicción emitida por el programa. Este proceso se realizó mediante la librería matemática scikit-learn, obteniendo una evaluación directa del rendimiento del modelo sin depender de la cámara web en tiempo real.

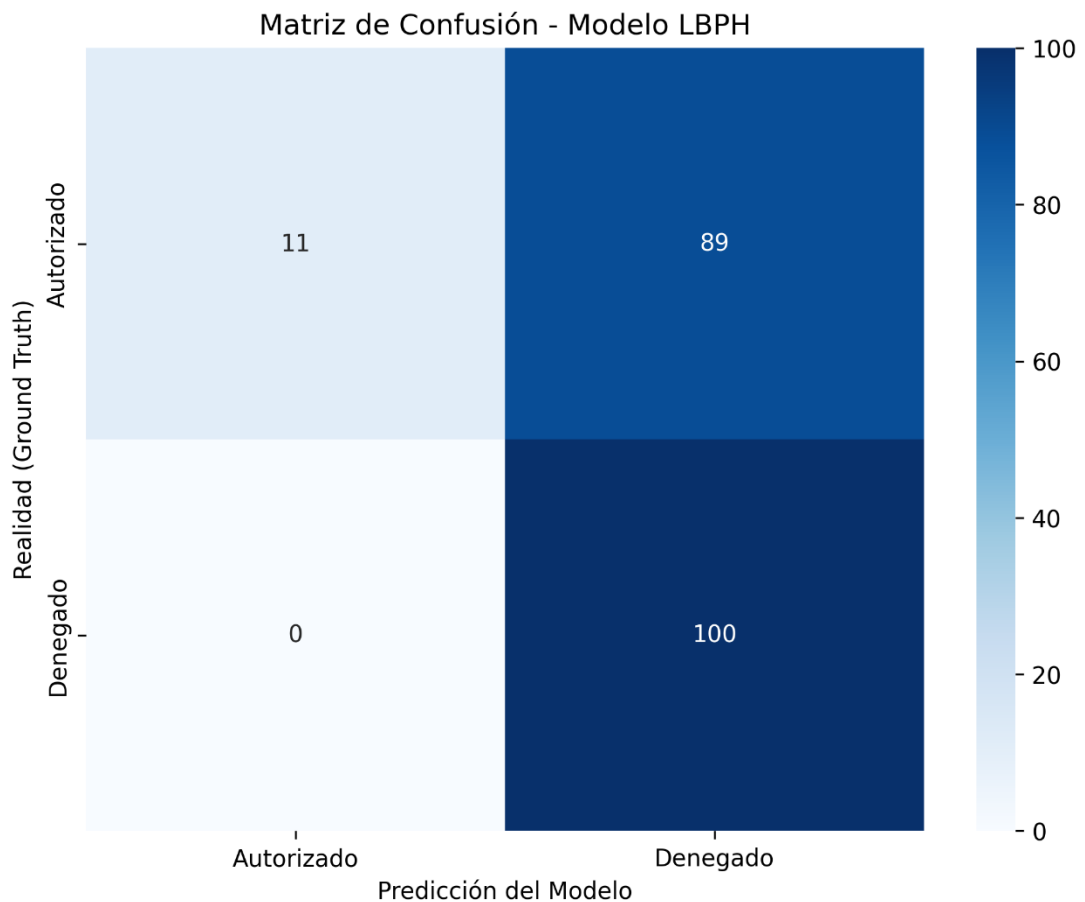


Figura 28. Matriz de confusión modelo Machine Learning

Exactitud

$$Exactitud = \frac{VP + VN}{VP + VN + FP + FN} = \frac{11 + 100}{200} = 55\%$$

Precisión

$$Precisión = \frac{VP}{VP + FP} = \frac{11}{11 + 0} = 100\%$$

Sensibilidad

$$Sensibilidad = \frac{VP}{VP + FN} = \frac{11}{11 + 89} = 11\%$$

En cuanto a los fallos del software la evaluación contabilizó 89 falsos negativos donde el sistema denegó el acceso al propio empleado debido a la enorme rigurosidad del umbral de confianza matemático, por otro lado se contabilizaron 0 falsos positivos confirmando que el programa jamás cometió la equivocación severa de autorizar la

entrada a un sujeto desconocido, por consiguiente estos números exponen que el algoritmo es extremadamente restrictivo logrando una precisión perfecta para resguardar las áreas de cajas, aunque esta configuración estricta causa una evidente fricción operativa al obligar al trabajador a posicionarse varias veces frente a la cámara hasta lograr ser reconocido.

3.4.8 Consideraciones técnicas del diseño

El diseño del programa responde a criterios de utilidad y adaptabilidad operativa dentro de la cooperativa, en términos de procesamiento la arquitectura elaborada en Python permite ejecutar la tubería completa de aprendizaje automático utilizando únicamente el procesador central del equipo informático, por consiguiente el uso del algoritmo matemático LBPH elimina la necesidad de adquirir tarjetas gráficas especializadas o servidores externos, logrando así que la captura de las 300 fotografías y el entrenamiento del modelo se realicen ágilmente en cualquier computadora convencional de la institución financiera.

