UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE INGENIERÍA

CARRERA DE INGENIERÍA EN CIENCIAS DE LA COMPUTACIÓN

TEMA:

Implementación de un sistema de registro de accesos para empleados mediante reconocimiento facial con aprendizaje profundo en una bitácora digital para una empresa de seguridad.

AUTOR:
Sangurima Martínez, Joseph Andrick
Orellana Suarez, Hugolino

Trabajo de Integración Curricular previo a la obtención del título de INGENIERO EN CIENCIAS DE LA COMPUTACIÓN

TUTOR:
PhD. Castro Aguilar, Gilberto Fernando MSc.

Guayaquil – Ecuador
17 de febrero de 2025

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE INGENIERÍA

CARRERA DE INGENIERÍA EN CIENCIAS DE LA COMPUTACIÓN

CERTIFICACIÓN

Certificamos que el presente trabajo de integración curricular fue realizado en su totalidad por el **Sr. Sangurima Martínez, Joseph Andrick y Sr. Orellana Suarez, Hugolino** como requerimiento para la obtención del título de **Ingeniero en Ciencias de la Computación.**

TUTOR

f. _____
PhD. Castro Aguilar, Gilberto Fernando MSc.

Guayaquil, 17 de febrero del año 2025

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE INGENIERÍA

CARRERA DE INGENIERÍA EN CIENCIAS DE LA COMPUTACIÓN

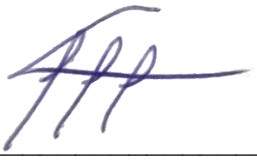
DECLARACIÓN DE RESPONSABILIDAD

Nosotros**, Sangurima Martínez, Joseph Andrick**
Orellana Suarez, Hugolino

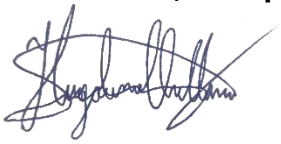
DECLARAMOS QUE:

El Trabajo de Integración Curricular, "**Implementación de un Sistema de Registro de Accesos para Empleados mediante Reconocimiento Facial con Aprendizaje Profundo en una Bitácora Digital para una Empresa de Seguridad''** previo a la obtención del título de **INGENIERO EN CIENCIAS DE LA COMPUTACIÓN**.' ha sido desarrollado respetando derechos intelectuales de terceros conforme las citas que constan en el documento, cuyas fuentes se incorporan en las referencias o bibliografías. Consecuentemente este trabajo es de nuestra total autoría.
En virtud de esta declaración, nos responsabilizamos del contenido, veracidad y alcance del Trabajo de Integración Curricular referido.

Guayaquil, 17 de febrero del año 2025



f. _____
Sangurima Martínez, Joseph Andrick



f. _____
Orellana Suarez, Hugolino

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE INGENIERÍA

CARRERA DE INGENIERÍA EN CIENCIAS DE LA COMPUTACIÓN

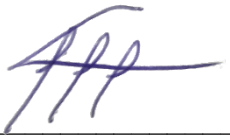
AUTORIZACIÓN

Nosotros**, Sangurima Martínez, Joseph Andrick**
Orellana Suarez, Hugolino

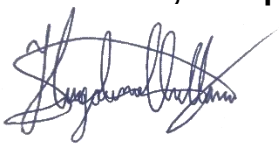
Autorizamos a la Universidad Católica de Santiago de Guayaquil a la **publicación** en la biblioteca de la institución del Trabajo de Integración Curricular, "**Implementación de un Sistema de Registro de Accesos para Empleados mediante Reconocimiento Facial con Aprendizaje Profundo en una Bitácora Digital para una Empresa de Seguridad"**, cuyo contenido, ideas y criterios son de nuestra exclusiva responsabilidad y total autoría.

Guayaquil, a los 17 días del mes de febrero del año 2025

LOS AUTORES:



f. _____
Sangurima Martínez, Joseph Andrick



f. _____
Orellana Suarez, Hugolino

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE INGENIERÍA

CARRERA DE INGENIERÍA EN CIENCIAS DE LA COMPUTACIÓN

REPORTE ANTIPLAGIO

INFORME DE ANÁLISIS
magister

20250206-PT FORMATO TRABAJO INTEGRACION CURRICULAR COMPUTACION

4% Textos sospechosos

< 1% Similitudes
0% similitudes entre comillas
< 1% entre las fuentes mencionadas
2% Idiomas no reconocidos
41% Textos potencialmente generados por la IA (ignorado)

Nombre del documento: 20250206-PT FORMATO TRABAJO INTEGRACION CURRICULAR COMPUTACION.docx
ID del documento: 40316a7dcb832d8b42867612d287aee9361d359c
Tamaño del documento original: 8,67 MB
Autores: []

Depositante: Gilberto Fernando Castro Aguilar
Fecha de depósito: 6/2/2025
Tipo de carga: interface
fecha de fin de análisis: 6/2/2025

Número de palabras: 19.169
Número de caracteres: 131.692

Ubicación de las similitudes en el documento:

Firma:

Firmado electrónicamente por:
GILBERTO FERNANDO CASTRO AGUILAR

PhD. Gilberto Fernando Castro Aguilar, MSc.
Tutor de Trabajo de Integración Curricular
Carrera de Ingeniería en Ciencias de la Computación

AGRADECIMIENTO

Agradezco a Dios y a mis padres cuyo apoyo incondicional fue el cimiento de cada logro que alcancé. Gracias por siempre estar presentes. Por sus palabras de aliento en los momentos difíciles. Y por siempre creer en mí, incluso cuando yo mismo no lo hacía.

A los profesores y tutores: por guiarme y mostrarme el valor de la interdisciplinariedad. Sus enseñanzas que no solo enriquecieron mi formación académica, sino también inspiraron la visión integradora de este trabajo. Sus criticas constructivas y consejos fueron faros en este proceso.

A mi familia, a mis amigos, a mis compañeros de estudios y a todos lo que aportaron con su entusiasmo para poder concluir con este trabajo. Agradezco cada pequeño gesto, desde una sugerencia técnica, hasta una palabra de ánimo. Gracias a ustedes.

Hugolino Orellana Suarez

Le doy gracias a mi padre y mi madre que fueron las personas que me ayudaron a lograr este objetivo en mi vida, me dieron en cada momento su apoyo y amor incondicional incluso cuando me sentía perdido y sin saber a donde ir, ellos me ayudaron a encontrar el camino correcto y me ayudaron a superarme cada día, por eso cada día trato de ser mejor que ayer. A mi esposa y a mi hija que siempre supieron que decirme cuando me sentía muy desanimado.

A mis abuelitos que en paz descansen que me enseñaron todo lo que se y me enseñaron como ser una mejor persona, gracias papito Pepe, gracias mamita Clara, gracia abuelita Vicenta. A toda mi familia que siempre confió en mí en cada paso que daba, mis primos que son mis hermanos.

Gracias a los amigos que conocí en esta travesía que me apoyaban en todo momento, que siempre estuvieron apoyándome y enriqueciendo mis conocimientos con cosas nuevas. A los buenos profesores y tutores que nos brindaron su ayuda, críticas constructivas. Gracias a todos ustedes y a Dios.

Joseph Andrick Sangurima Martínez

DEDICATORIA

A mis abuelos y a mis padres por ser mis mentores en la vida.

Hugolino Orellana Suarez

A mi abuelito Pepe, a mi abuelita Clara, mi abuelita Vicenta, a mi padre, a mi madre, a mi hija, a mi esposa por ser las personas que mas me apoyaron en esta etapa de mi vida.

Joseph Andrick Sangurima Martínez

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE INGENIERÍA

CARRERA DE INGENIERÍA EN CIENCIAS DE LA COMPUTACIÓN

TRIBUNAL DE SUSTENTACIÓN

f. _____
Mgs. Camacho
Coronel, Ana Ing.
DIRECTORA DE CARRERA

f. _____
Mgs. Erazo Ayón, José Miguel Ing.
DOCENTE DE LA CARRERA

f. _____
Mgs. Sosa Rendon, Ismael Alberto, Ing.
OPONENTE

ÍNDICE

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

El presente trabajo de integración curricular propone el desarrollo de un sistema de registro de accesos para empleados usando reconocimiento facial con aprendizaje profundo, cuyo objetivo es el reconocimiento eficiente del rostro de los empleados de la empresa de seguridad mediante algoritmos de aprendizaje profundo mejorando así el sistema de reconocimiento facial para evitar falsos positivos y falsos negativos. La investigación empleo una metodología aplicada y especifica, así como un marco SCRUM, utilizando técnicas de reconocimiento facial, redes neuronales convolucionales (CNN), algoritmos de aprendizaje profundo para para optimizar los tiempos en el proceso de entrada y salida de los empleados de la empresa. Se diseño y desarrollo un prototipo funcional que se adaptó a las mejoras que se dieron a conocer a medida que se realizaban las reuniones que se dieron tanto virtuales como presenciales, se desarrolló una serie de pruebas en entornos controlados con cada versión del sistema desde la versión 1.0 hasta la versión 4.0 para comprobar el correcto funcionamiento en cada uno de ellos de la conexión con la base de datos, la carga de los datos a la base de datos, la muestra de los datos de la persona una vez que se reconozca su rostro para indicar su entrada o salida, el reconocimiento continuo del rostro en la sección de reconocimiento facial, las validaciones pertinentes y el sistema de reconocimiento facial con aprendizaje profundo, la versión final del sistema es la versión 4.0, dicha versión se implementó de manera correcta en la empresa cumpliendo las expectativas de la empresa y funcionando de manera óptima en medida de lo solicitado.

Palabras clave: Reconocimiento facial, Aprendizaje profundo, Registro de accesos, Redes neuronales convolucionales (CNN), SCRUM, Python.

ABSTRACT

The present study proposes the development of an access registration system for employees using facial recognition with deep learning, whose objective is the efficient recognition of the face of employees of the security company using deep learning algorithms, thus improving the facial recognition system. to avoid false positives and false negatives. The research used an applied and specific methodology, as well as a SCRUM framework, using facial recognition techniques, convolutional neural network (CNN), deep learning algorithms to optimize times in the entry and exit process of the company's employees. company. A functional prototype was designed and developed that was adapted to the improvements that were announced as the meetings were held, both virtual and in-person, a series of tests were developed in controlled environments with each version of the system from the previous version. 1.0 to version 4.0 to check the correct operation in each of them of the connection with the database, the loading of the data to the database, the display of the person's data once their face is recognized to indicate your entry or exit, the continuous recognition of the face in the facial recognition section, the relevant validations and the facial recognition system with deep learning, the final version of the system is version 4.0, this version was implemented correctly in the company, meeting the expectations of the company and functioning optimally as requested.

Key words: Face recognition, Deep learning, Access logging, Convolutional neural networks (CNN), SCRUM, Python.

INTRODUCCIÓN

En la actualidad, una de las innovaciones que mayor impacto han tenido en la tecnología, es la inteligencia artificial, que representa un campo de estudio y desarrollo que ha transfigurado significativamente diversos sectores, como en la medicina, sectores industriales o la informática.

La IA, se refiere a la habilidad de los aparatos para utilizar algoritmos, adquirir conocimientos de datos y utilizar este aprendizaje en la toma de decisiones, replicando conductas humanas.

Según Rouhiainen (2018), la inteligencia artificial permite a los sistemas realizar tareas complejas como el análisis de datos, la clasificación y el reconocimiento de patrones, lo que ha dado lugar a aplicaciones prácticas de gran relevancia en múltiples áreas.

Se conoce como *machine Learning*, a una subdivisión de la IA. Esta técnica es el entrenamiento automático que utiliza la máquina, para obtener conocimientos, sin ser programadas en una circunstancia específica, es aseverar que se puede deducir que la maquina en su término aprende en forma autónoma.

El aprendizaje automático, a través de la exploración de patrones en grandes cantidades de datos, facilita la implementación de soluciones automatizadas y adaptativas. Por ejemplo, filtros de spam en correos electrónicos son capaces de distinguir entre mensajes legítimos y no deseados basándose en patrones antes identificados (Rouhiainen, 2018).

The Deep Learning (aprendizaje profundo), que es una rama del aprendizaje

automático, se emplea para resolver problemas de gran complejidad que usualmente requieren grandes volúmenes de información. Ocurre a través de la utilización de redes neuronales, que se estructuran en niveles para identificar relaciones y patrones complejos en la información. Su implementación protesta una amplia cantidad de datos y una robusta preparación para procesarlos.

Uno de los campos más destacados que ha aprovechado el aprendizaje profundo es el reconocimiento facial, una herramienta que combina la visión por computadora y técnicas avanzadas de IA para identificar y autenticar personas en lapso real.

Según autores como Pokhrel informan que, desde sus primeras aplicaciones en la década de 1990, esta tecnología ha evolucionado incluso convertirse en una pieza clave en sistemas de seguridad, comercio electrónico y dispositivos móviles. (Pokhrel, 2020)

En el sector de la informática, la dependencia de accesos y registros es una labor fundamental para atenazar el funcionamiento justo de sistemas y plataformas tecnológicas. Históricamente, estas operaciones se han administrado a través de bitácoras manuales, que tienen restricciones como fallos humanos, ausencia de datos y demoras en el registro.

Estas falencias ponen en riesgo la fiabilidad, complicando la toma de decisiones en circunstancias críticas. Las tecnologías de vanguardia, como la visión computacional y el aprendizaje profundo, contribuyen a superar estas restricciones, al facilitar la mecanización de los procedimientos de registro y gestión de accesos.

Desde esta perspectiva, las bitácoras digitales han emergido como una solución adecuada para afrontar estas carencias, al sustituir los registros tradicionales en papel

por sistemas electrónicos que facilitan la administración y supervisión de entradas y salidas de forma exacta. Una bitácora digital alude a un sistema creado para documentar y vigilar los movimientos de trabajadores, visitantes o cualquier otro individuo que ingrese a las instalaciones. No solo mejoran el proceso de registro estas herramientas, sino que incluso ofrecen un escenario más seguro para la administración de accesos.

La aplicación de tecnologías de vanguardia, como el reconocimiento facial, en estos sistemas digitales potencia incluso más su efectividad en las operaciones, estableciéndolos como una solución esencial en el sector de la seguridad.

El principal propósito de este trabajo de Integración curricular es crear un sistema automatizado de registro de accesos a través de métodos de aprendizaje profundo, incorporado a una bitácora digital ya existente en una compañía de seguridad.

Este sistema no solo facilitará el reconocimiento exacto y rápido de los trabajadores, sino incluso el robustecimiento de las acciones de seguridad en las instalaciones.

Al rebajar el riesgo de fallos y mejorar la administración de registros, el sistema aportará a una gestión eficaz y segura de los accesos. Asimismo, su incorporación tecnológica tiene como objetivo fomentar un modelo operativo más sólido y ajustado a las demandas del contexto actual.

El desarrollo de la solución sigue una estructura organizada de la siguiente manera: Capítulo I: Planteamiento y descripción del problema, objetivos del trabajo de Integración curricular y su justificación. Capítulo II: Marco teórico, literatura relacionada con inteligencia artificial, aprendizaje profundo, sistemas de reconocimiento facial y seguridad. Capítulo III: Metodología de la investigación, diseño del trabajo de Integración

curricular, herramientas utilizadas, desarrollo del sistema y evaluación de su desempeño en un entorno controlado. Capítulo IV: Desarrollo del trabajo de Integración curricular, descripción detallada de la construcción del sistema, incluyendo la selección de algoritmos, programación, integración con la bitácora digital y las pruebas realizadas en entornos controlados.

CAPÍTULO I

EL PROBLEMA

1.1 Descripción del problema.

Ecuador atraviesa en los últimos años una profunda crisis de seguridad. Una ola de delitos del catálogo de la delincuencia organizada, como extorsiones, robos de autos, secuestros, asaltos a negocios, narcotráfico y asesinatos han puesto en estado de alerta a la ciudadanía. Uno de los indicadores más alarmantes es el de muertes violentas. (Nino Cassanello Foghini, 2023)

Esta situación de inseguridad ha permitido un crecimiento y mayor creación de empresas de seguridad privada en el Ecuador, pero también se ha evidenciado que han surgido algunas de este tipo de empresas que podrían estar siendo infiltradas por organizaciones criminales, planteando el riesgo de que su funcionamiento termine beneficiando tanto a los delincuentes como a los sectores privados y gubernamentales que buscan protegerse. (Voss, 2024)

Las empresas de seguridad privada se han convertido en socios esenciales para las compañías y para el mismo gobierno aunando esfuerzos en la lucha contra el crimen organizado. (Voss, 2024)

El control preciso de accesos es un factor crucial en aspectos de seguridad para la protección de las instalaciones. Aunque muchas de estas empresas ya cuentan con bitácoras digitales, el registro manual de los accesos sigue siendo un proceso lento y

susceptible a errores humanos. Estos errores pueden incluir omisiones o datos inexactos, lo que compromete la calidad de los registros y dificulta la rápida verificación en situaciones de emergencia o auditoría.

La falta de procesos automatizados en el control de accesos incrementa las vulnerabilidades en las empresas de seguridad privada, dejando espacio para ineficiencias y riesgos potenciales. Esta problemática no solo afecta a las empresas que intentan proteger sus instalaciones y personal, sino que también repercute en la confianza de los clientes y en la percepción general de seguridad en el país.

La situación actual evidencia la necesidad de analizar las deficiencias en los procesos tradicionales de registro y control de accesos en el sector de seguridad privada. Este análisis servirá de apoyo para identificar las principales causas y síntomas de esta problemática, como los errores recurrentes en los registros manuales y la insuficiencia de herramientas tecnológicas para optimizar estas tareas. Asimismo, se plantea la importancia de estudiar el impacto que esta situación tiene en las empresas y en la sociedad, definiendo claramente las variables implicadas, como la precisión de los registros, la rapidez en la verificación y la capacidad de mitigar riesgos en tiempo real.

1.2 Formulación del problema.

El Ecuador atraviesa una grave crisis de seguridad que ha impactado significativamente a la sociedad y los sectores productivos. En 2023, el país registró más de 7.000 muertes violentas, lo que evidencia un incremento alarmante en la actividad delictiva, incluyendo extorsiones, robos, secuestros y narcotráfico, afectando principalmente a las provincias costeras (Ministerio del Interior, 2023). Este contexto ha llevado a un aumento en la demanda de servicios de seguridad privada, lo que ha

impulsado la proliferación de empresas dedicadas a la protección de personas e instalaciones.

Sin embargo, a pesar de su importancia estratégica, la gestión operativa de estas empresas presenta limitaciones significativas. Un aspecto crítico es el control de accesos, donde aún prevalecen métodos tradicionales basados en registros manuales o digitales simples. Estas prácticas son propensas a errores humanos, omisiones y manipulaciones, lo que compromete la confiabilidad de los registros y dificulta la verificación ágil en situaciones de emergencia o auditoría. Adicionalmente, la falta de estandarización en estos procesos genera vulnerabilidades que pueden ser explotadas tanto por actores externos como internos.

