UNIVERSIDAD NACIONAL DEL ALTIPLANO

FACULTAD DE INGENIERÍA MECÁNICA ELÉCTRICA ELECTRÓNICA Y SISTEMAS

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

SISTEMA INFORMÁTICO CON RECONOCIMIENTO FACIAL PARA MEJORAR EL CONTROL BIOMÉTRICO EN EL EXAMEN DE ADMISIÓN EXTRAORDINARIO DE LA UNIVERSIDAD NACIONAL DEL ALTIPLANO PUNO, 2024

TESIS

PRESENTADA POR:

ADDERLY MENDOZA NINA

PARA OPTAR EL TÍTULO PROFESIONAL DE:

INGENIERO DE SISTEMAS

PUNO – PERÚ

2024

Reporte de similitud

NOMBRE DEL TRABAJO

SISTEMA INFORMÁTICO CON RECONOCIMIENTO FACIAL PARA MEJORAR EL CONTROL BIOMÉTRICO EN EL EXAMEN DE ADM

AUTOR

ADDERLY MENDOZA NINA

RECUENTO DE PALABRAS

39447 Words

RECUENTO DE CARACTERES

234469 Characters

RECUENTO DE PÁGINAS

216 Pages

TAMAÑO DEL ARCHIVO

3.4MB

FECHA DE ENTREGA

Nov 19, 2024 8:42 PM GMT-5

FECHA DEL INFORME

Nov 19, 2024 8:47 PM GMT-5

14% de similitud general

El total combinado de todas las coincidencias, incluidas las fuentes superpuestas, para cada base de datos.

- 12% Base de datos de Internet
- 1% Base de datos de publicaciones
- Base de datos de Crossref
- Base de datos de contenido publicado de Crossref
- 10% Base de datos de trabajos entregados

Excluir del Reporte de Similitud

- Material bibliográfico
- Coincidencia baja (menos de 12 palabras)

Dr. Miguel Romilio Aceituno Rojo
INGENIERO DE SISTEMAS

Dr. Ing. Henry Iván Condori Alejo
CIP: 56684

DEDICATORIA

Dedico este trabajo de investigación a todos aquellos que han sido fundamentales en mi vida y en este proceso académico.

A Dios, por darme la fortaleza, la sabiduría y la guía para superar cada obstáculo en el camino. Tu presencia ha sido mi sostén constante.

A mi madre, Lourdes Nina, por su amor incondicional, sacrificio y por ser mi mayor fuente de inspiración. Sin tu apoyo, este logro no habría sido posible.

A mi padre, Juan Mendoza, por enseñarme los valores del esfuerzo, la perseverancia y la honestidad. Gracias por tu sabiduría y por siempre creer en mí.

A mi pareja, Liseth Ccama, por tu amor, paciencia y apoyo en cada momento, siendo mi compañera y mi fortaleza en los momentos más desafiantes.

A mi hijo, Fabio Sebastian, por ser mi mayor motivación y por darme la energía para seguir adelante con una sonrisa en el rostro.

A mis hermanos Alex y Yesenia, quienes, con su apoyo constante, su cariño y comprensión, han sido mis pilares en todo este viaje. Gracias por estar siempre a mi lado.

Este logro es tanto mío como de todos ustedes, quienes con su amor, aliento y motivación han hecho posible que alcance esta meta. Gracias, de todo corazón.

Adderly Mendoza Nina

AGRADECIMIENTOS

Quiero expresar mi más sincero agradecimiento a todas las personas que han sido fundamentales en la culminación de este proyecto de investigación. En primer lugar, a mi Escuela Profesional de Ingeniería de Sistemas, por brindarme la formación integral que me permitió alcanzar este logro.

Mi más profundo agradecimiento a mis asesores, quienes han sido pilares clave en mi desarrollo académico: a la Dra. Zulema Lilian Mamani Huacani, por su guía experta y valiosas sugerencias; al Mg. Aldo Hernán Zanabria Gálvez, por su apoyo constante y recomendaciones oportunas; al Mtr. Víctor Hugo Bejar Gonzales, por su colaboración y conocimientos; y, especialmente, al Dr. Miguel Romilio Aceituno Rojo, por su paciencia, dedicación y orientación constante.