En cuanto a la escalabilidad y el almacenamiento el sistema está estructurado para optimizar el uso de la memoria local durante las validaciones en tiempo real, esto se consigue mediante el redimensionamiento geométrico de los rostros a 150 píxeles y su conversión a escala monocromática para reducir el peso de los datos visuales, asimismo el modelo matemático asimilado se exporta en un único archivo ligero con extensión YML que concentra todas las características biométricas del personal, facilitando de esta manera la incorporación futura de nuevos empleados al directorio sin ralentizar el rendimiento general del software de seguridad.

Finalmente, respecto a la trazabilidad operativa, el sistema garantiza el registro continuo de cada intento de acceso mediante una bitácora digital. Este método, basado en un archivo de formato CSV, es una solución sumamente ligera que permite almacenar miles de eventos —fecha, hora, identidad y estado de acceso— con un consumo mínimo de espacio en el almacenamiento local. Al ser un archivo de texto estructurado, evita la saturación del disco duro a largo plazo y facilita la auditoría posterior, permitiendo que los administradores de la cooperativa exporten, filtren y analicen los datos con herramientas convencionales como hojas de cálculo, asegurando así un control histórico eficiente y ordenado sin comprometer el rendimiento del

hardware, permitiendo así reconstruir el historial exacto de los movimientos para emitir reportes rápidos en hojas de cálculo, consolidando de este modo una herramienta técnica eficiente que respalda plenamente las labores de auditoría requeridas para proteger las áreas de cajas y bóvedas.

3.5 Resultados

La fase inicial de la investigación permitió evaluar los procesos actuales para determinar las debilidades del control manual, logrando mitigar exitosamente 4 riesgos críticos identificados en la matriz inicial, entre ellos se neutralizó la vulnerabilidad por ingeniería social al eliminar la dependencia de la validación verbal, asimismo se redujo el peligro de colusión al forzar una autenticación biométrica ineludible, erradicando también la falsificación de la libreta física y solucionando la pérdida de trazabilidad al guardar automáticamente cada ingreso, cumpliendo de esta forma con los 7 requerimientos establecidos para el diseño como son la identificación precisa, el registro continuo, el rechazo de sujetos desconocidos, la trazabilidad, la emisión de reportes, la seguridad y la eficiencia operativa para resguardar las instalaciones financieras.

Para la implementación definitiva del sistema en la cooperativa, se realizó un estudio comparativo entre dos arquitecturas tecnológicas distintas, evaluando el desempeño del modelo preentrenado mediante la librería DeepFace frente a otras alternativas. Este contraste permitió determinar cuál de los motores de inferencia ofrecía el mejor equilibrio entre precisión biométrica, velocidad de respuesta y consumo de recursos dentro de las estaciones de trabajo estándar de la entidad.

Esta evaluación técnica se centró en medir cómo cada arquitectura gestiona la extracción de embeddings (vectores faciales) y qué tan efectiva resulta su capacidad de generalización en condiciones de iluminación no controlada, factores críticos para garantizar la automatización de la toma de decisiones sin comprometer la seguridad de las áreas de bóveda.

Deep Face frente al algoritmo de aprendizaje supervisado construido desde cero con LBPH, resultando seleccionado el modelo preentrenado para su despliegue final debido a su mejor desempeño técnico bajo las condiciones evaluadas para reconocer los rostros bajo condiciones reales, esta decisión se fundamenta en que la red neuronal

convolucional hereda el aprendizaje de millones de imágenes logrando identificar al personal utilizando 100 fotografías de referencia por empleado autorizado, mientras que el modelo local demandó capturar 300 fotografías por empleado resultando en un mayor esfuerzo operativo, por consiguiente a continuación se expone la Tabla 30 comparativa que justifica la elección de la tecnología preentrenada para proteger la bóveda.

Tabla 30. Comparativa técnica de los modelos evaluados

Criterio evaluado	Modelo preentrenado (Deep Face)	Modelo entrenado desde cero (LBPH)
Fotografías requeridas por empleado	100 fotografías	300 fotografías
Tipo de arquitectura	Red Neuronal Convolucional (VGG-Face)	Machine Learning Clásico (Histogramas binarios)
Esfuerzo de implementación	Bajo (Transferencia de aprendizaje)	Alto (Captura masiva y entrenamiento local)
Tolerancia a cambios de luz o postura	Muy alta	Baja
Decisión final	Seleccionado para implementación	Descartado por ineficiencia operativa

La validación matemática del desempeño se ejecutó procesando 200 imágenes de prueba para extraer las métricas de ambos algoritmos, evidenciando una brecha de rendimiento sustancial donde el modelo preentrenado demostró una exactitud del 98% frente al 55% de exactitud alcanzado por el programa entrenado localmente, asimismo el enfoque con Deep Face logró una sensibilidad del 100% al no generar ningún falso negativo evidenciando un control de ingreso más eficiente para el personal autorizado bajo las condiciones evaluadas, por el contrario el modelo LBPH obtuvo apenas un 11% de sensibilidad al rechazar a los trabajadores en 89 ocasiones, finalmente en el parámetro de precisión el sistema preentrenado alcanzó un sólido 96.15% cometiendo únicamente 4 equivocaciones, evidenciando un mejor desempeño comparativo del modelo preentrenado como se detalla en la Tabla 31 de resultados biométricos.