El impacto de estas deficiencias operativas se manifiesta en una creciente desconfianza hacia las empresas de seguridad privada y en la reducción de su capacidad para proteger eficazmente bienes y personas. Esta problemática afecta no solo a las empresas del sector, sino también a la percepción general de seguridad en la sociedad. Las limitaciones técnicas, como la dependencia de métodos tradicionales para el control de accesos, evidencian la carencia de herramientas tecnológicas avanzadas capaces de optimizar estos procesos críticos.

En un contexto donde la seguridad es una prioridad creciente, se hace necesario analizar y comprender las deficiencias de los sistemas actuales de registro de accesos. Este análisis permitirá identificar los factores clave que limitan la precisión, la confiabilidad y la rapidez en estos procesos, estableciendo una base sólida para abordar las necesidades del sector de seguridad privada en el Ecuador.

1.3 Justificación.

El Ecuador enfrenta una preocupante crisis de inseguridad que ha impulsado una creciente demanda de servicios de seguridad privada. Sin embargo, gran parte de las empresas de este sector sigue utilizando métodos manuales o sistemas digitales básicos para llevar a cabo el registro de accesos. Estas prácticas, aunque comunes, tienen importantes debilidades: son propensas a errores humanos, omisiones y manipulaciones, lo que compromete la precisión de los datos y dificulta la toma de decisiones en momentos clave. Esta situación no solo pone en riesgo la seguridad interna de las organizaciones, sino que también impacta negativamente en la confianza de sus clientes y en la efectividad general de las operaciones.

En contraste, los avances tecnológicos recientes ofrecen alternativas prácticas y poderosas para abordar este tipo de desafíos. Tecnologías como el reconocimiento facial y el aprendizaje profundo (*Deep Learning*) han demostrado ser herramientas de alto rendimiento para optimizar procesos sensibles como el control de accesos. Estas innovaciones permiten identificar a las personas con rapidez y precisión, minimizando errores y mejorando significativamente la eficiencia operativa.

Además, el entorno tecnológico actual en el Ecuador facilita la implementación de estas soluciones. La disponibilidad de hardware avanzado, redes de alta velocidad como la fibra óptica, conexiones inalámbricas robustas y plataformas de inteligencia artificial de código abierto ofrecen una base sólida para desarrollar sistemas de registro de accesos más confiables y modernos. Estas tecnologías no solo garantizan resultados más eficientes, sino que también hacen viable el desarrollo y la adopción de este tipo de proyectos con una inversión razonable.

Además, este proyecto muestra un punto muy importante como lo es el manejo

del código fuente del sistema, los beneficios que esto brinda son: mayor optimización y capacidad de modificación del código en medida que sea necesario ya sea para agregar funcionalidades extras o modificar aspectos visuales. Así mismo permite la integración con cualquier otro sistema en medida que sea solicitado o necesario, esto a largo plazo ayuda a la empresa a ahorrar el costo de depender de una empresa externa para mantenimiento o cualquier modificación que sea necesaria.

Esto también presenta una gran ventaja como lo es la escalabilidad ya que a medida que la empresa crece el sistema también lo puede hacer pudiendo así registrar un mayor número de usuarios o gestionar una mayor cantidad de datos, así mismo se puede agregar las nuevas tecnologías que vayan surgiendo con el paso del tiempo añadiendo nuevas funciones innovadoras y útiles

La combinación de la crisis de inseguridad, las limitaciones de los métodos tradicionales en la seguridad privada y la accesibilidad a herramientas tecnológicas de última generación subraya la urgencia y relevancia de implementar una solución basada en reconocimiento facial. Este enfoque no solo aborda un problema crítico, sino que también muestra cómo la tecnología puede transformar y fortalecer un sector fundamental para el bienestar y la estabilidad del país.

1.4 Alcance.

- El sistema está orientado al control de accesos de personas en instalaciones de seguridad, proporcionando beneficio tanto para la gestión operativa como para la seguridad de la empresa.
- Se utilizará modelos avanzados de *Deep Learning* para el reconocimiento facial, asegurando una alta precisión y minimizando falsos positivos o negativos.

- El sistema integrará una bitácora digital automatizada que registrará cada acceso con información detallada, incluyendo fecha, hora, foto del ingreso o salida y otros datos relevantes.
- Se entregará un programa funcional y operativo, capaz de gestionar múltiples cámaras y punto estratégicos dentro de la empresa.
- Se proporcionará documentación técnica, incluyendo los requisito funcionales y no funcionales del sistema, así como manuales de usuario y administrado.
- El trabajo de Integración curricular no cubrirá la instalación física de cámaras o infraestructura adicional.
- No se incluirán funcionalidades avanzadas como la detección de emociones, análisis de comportamiento o integraciones con sistemas externos no definidos previamente en los requisitos del trabajo de Integración curricular.
- El desarrollo del sistema de Registro de Accesos para empleados será implementado en la empresa de seguridad solicitante. Se realizará el despliegue gradual en un entorno real, para que se puedan realizar ajustes ante posibles problemas o imprevistos que pudieran surgir posterior a la implementación.

1.5 Objetivos.

1.5.1 Objetivo General.

Desarrollar un sistema de registro de acceso mediante reconocimiento facial usando *Deep Learning* para almacenar los datos en una bitácora digital para una empresa de seguridad física.

1.5.2 Objetivos Específicos.

- Diseñar un sistema de reconocimiento facial utilizando técnicas avanzada de

inteligencia artificial.

- Implementar algoritmos de *Deep Learning* para mejorar el sistema de reconocimiento facial aumentando su precisión y reduciendo errores al momento de identificar personas.
- Integrar el sistema de reconocimiento facial con una bitácora digital que registre automáticamente los accesos y genere reportes en tiempo real.
- Realizar pruebas de usabilidad y desempeño del sistema en un entorno local, identificando oportunidades de mejora.

1.5.3 Pregunta de investigación.

La pregunta planteada para el proceso de investigación de este trabajo de Integración curricular es el siguiente

¿Cómo puede un sistema de registro de accesos mediante reconocimiento facial basado en *Deep Learning* mejorar la precisión, seguridad y eficiencia en la gestión de accesos en una empresa de seguridad física en el Ecuador?

¿Cuál es el impacto de la integración de un sistema de reconocimiento facial con aprendizaje profundo en la mejora de la gestión de accesos y la eficiencia operativa de una empresa de seguridad física?

CAPITULO II

MARCO TEÓRICO Y CONCEPTUAL

2.1 Seguridad Física y Control de Accesos.

La seguridad física es esencial para proteger tanto los activos de una organización como la información digital. El control de accesos cumple un rol clave al restringir el acceso a zonas sensibles y salvaguardar la integridad de sistemas, servidores y bases de datos.

Hoy en día, la convergencia entre seguridad física y digital impulsa la adopción de tecnologías avanzadas, como controles biométricos, reconocimiento facial y autenticación multifactor. Estas soluciones refuerzan la protección y permiten un monitoreo en tiempo real.

Este capítulo analiza las tecnologías de control de acceso, su integración en las infraestructuras actuales y su impacto en la prevención de intrusiones y la gestión eficiente de recursos físicos y digitales.

2.1.1 Importancia del Control de Accesos en Empresas de Seguridad.

Un control de acceso puede definirse como un mecanismo o sistema que permite, restringe o regula el paso de un objeto o persona a un área determinada. En palabras más sencillas, un control de acceso puede ser una puerta, cerradura, persona, software, etc. que controla el paso de un lugar a otro. (*Control de Acceso*, s/f)

Un sistema eficaz de control de accesos asegura que únicamente el personal autorizado puede ingresar a las áreas restringidas, reduciendo riesgos como el robo, el espionaje corporativo o la entrada de individuos no deseados. Además, estos sistemas pueden ayudar con la agilización de gestión administrativa, al proporcionar un registro

detallado y verificable de las actividades relacionadas con los accesos.

2.1.2 Métodos Tradicionales de Registro de Accesos.

El control de acceso es un aspecto esencial de la seguridad que implica la gestión del acceso a los recursos de un sistema. Los métodos tradicionales de control de acceso se han utilizado durante décadas e implican el uso de claves físicas, contraseñas y tarjetas de identificación para controlar el acceso a edificios, habitaciones y sistemas informáticos. Estos métodos siguen siendo relevantes hoy en día, pero sus limitaciones han llevado al desarrollo de tecnologías de control de acceso más avanzadas.(*Métodos Tradicionales Control Acceso*, s/f)

Los métodos tradicionales de control de acceso se han utilizado durante décadas y siguen siendo relevantes en la actualidad. Sin embargo, sus limitaciones han llevado al desarrollo de tecnologías de control de acceso más avanzadas, como el control de acceso biométrico.

*Figura 1 Métodos tradicionales de control de acceso (*Métodos Tradicionales Control Acceso*, s/f)*

Las organizaciones deben evaluar cuidadosamente sus necesidades de control de acceso y elegir el método de control más adecuado (figura 1) en función de sus requisitos de seguridad, presupuesto e infraestructura.(*Métodos Tradicionales Control*

Acceso, s/f).

2.2 Tecnologías de Reconocimiento Biométrico.

El reconocimiento biométrico ha transformado la seguridad moderna al proporcionar métodos avanzados para la identificación precisa y eficiente de personas. Este capítulo se centra en el reconocimiento facial, una de las tecnologías biométricas más empleadas en la actualidad. En primer lugar, se analizan los principios fundamentales del reconocimiento facial, su funcionamiento y las tecnologías que lo sustentan. Posteriormente, se examinan la evolución y los avances en los algoritmos que han incrementado su precisión y capacidad de adaptación. Finalmente, se presentan sus aplicaciones prácticas en seguridad, como el control de accesos, la vigilancia en tiempo real y la autenticación en sistemas físicos y digitales.

2.2.1 Principios y Fundamentos del Reconocimiento Facial.

Durante los últimos años, el reconocimiento facial se ha convertido en una de las aplicaciones más estudiadas en campos como la biometría, el procesado de imagen o el reconocimiento de patrones. Una de las razones que ha llevado a este crecimiento son las necesidades cada vez mayores de aplicaciones de seguridad y vigilancia utilizadas en diferentes ámbitos.(Hernández, s/f)

El reconocimiento facial es una tecnología biométrica que identifica o verifica la identidad de una persona al analizar sus características faciales únicas. Este proceso se basa en la captura de una imagen facial, que luego es procesada y comparada con un modelo previamente almacenado en una base de datos. Los puntos clave del rostro, como la distancia entre los ojos, la forma de la mandíbula y la estructura ósea, se utilizan para generar un "mapa facial" único.

El principio fundamental del reconocimiento facial es su capacidad para convertir la información visual en datos matemáticos. Esto se logra mediante algoritmos que extraen características clave del rostro, permitiendo la identificación precisa incluso en entornos cambiantes o con variaciones como el ángulo de la cabeza o la iluminación.

El procedimiento que utiliza este software necesita de una tecnología fotográfica digital para obtener las imágenes y los datos necesarios para procesar la cara. Una vez obtenida la imagen, será necesario crear y registrar el patrón facial biométrico de la persona. Este patrón queda guardado en una base de datos para que pueda ser utilizado en el futuro.(*Reconocimiento facial*, s/f)

El sistema de reconocimiento facial utiliza patrones matemáticos y dinámicos únicos, y emplea complejos algoritmos que hacen de este sistema uno de los más seguros y efectivos en cuanto a la identificación de personas. Cada imagen facial da lugar a unos valores numéricos concretos que, agrupados, componen el patrón característico de la cara. Estos patrones no solo sirven para identificar personas o verificar su identidad, sino también para comparar el parecido entre dos personas.(*Reconocimiento facial*, s/f).

El reconocimiento facial, sigue tres pasos en el proceso (Tabla 1).

Primer paso	Segundo paso	Tercer paso
Detección del rostro	Captura de información y traducción de rasgos	Comparación y verificación.

Tabla 1 Elaboración Propia

El primer paso es la detección del rostro, donde se verifica la identificación del usuario a través de un dispositivo de captura de imagen sea correspondiente a un rostro, luego se produce la captura de la información analógica, se fotografía el rostro de la

persona y se traducen los rasgos a información digital, en patrones algorítmico, y por último se compara y verifica con una imagen digital con la persona real previamente registrada.

Este proceso se visualiza en la figura 2.

*Figura 2 Proceso del reconocimiento facial (*Reconocimiento facial*, s/f)*

2.2.1 Evolución y Avances en Algoritmos de Reconocimiento Facial.

El reconocimiento facial ha evolucionado significativamente con el desarrollo de tecnologías avanzadas. Los primeros pasos en el reconocimiento facial se atribuyen a Woodrow Wilson Bledsoe, un matemático que en la década de los sesenta ideó un primer prototipo basado en el uso de tabletas *RAND*. Esta herramienta permitía recrear los rasgos faciales a través de coordenadas con la ayuda de un lápiz que transmitía impulsos electromagnéticos a una cuadrícula.(Campillo, 2020)

Inicialmente, se utilizaban métodos basados en técnicas estadísticas, como el análisis de componentes principales (*PCA*) o patrones locales binarios (*LBP*). Sin

embargo, estos métodos tradicionales tenían limitaciones en términos de precisión y capacidad de adaptación a diferentes condiciones.

En los últimos años los avances más relevantes en el ámbito del reconocimiento facial han venido propiciados por el uso de entornos de trabajo de aprendizaje profundo. A diferencia de los métodos clásicos (donde deben escogerse de antemano los descriptores a aplicar sobre la imagen de entrada), los algoritmos de aprendizaje profundo mediante el proceso de aprendizaje crean sus propios extractores de características analizando relaciones complejas entre el conjunto de datos de entrada. El aumento significativo de la capacidad de cómputo unido a la inmensa cantidad de imágenes disponibles gracias a internet ha permitido a los sistemas de reconocimiento facial basados en aprendizaje profundo obtener tasas de éxito muy elevadas incluso en los entornos más exigentes.(Campillo, 2020)

Con el auge del aprendizaje profundo, las redes neuronales convolucionales (*CNN*) revolucionaron el campo, permitiendo:

- Mayor precisión: Las CNN pueden identificar características faciales más complejas y sutiles.
- Adaptabilidad: Los algoritmos modernos pueden adaptarse a cambios en el entorno, como iluminación o expresiones faciales.
- Velocidad: La optimización en el procesamiento de imágenes permite identificaciones en tiempo real.

2.2.3 Aplicaciones en Entornos de Seguridad.

El reconocimiento facial se ha convertido en una herramienta fundamental para reforzar la seguridad en entornos críticos. Su capacidad para identificar a individuos de

manera precisa y en tiempo real lo ha posicionado como una de las tecnologías más efectivas en la gestión de accesos y vigilancia.*(Boult et al., 2003; Goodfellow et al., 2016a*)

En el control de accesos, el reconocimiento facial automatiza la verificación de identidad, permitiendo que solo personal autorizado pueda ingresar a áreas restringidas. Este enfoque no solo reduce el tiempo requerido para validar identidades, sino que también minimiza los errores y riesgos asociados con los métodos tradicionales, como tarjetas de acceso o claves. En empresas de seguridad, esta tecnología garantiza una supervisión más estricta de quién entra y sale de las instalaciones, fortaleciendo la protección de activos y personal.(Jain et al., 2011a)

En el ámbito de la vigilancia y el monitoreo, los sistemas de reconocimiento facial integrados con cámaras de seguridad permiten identificar a individuos en tiempo real, lo que resulta crucial para prevenir delitos o rastrear a personas de interés. Por ejemplo, en aeropuertos y estaciones de transporte público, esta tecnología se utiliza para detectar a sospechosos y mejorar la seguridad de los pasajeros.(Boult et al., 2003)

El reconocimiento facial también se emplea en la autenticación biométrica, protegiendo datos sensibles y asegurando accesos seguros en entornos físicos y digitales. Esta aplicación es particularmente útil en la protección de instalaciones estratégicas y gubernamentales, donde la seguridad es prioritaria.(Boult et al., 2003; Jain et al., 2011a)

Además, el reconocimiento facial contribuye a la prevención de fraudes, detectando intentos de suplantación de identidad en procesos que requieren alta confiabilidad, como operaciones bancarias o servicios de atención al cliente. En este sentido, los avances en inteligencia artificial han mejorado la capacidad de estos

sistemas para distinguir rostros reales de imágenes o videos manipulados, enfrentando desafíos como los ataques de "*deepfake*".(Boult et al., 2003; Zhang et al., 2018)

La implementación de estas tecnologías no solo mejora la seguridad, sino que también optimiza procesos, haciéndolos más eficientes y reduciendo la dependencia de sistemas manuales o de vigilancia humana.

2.3 Inteligencia Artificial y Aprendizaje Profundo.

La inteligencia artificial (*IA*) y el aprendizaje profundo han transformado significativamente el abordaje de problemas complejos en campos como la seguridad, la medicina y el análisis de datos. Este capítulo analiza los principios fundamentales de la IA, destacando su capacidad para emular procesos cognitivos humanos, como el razonamiento y la toma de decisiones. Además, se profundiza en el aprendizaje profundo, una rama avanzada de la IA que emplea redes neuronales para procesar grandes volúmenes de datos y aprender de ellos de manera similar al cerebro humano. También se examina el impacto de estas tecnologías, particularmente mediante redes neuronales convolucionales, en la mejora del reconocimiento facial, incrementando su precisión y eficacia en aplicaciones como el control de accesos y la vigilancia, así como la demostración de cómo la integración de IA y aprendizaje profundo ha impulsado avances en la automatización y optimización de sistemas de seguridad inteligentes.

2.3.1 Conceptos Básicos de Inteligencia Artificial (*IA*).

La inteligencia artificial (*IA*) es una disciplina de la informática que tiene como objetivo desarrollar sistemas capaces de emular comportamientos humanos como el razonamiento, el aprendizaje, la percepción sensorial y la toma de decisiones. Estos sistemas se basan en algoritmos que les permiten analizar grandes volúmenes de datos,

identificar patrones significativos y realizar acciones en función de lo aprendido. Este enfoque ha permitido la automatización de tareas complejas en campos como la medicina, el transporte y la seguridad.