Agradezco también al Dr. Juan Carlos Benavides Huanca por permitirme realizar mi investigación en la Dirección de Admisión y facilitarme los recursos necesarios. A los trabajadores de la Dirección de Admisión, por su apoyo incondicional, por estar siempre dispuestos a colaborar y por ser no solo colegas, sino grandes amigos. Su compañía y ayuda constante han sido fundamentales para que este proyecto avanzara con éxito.

Un agradecimiento muy especial al Dr. Edgar Holguín Holguín, quien fue la primera persona en creer en mi capacidad para realizar este proyecto. Su confianza en mí desde el principio no solo fue una fuente de motivación y fortaleza, sino que además, me brindó una guía invaluable en el desarrollo del sistema. Su apoyo y asesoramiento fueron esenciales para que pudiera llevar a cabo este desafío con éxito.

Finalmente, a todos aquellos que me han acompañado en este camino, gracias por su apoyo, paciencia y aliento. Este logro es tanto mío como de ustedes.

Adderly Mendoza Nina

ÍNDICE GENERAL

Pág.

CAPÍTULO III

MATERIALES Y MÉTODOS

Área: Inteligencia Artificial y Sistemas Bio-Inspirados

Tema: Reconocimiento Facial

FECHA DE SUSTENTACIÓN: 03 de diciembre de 2024

ÍNDICE DE TABLAS

Pág.

ÍNDICE DE FIGURAS

Pág.

ÍNDICE DE ANEXOS

Pág.

RESUMEN

La presente investigación se enfoca en los desafíos del control biométrico durante el proceso de admisión extraordinario de la Universidad Nacional del Altiplano, abarcando aspectos críticos como la precisión en la identificación, el tiempo de respuesta y la seguridad del sistema. Un control ineficaz en la identificación puede dar lugar a problemas de suplantación de identidad, mientras que una respuesta lenta puede ocasionar malestar entre los postulantes, lo que subraya la importancia de implementar herramientas tecnológicas precisas, ágiles y seguras que optimicen esta tarea. El objetivo principal de esta investigación fue mejorar el control biométrico mediante la implementación de un sistema con reconocimiento facial. El desarrollo del sistema se llevó a cabo utilizando la metodología *Extreme Programming* (XP), bajo un enfoque aplicado y cuantitativo, con un diseño cuasiexperimental de corte transversal. Se empleó un muestreo de tipo no probabilístico por conveniencia que abarcó a 100 postulantes. Los resultados obtenidos evidenciaron una mejora significativa en la precisión de identificación, incrementándola del 84% al 93%, y reduciendo el tiempo promedio de reconocimiento de 10 segundos a tan solo 2 segundos. Asimismo, el sistema desarrollado cumple con los estándares de seguridad establecidos, garantizando un proceso de identificación robusto y confiable. En conclusión, la implementación del sistema de reconocimiento facial para el control biométrico en el proceso de admisión ha demostrado ser una solución eficaz, contribuyendo de manera sustancial a mejorar la precisión, tiempo de control y la seguridad del proceso, reforzando así su aplicabilidad en entornos académicos que demandan un control riguroso y eficiente.

Palabras clave: Control biométrico, Proceso de admisión, Reconocimiento facial, Seguridad en exámenes.