Tabla 31. Comparativa de métricas biométricas entre los modelos

Métrica de validación	Modelo preentrenado (Deep Face)	Modelo entrenado desde cero (LBPH)
Exactitud global	98%	55%

Métrica de validación	Modelo preentrenado (Deep Face)	Modelo entrenado desde cero (LBPH)
Precisión	96.15%	100%
Sensibilidad	100%	11%
Falsos Negativos (Rechazo al empleado)	0 casos	89 casos
Falsos Positivos (Acceso a intrusos)	4 casos	0 casos
Tiempo de validación por fotograma	Asíncrono (1 análisis cada 30 cuadros)	Continuo (Análisis de cada fotograma)

CAPÍTULO IV. CONCLUSIONES Y RECOMENDACIONES

4.1 Conclusiones

- El desarrollo del sistema automatizado de control de acceso permitió cumplir con el objetivo planteado al implementar un modelo fundamentado en redes neuronales convolucionales mediante la librería Deep Face, logrando automatizar de forma significativa la validación biométrica en las áreas de cajas y bóvedas de la Cooperativa de Ahorro y Crédito SOL, de esta manera se evidenció un mejor desempeño comparativo frente a los enfoques clásicos de aprendizaje supervisado para entregar una herramienta tecnológica que fortalece la seguridad física y elimina parte de los fallos en la trazabilidad de los registros.
- El análisis exhaustivo de los procesos actuales de registro permitió identificar limitaciones severas en el uso de las bitácoras físicas y la autorización verbal, demostrando que este esquema manual generaba riesgos críticos de ingeniería social, colusión y pérdida de trazabilidad operativa, lo cual facilitó la definición de 7 requerimientos técnicos indispensables para estructurar una solución digital capaz de mitigar estas vulnerabilidades mediante la validación ineludible y la trazabilidad automática de cada suceso.
- El diseño y la implementación tecnológica permitieron contrastar la eficiencia de 2 arquitecturas de aprendizaje automático, determinando que el despliegue del modelo preentrenado resultó ser la alternativa con mejor desempeño comparativo frente al algoritmo LBPH creado desde cero, esto se debe a que la red neuronal profunda logró identificar a los empleados utilizando 100 fotografías de referencia por empleado autorizado, logrando una mayor tolerancia frente a variaciones del entorno de luz sin someter a la institución al mayor esfuerzo operativo asociado a la captura de 300 imágenes para un entrenamiento local.
- La evaluación matemática del desempeño, ejecutada mediante matrices de confusión con 200 imágenes de prueba, confirmó un mejor desempeño comparativo del sistema preentrenado al registrar una exactitud global del 98 %, una precisión del 96.15 % y una sensibilidad del 100 % en el entorno de

prueba. Estos resultados evidencian que el modelo no generó rechazos equivocados hacia el personal autorizado. En comparación, el clasificador clásico obtuvo una exactitud del 55 %, por lo que el modelo preentrenado presentó mayor eficiencia operativa para el control de ingreso bajo las condiciones evaluadas.

4.2 Recomendaciones

- Se recomienda a las autoridades de la Cooperativa de Ahorro y Crédito SOL valorar la adopción del modelo preentrenado DeepFace como alternativa principal, ajustando ligeramente su umbral de confianza matemático con el propósito de reducir los cuatro falsos positivos detectados durante las pruebas, sin afectar de manera significativa la experiencia de validación del personal autorizado frente a la cámara web.¿.
- Se sugiere establecer rutinas de mantenimiento periódico para la cámara de captura y garantizar una iluminación constante en el punto de acceso, permitiendo que el preprocesamiento de las imágenes y el recorte facial a 150 píxeles se ejecuten bajo condiciones visuales óptimas para contribuir a mantener un desempeño estable del sistema a lo largo del tiempo.
- Es recomendable actualizar el manual de procedimientos internos para establecer el uso del aplicativo informático como mecanismo principal de control de acceso para el personal operativo. Además, se debe capacitar al personal sobre la alternancia manual entre las modalidades de entrada y salida mediante el teclado del equipo, con el fin de evitar inconsistencias en el seguimiento y reemplazar progresivamente el uso de bitácoras físicas.
- Se aconseja al coordinador de seguridad realizar la exportación semanal del archivo de valores separados por comas generado por el sistema automatizado, permitiendo auditar los movimientos diarios mediante hojas de cálculo para identificar rápidamente los ingresos denegados y respaldar la toma de decisiones institucionales frente a cualquier incidente en la bóveda.
- Se sugiere que se genere un cambio de equipo con uno que tenga propiedades de reconocimiento facial tridimensional, considerando varios ángulos de captura mediante distintas cámaras o técnicas complementarias de visión

artificial, con el propósito de reducir el riesgo de suplantación mediante fotografías impresas.