La IA puede dividirse en dos categorías principales. La *IA* estrecha, también conocida como específica, se centra en resolver tareas concretas, como el reconocimiento facial o la clasificación de objetos en imágenes. En cambio, la IA general aspira a desarrollar sistemas con capacidades intelectuales equivalentes o superiores a las humanas, un objetivo que actualmente se encuentra en etapas teóricas y experimentales. La inteligencia artificial estrecha ha encontrado un amplio uso en aplicaciones industriales y de seguridad, como el monitoreo automatizado y el análisis de riesgos en tiempo real.(*Goodfellow et al., 2016a; Russell & Norvig, 2021)*

2.3.2 Fundamentos del Aprendizaje Profundo (*Deep Learning*).

El aprendizaje profundo es una subdisciplina dentro del aprendizaje automático que utiliza redes neuronales profundas para procesar y analizar datos complejos. El *Deep Learning* se basa en algoritmos de aprendizaje profundo que imitan la forma en que funciona el cerebro humano. Estos algoritmos, como redes neuronales artificiales, son capaces de procesar grandes cantidades de datos y aprender de ellos. Cada capa de la red se especializa en aprender características únicas de los datos, desde los patrones básicos hasta los detalles más complejos. (Sandra Domínguez, 2023)

El aprendizaje profundo en el campo de la visión por computadora ha innovado debido a su capacidad para analizar imágenes con precisión y adaptarse a variaciones como cambios en la iluminación, expresiones faciales o posiciones de los objetos. Estas características han sido fundamentales para la implementación de sistemas de

reconocimiento facial en entornos desafiantes, como aeropuertos o empresas de seguridad física. Además, las redes neuronales convolucionales, un tipo especializado de red neuronal, son ampliamente utilizadas en el procesamiento de imágenes debido a su capacidad para identificar características espaciales específicas, como bordes, texturas y formas. (*Goodfellow et al., 2016a; LeCun et al., 2015; Schroff et al., 2015)*

2.3.3 Técnicas de Aprendizaje Profundo Aplicadas al Reconocimiento Facial.

El aprendizaje profundo ha permitido avances significativos en el reconocimiento facial, mejorando la precisión, velocidad y confiabilidad de estos sistemas. A través de redes neuronales convolucionales, los modelos pueden procesar imágenes faciales para identificar características únicas como la distancia entre los ojos, la forma de la mandíbula y otros rasgos biométricos. Estas características se transforman en representaciones matemáticas conocidas como *embeddings* faciales, que se utilizan para comparar e identificar rostros con alta precisión.

El uso de técnicas como el aprendizaje por transferencia ha reducido considerablemente los recursos necesarios para entrenar modelos avanzados. Modelos preentrenados, como *FaceNet* y *VGGFace*, han demostrado ser altamente efectivos en tareas de verificación e identificación facial. Estas redes han sido entrenadas con grandes conjuntos de datos, lo que les permite generalizar en diferentes contextos y adaptarse a nuevas aplicaciones (*Parkhi et al., 2015; Schroff et al., 2015*).

El aprendizaje profundo también ha abordado desafíos como la detección de rostros en condiciones de baja calidad o con ángulos extremos. Mediante el uso de algoritmos especializados, los sistemas actuales pueden identificar y reconocer rostros incluso en escenarios de alta complejidad, como eventos multitudinarios o entornos con

iluminación variable. Esto ha consolidado al aprendizaje profundo como una herramienta esencial en aplicaciones de alta seguridad y control de accesos *(Goodfellow et al., 2016b*).

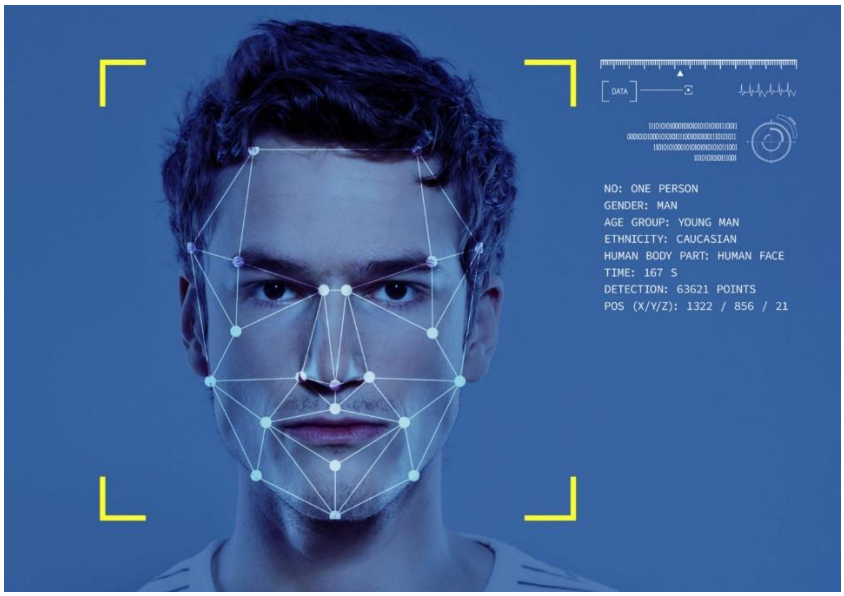


Figura 3 Reconocimiento Facial (Duckerman, 2022)

2.4. Sistemas de Registro de Accesos Automatizados.

Se analiza los sistemas de registro de accesos automatizados basados en reconocimiento facial, los cuales combinan hardware y software para mejorar la seguridad y la eficiencia en la gestión de accesos. Se examinan sus componentes clave, como cámaras de alta resolución, dispositivos de procesamiento y algoritmos de reconocimiento facial, que permiten la identificación precisa de usuarios en tiempo real. También se detalla su integración con bitácoras digitales, automatizando el registro de datos como nombres, horarios de entrada y salida, y fotografías, lo que reduce errores humanos y optimiza la gestión. Por último, se abordan aspectos de seguridad, privacidad y ética, resaltando la necesidad de proteger los datos biométricos, cumplir con normativas de privacidad y garantizar un uso ético y no discriminatorio de estas

tecnologías.

2.4.1 Arquitectura y Componentes de un Sistema de Registro de Accesos Basado en Reconocimiento Facial.

Un sistema de registro de accesos automatizado mediante reconocimiento facial combina hardware y software para garantizar la identificación precisa de los usuarios. La arquitectura incluye cámaras de captura, dispositivos de procesamiento, algoritmos de reconocimiento facial y base de datos para almacenar y gestionar la información.

El hardware está compuesto por cámaras de alta resolución, que capturan imágenes y dispositivos de procesamiento, como servidores o sistemas embebidos, que ejecutan los algoritmos de reconocimiento. Por su parte, el software utiliza modelos de aprendizaje profundo entrenados para identificar características únicas del rostro, como la distancia entre los ojos o la forma de la mandíbula. Este software se integra con bases de datos que almacenan perfiles de usuarios, permitiendo la comparación en tiempo real para validar la identidad.

El diseño de estos sistemas debe considerar elementos clave como la precisión de los algoritmos, la capacidad de la base de datos y la velocidad de procesamiento. Además, la arquitectura debe ser modular para facilitar su integración con sistemas existentes, como bitácoras digitales o controles de seguridad física.

2.4.2 Integración con bitácoras digitales.

La integración de un sistema de reconocimiento facial con una bitácora digital transforma la manera en que las empresas gestionan el control de accesos. Este proceso automatiza la captura de datos, registrando automáticamente información como el nombre del usuario, la hora de entrada y salida, y su fotografía. En entornos de seguridad

física, esta integración reduce los errores humanos asociados con los registros manuales y agiliza el acceso de los empleados.

Los sistemas de bitácoras digitales funcionan mediante bases de datos relacionales que almacenan los registros de manera estructurada. La conexión entre el reconocimiento facial y la bitácora se realiza mediante *APIs* o servicios *web*, que permiten la transferencia de datos entre ambos sistemas. Esto garantiza que cada acceso quede registrado en tiempo real, proporcionando un historial confiable y accesible para auditorías o análisis de seguridad *(“Face Recognition Vendor Test (FRVT)”, s/f; System Front Information, 2023*).

2.4.3 Consideraciones de Seguridad, Privacidad y Ética en el Uso de Tecnologías Biométricas.

El uso de tecnologías biométricas, como el reconocimiento facial, plantea importantes desafíos en términos de seguridad, privacidad y ética. La captura y almacenamiento de datos biométricos requiere la implementación de medidas robustas para prevenir accesos no autorizados y garantizar el cumplimiento de normativas de protección de datos, como el Reglamento General de Protección de Datos (*GDPR*) en Europa.

En términos de privacidad, es fundamental que los sistemas biométricos limiten la cantidad de datos recopilados al mínimo necesario, utilizando técnicas como el cifrado para proteger la información almacenada. Además, deben implementarse políticas de consentimiento informado para garantizar que los usuarios comprendan cómo se utilizarán sus datos y tengan la posibilidad de retirarlos si lo desean *(Mittelstadt et al., 2016; Protección de datos - Comisión Europea, 2021*).

Desde una perspectiva ética, el diseño de estos sistemas debe evitar sesgos algorítmicos que puedan discriminar a ciertos grupos de personas, como aquellos basados en género o raza. Asimismo, es importante evaluar los posibles usos indebidos de la tecnología, como la vigilancia masiva sin el consentimiento de las personas involucradas (*EFF Comments on DHS Proposed Rule on Collection and Use of Biometrics - October 2020, 2020; Kennedy, 2019; Mittelstadt et al., 2016*).

2.5 Tendencias y Casos de Éxito en la Implementación de Sistemas de Reconocimiento Facial.

Se analiza el reconocimiento facial y su creciente popularidad en diversas industrias, especialmente en el sector de la seguridad, debido a su capacidad para mejorar la precisión y eficiencia en el control de accesos. Esta tecnología se utiliza ampliamente en empresas de seguridad y aeropuertos, donde facilita el flujo de personas sin comprometer la protección. Asimismo, se examinan métricas clave para evaluar el desempeño de estos sistemas, como la precisión del reconocimiento, el tiempo de respuesta y las tasas de verificación, incluyendo la incidencia de falsos positivos y negativos. Estas métricas son esenciales para asegurar un rendimiento confiable en entornos de alta seguridad y tráfico elevado.

2.5.1 Ejemplos de Implementaciones en Empresas de Seguridad.

El reconocimiento facial ha sido adoptado ampliamente en diversas industrias, destacándose en el sector de la seguridad física. Empresas de vigilancia y protección han integrado esta tecnología en sus sistemas de control de accesos, obteniendo mejoras significativas en la precisión y la velocidad de identificación. Un ejemplo notable es el uso de reconocimiento facial en aeropuertos como el de Bangkok (*Hong Kong*

International Airport), donde se ha implementado para agilizar el flujo de pasajeros mientras se mantiene un alto nivel de seguridad *(Fully Digital Travel Experience Closer to Reality, s/f*).

En el sector corporativo, compañías como *NEC Corporation* han desarrollado soluciones personalizadas de reconocimiento facial para empresas de seguridad. Estos sistemas permiten la gestión de accesos en tiempo real, identificando automáticamente a los empleados y visitantes sin necesidad de intervención humana. Este enfoque reduce los riesgos de suplantación de identidad y asegura un registro confiable de entradas y salidas (*Frost & Sullivan Recognizes NEC with the 2020 Global Biometrics in Security Market Growth Innovation & Leadership Excellence Frost Radar™ Award, s/f; Jain et al., 2011b)*.

2.5.2 Métricas de desempeño y eficiencia.

La eficiencia de los sistemas de reconocimiento facial se mide a través de métricas clave como la tasa de falsos positivos, la tasa de falsos negativos y el tiempo de respuesta. En entornos reales, los sistemas modernos han logrado tasas de precisión superiores al 98% en condiciones controladas, demostrando su efectividad para identificar a individuos en tiempo real *(“Face Recognition Vendor Test (FRVT)”, s/f; Schroff et al., 2015)*.

Además, los avances en hardware y optimización de algoritmos han reducido significativamente los tiempos de procesamiento. Modelos como *FaceNet* y *ArcFace* pueden procesar miles de comparaciones por segundo, lo que los hace ideales para entornos con un alto volumen de tráfico, como centros comerciales, aeropuertos y eventos masivos *(Deng et al., 2019*).

2.5.2.1 Precisión del Reconocimiento.

La precisión se refiere a la capacidad del sistema para identificar correctamente a las personas. Se evalúa a través de dos métricas principales:

Tasa de Falsos Positivos (*FPR, False Positive Rate*): Representa la proporción de casos en los que el sistema identifica incorrectamente a una persona no autorizada como válida. Una FPR baja es crucial en entornos de alta seguridad para evitar accesos no autorizados (*Schroff et al., 2015*).

Tasa de Falsos Negativos (*FNR, False Negative Rate*): Indica la proporción de ocasiones en las que el sistema no reconoce a una persona autorizada. Minimizar esta tasa es importante para garantizar que los empleados o usuarios legítimos no enfrenten problemas al acceder a las instalaciones (*Schroff et al., 2015*).

2.5.2.2 Tiempo de Respuesta.

El tiempo de respuesta mide la velocidad con la que el sistema procesa una imagen facial y proporciona un resultado (aceptación o rechazo). En aplicaciones de tiempo real, como el control de accesos en entornos con alto tráfico, un tiempo de respuesta inferior a 5000 milisegundos es ideal para garantizar una experiencia fluida y eficiente (*Deng et al., 2019*).

2.5.2.3 Tasa de Verificación y Clasificación.

La tasa de verificación y clasificación es un conjunto de métricas clave para evaluar el desempeño de un sistema de reconocimiento facial. Estas métricas determinan la capacidad del sistema para identificar correctamente a los usuarios autorizados y rechazar a los no autorizados. Se utilizan principalmente en dos contextos: verificación de identidad y clasificación de personas dentro de una base de datos.

Tasa de Igualdad Verdadera (*TAR, True Accept Rate*): Mide la proporción de veces que el sistema reconoce correctamente a una persona autorizada. Una *TAR* alta es necesaria para garantizar la fiabilidad del sistema *("Face Recognition Vendor Test (FRVT)", s/f; Schroff et al., 2015*) .

Tasa de Rechazo Verdadero (*TNR, True Negative Rate*): Refleja la proporción de casos en los que el sistema rechaza correctamente a usuarios no autorizados. Es crucial en aplicaciones donde la seguridad es prioritaria, ya que evita que personas no registradas o no autorizadas accedan a las instalaciones protegidas *(Deng et al., 2019; Jain et al., 2011b*) .

Curva de Característica Operativa del Receptor (*ROC, Receiver Operating Characteristic*): Permite analizar el equilibrio entre la *FPR* y la *TAR*, evaluando el desempeño del sistema en diferentes umbrales de decisión *(Boult et al., 2003; "Face Recognition Vendor Test (FRVT)", s/f*).

Tasa de Falsos Positivos (*FPR, False Positive Rate*): La FPR mide el porcentaje de ocasiones en las que el sistema identifica erróneamente a una persona no autorizada como válida. Una FPR alta puede ser desastrosa en entornos de alta seguridad, ya que aumenta el riesgo de accesos no autorizados. En la práctica, un sistema bien diseñado debe mantener la FPR por debajo del 1% para aplicaciones críticas *("Face Recognition Vendor Test (FRVT)", s/f*).

Tasa de Falsos Negativos (*FNR, False Negative Rate*): Indica el porcentaje de veces en que el sistema no reconoce a una persona autorizada. Una FNR alta afecta negativamente la experiencia del usuario, especialmente en aplicaciones donde la comodidad y la rapidez son indispensables (*"Face Recognition Vendor Test (FRVT)", s/f*).

2.6 Marco Legal y Normativo.

Se analiza el marco legal y normativo sobre el uso de tecnologías biométricas, como el reconocimiento facial, que es esencial para proteger los derechos de privacidad y evitar abusos. A nivel internacional, regulaciones como el Reglamento General de Protección de Datos (*GDPR*) en la Unión Europea y la Ley de Privacidad de Información Biométrica (*BIPA*) en Estados Unidos establecen principios sobre el consentimiento, la limitación de datos y la transparencia. En América Latina, países como Brasil han adoptado leyes similares, mientras que en el Ecuador la regulación aún está en desarrollo.

En el Ecuador, la protección de datos personales está regida por la Constitución y la Ley Orgánica de Protección de Datos Personales (*LOPDP*), que exige medidas de seguridad robustas, como la encriptación y auditorías, aunque no aborda específicamente las tecnologías biométricas.

El uso de tecnologías biométricas también plantea riesgos éticos, como el sesgo algorítmico y la vigilancia sin consentimiento. Por ello, se promueven principios de transparencia, equidad y evaluación del impacto social y ético antes de su implementación.

2.6.1 Regulaciones Internacionales sobre el Uso de Tecnologías Biométricas.

El uso de tecnologías biométricas, como el reconocimiento facial, está regulado en diversas jurisdicciones para garantizar la protección de los derechos de privacidad y prevenir abusos. Una de las normativas más relevantes es el Reglamento General de Protección de Datos (*GDPR, por sus siglas en inglés*) de la Unión Europea, que establece

principios clave para el procesamiento de datos biométricos, como:

- Consentimiento explícito del usuario.
- Limitación en la recopilación y procesamiento de datos a lo estrictamente necesario.
- Derechos del usuario para acceder, rectificar o eliminar sus datos personales (*"Art. 22 GDPR – Automated Individual Decision-Making, Including Profiling", s/f)*.

En los Estados Unidos, las regulaciones varían por estado. Por ejemplo, la Ley de Privacidad de Información Biométrica (*BIPA*) de Illinois exige que las empresas obtengan consentimiento informado antes de recopilar datos biométricos y prohíbe su venta a terceros sin autorización (*Illinois Compiled Statutes, s/f*).

En América Latina, algunos países como Brasil, con su Ley General de Protección de Datos (*LGPD*), han adoptado principios similares a los del *GDPR*. Sin embargo, en muchos países de la región, incluido el Ecuador, la regulación específica para tecnologías biométricas aún está en desarrollo *(Lei Geral de Proteção de Dados Pessoais (LGPD), s/f; OEA & OEA, 2009*).

2.6.2 Contexto Normativo en el Ecuador.

La protección de datos personales está contemplada en el artículo 66 de la Constitución de la República del Ecuador, que garantiza el derecho a la protección de la información personal. Además, la Ley Orgánica de Protección de Datos Personales (LOPDP), aprobada en 2021, establece principios clave para el tratamiento de datos, como la transparencia, la seguridad y el consentimiento informado (Asamblea Nacional de Ecuador, s/f).

Aunque la LOPDP no aborda específicamente el uso de tecnologías biométricas,

sus disposiciones sobre el manejo de datos sensibles, que incluyen los datos biométricos, obligan a las empresas a implementar medidas de seguridad robustas. Esto incluye la encriptación de datos, el acceso restringido y la realización de auditorías regulares para garantizar el cumplimiento (*Aviso de Privacidad*, s/f).

2.6.3 Consideraciones Éticas en el Uso de Tecnologías Biométricas.

El uso de reconocimiento facial plantea importantes dilemas éticos relacionados con la privacidad, la equidad y el consentimiento. Uno de los principales riesgos es el sesgo algorítmico, donde los sistemas de reconocimiento facial pueden ser menos precisos para ciertos grupos demográficos, como minorías étnicas o mujeres, debido a la falta de diversidad en los datos de entrenamiento *(Kennedy, 2019; Mittelstadt et al., 2016*).

Además, existe preocupación por el uso indebido de estas tecnologías, como la vigilancia masiva sin el consentimiento de los ciudadanos. Para mitigar estos riesgos, organizaciones como la *Electronic Frontier Foundation (EFF*) han propuesto principios éticos para el diseño y uso de tecnologías biométricas, que incluyen:

- Transparencia en el desarrollo y uso de sistemas.
- Participación de las comunidades afectadas.
- Evaluaciones de impacto ético y social antes de la implementación.