ABSTRACT

This research focuses on the challenges of biometric control during the extraordinary admission process at the National University of the Altiplano, addressing critical aspects such as identification accuracy, response time, and system security. Ineffective identification control can lead to issues such as identity fraud, while slow response times may cause discomfort among applicants, emphasizing the importance of implementing precise, agile, and secure technological tools to optimize this task. The primary objective of this research was to improve biometric control through the implementation of a facial recognition system. The system was developed using the Extreme Programming (XP) methodology, adopting an applied and quantitative approach with a quasi-experimental cross-sectional design. A non-probabilistic convenience sampling method was employed, covering 100 applicants. The results showed a significant improvement in identification accuracy, increasing from 84% to 93%, and reducing the average recognition time from 10 seconds to just 2 seconds. Additionally, the developed system meets established security standards, ensuring a robust and reliable identification process. In conclusion, the implementation of the facial recognition system for biometric control in the admission process has proven to be an effective solution, substantially contributing to the improvement of accuracy, control time, and security, thus reinforcing its applicability in academic environments that demand rigorous and efficient control.

Keywords: Admission process, Biometric control, Exam security, Facial recognition.

CAPÍTULO I

INTRODUCCIÓN

1.1. PLANTEAMIENTO DEL PROBLEMA

En los últimos años, la tecnología se ha vuelto esencial para todas las empresas al facilitar la automatización de procesos clave (Aquijes & Ampuero, 2021). La seguridad y el control de acceso, tanto en entornos públicos como privados, son de vital importancia para prevenir robos de información y la suplantación de identidad. En este sentido, el reconocimiento facial como forma de control biométrico desempeña un papel fundamental en mejorar esta área crítica.

El control biométrico es un sistema de seguridad que utiliza características físicas o comportamentales únicas de una persona para autenticar su identidad (Castro, 2018). Sin embargo, un control biométrico deficiente puede presentar lentitud en el proceso de autenticación. Cuando el sistema tarda demasiado en verificar la identidad de una persona, puede ocasionar molestias y frustraciones en los usuarios. Es esencial que los sistemas biométricos sean rápidos y eficientes para garantizar una experiencia fluida y satisfactoria para los usuarios.

Una de las herramientas mejor valoradas en cuanto a control biométrico es el reconocimiento facial (Vera, 2015). A diferencia de otros métodos de autenticación, como tarjetas de identificación o contraseñas, el control facial permite el acceso sin contacto físico, lo que es especialmente relevante en el contexto actual.

A nivel global, se ha mostrado un considerable interés en el desarrollo de la tecnología de reconocimiento facial. La reciente implementación de esta tecnología por parte de la Patrulla Fronteriza permitió la captura de un impostor en el puerto fronterizo

de San Luis. Un hombre de 30 años proveniente de México intentó ingresar a Estados Unidos con una tarjeta de cruce fronterizo falsificada, pero fue identificado rápidamente gracias al sistema biométrico. El hombre fue arrestado y enfrenta cargos penales, lo que subraya la eficacia de esta tecnología en la detección de infractores (Tapia, 2024).

La república en una pasada publicación menciona que “En el examen de admisión de la Universidad Nacional de Trujillo detuvieron a un suplantador, quien iba a postular a la carrera de Medicina, los agentes detectaron que el supuesto postulante tenía adherido al índice derecho una capa de polímero simulando una huella digital” (LaRepública, 2021)

Por su parte, en una pasada publicación del diario voces nos dice que “En la Universidad Nacional de San Martín lograron detectar tres casos de suplantaciones de identidad, donde los suplantadores eran procedentes de la costa del país” (Voces, 2023), también nos menciona que en la ciudad de Arequipa siete jóvenes fueron detenidos durante el examen de admisión de la Universidad Nacional San Agustín, se menciona que la banda criminal cobraba hasta diez mil soles para suplantar a un postulante

La Universidad de Puno no fue la excepción. En marzo de 2023, una de las noticias más destacadas informaba que esta institución había identificado a cinco ciudadanos limeños que intentaban suplantar la identidad de postulantes para rendir el examen de admisión (Panamericana, 2023).