REFERENCIAS BIBLIOGRÁFICAS

- [1] J. Reyes, C. Castañeda y L. Alva, «Facial recognition system for access control through Artificial Intelligence,» *Innovación y software*, vol. II, nº 2, pp. 1-12, 2023.
- [2] G. Sain, «Cibercrimen y delitos informaticos,» Erreius, 2022.
- [3] K. Alkanan, Y. Zhong, X. Luo y R. Dong, «Advanced multimodal biometric authentication for IoT-enabled smart home security: Integrating deep learning-based face recognition with behavioral patterns,» *Kuwait Journal of Science*, vol. 53, p. 100548, 2026.
- [4] V. Koreddi, V. Kshatriya, D. Bhavishya, C. Gowtami, K. Divya y K. Anitha, «Real-Time Menstrual Discomfort Detection Using AI-Powered Facial Recognition in Structured Environments,» *International Journal of Engineering and Manufacturing (IJEM)*, vol. 16, nº 6, pp. 60-71, 2025.
- [5] B. Koşmaz, Ö. Bingöl, E. Gedikli, M. Ekinici, R. Doğan, S. Türk y N. Güngör, «A Video-Based Mobile Palmprint Dataset and an Illumination-Robust Deep Learning Architecture for Unconstrained Environments,» *Applied Sciences*, vol. 15, nº 21, p. 11368, 2025.
- [6] S. Chong, L. Chong y K. Wee, «Enhancing Masked Face Recognition with Real-Time Eye Blink Detection for Secure Access Control,» *2025 14th International Conference on Software and Computer Applications*, vol. 2, nº 3, p. 198–203, 2025.
- [7] J. Redmon, «YOLO9000: Better, Faster, Stronger,» 2016.
- [8] R. Girshick, «Fast R-CNN,» 2015.

- [9] L. Tovar y E. Martín, «Diseño e implementación de un sistema de biometría facial para el control de acceso en instituciones de educación superior,» *Revista espacios* , 2020.
- [10] K. Cumbe y L. Potosí, «Desarrollo de un sistema de control de acceso mediante reconocimiento facial,» ISU, 2023.
- [11] J. Mite, "Diseño de una infraestructura que permita el ingreso al campamento comercial de TELCONET Guayaquil," UPS, 2025.
- [12] J. González y M. Zhindón, «Plataforma de servicios de reconocimiento facial para detección de prófugos de la justicia en Ecuador,» *SCIENCE AND RESEARCH*, vol. II, nº 2, pp. 32-41, 2020.
- [13] J. Guevara, «Sistema de reconocimiento facial en tiempo real basado en CNN para el control de acceso de los residentes de un conjunto habitacional,» Universidad de Lima, 2024.
- [14] D. Salcedo, «Diseño e implementación de un sistema de reconocimiento facial como medida de identificación para los sistemas de control de acceso del Metro de Medellín,» 2023.
- [15] S. Elnozahy, S. Pari y L. Liang, «Raspberry Pi-Based Face Recognition Door Lock System,» *IoT*, vol. 6, nº 2, p. 31, 2025.
- [16] Z. Khan, W. Ahmed y P. Liatsis, «AMD-FV: Adaptive margin loss and dual path network+ for deep face verification,» *PLOS One*, vol. 20, nº 5, p. e0324485, 2025.
- [17] A. Silva y R. Farias, «AD-VAE: Adversarial Disentangling Variational Autoencoder,» *Sensors*, vol. 25, nº 5, p. 1574, 2025.
- [18] C. M. O. Moncayo, «SISTEMA DE DETECCIÓN TEMPRANA DE EVENTOS DELICTIVOS EN ENTIDADES COMERCIALES CON VISIÓN ARTIFICIAL Y DEEP LEARNING,» Universidad Técnica de Ambato, AMBATO, 2025.

- [19] S. Hernández , C. Fernández y P. Baptista, Metodología de la investigación, Printed: Mc Graw Hill, 2021.
- [20] L. Matilla, «Análisis de fiabilidad de sistema de reconocimiento facial centralizado basado en técnicas de Deep Learning,» 2025.
- [21] A. Mohamed, A. Salama, N. Shebka y A. Ismail, «Enhancing Network Access Control using Multi-Modal Biometric Authentication Framework,» *Engineering, Technology & Applied Science Research*, vol. 15, nº 1, pp. 20144-20150, 2025.
- [22] S. Pecolt, A. Błażejowski, T. Królikowski, I. Maciejewski, K. Gierula y S. Glowinski, «Personal Identification Using Embedded Raspberry Pi-Based Face Recognition Systems,» *Applied Sciences*, vol. 15, nº 2, p. 887, 2025.
- [23] U. Sumalatha, K. Prakasha, S. Prabhu y V. Nayak, «Secure Knuckle Print Authentication: Template Protection and Attack Analysis,» *IEEE Access*, vol. 13, p. 144560–144577, 2025.
- [24] F. Abdiwi, «Account Login and Database Access Control System with Time Attendance through Facial Recognition,» *Journal of Applied Engineering and Technological Science*, vol. 6, nº 1, p. 380–392, 2024.
- [25] H. Ma, S. Wang, Y. Gao, Z. Zhang, H. Qiu, M. Xue, A. Abuadbbba, A. Fu, S. Nepal y D. Abbott, «Watch Out! Simple Horizontal Class Backdoor Can Trivially Evade Defense,» *Proceedings of the 2024 ACM SIGSAC Conference on Computer and Communications Security (CCS '24)*, vol. 6, nº 2, p. 4465–4479, 2024.
- [26] D. Tribuana, Hazriani y A. Arda, «Face recognition for smart door security access with convolutional neural network method,» *TELKOMNIKA Telecommunication Computing Electronics and Control*, vol. 22, nº 3, p. 702–710, 2024.