2.6 Tecnologías usadas.

2.6.1 PHP.

PHP es un acrónimo recursivo para “PHP: *Hypertext Preprocessor*”, originalmente Personal Home Page, es un lenguaje interpretado libre, usado originalmente solamente para el desarrollo de aplicaciones presentes y que actuarán en el lado del servidor,

capaces de generar contenido dinámico en la *World Wide Web*. Se evidencia entre los primeros lenguajes posibles para la inserción de documento *HTML*, dispensando en muchos casos el uso de archivos externos para eventuales procesamientos de datos. El código es interpretado en el lado del servidor por el módulo PHP, que también genera la página web para ser visualizada en el lado del cliente. El lenguaje evoluciono, paso a ofrecer funcionalidades en la línea de comandos, y, además, gano características adicionales, que posibilitaron usos adicionales del PHP. Es posible instalar el PHP en la mayoría de los sistemas operativos, totalmente de manera gratuita. Siendo competidor directo de la tecnología ASP perteneciente a Microsoft, PHP es utilizado en aplicaciones como *MediWiki*, *Facebook*, *Drupal*, *Joomla*, *WoordPress*, *Magento* y *Oscommerce*. (Arias, 2013).

PHP es un software libre, licenciado bajo la PHP License, una licencia incompatible con la *GNU General Public License (GPL)* debido a las restricciones en los términos de uso de PHP. (Arias, 2013).

El lenguaje surgió a mediados de 1994, como un paquete de programas CGI creados por Rasmus Lerdorf, con el nombre de *Personal Home Page Tools*, para sustituir un conjunto de *scripts Perl* que este usaba en el desarrollo de su página personal, En 1997 fue lanzado el nuevo paquete de lenguaje con el nombre de *PHP/FI*, trayendo la herramienta *Forms Interpreter*, un interpretador de comandos *SQL*. Mas tarde, Zeev Suraski desarrollo el analizador de *PHP3* que contaba con el primer recurso orientado a objetos, que daba poder de alcanzar algunos paquetes, tenía herencia y daba a los desarrolladores solamente la posibilidad de implementar propiedades y métodos. Poco después, Zeev y Andi Gutmans, escribieron el *PHP4*, abandonando por completo el

PHP3, creando un mayor número de recursos orientados a objetos. El problema serio que presento el *PHP4* fue la creación de copias de objetos, ya que el lenguaje aun no trabajaba con apuntadores o *handlers*, como son los lenguajes *Java* o *Ruby*. El problema fue resuelto en la versión 5 de PHP, que ya trabaja con *handlers*. Si copia un objeto, en realidad se copia un apuntador, ya que, si haya algún cambio en la versión original del objeto, todas las otras también sufren la modificación, lo que no sucedía en la versión de PHP 4. (Arias, 2013).

2.6.2 Python.

Python es un lenguaje de programación ampliamente utilizado en las aplicaciones web, el desarrollo de software, la ciencia de datos y el *machine learning* (ML). Los desarrolladores utilizan Python porque es eficiente y fácil de aprender, además de que se puede ejecutar en muchas plataformas diferentes. El software Python se puede descargar gratis, se integra bien a todos los tipos de sistemas y aumenta la velocidad del desarrollo. (*¿Qué es Python?*, s/f).

Según la documentación oficial de Python (*¿Qué es Python?*, s/f) El lenguaje Python se aplica a varios casos de uso en el desarrollo de aplicaciones, incluidos los ejemplos siguientes:

Desarrollo web del lado del servidor.- El desarrollo web del lado del servidor incluye las funciones complejas de backend que los sitios web llevan a cabo para mostrar información al usuario. Por ejemplo, deben interactuar con las bases de datos, comunicarse con otros sitios web y proteger los datos cuando se envía a través de la red.

Python es útil para escribir código del lado del servidor debido a que ofrece muchas bibliotecas que constan de código prescrito para crear funciones de *backend*

complejas. Los desarrolladores también utilizan un amplio rango de marcos de Python que proporcionan todas las herramientas necesarias para crear aplicaciones web con mayor rapidez y facilidad. Por ejemplo, los desarrolladores pueden crear la aplicación web esqueleto en segundos porque no deben escribirla desde cero. Pueden probarla por medio de las herramientas de prueba del marco, sin depender de herramientas de prueba externas.

Automatización con scripts de Python.- Un lenguaje de scripting es un lenguaje de programación que automatiza las tareas que suelen llevar a cabo las personas. Los programadores utilizan ampliamente los scripts de Python para automatizar muchas tareas diarias, como las siguientes:

- Cambiar el nombre de una gran cantidad de archivos a la vez
- Convertir un archivo en otro tipo de archivo
- Eliminar palabras duplicadas de un archivo de texto
- Llevar a cabo operaciones matemáticas básicas
- Enviar mensajes por email
- Descargar contenido
- Efectuar análisis básicos de registros
- Encontrar errores en varios archivos

Realizar tareas de ciencia de datos y *machine learning*.

La consiste en extraer conocimientos valiosos a partir de los datos, mientras que el enseña a las computadoras a aprender automáticamente de los datos y a efectuar predicciones precisas. Los científicos de datos utilizan Python para realizar tareas de ciencia de datos, como las que se indican a continuación:

- Corregir y eliminar datos incorrectos, lo que se conoce como limpieza de datos
- Extraer y seleccionar varias características de los datos
- Etiquetar datos, que consiste en agregar nombres significativos a los datos
- Buscar diferentes estadísticas a partir de los datos
- Visualizar los datos mediante el uso de tablas y gráficos, como los gráficos de líneas, los de barras, los circulares y los histogramas

Los científicos de datos utilizan las bibliotecas de ML de Python para entrenar los modelos de ML y crear clasificadores que clasifiquen los datos con precisión. Las personas que trabajan en diferentes campos utilizan clasificadores basados en Python para efectuar tareas de clasificación, como la clasificación de imágenes, texto y tráfico de red; el reconocimiento de habla; y el reconocimiento facial. Los científicos de datos también utilizan Python para las tareas de aprendizaje profundo, una técnica avanzada de ML.

Desarrollo de software.

Los desarrolladores de software suelen utilizar Python para realizar distintas tareas de desarrollo y aplicaciones de software, como las que se indican a continuación:

- Realizar un seguimiento de los errores en el código del software
- Crear el software de forma automática
- Administrar los proyectos de software
- Desarrollar prototipos de software
- Desarrollar aplicaciones de escritorio por medio de las bibliotecas de interfaz gráfica de usuario (GUI)
- Desarrollar juegos simples basados en texto a videojuegos más complejos

Automatización de pruebas de software.

La prueba de software es el proceso de verificar si los resultados reales del software coinciden con los resultados esperados, para garantizar que el software esté libre de errores.

- Los desarrolladores utilizan marcos de prueba de unidad de Python, como *Unittest*, *Robot* y *PyUnit*, para probar las funciones que escriben.
- Los encargados de probar el software utilizan Python para escribir casos de prueba para diversos escenarios de prueba. Por ejemplo, lo utilizan para probar la interfaz de usuario de una aplicación web, los diversos componentes de software y las nuevas características.

Los desarrolladores pueden utilizar varias herramientas para ejecutar scripts de prueba de manera automática. Estas herramientas se conocen como herramientas de integración e implementación continuas (CI/CD). Los encargados de probar el software y sus desarrolladores utilizan las herramientas de CI/CD, como Travis CI y Jenkins, para automatizar las pruebas. La herramienta de CI/CD ejecuta automáticamente los scripts de prueba de Python e informa los resultados de las pruebas cada vez que los desarrolladores presentan nuevos cambios de código.

2.6.3 Laravel.

Según la documentación oficial de Laravel (“¿Qué Es Laravel y Para Qué Sirve?”, 2022). Laravel es un *framework* PHP gratis y de código abierto que brinda un conjunto de herramientas y recursos para crear aplicaciones modernas. Posee un ecosistema integral que combina funciones integradas y una variedad de paquetes y extensiones compatibles.

Según la documentación oficial de Laravel (“¿Qué Es Laravel y Para Qué Sirve?”, 2022). Es *backend*, aunque tiene algunas cuestiones de *frontend*, como herramientas de construcción de estilo *frontend* como sistemas de validación, consultas dinámicas y paginación, permitiendo que los desarrolladores puedan concentrarse en otras cosas en el código.

Según la documentación oficial de Laravel (“¿Qué Es Laravel y Para Qué Sirve?”, 2022). Incluye herramientas que facilitan la construcción de aplicaciones web, haciendo de este proceso algo mucho más rápido y dando como resultado un código bien estructurado y fácil de mantener.

Según la documentación oficial de Laravel (“¿Qué Es Laravel y Para Qué Sirve?”, 2022). Hoy en día, existen muchísimos sitios web creados con esta tecnología, incluyendo grandes empresas como Disney, Twitch, The New York Times, entre otros (¡también se usa en Talently!).

Según la documentación oficial de Laravel (“¿Qué Es Laravel y Para Qué Sirve?”, 2022). Al ser uno de los pocos *frameworks* PHP, Laravel es muy versátil y puede ser usado por empresas IT, de medicina, de viajes, comercios, etc. Según el *sitio web mDevelopers*, estas son sus aplicaciones más habituales:

- Sitios de redes sociales.
- Aplicaciones de varias páginas y de una sola página (MPA y SPA).
- Sitios web estáticos y dinámicos.
- Aplicaciones de nivel empresarial.
- Sitios web de comercio electrónico.
- Sistemas de administración de contenido.

2.6.4 MySql.

Según la documentación oficial de Laravel (*MySQL :: MySQL para principiantes*, s/f). MySQL es la base de datos *open source* más popular del mundo. Soporta las webs con mayor tráfico del planeta como Facebook, Twitter y YouTube. Además de ser una de las bases de datos más fáciles de usar, es ideal para principiantes.

Según la documentación oficial de (*MySQL :: MySQL Database*, s/f). MySQL impulsa la Web, el comercio electrónico, el SaaS y el procesamiento de transacciones en línea (OLTP) más exigentes Aplicaciones. Es una base de datos totalmente integrada, segura para las transacciones, que cumple con ACID con compromiso completo, Capacidades de reversión, recuperación de bloqueos y bloqueo a nivel de fila. MySQL ofrece la facilidad de uso, escalabilidad y rendimiento para impulsar Facebook, Twitter, Uber y Booking.com.

Según la documentación oficial de (*MySQL :: MySQL Database*, s/f).MySQL mejora la seguridad, la escalabilidad, la productividad de los desarrolladores y el rendimiento de las aplicaciones web, móviles, integradas y en la nube.

Según la documentación oficial de (*MySQL :: MySQL Database*, s/f) MySQL ofrece:

- Diccionario de datos transaccional implementado como un conjunto de tablas SQL almacenadas en un único espacio de tablas *InnoDB*.
- Expresiones de tabla comunes, también conocidas como consultas WITH.
- Funciones de ventana para reducir la complejidad del código y ayudar a los desarrolladores a ser más productivos.
- Índices invisibles para administrar mejor las actualizaciones de *software* y los cambios en la base de datos para aplicaciones que se ejecutan las 24 horas del

día, los 7 días de la semana.

- Índices descendentes para eliminar la necesidad de ordenar los resultados y conduce a mejoras en el rendimiento.
- Compatibilidad con JSON con numerosas adiciones, incluida la función JSON_TABLE() que acepta datos JSON y los devuelve como una tabla relacional.
- Almacén de documentos para desarrollar aplicaciones de documentos SQL y NoSQL utilizando una sola base de datos.
- Roles SQL para conceder y denegar permisos a grupos de usuarios, lo que reduce en gran medida la carga de trabajo de seguridad.
- OpenSSL como la biblioteca TLS/SSL predeterminada en MySQL.
- El valor predeterminado es el juego de caracteres utf8mb4 para aplicaciones móviles más completas y conjuntos de caracteres internacionales.
- Los SIG se han mejorado para admitir la geografía y los sistemas de referencia espacial (SRS).
- *InnoDB Cluster* para mejorar la alta disponibilidad.
- *InnoDB ClusterSet* para la recuperación ante desastres entre regiones.
- Replicación que proporciona topologías flexibles para el escalado horizontal y la alta disponibilidad.
- Confiabilidad que requiere poca o ninguna intervención para lograr un tiempo de actividad continuo.
- Particionamiento para mejorar el rendimiento y la gestión de entornos de bases de datos muy grandes.
- Transacciones ACID para crear aplicaciones críticas para el negocio fiables y

seguras.

- Procedimientos almacenados para mejorar la productividad de los desarrolladores.
- Desencadenadores para aplicar reglas de negocio complejas en el nivel de base de datos.
- Vistas para garantizar que la información confidencial no se vea comprometida.
- Facilidad de uso con instalación y configuración de "3 minutos desde la descarga hasta el desarrollo".
- Baja administración con muy poco mantenimiento de la base de datos.

2.6.5 *Face_recognition*.

"Una técnica llamada reconocimiento facial, a veces llamada reconocimiento facial, examina y reconoce rostros humanos en imágenes y videos. Es una tecnología biométrica que reconoce y detecta las características faciales distintivas de las personas utilizando una variedad de algoritmos y metodologías."*(Face Recognition in Python - Javatpoint, s/f*).

"Hay varios procesos involucrados en el proceso de reconocimiento facial. La detección de rostros comienza localizando y extrayendo las características faciales de una imagen o fotograma de vídeo. La ubicación de los ojos, la nariz, la boca y otras marcas faciales reconocibles son ejemplos de estos rasgos." *(Face Recognition in Python - Javatpoint, s/f)*.

"El módulo Python *face_recognition* proporciona una interfaz de usuario sencilla para las tareas de detección y reconocimiento facial. Hace uso del algoritmo de identificación facial basado en aprendizaje profundo de Dlib. Puede utilizar la biblioteca

para encontrar rostros en imágenes y vídeos, y puede identificar rostros conocidos comparándolos con una base de datos de codificaciones faciales reconocidas. Agiliza el reconocimiento facial al ofrecer funciones de alto nivel para actividades típicas relacionadas con el rostro.” *(Face Recognition in Python - Javatpoint, s/f)*.

2.6.6 OpenCv.

Según la documentación oficial de OpenCv (*OpenCv*, s/f). OpenCV (*Open Source Computer Vision Library*) es una biblioteca de software de visión artificial y aprendizaje automático de código abierto. OpenCV se creó para proporcionar una infraestructura común para aplicaciones de visión artificial y para acelerar el uso de la percepción de máquinas en los productos comerciales. Al ser un producto con licencia Apache 2, OpenCV facilita a las empresas la utilización y modificación del código.

Según la documentación oficial de OpenCv (*OpenCv*, s/f). La biblioteca cuenta con más de 2500 algoritmos optimizados, que incluyen un conjunto completo de algoritmos clásicos y de última generación de visión por computadora y aprendizaje automático. Estos algoritmos se pueden utilizar para detectar y reconocer rostros, identificar objetos, clasificar acciones humanas en videos, rastrear movimientos de cámara, rastrear objetos en movimiento, extraer modelos 3D de objetos, producir nubes de puntos 3D a partir de cámaras estéreo, unir imágenes para producir una imagen de alta resolución de una escena completa, encontrar imágenes similares de una base de datos de imágenes, eliminar los ojos rojos de las imágenes tomadas con flash, seguir los movimientos de los ojos, reconocer el paisaje y establecer marcadores para superponerlo con realidad aumentada.

2.6.7 Mysql.connector.

Según la documentación oficial de MySql *(MySQL: MySQL Connector/Python Developer Guide: 1 Introduction to MySQL Connector/Python, s/f)*. MySQL *Connector*/*Python* permite que los programas Python accedan a bases de datos MySQL, utilizando una API que cumple con la Especificación de API de base de datos de Python v2.0 (PEP 249).

Según la documentación oficial de MySql *(MySQL: MySQL Connector/Python Developer Guide: 1 Introduction to MySQL Connector/Python, s/f)*. MySQL *Connector*/*Python* incluye compatibilidad con:

- Casi todas las funciones proporcionadas por MySQL Server versión 8.0 y posteriores.
- *Connector*/*Python* es compatible con X DevAPI.
- Conversión de valores de parámetros entre tipos de datos de *Python* y *MySQL*, por ejemplo, *datetime* de Python y *DATETIME* de MySQL. Puede activar la conversión automática para mayor comodidad o desactivarla para obtener un rendimiento óptimo.
- Todas las extensiones de MySQL a sintaxis SQL estándar.
- Compresión de protocolo, que permite comprimir el flujo de datos entre el cliente y el servidor.
- Conexiones mediante *sockets* TCP/IP y en Unix mediante *sockets* Unix.
- Conexiones TCP/IP seguras mediante SSL.
- Controlador autónomo. *Connector*/*Python* no requiere la biblioteca de cliente MySQL ni ningún módulo Python fuera de la biblioteca estándar.

2.6.8 HOG.

El histograma de gradientes orientados, comúnmente conocido como HOG, es una técnica de extracción de características utilizada en la visión por computadora y el procesamiento de imágenes. Ha encontrado aplicaciones generalizadas en la detección de objetos, reconocimiento de imágenes. *(What Is Histogram of Oriented Gradients (HOG)?, s/f)*.

La extracción de características es fundamental en diversas tareas de visión por computadora, pues busca representar datos visuales complejos de una manera más significativa y compacta. El método HOG se enfoca en la distribución de las orientaciones de los gradientes dentro de una imagen. Básicamente, HOG capta los gradientes de intensidad locales y sus direcciones, lo cual es vital para describir las formas y estructuras de los objetos.

Según (*What Is Histogram of Oriented Gradients (HOG)?, s/f)* El proceso de cálculo del histograma de gradientes orientados implica varios pasos:

- Preprocesamiento de imágenes: La imagen de entrada se preprocesa para mejorar su robustez frente a las variaciones de iluminación y el ruido. Los pasos comunes de preprocesamiento incluyen la conversión de la imagen a escala de grises, la normalización de las intensidades de píxeles y la aplicación de la normalización del contraste.
- Cálculo de gradiente: HOG calcula las magnitudes de gradiente y las orientaciones de los píxeles de la imagen. Este paso ayuda a identificar los bordes y los límites de la textura.
- Construcción de células: La imagen se divide en pequeñas celdas superpuestas.

Normalmente, cada celda cubre una región de 8x8 píxeles.

- Cálculo del histograma: Para cada celda, se calcula un histograma de orientaciones de gradiente. Las orientaciones se cuantifican en bins y el histograma representa la distribución de las orientaciones de gradiente dentro de la celda.
- Normalización de bloques: Las celdas se agrupan en bloques más grandes (generalmente formados por celdas de 2x2 o 3x3). La normalización se aplica dentro de cada bloque para mejorar la robustez del algoritmo a los cambios en la iluminación y el contraste.
- Formación de descriptores: Los histogramas normalizados de todos los bloques se concatenan para formar el descriptor HOG final de la imagen. Este descriptor captura la distribución espacial de los gradientes y sus orientaciones.