Otro de los principales problemas que enfrenta la universidad durante los procesos de admisión es el tiempo que toma realizar el control biométrico. Según una encuesta realizada a los responsables de esta tarea, algunos postulantes se han quejado de la demora en cada control. Además, factores como el sudor o dedos lastimados pueden dificultar un reconocimiento adecuado. De acuerdo con el informe del Ministerio de Trabajo y

Promoción del Empleo (2022), la principal actividad económica en Puno es la agricultura. Asimismo, el Gobierno Regional de Puno (2023), en su boletín económico laboral, informa que "la población joven en edad de trabajar en el departamento de Puno ascendió a 413,399 personas". A partir de estos datos, se puede inferir que una gran parte de la población joven está empleada en actividades físicas, lo que podría provocar desgaste o daño en las huellas dactilares, dificultando el reconocimiento biométrico a través de estas.

Como se evidencia en los casos presentados, el sistema de reconocimiento facial permite controlar el acceso de personas no autorizadas o indeseadas, monitoreando de forma continua y eficaz (Yañez, 2019) evitando así que las irregularidades se conviertan en problemas mayores.

1.2. FORMULACIÓN DEL PROBLEMA

1.2.1. Problema general

¿Es posible mejorar el control biométrico en el examen de admisión extraordinario de la Universidad Nacional del Altiplano mediante un sistema informático con reconocimiento facial?

1.2.2. Problemas específicos

- ¿Cuál es la precisión del sistema informático con reconocimiento facial en el control biométrico de los postulantes al examen de admisión extraordinario de la Universidad Nacional del Altiplano?
- ¿Qué tiempo de respuesta tiene el sistema informático con reconocimiento facial en el control biométrico de los postulantes al examen de admisión extraordinario de la Universidad Nacional del Altiplano?

- ¿Cuál es el nivel de seguridad del sistema informático con reconocimiento facial en el control biométrico de los postulantes al examen de admisión extraordinario de la Universidad Nacional del Altiplano?

1.3. HIPÓTESIS DE LA INVESTIGACIÓN

1.3.1. Hipótesis general

El sistema informático con reconocimiento facial incidirá positivamente en el control biométrico del examen extraordinario de la Universidad Nacional del Altiplano Puno en el año 2024.

1.3.2. Hipótesis específicas

- La precisión del sistema informático con reconocimiento facial es mayor que la de los métodos tradicionales en el control biométrico de los postulantes.
- El tiempo de respuesta del sistema informático con reconocimiento facial es menor que el de los métodos tradicionales en el control biométrico de los postulantes.
- El nivel de seguridad del sistema informático con reconocimiento facial es mayor que el de los sistemas tradicionales en el control biométrico de los postulantes.

1.4. JUSTIFICACIÓN DE LA INVESTIGACIÓN

La Universidad Nacional del Altiplano de Puno enfrenta el desafío persistente de garantizar la integridad y la equidad en sus procesos de admisión. En un examen pasado se descubrió la presencia de estudiantes suplantadores que viajaban desde otras ciudades del Perú, así como un caso de suplantación por parte de un estudiante matriculado en la

Universidad Nacional del Altiplano Puno. Estos incidentes resaltan la urgente necesidad de implementar medidas más efectivas para combatir la suplantación de identidad y fortalecer la seguridad en los exámenes de admisión.

Además, se ha observado que el proceso actual de control biométrico con huellas dactilares, utilizado en esta casa superior de estudios presenta ciertas limitaciones, por un lado, el tiempo necesario para realizar este control puede resultar excesivo, lo que genera molestias entre los postulantes y afecta su capacidad para desarrollar el examen de manera óptima. También, existe la preocupación acerca de la seguridad del sistema biométrico actual por medio de las huellas dactilares, con el avance de la tecnología se puede llegar a burlar este medio de control, como nos lo menciona el diario la república “Las autoridades de la Universidad Nacional de Trujillo descubrieron que un postulante llevaba un recubrimiento de plástico en el dedo índice derecho”

En respuesta a estos desafíos, se propone el desarrollo de un sistema informático con reconocimiento facial como una solución innovadora y efectiva para mejorar el control biométrico de los postulantes al examen de admisión extraordinario de la Universidad Nacional del Altiplano Puno en el año 2024. Este sistema utilizó tecnología biométrica avanzada para verificar la identidad de los postulantes en tiempo real, reduciendo significativamente el tiempo necesario para el control y mejorando la seguridad del proceso. Según (Cristián Bravo et al., 2018) el reconocimiento facial está siendo cada vez más adoptado y aceptado por la sociedad debido a su uso para mejorar la seguridad, como señala (Pérez, 2021) que el reconocimiento facial tiene una significativa utilización en el ámbito de la seguridad, tanto en lo privado como en lo público. Esto resalta la utilidad significativa de esta tecnología como medida de seguridad, dada su capacidad para manejar diversas vulnerabilidades y ofrecer soluciones.