- [27] L. Xu y D. Zheng, «Face Mask Segmentation Method Combining Salient Features and Gender Constraints,» *Traitement du Signal*, vol. 40, nº 2, p. 629–637, 2023.
- [28] R. Hwang, J. Lin, S. Hsieh, H. Lin y C. Lin, «Adversarial Patch Attacks on Deep-Learning-Based Face Recognition Systems Using Generative Adversarial Networks,» *Sensors*, vol. 23, nº 2, p. 853, 2023.
- [29] X. Ibarreche, C. Martínez y C. Di Lorenzo, «Reconocimiento facial y tecnologías de vigilancia en América Latina,» de *Reconocimiento facial y tecnologías de vigilancia en América Latina*, A1sur, 2020, p. 320.
- [30] C. Niola y W. Sanango, «Desarrollo de un software de seguridad para detección y reconocimiento facial basados en los algoritmos de Viola-Jones,» UPS, 2020.
- [31] J. Herrera, «Implementación de un prototipo para la detección de rostros utilizando el lenguaje de programación Python,» 2022.

ANEXOS

Anexo A Matriz validación entrevista

Título del instrumento:

Entrevista dirigida al personal directivo o encargado de seguridad institucional

Objetivo del instrumento: Validar la pertinencia de las preguntas orientadas al diagnóstico del proceso actual de control de acceso en las áreas de cajas y bóveda de la Cooperativa de Ahorro y Crédito SOL.

Técnica de recolección de información: Entrevista

Tipo de instrumento: Guía de entrevista semiestructurada

Método de validación: Juicio de expertos

Escala de valoración:

Valor Criterio

1 Deficiente

2 Regular

3 Bueno

4 Excelente

Criterios de evaluación:

Criterio Descripción

Claridad La pregunta está redactada de forma comprensible y sin ambigüedad.

Coherencia La pregunta guarda relación lógica con el tema de investigación.

Pertinencia La pregunta aporta al cumplimiento de los objetivos de la investigación.

Relevancia La pregunta permite obtener información útil para el diagnóstico del problema.

Matriz de validación del instrumento:

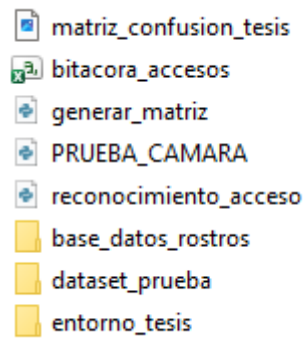
N.º	Pregunta	de Claridad	Coherencia	Pertinencia	Relevancia	Promedio	Resultado	Observación
1	Desde su perspectiva, ¿cómo evalúa el sistema actual de control de acceso en las áreas de cajas y bóveda?	4	4	4	4	4.00	Aceptada	Sin observaciones
2	¿Qué riesgos considera que existen actualmente en el control de acceso a estas áreas críticas?	4	4	4	4	4.00	Aceptada	Sin observaciones
3	¿Ha experimentado la institución situaciones de anomalía o eventos vinculados con el ingreso de personal sin	4	4	4	4	4.00	Aceptada	Sin observaciones

	de las actividades del personal?							
	¿Qué importancia considera que tiene							
6	fortalecer los sistemas de protección en dichos espacios?	4	4	4	4	4.00	Aceptada	Sin observaciones
	¿Qué atributos debería reunir una plataforma óptima de gestión de ingresos para alinearse con los protocolos de seguridad requeridos por la institución?							
7		4	4	4	4	4.00	Aceptada	Sin observaciones
	¿Cuál es su opinión sobre la							
8		4	4	4	4	4.00	Aceptada	Sin observaciones

	implementación de tecnologías biométricas, específicamente el reconocimiento facial, para el control de acceso?								
9	¿Considera factible integrar una plataforma automatizada de identificación mediante rasgos faciales en la cooperativa?	4	4	4	4	4.00	Aceptada	Sin observaciones	
	¿Cuáles serían sus razones?								
10	¿Qué ventajas prevé alcanzar mediante la adopción de una solución	4	4	4	4	4.00	Aceptada	Sin observaciones	

11	automatizada para la gestión de accesos? ¿Qué factores económicos, tecnológicos o humanos podrían influir en la adopción de este tipo de solución? ¿Qué sugerencias ofrecería para garantizar el despliegue adecuado y la durabilidad a largo plazo de la solución tecnológica?	4	4	4	4	4.00	Aceptada	Sin observaciones
12	¿Qué sugerencias ofrecería para garantizar el despliegue adecuado y la durabilidad a largo plazo de la solución tecnológica?	4	4	4	4	4.00	Aceptada	Sin observaciones