CAPÍTULO III

METODOLOGÍA DE LA INVESTIGACIÓN

3.1 Metodología del Trabajo de Integración curricular.

La implementación de un sistema de registro de acceso mediante reconocimiento facial con *Deep Learning* en una bitácora digital representa un desafío complejo que requiere un enfoque metodológico estructurado y dinámico. Este trabajo de Integración curricular se basa en la integración sinérgica de tres marcos metodológicos complementarios: la metodología de investigación aplicada y especifica, así como un marco *SCRUM* para el desarrollo de software, donde la metodología de investigación constituye la recolección, análisis, validación y optimización de la solución informática.

Esta convergencia metodológica permite abordar tanto los aspectos técnicos del reconocimiento facial como los requisitos operativos de la empresa de seguridad.

3.2 Metodología Investigativa Aplicada.

La metodología de investigación elegida para este trabajo de Integración curricular es de carácter aplicado y se basa en los principios de la investigación científica orientada a la solución de problemas prácticos. Como lo señala Hernández et al. enfatizar. (2014) La investigación aplicada se caracteriza por centrarse en la solución de problemas específicos en contextos definidos, utilizando el conocimiento teórico existente para desarrollar soluciones prácticas y medibles.

En el contexto específico de este trabajo de Integración curricular, la metodología

aplicada se divide en tres dimensiones básicas:

3.3 Capacidad tecnológica.

La investigación se centra en la aplicación práctica de algoritmos de reconocimiento facial y técnicas de aprendizaje profundo basados en los avances recientes en visión por computadora. Esta dimensión incluye el análisis y selección de una red neuronal convolucional (*CNN*) óptima para el reconocimiento facial en tiempo real, teniendo en cuenta las contribuciones de autores como Zhang et al. (2019) en el área de aprendizaje profundo en seguridad.

3.4 Dimensión Operativa.

Se examinan los procesos actuales de control de acceso en la empresa de seguridad y se analizan los procesos de trabajo, puntos críticos y requisitos específicos del personal. Este análisis sistemático permite identificar áreas de mejora y oportunidades de optimización a través de la implementación del sistema automatizado.

3.5 Dimensión evaluativa.

Se establecerá un marco de evaluación continua para medir la eficacia del sistema en términos de precisión de reconocimiento facial, tiempo de respuesta y usabilidad. Esta dimensión se basa en métricas estandarizadas para evaluar sistemas biométricos y sigue las recomendaciones de organismos internacionales como *NIST (National Institute of Standards and Technology).*

3.6 Metodología de Investigación Específica.

La metodología específica desarrollada para este trabajo de Integración curricular se fundamenta en un marco metodológico especializado para sistemas de reconocimiento facial con *deep learning*, considerando las particularidades y

complejidades inherentes a los sistemas biométricos en entornos de seguridad. Esta metodología se ha diseñado siguiendo los estándares internacionales *ISO/IEC* 19794-5 para datos biométricos faciales y las recomendaciones del NIST para sistemas de reconocimiento facial *(NIST Special Publication 800-76).*

En el marco de este trabajo de Integración curricular, la metodología detallada se organiza en tres dimensiones fundamentales que permiten abordar de manera integral el tema de estudio. Cada una de estas dimensiones está diseñada para proporcionar una perspectiva amplia y coherente, facilitando así el análisis y desarrollo de los objetivos planteados en la investigación:

3.7 Dimensión Tecnológica.

La implementación tecnológica del sistema se fundamenta en una arquitectura multicapa que integra diferentes tecnologías. El *backend* se desarrolla utilizando el *framework* Laravel en PHP, proporcionando una base robusta para la gestión de rutas, validaciones y acceso a datos. La capa de procesamiento de reconocimiento facial se implementa en Python, utilizando bibliotecas especializadas como *face_recognition* y *OpenCV* (cv2) para el procesamiento de imágenes y la extracción de características faciales.

El almacenamiento de datos se gestiona mediante MySQL, donde se implementa un esquema de base de datos relacional que permite almacenar tanto la información de usuarios como los *encodings* faciales. La estructura de la base de datos se diseña considerando la eficiencia en el almacenamiento y recuperación de datos biométricos, con tablas específicas para personas y registros faciales.

3.8 Dimensión de Procesamiento Facial.

El procesamiento facial se estructura en dos componentes principales:

El primer componente se encarga del registro de rostros, donde se implementa un proceso de captura mediante cámara que genera imágenes en formato *base64*. Estas imágenes son procesadas por *scripts* especializados en Python que extraen los *encodings* faciales utilizando la biblioteca *face_recognition*. Estos *encodings* constituyen una representación matemática única de cada rostro y se almacenan en la base de datos junto con la información del usuario.

El segundo componente gestiona el reconocimiento facial en tiempo real, implementando un sistema de procesamiento que compara los *encodings* de los rostros capturados con aquellos almacenados en la base de datos. Este proceso utiliza algoritmos optimizados para garantizar una comparación eficiente y precisa.

3.9 Dimensión de Implementación.

La implementación del sistema sigue una arquitectura cliente-servidor. En el *frontend*, se implementa una interfaz para la captura de imágenes y gestión de usuarios. El *backend* procesa las solicitudes mediante controladores Laravel que coordinan la comunicación entre la interfaz de usuario y los scripts de procesamiento en Python.

La integración entre los diferentes componentes se realiza mediante APIs bien definidas que permiten una comunicación eficiente entre el *frontend*, el *backend* en Laravel y los scripts de procesamiento en Python. El sistema implementa un manejo robusto de fechas y zonas horarias, configurado específicamente para la zona horaria de Guayaquil (America/Guayaquil).

3.10 Metodología de desarrollo de software.

El desarrollo del sistema se basa en la metodología *SCRUM*, la cual fue elegida

por su capacidad de gestionar proyectos complejos de forma ágil y adaptable. Como señalan Schwaber y Sutherland (2020), SCRUM proporciona un marco que permite abordar problemas complejos de forma adaptativa y al mismo tiempo ofrecer valor añadido paso a paso y sistemático.

A criterio de Menzinsky et al. (2019), *SCRUM* se basa en la teoría empírica de control de procesos y el pensamiento Lean, fundamentándose en tres pilares principales: transparencia, inspección y adaptación. La transparencia requiere que los aspectos significativos del proceso sean visibles para todos los responsables del resultado. La inspección establece que los artefactos de *SCRUM* y el progreso hacia el objetivo deben inspeccionarse frecuentemente. La adaptación indica que, si algún aspecto se desvía de los límites aceptables, el proceso debe ajustarse.

El marco de trabajo *SCRUM*, según Rubin (2018), se estructura en cinco fases fundamentales para el desarrollo del proyecto:

- **Inicio:** En esta fase se realiza el análisis y la identificación de necesidades utilizando como base los *Sprints*. Como indica Kniberg (2015), esta etapa es crucial para establecer la visión del producto y definir el *Product Backlog* inicial.
- **Planificación:** Durante esta etapa se dedica tiempo a estimar tareas y elaborar historias de usuarios a partir del *backlog* o la iteración de tareas. Según Bass (2019), esta fase es fundamental para establecer los objetivos claros y medibles para cada sprint.
- **Implementación:** En esta fase se explora el proceso del sprint y se decide si se realizarán cambios o no, lo que conduce a la creación de los entregables correspondientes. Como señalan Maximini y Maximini (2018), esta etapa requiere

una gestión efectiva del equipo y los recursos.

- **Revisión y retrospectiva:** Esta etapa se encarga de la evaluación interna del grupo en relación con el trabajo desarrollado, demostrando y validando que el *sprint* cumpla con su objetivo. Según Pries y Quigley (2020), esta fase es esencial para la mejora continua del proceso.
- **Lanzamiento:** Representa el desenlace del proyecto en el cual se entrega el producto o servicio, incluyendo los entregables y la retrospectiva del proyecto. Como indican Derby y Larsen (2019), esta fase cierra el ciclo de desarrollo y prepara para futuras iteraciones.

Nombres	*Rol*
Jefe de la empresa	*Scrum Máster*
Ing. José Miguel Erazo	*Product Owner*
Hugolino Orellana **Joseph Sangurima**	*Scrum Team*

Tabla 2 Fuente: Elaboración Propia Metodología SCRUM

3.11 Product Backlog.

"El *product backlog* se refiere a un conjunto de funciones y elementos organizados por orden de prioridad, esenciales para alcanzar los objetivos y satisfacer las expectativas del proyecto. Como norma general, se crea un *backlog* específico para cada producto, asignando a un equipo la responsabilidad de gestionar y desarrollar los elementos pendientes de dicho conjunto"(Asana, s/f).

N*	Descripción de la historia	*Product Backlog Sprint*	*Sprint*
1	Análisis de campo	1	Identificación las tecnologías que se podían usar

2	Validación de tecnologías	1	Corroborar que las tecnologías sean la optimas
3	Diseño de interfaz	2	Planteo del diseño de la interfaz
4	Desarrollo de Interfaz	2	Creación de la interfaz basada en los requisitos del cliente
5	Desarrollo de pruebas	3	Pruebas de usabilidad en tecnologías previamente seleccionadas.

Tabla 3 Fuente: Elaboración propia Product Backlog

3.12 Población y muestra.

La población objetivo para este estudio está constituida por el personal de la empresa de seguridad que interactuará directa o indirectamente con el sistema de reconocimiento facial, por lo que la muestra es igual a la población al no ser un grupo extenso de personas las cuales tendrán acceso y harán uso del sistema de reconocimiento facial.

Se basa principalmente en recolectar la matriz facial base64 de la cara de los usuarios de la empresa usando una cámara para posteriormente verificarla usando el aprendizaje profundo con las matrices que contienen la base de datos y al dar con la matriz correcta se procederá a registrar su entrada o salida mostrando los datos del usuario.

3.13 Procesamiento y análisis.

La metodología empleada para el procesamiento y análisis de datos se estructura de la siguiente manera:

3.13.1 Encuestas y evaluaciones.

Se diseñaron instrumentos específicos para evaluar las métricas de las propiedades emergentes del software:

- Usabilidad del sistema de reconocimiento facial
- Eficiencia en el proceso de registro
- Satisfacción del usuario
- Necesidades específicas de seguridad

Las encuestas constan de preguntas que agrupan las consideraciones por cada uno de los instrumentos

- ¿Qué tan bien considera que el sistema diseñado cumple con la capacidad de reconocer rostros de manera precisa y confiable utilizando métodos avanzados?
- ¿Qué tan bien considera que el sistema reconoce a las personas de forma precisa y sin errores?
- ¿Qué tan bien considera que el sistema registra automáticamente las entradas y salidas y genera reportes en tiempo real?
- ¿Qué tan útil considera que ha sido probar el sistema para ajustarlo a las necesidades de la empresa?

3.14 Técnicas de recolección de datos.

Para asegurar la calidad y confiabilidad de los datos recolectados, se implementaron los siguientes instrumentos:

3.14.1 Encuestas.

“La encuesta es una técnica de investigación que se efectúa mediante la elaboración de cuestionarios y entrevistas de manera verbal o escrita (aunque actualmente se está desarrollando mejor de manera digital) que se hace a una población, ésta generalmente se hace a un grupo de personas y pocas veces a un solo individuo, el propósito es el de obtener información mediante el acopio de datos cuyo análisis e

interpretación permiten tener una idea de la realidad para sugerir hipótesis y poder dirigir las fases de investigación. Se deben complementar con otros métodos permitiendo el seguimiento de resultados inesperados validando otros métodos y profundizando en las razones de las respuestas de las personas.”(Quispe Parí & Sánchez Mamani, /).

Esta técnica se empleó después de la presentación del prototipo desarrollado, con el fin de obtener retroalimentación detallada y relevante. Las preguntas formuladas durante esta etapa fueron diseñadas específicamente en función de los objetivos particulares del proyecto, buscando evaluar de manera precisa si el prototipo cumplía con las expectativas y requisitos establecidos. Cada pregunta estuvo orientada a explorar aspectos clave del diseño, funcionalidad y usabilidad, permitiendo identificar tanto fortalezas como áreas de mejora. De esta manera, se promovió un análisis profundo y estructurado que facilitó la toma de decisiones informadas para el perfeccionamiento del producto final.

Es fundamental realizar una nueva presentación del prototipo después de implementar las sugerencias y correcciones derivadas de la retroalimentación obtenida. Este proceso debe repetirse tantas veces como sea necesario, refinando el diseño y ajustando las funcionalidades según los comentarios del cliente, hasta alcanzar su completa satisfacción. Al realizar una serie de presentaciones y encuestas continuas, no solo se asegura que el producto final cumpla con los requisitos específicos del cliente, sino que también se fomenta una comunicación constante y un enfoque colaborativo, permitiendo que el cliente participe activamente en el proceso de desarrollo. Esta iteración constante es clave para identificar detalles que podrían haberse pasado por alto y garantizar que el prototipo evolucione de manera acorde a las expectativas del cliente,

aumentando así las probabilidades de éxito del producto final.

3.14.2 Entrevistas Estructuradas.

“Consiste en la comunicación verbal entre el entrevistador y entrevistado con el fin de obtener datos. Debe ser previamente diseñada en función al tema de estudio, a la vez de ser planteada por el entrevistador, "Según Kerlinger (1997), la entrevista del tipo estructurada será mejor que los cuestionarios autoadministrados para sondear el comportamiento de las personas, sus intenciones, sus emociones, sus actitudes y sus programas de comportamiento".”(Quispe Parí & Sánchez Mamani, /)

A lo largo del desarrollo del proyecto, se llevaron a cabo varias entrevistas breves de manera virtual, las cuales se realizaron según fue necesario para aclarar puntos clave relacionados con la funcionalidad y el diseño del prototipo. Estas entrevistas fueron esenciales para resolver dudas específicas y asegurar que el producto estuviera alineado con los objetivos del proyecto. Además, en una reciente visita a las instalaciones, se organizó una entrevista de satisfacción con los usuarios, lo que permitió obtener un valioso *feedback* sobre el desempeño del prototipo. A través de esta entrevista, se pudo identificar áreas de mejora y conocer nuevas funcionalidades que los usuarios consideraban necesarias para optimizar la experiencia. Esta retroalimentación detallada y directa ha sido fundamental para guiar las modificaciones y ajustes en el prototipo, asegurando que el producto final cumpla con las expectativas y necesidades de los usuarios, y se ajuste a los requerimientos del cliente.

CAPÍTULO IV

DESARROLLO DEL PROYECTO

El desarrollo de este trabajo de Integración curricular se fue logrando de manera progresiva, ya que a medida que se desarrollaban las reuniones de manera virtual o presencial se tomaban en cuenta los comentarios respectivos sobre el Sistema de Registros de Accesos.

Dentro de las reuniones de trabajo mantenidas con los *sponsors* se propuso el desarrollo de un Sistema de Registro de Accesos para Empleados mediante Reconocimiento Facial con Aprendizaje Profundo en una Bitácora Digital para una Empresa de Seguridad, las tecnologías sugeridas para desarrollar el sistema son:

- Python 3.10.11
- PHP 8.2.12
- SQL 8.0.41
- Laravel 8.75

Se inicio la prueba de varias tecnologías, para encontrar la solución viable y efectiva, para el inicio y desarrollo del sistema, comenzando con la librería de *mediapipe (Figura 4 Medipipe superficie).*

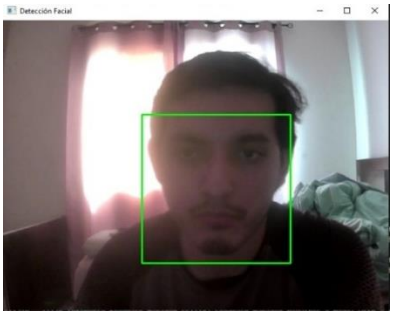


Figura 4 Medipipe superficie

Se inicio pruebas en modelos *facenet tensorflow (Figura 5 Facenet Tensorflow)*, para pruebas iniciales, en reconociendo por superficie, superficie vectorizada 3d (Figura 6 Vectores 3D) y de objeto.

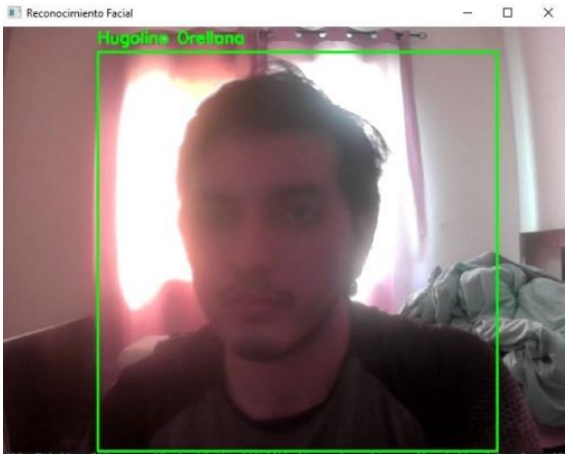


Figura 5 Facenet-TensorFlow

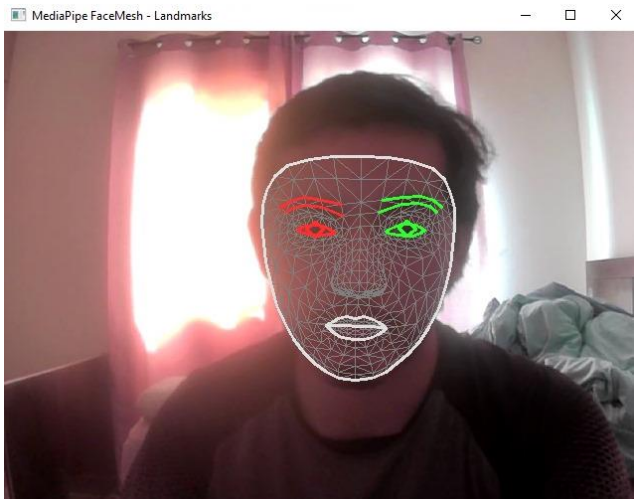


Figura 6 Vectores 3D

Luego realizar pruebas de funcionamiento, se decidió optar por una librería, óptima, ágil y segura, por sus capacidades amplias en integración a sistemas robustos y seguros, como php laravel, con sus respectivas librerías de Python, llamada *face_recognition.*

En una de las reuniones con el *sponsor* se comentó que el sistema debe registrar

las entradas y salidas de los empleados de la empresa de seguridad mediante un sistema de reconocimiento facial que usa algoritmos de aprendizaje profundo que se integrará con las cámaras de la empresa para poder reconocer a la persona que está ingresando o saliendo de la empresa, esto trabajo de Integración curricular no abarcará temas como la instalación y configuración de cámaras, detección de emociones o instalación de infraestructura adicional, o cualquier otro requisito que no fue previamente especificado en los requerimientos.

En el diseño del sistema se usó como base Bootstrap, ya que es una herramienta muy útil al momento de diseñar todo tipo de sistemas o páginas web por su facilidad de uso, adaptabilidad y amplia biblioteca de iconos.

En el diseño de la Tipografía se eligió Google Font API ya que es una herramienta con una amplia gama de opciones de diseño y maquetado muy llamativas a la vista de los usuarios finales.

Se desarrolló el diseño inicial del sistema, a través de la tecnología de *API* de laravel (Figura 7 Laravel) para manejar las solicitudes y a su vez por su seguridad al ser un *framework* de *backend* robusto y seguro.