La implementación de este sistema no solo abordará los desafíos actuales relacionados con la suplantación de identidad y los inconvenientes asociados al control biométrico con huellas dactilares, sino que también sentará las bases para futuras mejoras en los procesos de admisión. Además, proporciona una capa adicional de seguridad y confianza tanto para los postulantes como para la institución, promoviendo así la equidad y la transparencia en el acceso a la educación superior.

Desde el punto de vista teórico, se fundamenta en sólidos principios teóricos de tecnologías con reconocimiento facial e identificación. Al explorar las teorías detrás de las mencionadas tecnologías, se busca comprender en profundidad cómo estas herramientas pueden aplicarse de manera efectiva en universidades. Además, el análisis de teorías y modelos existentes en identificación respalda la necesidad de innovación y mejora en el control biométrico, proporcionando una buena base conceptual para la implementación del sistema.

Desde el punto de vista práctico, la viabilidad y beneficios del sistema se evidencian en los diferentes casos de estudio y ejemplos prácticos de instituciones que han implementado soluciones similares, como nos dice (UPC, 2019) “El sistema con reconocimiento facial ha sido implementado con éxito durante el mes de noviembre en los exámenes de inglés”, donde se destaca como el reconocimiento facial ha mejorado significativamente la eficiencia y la seguridad en situaciones de identificación.

Desde el punto de vista metodológico, este trabajo se enfocará en la creación de un sistema de reconocimiento facial para mejorar el control biométrico de los postulantes a la Universidad Nacional del Altiplano Puno. La implementación de este sistema se propone como una medida eficiente para reducir los riesgos de seguridad actuales,

especialmente el riesgo de suplantación de identidad, y también para disminuir el tiempo que toma el control biométrico actual.

1.5. OBJETIVOS DE LA INVESTIGACIÓN

1.5.1. Objetivo general

Desarrollar un sistema informático con reconocimiento facial para mejorar el control biométrico en el examen de admisión extraordinario de la Universidad Nacional del Altiplano en el año 2024.

1.5.2. Objetivos específicos

- Calcular la precisión del sistema informático con reconocimiento facial en el control biométrico del examen extraordinario de la Universidad Nacional del Altiplano Puno en el año 2024.
- Medir el tiempo de respuesta del sistema informático con reconocimiento facial en el control biométrico del examen extraordinario de la Universidad Nacional del Altiplano Puno en el año 2024.
- Evaluar el nivel de seguridad del sistema informático con reconocimiento facial en el control biométrico del examen extraordinario de la Universidad Nacional del Altiplano Puno en el año 2024.

CAPÍTULO II

REVISIÓN DE LITERATURA

2.1. ANTECEDENTES DE LA INVESTIGACIÓN

A continuación, se presenta la revisión de la literatura, entre ellos diversas tesis y artículos científicos publicados en el ámbito internacional y local sobre la aplicación de sistemas con reconocimiento facial y control biométrico.

2.1.1. Antecedentes internacionales

(Jiménez, 2020) aborda el reconocimiento facial como una tecnología comúnmente utilizada en sistemas de seguridad para identificar personas, dividiéndose en dos componentes: identificación y verificación. La identificación se centra en detectar características faciales distintivas, mientras que la verificación compara estas imágenes con las almacenadas en una base de datos mediante algoritmos matemáticos. El proyecto que presenta busca mejorar la seguridad de los automóviles, identificando a los usuarios autorizados y enviando alertas al propietario en caso de detectar a una persona no reconocida, junto con fotografías y la ubicación del vehículo. Utilizando Python y el algoritmo Eigenfaces, complementado por Análisis de Componentes Principales y Histogramas de Patrones Locales Binarios, el sistema se implementa en una Raspberry Pi 3 B® y se evalúa mediante métricas de la matriz de confusión para garantizar su precisión y eficiencia.