Anexo B. Captura de carpeta de desarrollo



Anexo C. Código del aplicativo con Deep Learning

```
import cv2
from deepface import DeepFace
import os
import csv
import time
from datetime import datetime

# 1. Configuraciones iniciales
db_path = "base_datos_rostros"
archivo_bitacora = "bitacora_accesos.csv"

# 2. Crear el archivo de bitácora con los encabezados si no existe
if not os.path.exists(archivo_bitacora):
    with open(archivo_bitacora, mode='w', newline="", encoding='utf-8') as file:
        writer = csv.writer(file)
        writer.writerow(["Fecha", "Hora", "Identidad", "Tipo_Evento", "Resultado"])

# 3. Inicializar la cámara web y el detector rápido
cap = cv2.VideoCapture(0)
face_cascade = cv2.CascadeClassifier(cv2.data.harcascades +
'haarcascade_frontalface_default.xml')

# Variables de estado
nombre_reconocido = "Analizando..."
```

```

color_interfaz = (255, 0, 0)
frame_count = 0
modo_evento = "Entrada" # Por defecto inicia registrando entradas
ultimo_registro_tiempo = 0
cooldown_segundos = 10 # Espera 10 segundos antes de volver a registrar a la
misma persona

print("Motor iniciado...")
print("Presiona 'e' para cambiar a modo Entrada.")
print("Presiona 's' para cambiar a modo Salida.")
print("Presiona 'q' en la ventana de video para salir.")

while True:
    ret, frame = cap.read()
    if not ret:
        break

    frame_count += 1
    tiempo_actual = time.time()

    gray = cv2.cvtColor(frame, cv2.COLOR_BGR2GRAY)
    rostros = face_cascade.detectMultiScale(gray, scaleFactor=1.1, minNeighbors=5,
minSize=(50, 50))

    if len(rostros) > 0 and frame_count % 30 == 0:
        try:
            resultados = DeepFace.find(img_path=frame, db_path=db_path,
enforce_detection=False, silent=True)

            # Variables por defecto para el registro
            identidad_registro = "Desconocido"
            resultado_registro = "Denegado"

```

```

if len(resultados) > 0 and len(resultados[0]) > 0:
    ruta_archivo = resultados[0].iloc[0]['identity']
    nombre_base = os.path.basename(ruta_archivo).split('.')[0]

    nombre_reconocido = f'Acceso Permitido: {nombre_base.upper()}'
    color_interfaz = (0, 255, 0)
    identidad_registro = nombre_base.upper()
    resultado_registro = "Autorizado"
else:
    nombre_reconocido = "Acceso Denegado: Desconocido"
    color_interfaz = (0, 0, 255)

# 4. Lógica de guardado en la bitácora digital
if (tiempo_actual - ultimo_registro_tiempo) > cooldown_segundos:
    ahora = datetime.now()
    fecha_str = ahora.strftime("%Y-%m-%d")
    hora_str = ahora.strftime("%H:%M:%S")

    # Escribir la fila en el archivo CSV
    with open(archivo_bitacora, mode='a', newline="", encoding='utf-8') as
file:
        writer = csv.writer(file)
        writer.writerow([fecha_str, hora_str, identidad_registro, modo_evento,
resultado_registro])

    ultimo_registro_tiempo = tiempo_actual
    print(f'Registro guardado: {fecha_str} {hora_str} | {identidad_registro} |
{modo_evento} | {resultado_registro}')

except ValueError:
    pass

# 5. Controles de teclado

```

```

tecla = cv2.waitKey(1) & 0xFF
if tecla == ord('q'):
    break
elif tecla == ord('e'):
    modo_evento = "Entrada"
elif tecla == ord('s'):
    modo_evento = "Salida"

# 6. Dibujar la interfaz
for (x, y, w, h) in rostros:
    cv2.rectangle(frame, (x, y), (x+w, y+h), color_interfaz, 2)
    cv2.rectangle(frame, (x, y - 35), (x + len(nombre_reconocido) * 15, y),
color_interfaz, cv2.FILLED)

    # Mostrar el modo actual en la esquina superior izquierda
    cv2.putText(frame, f'Modo: {modo_evento}', (10, 30),
cv2.FONT_HERSHEY_SIMPLEX, 0.8, (0, 255, 255), 2)
    # Mostrar el nombre sobre el rostro
    cv2.putText(frame, nombre_reconocido, (x + 5, y - 10),
cv2.FONT_HERSHEY_SIMPLEX, 0.6, (255, 255, 255), 2)

cv2.imshow('Sistema de Acceso - Boveda/Cajas', frame)

cap.release()
cv2.destroyAllWindows()

```

Anexo D. Código para la matriz de confusión del aplicativo de Deep Learning

```

import cv2
from deepface import DeepFace
import os
import matplotlib.pyplot as plt

```

```

import seaborn as sns
from sklearn.metrics import confusion_matrix, classification_report

# 1. Rutas de las carpetas
db_path = "base_datos_rostros" # Tu base de datos original (tu foto de referencia)
carpeta_prueba = "dataset_prueba"

# 2. Listas para guardar la realidad (y_true) y las predicciones (y_pred)
etiquetas_reales = []
predicciones_modelo = []

print("Iniciando evaluación del modelo. Esto tomará unos minutos...")

# 3. Función para evaluar una carpeta específica
def evaluar_carpeta(subcarpeta, etiqueta_real):
    ruta_completa = os.path.join(carpeta_prueba, subcarpeta)
    if not os.path.exists(ruta_completa):
        print(f"La carpeta {ruta_completa} no existe. Por favor créala.")
        return

    for archivo in os.listdir(ruta_completa):
        if archivo.lower().endswith(('png', 'jpg', 'jpeg')):
            ruta_imagen = os.path.join(ruta_completa, archivo)

            # La realidad es la que le indicamos nosotros
            etiquetas_reales.append(etiqueta_real)

            try:
                # El modelo intenta predecir quién es
                resultados = DeepFace.find(img_path=ruta_imagen, db_path=db_path,
enforce_detection=False, silent=True)

                # Analizar la predicción