Figura 7 Laravel

El sistema recopila los datos de los campos obligatorios proporcionados por el usuario y la respuesta es enviada a través del *backend* hacia los diferentes *Controllers* y rutas *API* previamente programadas para poder realizar las respuestas al *backend.*

Una vez se envía la información, se ejecuta un proceso de extracción por medio

de la API de Python *face_recognition*, esto resulta en una de matriz de puntos de rostro los cuales, se registrarán en la base de datos (Figura 8) en formato base64.

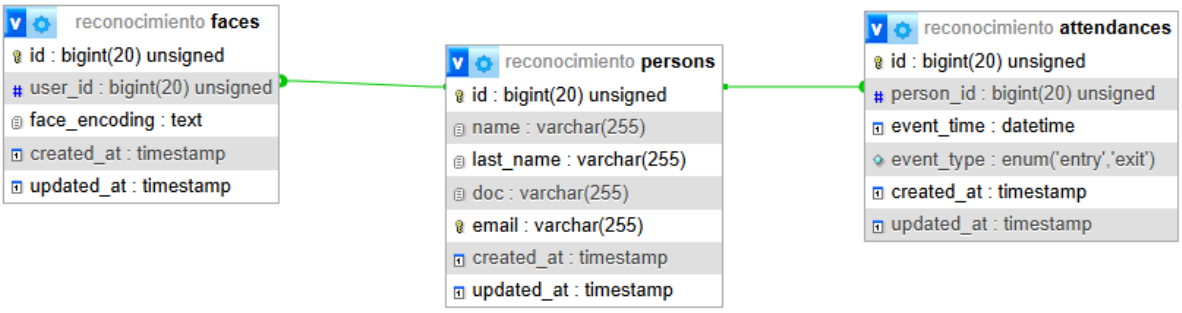


Figura 8 Modelo de entidad relación del sistema. Fuente: Elaboración propia

Para el diseño de la sección de registro de asistencias se optó por usar las mismas herramientas que en la sección de registro de usuario (Bootstrap, laravel, Google Font Api, JQuery).

El reconocimiento facial usa la *API Face_recognition* para obtener el embebido enviarlo a la base de datos y compararlo con el *face_encoding* previamente almacenado y si el script realiza una coincidencia con el rostro que actualmente está procesando, mediante una función *get* se obtiene los datos del usuario de la base de datos y se muestran en el apartado de Usuarios Detectados. Una vez el *script* del *face_recognition* cumple su función obtiene mediante *datetime* los datos necesarios para poder almacenar la hora de entrada o salida en la base de datos y mediante una función *get* se muestran en el apartado de Registros del día.

Para la implementación del sistema se optó por subir el sistema a un repositorio en *Git* y consecutivamente clonarlo al servidor, una vez clonado se realizó las respectivas configuraciones como lo son:

- La instalación de las librerías de Python.
- Configuración de conectividad hacia la base de datos.

- Se incluyeron rutas en los códigos para poder cargar las páginas y utilizar las librerías necesarias.

La conexión a la base de datos se logró usando *Laravel* como *Backend.* Para su correcto funcionamiento se eliminó y recreó la base de datos usando *php artisan migrate* que realiza las migraciones y crear las tablas y se usó *php artisan serve* para levantar el servicio y realizar las pruebas optimas.

Se realizó una serie 30 de pruebas en tres equipos diferentes en entornos locales para comprobar el correcto y óptimo funcionamiento del sistema de registro de accesos para empleados mediante reconocimiento facial con aprendizaje profundo, con los cuales el objetivo es medir los tiempos de respuesta y comprobar que estos dependen de las capacidades del equipo en donde se está implementando.

Equipo 1 - Bajo recursos

Características:

- Lenovo
- AMD A12 7Gn.
- 8GB Ram

Este equipo al ser de gama baja ralentizaba el proceso del face_recognition demorando el proceso de reconocimiento facial entre 15 a 20 segundos.

Equipo 2 - Medio recursos

- Hp
- Ryzen 3 5Gn
- 8GB Ram

En este equipo al ser de características decentes el proceso del face_recognition

se logró agilizar reduciendo los tiempos de reconocimiento facial a entre 4 y 5 segundos mejorando el performance,

Equipo 3 - Óptimos recursos

- Ryzen 7 12Gn
- 16GB Ram
- AMD GRAPHICS

En este equipo los resultados fueron más favorables en cuanto a reconocimiento facial ya que los tiempos se vieron reducidos gracias a sus características mejoradas logrando pasar de 20 segundos a 3 segundo en lograr reconocer el rostro del usuario. Se logró obtener una mejora del 85% en términos de reducción de tiempo en reconocimiento facial.

La fórmula de mejora porcentual mide la reducción relativa del tiempo tras una optimización. Se calcula restando el tiempo final del tiempo inicial, dividiendo el resultado por el tiempo inicial y multiplicando por 100 para expresarlo en porcentaje. Este cálculo permite evaluar mejoras en eficiencia al comparar el desempeño antes y después de una intervención.

$$Mejora(\%) = (\frac{Tiempo\ inicial - Tiempo\ final}{Tiempo\ inicial}) * 100$$

En el estudio, esta fórmula se aplicó para medir la reducción en los tiempos de registro de accesos tras implementar un sistema de reconocimiento facial con aprendizaje profundo. Se compararon los tiempos antes y después de la optimización, evidenciando una mejora significativa en la rapidez del proceso, lo que justificó la efectividad del nuevo sistema en la empresa.

En este caso, con un tiempo inicial de 20 unidades y un tiempo final de 3, la mejora

se obtuvo como

$$Mejora(\%) = (\frac{20 - 3}{20}) * 100$$

$$Mejora(\%) = (\frac{17}{20}) * 100$$

$$Mejora(\%) = 85\%$$

Lo que indica una reducción significativa del tiempo.

Este resultado demuestra que la implementación del sistema de reconocimiento facial con aprendizaje profundo optimizó el registro de accesos, reduciendo el tiempo de procesamiento en un 85%. Esto evidencia una mayor eficiencia operativa en la empresa, agilizando la identificación de los empleados y minimizando retrasos en el proceso.

El diseño del sistema de reconocimiento facial se logró mediante el uso de técnicas avanzadas de inteligencia artificial, específicamente con la implementación de *Deep Learning* a través de la librería *face_recognition* en Python. Se realizaron pruebas con diferentes modelos, como *Facenet TensorFlow* y *Mediapipe*, seleccionando finalmente una solución que optimizara la identificación de rostros en tiempo real. Para garantizar una integración eficiente, se utilizó Laravel como *backend*, permitiendo la gestión de usuarios y registros de acceso de manera estructurada. Además, se incorporaron tecnologías como Bootstrap y Google Font API para el diseño de una interfaz accesible y funcional, facilitando la interacción de los empleados con el sistema.

La implementación de algoritmos de *Deep Learning* mejoró significativamente la precisión del reconocimiento facial, reduciendo los errores de identificación y minimizando los falsos positivos y negativos. La integración con la bitácora digital permitió el almacenamiento automático de accesos y la generación de reportes en tiempo

real, asegurando un monitoreo constante del flujo de empleados en la empresa de seguridad. Finalmente, las pruebas de desempeño realizadas en equipos con distintos niveles de recursos demostraron la eficiencia del sistema, evidenciando una reducción del tiempo de reconocimiento en un 85%. Estos ensayos permitieron identificar y aplicar mejoras, asegurando un funcionamiento óptimo antes de su implementación definitiva en el entorno empresarial.

Consecuentemente, el objetivo general del trabajo de Integración Curricular se cumple mediante el desarrollo e implementación de un sistema de registro de accesos basado en reconocimiento facial con aprendizaje profundo, almacenando la información en una bitácora digital. Para ello, se integraron tecnologías como Python, PHP, Laravel y SQL, junto con la librería *face_recognition*, que permitió extraer y comparar los *face encodings* de los empleados en la base de datos. Durante las pruebas, se verificó la funcionalidad del sistema en diferentes equipos con distintos niveles de recursos, demostrando su capacidad para adaptarse y optimizar los tiempos de procesamiento. Además, se diseñó una interfaz utilizando Bootstrap y Google Font API para garantizar una experiencia de usuario intuitiva y eficiente.

El sistema cumplió con su propósito al registrar las entradas y salidas de los empleados de una empresa de seguridad, integrándose con las cámaras y asegurando una identificación precisa. Se realizaron pruebas en entornos controlados, evidenciando una mejora del 85% en la velocidad de reconocimiento facial en equipos de alto rendimiento. Esto validó la efectividad del sistema para optimizar los tiempos de acceso y fortalecer la seguridad en la empresa. Finalmente, su implementación en un servidor mediante Git y Laravel permitió una gestión estructurada de la base de datos,

asegurando su correcto funcionamiento y almacenamiento eficiente de registros en la bitácora digital.

Por otro lado, la primera pregunta de investigación formulada en el presente trabajo de integración curricular se cumple, ya que un sistema de registro de accesos basado en reconocimiento facial con *Deep Learning* mejora la precisión, seguridad y eficiencia en la gestión de accesos en una empresa de seguridad física en Ecuador. Esto se logra mediante la implementación de técnicas avanzadas de inteligencia artificial para la identificación de empleados, optimizando la detección y autenticación de rostros con el uso de la librería *face_recognition* en Python, lo que permite reducir falsos positivos y negativos. Además, la integración del sistema con una bitácora digital garantiza un registro automático y seguro de las entradas y salidas, minimizando errores humanos y asegurando la trazabilidad de los accesos. La combinación de estas tecnologías incrementa la precisión del sistema, disminuye las posibilidades de suplantación de identidad y refuerza el control de seguridad dentro de la empresa, cumpliendo así con los objetivos planteados en la investigación.En términos de eficiencia, el sistema demostró mejoras significativas en los tiempos de procesamiento, reduciendo el tiempo de reconocimiento facial en equipos de alto rendimiento. Esto permitió un acceso más ágil de los empleados, eliminando demoras innecesarias y optimizando el flujo de ingreso y salida. Las pruebas en distintos entornos validaron su desempeño y confiabilidad, asegurando su adaptabilidad a diferentes configuraciones tecnológicas. Finalmente, la implementación en un servidor con Laravel y Git posibilitó una gestión estructurada de la base de datos, asegurando su correcto funcionamiento y manteniendo la integridad de los registros en tiempo real. Esto evidencia cómo el uso de *Deep Learning* en un sistema

de reconocimiento facial puede transformar la gestión de accesos, elevando los estándares de seguridad y operatividad en una empresa de seguridad física en Ecuador.

La segunda pregunta del presente trabajo de integración curricular se cumple, ya que la integración de un sistema de reconocimiento facial con *Deep Learning* en la gestión de accesos de una empresa de seguridad física tiene un impacto significativo en la precisión, seguridad y eficiencia operativa. La implementación de algoritmos avanzados de inteligencia artificial optimiza la identificación de empleados, reduciendo los errores en el reconocimiento facial y minimizando los riesgos de suplantación de identidad. Además, el uso de la librería *face_recognition* en Python permitió mejorar la velocidad del proceso, logrando una reducción en los tiempos de autenticación, lo que agiliza el control de acceso y evita retrasos operativos. La integración con una bitácora digital automatiza el registro de entradas y salidas, eliminando errores manuales y garantizando la trazabilidad en tiempo real. Las pruebas realizadas en diferentes equipos también demostraron que el desempeño del sistema varía según los recursos del hardware, lo que resalta la importancia de contar con una infraestructura adecuada para maximizar la efectividad del sistema. En conjunto, estas mejoras incrementan la seguridad en la empresa, optimizan el flujo de trabajo y fortalecen la eficiencia operativa, al reducir tiempos y errores en la gestión de accesos.

Conclusiones.

El diseño se implementó usando las herramientas *Laravel, Bootstrap, JavaScript y Google Font Api*, logrando crear una base sólida entre el *Backend* y el *Frontend* ya que Laravel facilito la estructura y seguridad del *Backend*. Mientras que Bootstrap simplifico y optimizo el proceso de la creación de la interfaz. *JavaScript*, por su parte, aportó dinamismo e interactividad, mejorando la experiencia del usuario, y la integración de *Google Font* contribuyó a una estética visual coherente y accesible. La combinación de estas tecnologías, junto con un algoritmo eficiente, permitió una arquitectura robusta que garantizó un rendimiento óptimo y escalabilidad, satisfaciendo las necesidades del sistema de manera eficaz y ofreciendo una experiencia fluida y atractiva al usuario.

La implementación del algoritmo de *Deep Learning* se llevó a cabo mediante el uso de la librería *face_recognition*, utilizando su algoritmo *CNN (Convolutional Neural Network)* para el reconocimiento facial. Con el fin de optimizar el rendimiento y la precisión del sistema, se ajustó el nivel de confiabilidad a 7, lo que resultó ser la opción más adecuada para el contexto de la aplicación. Este ajuste permitió equilibrar la sensibilidad del algoritmo, reduciendo de manera significativa la tasa de falsos positivos sin afectar negativamente la capacidad de identificación. Al configurar el parámetro de esta manera, se consiguió una mayor fiabilidad en los resultados del reconocimiento facial, mejorando tanto la eficiencia como la robustez del sistema en entornos reales.

La integración se llevó al cabo mediante la clonación del sistema previamente subido a un repositorio de *GitHub* , se realizaron las correspondientes correcciones y se levantó la conexión con la base de datos, asegurando que las credenciales y parámetros de conexión fueran los correctos para el entorno del servidor, se realizó la migración de

la base de datos, garantizando que la estructura de las tablas y los datos necesarios fueran correctamente implementados, luego se procedió a levantar el servicio para una prueba la cual fue optima.

Se realizaron pruebas en tres entornos locales diferentes, utilizando equipos con características de hardware variadas, sobre el sistema ya implementado. Estas pruebas permitieron analizar el comportamiento del sistema en función de las especificaciones técnicas de cada equipo, evidenciando una variabilidad en su desempeño. Los resultados mostraron que el rendimiento del sistema estaba estrechamente relacionado con las capacidades de hardware de los equipos utilizados. En particular, el equipo con las mejores características de hardware demostró una mejora del 85% en el tiempo de reconocimiento facial en comparación con el primer equipo, lo que subraya la importancia de contar con recursos adecuados para optimizar la eficiencia del sistema. Esto destaca la necesidad de considerar las especificaciones del hardware al momento de implementar el sistema en entornos reales, ya que influye directamente en la rapidez y precisión de los procesos de reconocimiento.

Recomendaciones.

Para que el sistema funcione de manera correcta y optima se recomienda:

- El área en donde se ubica la cámara cuente con una apropiada fuente de iluminación, aunque el sistema ha demostrado un buen funcionamiento con poca iluminación es prescindible especificar que se debe tener un área bien iluminada.
- Verificar de manera regular el sistema de registros en caso de que se presenten visitantes sería una buena práctica eliminar esos registros para que no ocupen un espacio ya que son datos temporales.
- Se recomienda usar un equipo con hardware moderno ya que en las pruebas que se realizó el equipo A tiene componentes más viejos a comparación del equipo B ya que el equipo B es más moderno y se notó la diferencia en el tema del tiempo de reconocimiento facial ya que este mismo se está realizando de manera ininterrumpida.
- Realizar una charla breve sobre el correcto funcionamiento del sistema para facilitar el entendimiento del sistema y así evitar errores humanos al momento de usarlo.

Bibliografía

¿Qué es Laravel y para qué sirve? (2022, julio 26). Talently Blog. https://talently.tech/blog/que-es-laravel/

¿Qué es Python? - Explicación del lenguaje Python - AWS. (s/f). Amazon Web Services, Inc. Recuperado el 30 de enero de 2025, de https://aws.amazon.com/es/what-is/python/

Arias, M. A. (2013). Introducción a PHP. IT Campus Academy.

Art. 22 GDPR – Automated individual decision-making, including profiling. (s/f). General Data Protection Regulation (GDPR). Recuperado el 27 de noviembre de 2024, de https://gdpr-info.eu/art-22-gdpr/

Asamblea Nacional de Ecuador. (s/f). Ley de Protección de Datos Personales. Dirección Nacional de Registros Públicos. Recuperado el 27 de noviembre de 2024, de https://www.registrospublicos.gob.ec/programas-servicios/servicios/proyecto-de-ley-de-proteccion-de-datos/

Asana. (s/f). This specialized to-do list keeps developers focused [2024]. Asana. Recuperado el 30 de enero de 2025, de https://asana.com/es/resources/product-backlog

Aviso de Privacidad. (s/f). Deloitte Ecuador. Recuperado el 27 de noviembre de 2024, de https://www2.deloitte.com/ec/es/legal/about-Deloitte-Ecuador/Proveedores.html

Boult, T. E., Micheals, R. J., & Aagaard, M. (2003). Face Recognition and its Security Applications. Proceedings of the IEEE, 91(12), 2019–2049. https://doi.org/10.1109/JPROC.2003.819619

Campillo, R. (2020, noviembre 23). Historia del Reconocimiento Facial. Mobbeel. https://www.mobbeel.com/blog/historia-del-reconocimiento-facial/

Control de Acceso: Definición, Para qué sirve y Dónde utilizarlo. (s/f). Recuperado el 15 de noviembre de 2024, de https://es.linkedin.com/pulse/control-de-acceso-definici%C3%B3n-para-qu%C3%A9-sirve-

Deng, J., Guo, J., Xue, N., & Zafeiriou, S. (2019). ArcFace: Additive Angular Margin Loss for Deep Face Recognition. 2019 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR), 4685–4694. https://doi.org/10.1109/CVPR.2019.00482

Duckerman, W. (2022, febrero 7). ¿Qué es la tecnología de reconocimiento facial de IA y cómo funciona? Brita Inteligencia Artificial. https://brita.mx/que-es-la-tecnologia-de-reconocimiento-facial-de-ia-y-como-funciona/

EFF Comments on DHS Proposed Rule on Collection and Use of Biometrics—October 2020. (2020, octubre 22). Electronic Frontier Foundation. https://www.eff.org/document/eff-comments-dhs-proposed-rule-collection-and-use-biometrics-october-2020

Face Recognition in Python—Javatpoint. (s/f). Www.Javatpoint.Com. Recuperado el 31 de enero de 2025, de https://www.javatpoint.com/face-recognition-in-python

Face Recognition Vendor Test (FRVT). (s/f). NIST. Recuperado el 25 de noviembre de 2024, de https://www.nist.gov/programs-projects/face-recognition-vendor-test-frvt

Frost & Sullivan Recognizes NEC with the 2020 Global Biometrics in Security Market Growth Innovation & Leadership Excellence Frost RadarTM Award. (s/f). NEC. Recuperado el 25 de noviembre de 2024, de https://www.nec.com/en/press/202103/global_20210317_01.html

Fully Digital Travel Experience Closer to Reality. (s/f). Recuperado el 25 de noviembre de 2024, de https://www.iata.org/en/pressroom/2024-releases/2024-10-30-03/

Goodfellow, I., Bengio, Y., & Courville, A. (2016a). Deep Learning. MIT Press.