```

```

        if len(resultados) > 0 and len(resultados[0]) > 0:
            predicciones_modelo.append("Autorizado")
        else:
            predicciones_modelo.append("Denegado")

    except ValueError:
        # Si no detecta rostro o hay error, asumimos que deniega el acceso
        predicciones_modelo.append("Denegado")

# 4. Procesar las fotos de prueba
evaluar_carpeta("autorizados", "Autorizado")
evaluar_carpeta("denegados", "Denegado")

# 5. Generar la Matriz de Confusión Matemática
clases = ["Autorizado", "Denegado"]
matriz = confusion_matrix(etiquetas_reales, predicciones_modelo, labels=clases)

# 6. Dibujar y guardar el gráfico de la Matriz
plt.figure(figsize=(8, 6))
sns.heatmap(matriz, annot=True, fmt='d', cmap='Blues', xticklabels=clases,
            yticklabels=clases)
plt.title('Matriz de Confusión - Sistema de Acceso')
plt.xlabel('Predicción del Modelo')
plt.ylabel('Realidad (Ground Truth)')

# Guardar la imagen en alta calidad para la tesis
plt.savefig('matriz_confusion_tesis.png', dpi=300, bbox_inches='tight')
print("\n¡Evaluación terminada! Se ha guardado el archivo 'matriz_confusion_tesis.png'")

# 7. Mostrar un reporte de métricas en la terminal
print("\n--- Reporte de Métricas ---")
print(classification_report(etiquetas_reales, predicciones_modelo, labels=clases))

```

Anexo E. Código de la captura de datos

```
import cv2
import os

nombre = "Santiago"
ruta_datos = "data_rostros"
ruta_persona = os.path.join(ruta_datos, nombre)

if not os.path.exists(ruta_persona):
    os.makedirs(ruta_persona)

cap = cv2.VideoCapture(0)
face_cascade = cv2.CascadeClassifier(cv2.data.haarcascades +
'haarcascade_frontalface_default.xml')
count = 0

while True:
    ret, frame = cap.read()
    if not ret: break
    gray = cv2.cvtColor(frame, cv2.COLOR_BGR2GRAY)
    rostros = face_cascade.detectMultiScale(gray, 1.1, 5)

    for (x, y, w, h) in rostros:
        rostro_recortado = gray[y:y+h, x:x+w]
        rostro_redimensionado = cv2.resize(rostro_recortado, (150, 150))
        cv2.imwrite(f'{ruta_persona}/rostro_{count}.jpg', rostro_redimensionado)
        cv2.rectangle(frame, (x, y), (x+w, y+h), (0, 255, 0), 2)
        count += 1

cv2.imshow('Capturando Rostros', frame)
```

```
# Se detiene al llegar a 300 fotos o al presionar la letra q
if cv2.waitKey(1) == ord('q') or count >= 300:
    break

cap.release()
cv2.destroyAllWindows()
print(f'Se capturaron {count} rostros exitosamente')
```

Anexo F. Código del entrenamiento del modelo

```
import cv2
import os
import numpy as np

ruta_datos = "data_rostros"
lista_personas = os.listdir(ruta_datos)
etiquetas = []
datos_rostros = []
etiqueta_actual = 0

for persona in lista_personas:
    ruta_persona = os.path.join(ruta_datos, persona)
    for archivo in os.listdir(ruta_persona):
        ruta_imagen = os.path.join(ruta_persona, archivo)
        imagen = cv2.imread(ruta_imagen, 0)
        datos_rostros.append(imagen)
        etiquetas.append(etiqueta_actual)
    etiqueta_actual += 1

recognizer = cv2.face.LBPHFaceRecognizer_create()
print("Entrenando el modelo, espera un momento...")
recognizer.train(datos_rostros, np.array(etiquetas))
```

```
recognizer.write("modelo_lbph.yml")
print("Modelo entrenado y guardado como modelo_lbph.yml")
```

Anexo G. Código del reconocimiento facial con Aprendizaje supervisado

```
import cv2
import os
import csv
import time
from datetime import datetime

# 1. Configuraciones iniciales
ruta_datos = "data_rostros"
lista_personas = os.listdir(ruta_datos)
archivo_bitacora = "bitacora_accesos_lbph.csv"

# 2. Crear el archivo de bitácora con los encabezados si no existe
if not os.path.exists(archivo_bitacora):
    with open(archivo_bitacora, mode='w', newline="", encoding='utf-8') as file:
        writer = csv.writer(file)
        writer.writerow(["Fecha", "Hora", "Identidad", "Tipo_Evento", "Resultado"])

# 3. Cargar el modelo LBPH y la cámara
recognizer = cv2.face.LBPHFaceRecognizer_create()
recognizer.read("modelo_lbph.yml")
face_cascade = cv2.CascadeClassifier(cv2.data.haarcascades +
'haarcascade_frontalface_default.xml')
cap = cv2.VideoCapture(0)

# Variables de estado
modo_evento = "Entrada"
ultimo_registro_tiempo = 0
```

```

cooldown_segundos = 10

print("Motor LBPH iniciado...")
print("Presiona 'e' para cambiar a modo Entrada.")
print("Presiona 's' para cambiar a modo Salida.")
print("Presiona 'q' para salir.")

while True:
    ret, frame = cap.read()
    if not ret: break

    tiempo_actual = time.time()
    gray = cv2.cvtColor(frame, cv2.COLOR_BGR2GRAY)
    rostros = face_cascade.detectMultiScale(gray, 1.1, 5)

    for (x, y, w, h) in rostros:
        rostro_recortado = gray[y:y+h, x:x+w]
        rostro_redimensionado = cv2.resize(rostro_recortado, (150, 150))

        etiqueta, confianza = recognizer.predict(rostro_redimensionado)

        identidad_registro = "Desconocido"
        resultado_registro = "Denegado"

        if confianza < 70:
            nombre = lista_personas[etiqueta]
            identidad_registro = nombre.upper()
            resultado_registro = "Autorizado"
            color = (0, 255, 0)
            texto = f"Permitido: {identidad_registro}"
        else:
            color = (0, 0, 255)
            texto = "Denegado: Desconocido"