Goodfellow, I., Bengio, Y., & Courville, A. (2016b). Deep Learning. MIT Press. https://www.deeplearningbook.org

Hernández, R. G. (s/f). ESTUDIO DE TÉCNICAS DE RECONOCIMIENTO FACIAL.

Illinois Compiled Statutes. (s/f). Illinois General Assembly. Recuperado el 27 de noviembre de 2024, de https://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004

Jain, A. K., Ross, A. A., & Nandakumar, K. (2011a). Introduction to Biometrics. Springer US. https://doi.org/10.1007/978-0-387-77326-1

Jain, A. K., Ross, A. A., & Nandakumar, K. (2011b). Introduction to Biometrics. Springer US. https://doi.org/10.1007/978-0-387-77326-1

Kennedy, G. (2019). Artificial Intelligence and Privacy: Towards an Ethical Framework for AI Deployment. Computer Law & Security Review, 35(3), 361–368. https://doi.org/10.1016/j.clsr.2019.04.002

LeCun, Y., Bengio, Y., & Hinton, G. (2015). Deep learning. Nature, 521(7553), 436–444. https://doi.org/10.1038/nature14539

Lei Geral de Proteção de Dados Pessoais (LGPD). (s/f). Ministério do Esporte. Recuperado el 27 de noviembre de 2024, de https://www.gov.br/esporte/pt-br/acesso-a-informacao/lgpd/lei-geral-de-protecao-de-dados-pessoais-lgpd

Métodos Tradicionales Control Acceso. (s/f). FasterCapital. Recuperado el 15 de noviembre de 2024, de https://fastercapital.com/keyword/métodos-tradicionales-control-acceso.html

Mittelstadt, B. D., Allo, P., Taddeo, M., Wachter, S., & Floridi, L. (2016). The ethics of algorithms: Mapping the debate. Big Data & Society, 3(2), 2053951716679679. https://doi.org/10.1177/2053951716679679

MySQL :: MySQL Connector/Python Developer Guide: 1 Introduction to MySQL Connector/Python. (s/f). Recuperado el 25 de enero de 2025, de https://dev.mysql.com/doc/connector-python/en/connector-python-introduction.html

MySQL :: MySQL Database. (s/f). Recuperado el 31 de enero de 2025, de https://www.mysql.com/products/enterprise/database/

MySQL :: MySQL para principiantes. (s/f). Recuperado el 31 de enero de 2025, de https://www.mysql.com/news-and-events/web-seminars/mysql-para-principiantes/

Nino Cassanello Foghini. (2023, octubre 11). Crisis de seguridad en Ecuador: Pasado, presente y futuro - Agenda Estado de Derecho. Agenda Estado de Derecho. https://agendaestadodederecho.com/crisis-de-seguridad-en-ecuador/

OEA, & OEA. (2009, agosto 1). OEA - Organización de los Estados Americanos: Democracia para la paz, la seguridad y el desarrollo [Text]. https://www.oas.org/es/sla/ddi/proteccion_datos_personales.asp

OpenCv. (s/f). OpenCV. Recuperado el 25 de enero de 2025, de https://opencv.org/about/

Parkhi, O. M., Vedaldi, A., & Zisserman, A. (2015). Deep Face Recognition. Procedings of the British Machine Vision Conference 2015, 41.1-41.12. https://doi.org/10.5244/C.29.41

Protección de datos—Comisión Europea. (2021, junio 4). https://commission.europa.eu/law/law-topic/data-protection_es

Quispe Parí, D. J., & Sánchez Mamani, G. (/). Encuestas y entrevistas en investigación científica. Revista de Actualización Clínica Investiga, 490.

Reconocimiento facial: Descubre cómo funciona y quién (y para qué) lo utiliza. (s/f). LISA Institute. Recuperado el 18 de noviembre de 2024, de https://www.lisainstitute.com/blogs/blog/reconocimiento-facial-como-funciona-quien-utiliza

Russell, S. J., & Norvig, P. (with Chang, M., Devlin, J., Dragan, A., Forsyth, D., Goodfellow, I., Malik, J., Mansinghka, V., Pearl, J., & Wooldridge, M. J.). (2021). Artificial intelligence: A modern approach (Fourth Edition). Pearson.

Sandra Domínguez. (2023, agosto 4). Deep Learning: El corazón de la inteligencia artificial | OpenWebinars. OpenWebinars.net. https://openwebinars.net/blog/deep-learning-el-corazon-de-la-inteligencia-artificial/

Schroff, F., Kalenichenko, D., & Philbin, J. (2015). FaceNet: A unified embedding for face recognition and clustering. 2015 IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 815–823. https://doi.org/10.1109/CVPR.2015.7298682

System Front Information. (2023, noviembre 2). Biometrics and Authentication: A Comprehensive Guide. Systems Front - IT. https://www.asf-it.com/cybersecurity/biometrics-and-authentication-a-comprehensive-guide/

Voss, G. (2024, septiembre 10). Cómo los criminales ecuatorianos están aprovechando las empresas de seguridad privada. InSight Crime. http://insightcrime.org/es/noticias/criminales-ecuador-aprovechando-empresas-seguridad-privada/

What is Histogram of Oriented Gradients (HOG)? (s/f). Educative. Recuperado el 31 de enero de 2025, de https://www.educative.io/answers/what-is-histogram-of-oriented-gradients-hog

Zhang, Z., Zhang, J., & Wei, Y. (2018). Applications of Face Recognition Technology in Security. IEEE Access, 6, 12345–12356. https://doi.org/10.1109/ACCESS.2018.1234567

Anexos

Manual de instrucciones.

Sistema de reconocimiento facial versión 1.0.

Figura 9 Sistema de reconocimiento facial v1.0 Fuente: Elaboración propia

Figura 10 Sistema de reconocimiento facial v1.0 Fuente: Elaboración propia

El inicio del sistema de reconocimiento facial cuenta con una interfaz atractiva y moderna como se muestra en la Figura 9 el cual contiene una descripción de la

funcionalidad del sistema, con opción para poder cambiar la tonalidad de fondo a una más clara tal como se muestra en la Figura 10.

Figura 11 Sistema de reconocimiento facial v1.0 Fuente: Elaboración propia

En la Figura 11 se muestra el diseño del apartado de Reconocimiento Facial, en el cual están los campos de los datos personales, el área de visualización de la cámara y el área en el que se mostrarán los datos de los usuarios y su información de entrada o salida.

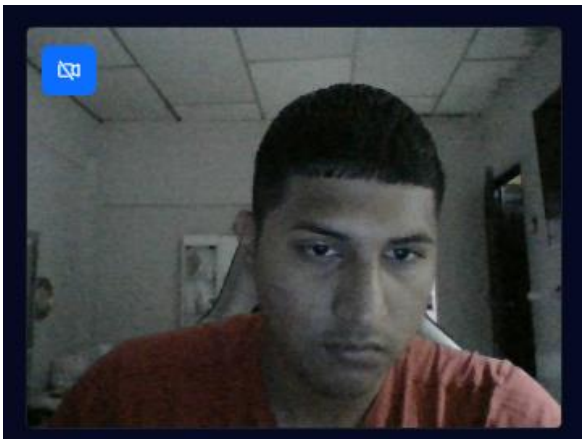


Figura 12 Sistema de reconocimiento facial v1.0 Fuente: Elaboración propia

Al conceder los permisos necesarios se logra obtener una imagen en vivo del usuario tal como se muestra en la Figura 12.

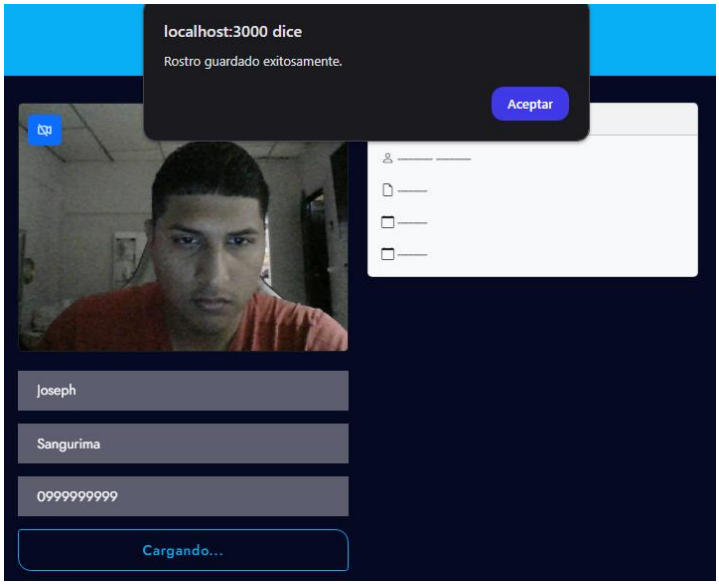


Figura 13 Sistema de reconocimiento facial v1.0 Fuente: Elaboración propia

Al llenar todos los campos necesarios presionar el botón Guardar Rostro se emite un mensaje que indica que el rostro fue guardado de manera exitosa en la base de datos tal como se muestra en la Figura 13

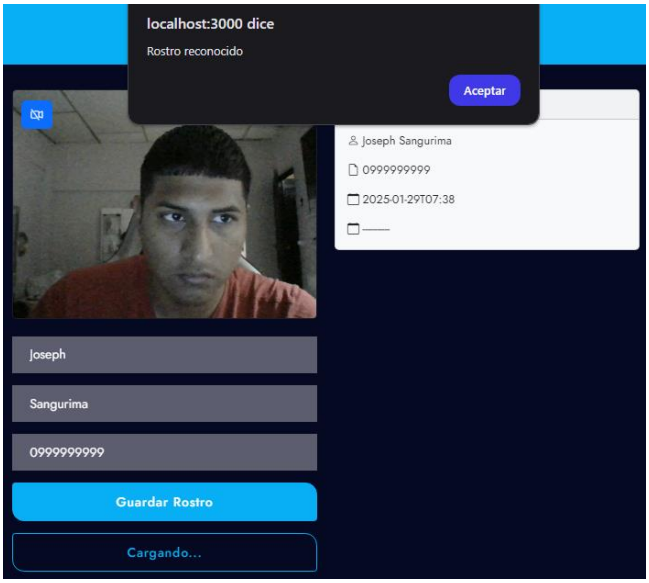


Figura 14 Sistema de reconocimiento facial v1.0 Fuente: Elaboración propia

Después de guardar el rostro se procede a hacer la validación la cual se ejecuta usando el botón Validar Rostro tal como se muestra en la Figura 14, de manera seguida

aparece un mensaje emergente indicando que el rostro fue reconocido o no reconocido.

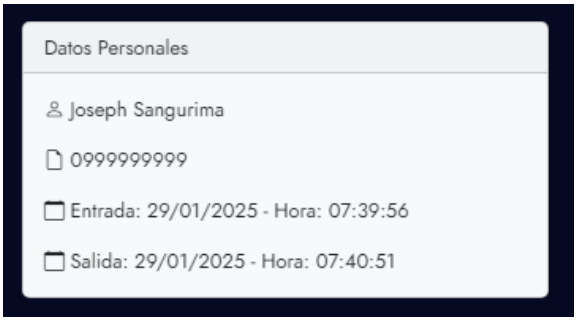


Figura 15 Sistema de reconocimiento facial v1.0 Fuente: Elaboración propia

Tal como se muestra en la Figura 15 después de hacer el proceso de validación del rostro se llena de manera automática la sección de Datos personales con las entradas y salidas del usuario las cuales dependerán de las veces que hagan uso del botón Validar Rostro.

Sistema de reconocimiento facial versión 2.0.

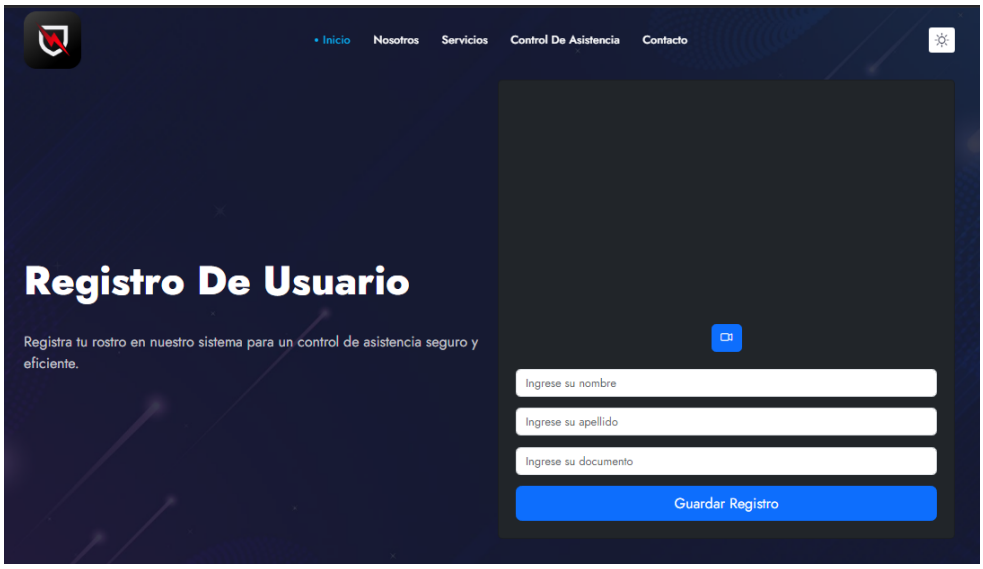


Figura 16 Sistema de reconocimiento facial v2.0 Fuente: Elaboración propia

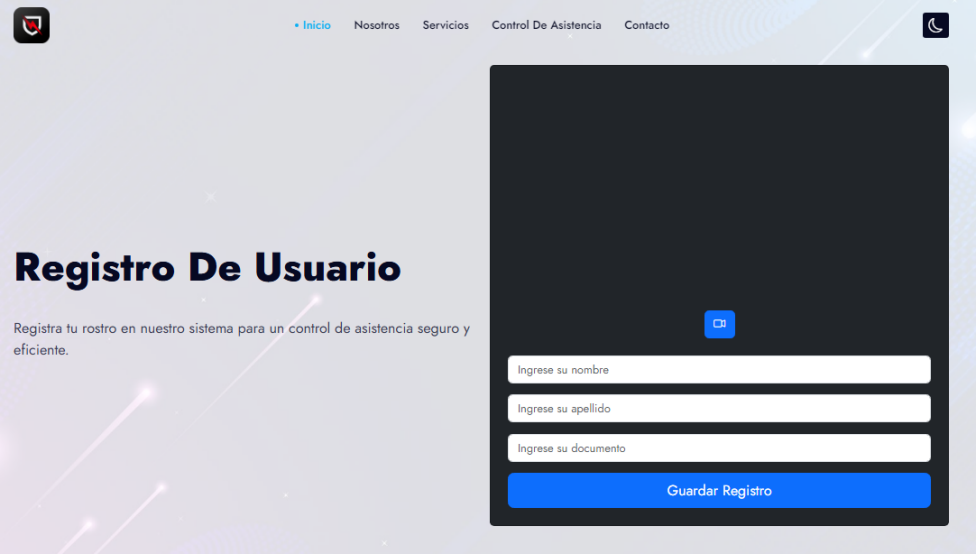


Figura 17 Sistema de reconocimiento facial v2.0 Fuente: Elaboración propia

Para esta versión se decidió simplificar su diseño ya que la versión anterior tenía demasiados detalles que no eran relevantes para el proyecto, en esta nueva versión se decidió simplificar el diseño y reducirlo a una única sección conservando el detalle de poder cambiar la tonalidad del sistema tal como se muestra en la Figura 16 y la Figura 17.

Sistema de reconocimiento facial versión 3.0.

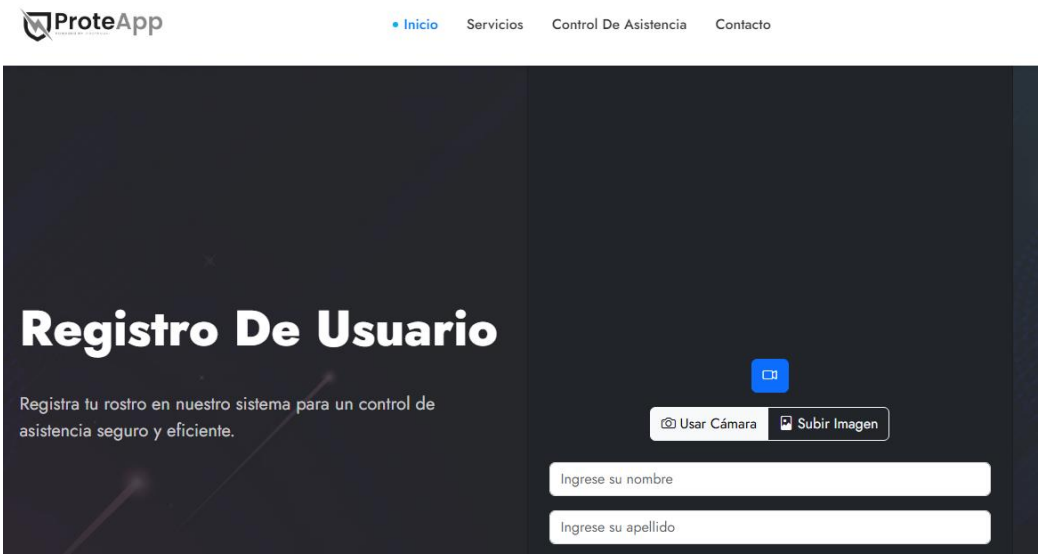


Figura 18 Sistema de reconocimiento facial v3.0 Fuente: Elaboración propia

En esta versión se cambió la paleta de colores de la sección de Registro de usuario por de escala de gris y se optó por agregar una opción de Subir imagen en caso de no tener cámaras en funcionamiento tal como se muestra en la Figura 18.

Figura 19 Sistema de reconocimiento facial v3.0 Fuente: Elaboración propia

En esta versión del sistema se agregó una pequeña sección de instrucciones en la parte inferior del sistema para poder guiar a los usuarios tal como se muestra en la Figura 19.

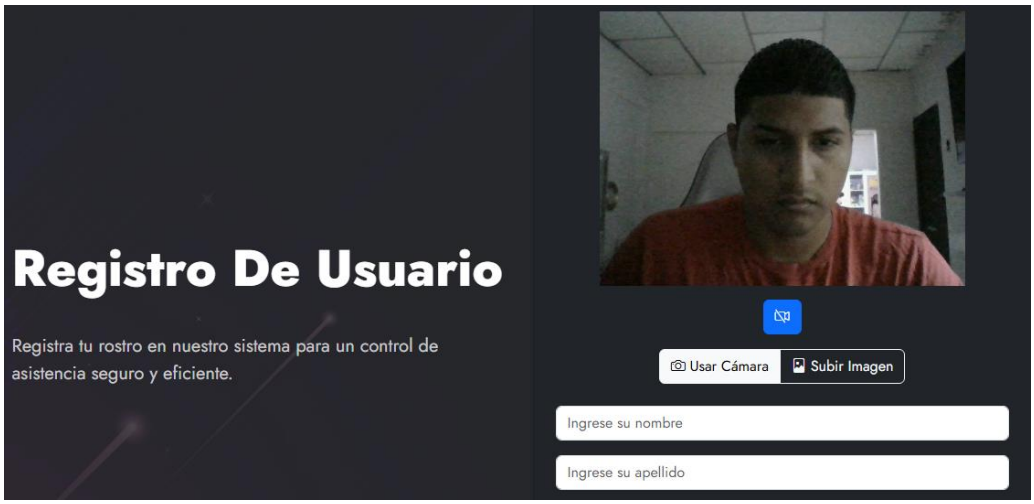


Figura 20 Sistema de reconocimiento facial v3.0 Fuente: Elaboración propia

Al conceder los permisos necesarios para el funcionamiento del sistema se puede activar la cámara para realizar el proceso de registro de los datos llenando los campos respectivos con la información adecuada tal como se muestra en la Figura 20.

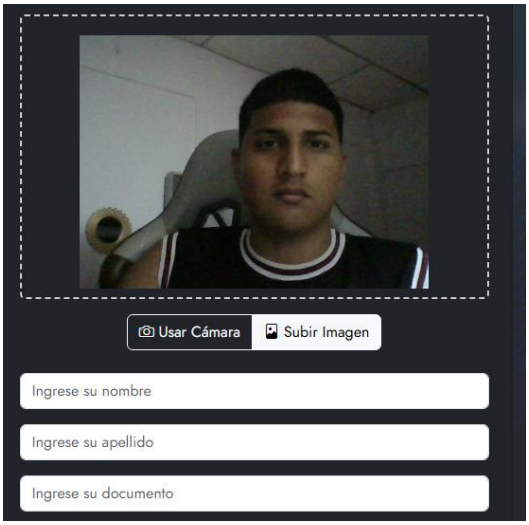


Figura 21 Sistema de reconocimiento facial v3.0 Fuente: Elaboración propia

En caso de no contar con cámaras en funcionamiento o como una segunda opción para poder realizar el proceso de registro de los datos se podrá subir una foto del usuario tal como se muestra en la Figura 21.

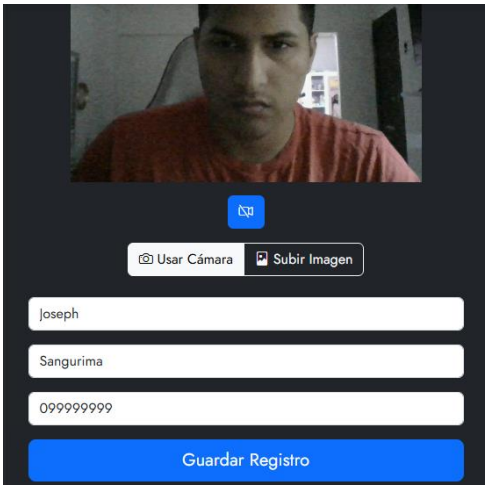


Figura 22 Sistema de reconocimiento facial v3.0 Fuente: Elaboración propia

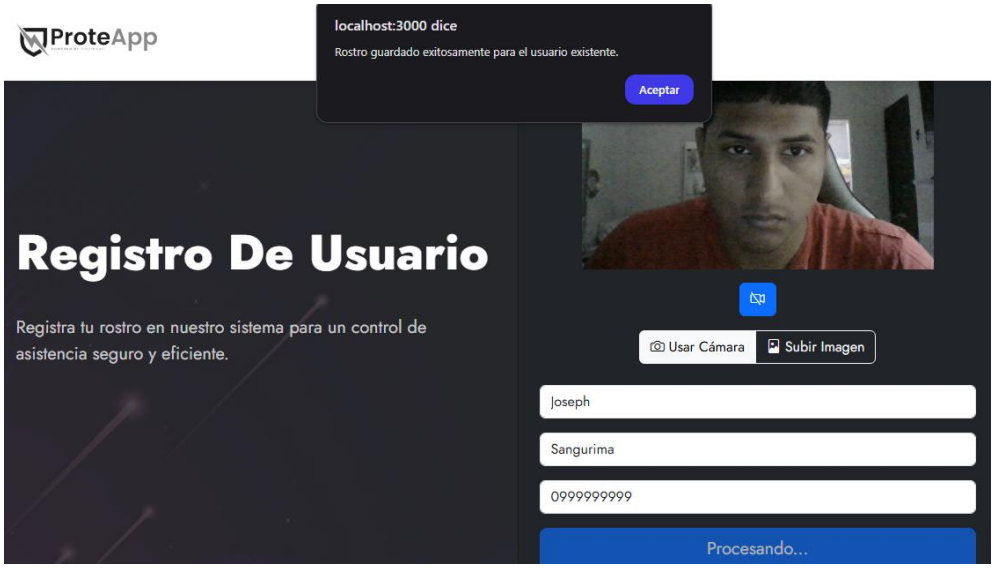


Figura 23 Sistema de reconocimiento facial v3.0 Fuente: Elaboración propia

Al momento de completar los campos necesarios teniendo activa la cámara o haber subido una imagen se procederá al almacenamiento de los datos y del rostro del usuario en la base de datos tal como se muestra en la Figura 22 y en la Figura 23.

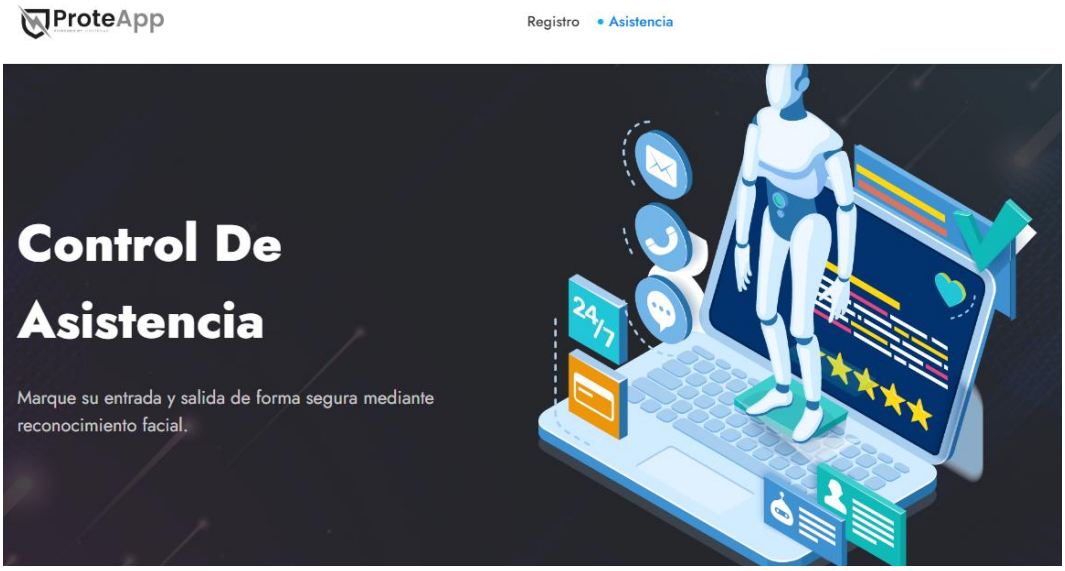


Figura 24 Sistema de reconocimiento facial v3.0 Fuente: Elaboración propia

Figura 25 Sistema de reconocimiento facial v3.0 Fuente: Elaboración propia

Una vez registrado los datos de los usuarios se procederá a la sección de Control de Asistencia tal como se muestra en la Figura 24 al apartado de reconocimiento Facial tal como se muestra en la Figura 25, en este caso se mejoró el sistema de reconocimiento facial ya que ahora no se debe estar presionando el botón de Verificar Rostro como se debía hacer en la versión 1 del sistema ya que ahora la detección del rostro es automático, una vez que el sistema detecte el rostro se mostrarán los datos del usuario y sus respectivos registros de entrada y salida.

Sistema de reconocimiento facial versión 4.0.

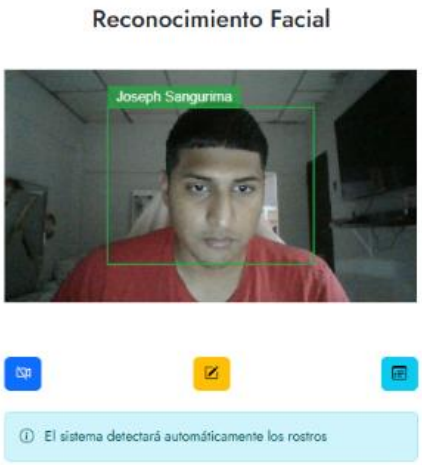


Figura 26 Sistema de reconocimiento facial v4.0. Fuente: Elaboración propia

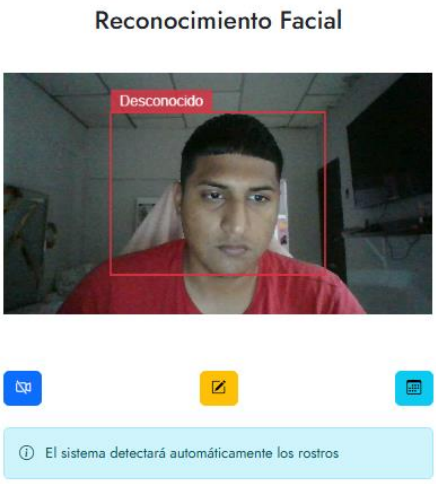


Figura 27 Sistema de reconocimiento facial v4.0. Fuente: Elaboración propia

En esta versión se mejoró el diseño de la interfaz de reconocimiento facial agregando un recuadro que indica el nombre de la persona y el recuadro en color verde cuando se logró identificar al usuario tal como se muestra en la Figura 26, cuando el sistema no tiene registros del rostro que está identificando el recuadro se torna de color rojo mostrando como nombre Desconocido tal como se muestra en la Figura 27.

Validaciones.

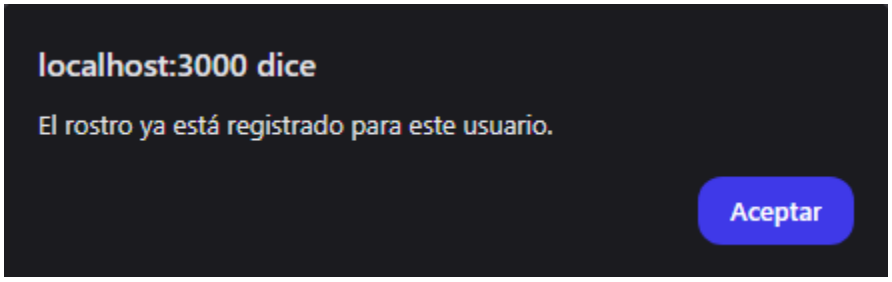


Figura 28 Validaciones Fuente: Elaboración propia

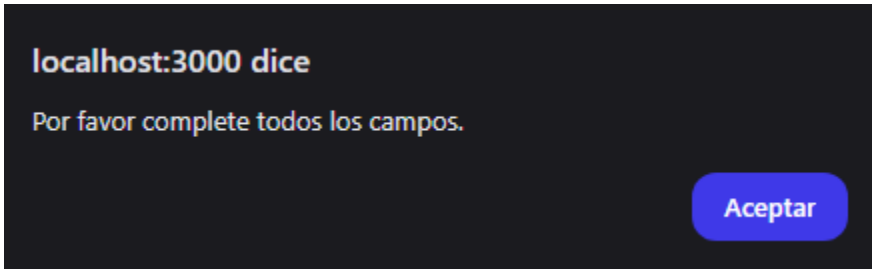


Figura 29 Validaciones Fuente: Elaboración propia

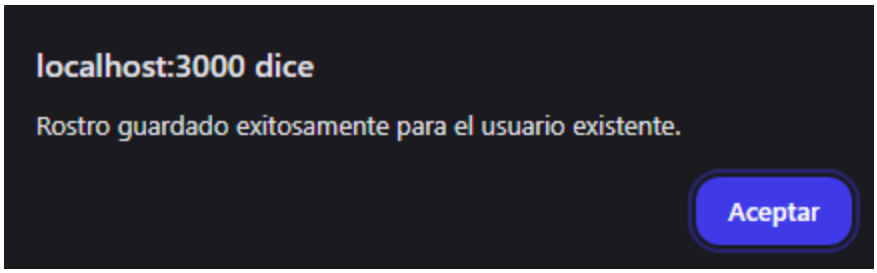


Figura 30 Validaciones Fuente: Elaboración propia

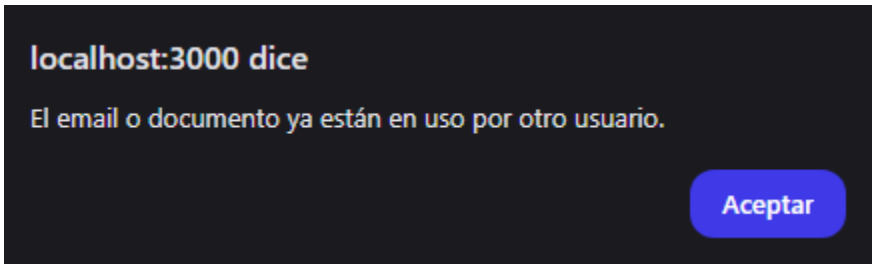


Figura 31 Validaciones Fuente: Elaboración propia

En todas las versiones del sistema han estado presentes las validaciones tal como se muestra en la Figura 28 que se usa cuando ya hay registro previo del rostro de ese usuario y se impide su registro para que no existan duplicados.

Se implementó una validación para cuando hay campos vacíos tal como se muestra en la Figura 29.

La validación de la Figura 30 hace referencia al caso en el que en la base de datos existen registrados los datos del usuario, pero en caso de requerir una nueva foto la anterior se eliminara y al guardar la nueva foto saltara el mensaje de rostro guardado exitosamente para el usuario existente.

Se implemento una validación para evitar casos en los que se dupliquen los documentos de identidad ya que el sistema mostrará un mensaje indicando que el documento de identidad ya está siendo usado por otro usuario como lo muestra la Figura 31.

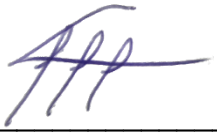
DECLARACIÓN Y AUTORIZACIÓN

Nosotros, **Sangurima Martínez**, **Joseph Andrick,** con C.C: # **0955576590 y Orellana Suarez, Hugolino** con C.C #**1207345982** autores del trabajo de Integración curricular: "**Implementación de un sistema de registro de accesos para empleados mediante reconocimiento facial con aprendizaje profundo en una bitácora digital para una empresa de seguridad."** previo a la obtención del título de **Ingeniero en Ciencias de la Computación** en la Universidad Católica de Santiago de Guayaquil.

1.- Declaramos tener pleno conocimiento de la obligación que tienen las instituciones de educación superior, de conformidad con el Artículo 144 de la Ley Orgánica de Educación Superior, de entregar a la SENESCYT en formato digital una copia del referido trabajo de Integración curricular para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.

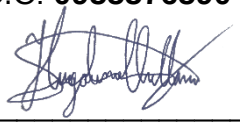
2.- Autorizamos a la SENESCYT a tener una copia del referido trabajo de Integración curricular, con el propósito de generar un repositorio que democratice la información, respetando las políticas de propiedad intelectual vigentes.

Guayaquil, 17 de febrero de 2025



_____

Nombre: **Sangurima Martínez, Joseph Andrick**
C.C: **0955576590**



_____

Nombre: **Orellana Suarez, Hugolino**
C.C: **1207345982**

REPOSITORIO NACIONAL EN CIENCIA Y TECNOLOGÍA			
FICHA DE REGISTRO DE TESIS/TRABAJO DE INTEGRACIÓN CURRICULAR			
TEMA Y SUBTEMA:	**Implementación de un sistema de registro de accesos para empleados mediante reconocimiento facial con aprendizaje profundo en una bitácora digital para una empresa de seguridad.**		
AUTORES	**Sangurima Martínez, Joseph Andrick** **Orellana Suarez, Hugolino**		
REVISOR/TUTOR	**PhD. Castro Aguilar, Gilberto Fernando**		
INSTITUCIÓN:	**Universidad Católica de Santiago de Guayaquil**		
FACULTAD:	**Ingeniería**		
CARRERA:	**Ingeniería en Ciencias de la Computación**		
TITULO OBTENIDO:	**Ingeniero en Ciencias de la Computación**		
FECHA DE PUBLICACIÓN:	17 de **febrero** de **2025**	**No. DE PÁGINAS:**	84 p.
ÁREAS TEMÁTICAS:	**Sistemas, Control de accesos, Reconocimiento facial, Inteligencia artificial**		
PALABRAS CLAVE/ KEYWORDS:	**Desarrollo de software, Base de datos, Control de accesos, Reconocimiento facial, Aprendizaje profundo**		

RESUMEN/ABSTRACT:

El presente estudio propone el desarrollo de un sistema de registro de accesos para empleados usando reconocimiento facial con aprendizaje profundo, cuyo objetivo es el reconocimiento eficiente del rostro de los empleados de la empresa de seguridad mediante algoritmos de aprendizaje profundo mejorando así el sistema de reconocimiento facial para evitar falsos positivos y falsos negativos. La investigación empleo una metodología aplicada y especifica, así como un marco SCRUM, utilizando técnicas de reconocimiento facial, redes neuronales convolucionales (CNN), algoritmos de aprendizaje profundo para para optimizar los tiempos en el proceso de entrada y salida de los empleados de la empresa. Se diseño y desarrollo un prototipo funcional que se adaptó a las mejoras que se dieron a conocer a medida que se realizaban las reuniones que se dieron tanto virtuales como presenciales, se desarrolló una serie de pruebas en entornos controlados con cada versión del sistema desde la versión 1.0 hasta la versión 4.0 para comprobar el correcto funcionamiento en cada uno de ellos de la conexión con la base de datos, la carga de los datos a la base de datos, la muestra de los datos de la persona una vez que se reconozca su rostro para indicar su entrada o salida, el reconocimiento continuo del rostro en la sección de reconocimiento facial, las validaciones pertinentes y el sistema de reconocimiento facial con aprendizaje profundo, la versión final del sistema es la versión 4.0, dicha versión se implementó de manera correcta en la empresa cumpliendo las expectativas de la empresa y funcionando de manera óptima en medida de lo solicitado.

ADJUNTO PDF:	☒ SI	☐ NO
CONTACTO CON AUTORES:	**Teléfono:** +593992426376 +593961223445	E-mail: hugolino.orellana@cu.ucsg.edu.ec joseph.sangurima@cu.ucsg.edu.ec
CONTACTO CON LA INSTITUCIÓN (C00RDINADOR DEL PROCESO UTE)::	**Toala Quimí, Edison José**	
	Teléfono: +593-990-976776	
	E-mail: edison.toala@cu.ucsg.edu.ec	

SECCIÓN PARA USO DE BIBLIOTECA	
Nº. DE REGISTRO (en base a datos):	
Nº. DE CLASIFICACIÓN:	
DIRECCIÓN URL (tesis en la web):	