```

```

# Lógica de guardado en la bitácora digital
if (tiempo_actual - ultimo_registro_tiempo) > cooldown_segundos:
    ahora = datetime.now()
    fecha_str = ahora.strftime("%Y-%m-%d")
    hora_str = ahora.strftime("%H:%M:%S")

    with open(archivo_bitacora, mode='a', newline="", encoding='utf-8') as file:
        writer = csv.writer(file)
        writer.writerow([fecha_str, hora_str, identidad_registro, modo_evento,
resultado_registro])

    ultimo_registro_tiempo = tiempo_actual
    print(f'Registro guardado: {fecha_str} {hora_str} | {identidad_registro} |
{modo_evento} | {resultado_registro}')

# Dibujar la interfaz sobre el video
cv2.rectangle(frame, (x, y), (x+w, y+h), color, 2)
cv2.rectangle(frame, (x, y - 35), (x + len(texto) * 15, y), color, cv2.FILLED)
cv2.putText(frame, texto, (x + 5, y - 10), cv2.FONT_HERSHEY_SIMPLEX,
0.6, (255, 255, 255), 2)

# Mostrar el modo actual en la esquina
cv2.putText(frame, f'Modo: {modo_evento}', (10, 30),
cv2.FONT_HERSHEY_SIMPLEX, 0.8, (0, 255, 255), 2)

# Controles de teclado
tecla = cv2.waitKey(1) & 0xFF
if tecla == ord('q'):
    break
elif tecla == ord('e'):
    modo_evento = "Entrada"
elif tecla == ord('s'):

```

```

modo_evento = "Salida"

cv2.imshow('Reconocimiento LBPH con Bitacora', frame)

cap.release()
cv2.destroyAllWindows()

```

Anexo H. Código para la matriz de confusión del aplicativo de Aprendizaje supervisado

```

import cv2
import os
import numpy as np
import matplotlib.pyplot as plt
import seaborn as sns
from sklearn.metrics import confusion_matrix, classification_report

carpeta_prueba = "dataset_prueba"
archivo_modelo = "modelo_lbph.yml"

recognizer = cv2.face.LBPHFaceRecognizer_create()
recognizer.read(archivo_modelo)

face_cascade = cv2.CascadeClassifier(cv2.data.haarcascades +
'haarcascade_frontalface_default.xml')

etiquetas_reales = []
predicciones_modelo = []

def evaluar_carpeta(subcarpeta, etiqueta_real):
    ruta_completa = os.path.join(carpeta_prueba, subcarpeta)
    if not os.path.exists(ruta_completa):
        print(f'Falta la carpeta {ruta_completa}')

```

```

return

for archivo in os.listdir(ruta_completa):
    if archivo.lower().endswith(('.png', '.jpg', '.jpeg')):
        ruta_imagen = os.path.join(ruta_completa, archivo)
        etiquetas_reales.append(etiqueta_real)

        imagen = cv2.imread(ruta_imagen)
        gray = cv2.cvtColor(imagen, cv2.COLOR_BGR2GRAY)
        rostros = face_cascade.detectMultiScale(gray, 1.1, 5)

        if len(rostros) > 0:
            # Tomar solo el primer rostro detectado en la foto
            (x, y, w, h) = rostros[0]
            rostro_recortado = gray[y:y+h, x:x+w]
            rostro_redimensionado = cv2.resize(rostro_recortado, (150, 150))

            etiqueta, confianza = recognizer.predict(rostro_redimensionado)

            # Menor a 70 significa buena similitud en LBPH
            if confianza < 70:
                predicciones_modelo.append("Autorizado")
            else:
                predicciones_modelo.append("Denegado")
        else:
            predicciones_modelo.append("Denegado")

evaluar_carpeta("autorizados", "Autorizado")
evaluar_carpeta("denegados", "Denegado")

clases = ["Autorizado", "Denegado"]
matriz = confusion_matrix(etiquetas_reales, predicciones_modelo, labels=clases)

```

```

plt.figure(figsize=(8, 6))
sns.heatmap(matriz, annot=True, fmt='d', cmap='Blues', xticklabels=clases,
yticklabels=clases)
plt.title('Matriz de Confusión - Modelo LBPH')
plt.xlabel('Predicción del Modelo')
plt.ylabel('Realidad (Ground Truth)')

plt.savefig('matriz_lbph_tesis.png', dpi=300, bbox_inches='tight')
print("Evaluación terminada y gráfico guardado exitosamente")
print(classification_report(etiquetas_reales, predicciones_modelo, labels=clases))

```

Anexo I Validación cámara