(Pico & Cordero, 2019) destacan en su proyecto que la tecnología juega un papel crucial en la mejora y optimización de los recursos disponibles, proponiendo la adopción de un sistema de voto electrónico en la Universidad

Estatal de Milagro (UNEMI) como una alternativa a los métodos de votación convencionales. Esta transformación podría tener un efecto beneficioso en la comunidad estudiantil al simplificar el proceso electoral y proporcionar la consistencia y fiabilidad que los votantes requieren. La propuesta busca diseñar un modelo que sistematice los procesos electorales en la UNEMI, asegurando tanto la accesibilidad como la confianza en los resultados. Para lograrlo, se examinó el estado actual del sistema de votación y se evaluó la confiabilidad que un nuevo enfoque podría ofrecer a través de la incorporación de tecnologías, incluida la tecnología de reconocimiento facial como medida de seguridad. Mediante un análisis de la literatura sobre sistemas biométricos, se exploraron sus características, ventajas y desventajas, concluyendo que el reconocimiento facial es la técnica más adecuada por su alta confiabilidad, bajo impacto ambiental, facilidad de uso y por no restringir físicamente el acceso de los usuarios autorizados.

En su investigación, (Guzmán, 2023) abordó un problema presentado por *Prey Incorporated*, una empresa de seguridad digital que permite marcar dispositivos perdidos y generar reportes periódicos con fotos del entorno del dispositivo. Estos reportes, a veces de baja calidad, obligan a los administradores a revisar manualmente grandes cantidades de imágenes para identificar a quienes tienen el dispositivo. La investigación evaluó modelos de redes neuronales capaces de analizar rostros y generar representaciones vectoriales, con el fin de desarrollar un panel de control que agrupe a los individuos presentes en los reportes, lo que agiliza significativamente el proceso de revisión. Se construyó una base de datos con miles de imágenes y se probaron seis modelos de reconocimiento facial, incluyendo un ajuste fino del modelo ArcFace, con un

balance entre errores de duplicación y ocultación de individuos. El modelo resultante alcanzó una precisión de 0.77, un recall de 0.89 y un accuracy de 0.72, demostrando que puede mejorar notablemente la usabilidad y eficiencia de la herramienta, facilitando la revisión de los reportes de manera más rápida y efectiva.

Camara (2021) realizó un estudio exploratorio sobre la regulación del reconocimiento facial en Brasil y Portugal, enfocado en su uso para fines de seguridad y privacidad. El objetivo del estudio fue evaluar el grado de madurez de los marcos legales en ambos países, tomando en cuenta que el reconocimiento facial implica el tratamiento de datos biométricos, los cuales suelen estar prohibidos o sujetos a condiciones legales específicas. La metodología utilizada fue un análisis comparativo de los ordenamientos jurídicos de Brasil y Portugal, destacando instrumentos legales relevantes. Aunque no se incluyó una población específica, se revisaron leyes y políticas públicas relacionadas con el tema. Los resultados mostraron que el uso del reconocimiento facial está extendido en varios sectores, especialmente en seguridad, pero plantea riesgos significativos para los derechos fundamentales. Se concluyó que Portugal tiene un marco legal más avanzado que Brasil, gracias a la implementación de la Directiva (UE) N° 2016/680 y la intervención de la Comisión Nacional de Protección de Datos (CNPD), que regula el uso de datos biométricos en seguridad.

(Bravo et al., 2018) llevaron a cabo una investigación con el objetivo de analizar cómo los ciudadanos aceptan la tecnología de reconocimiento facial como medida de seguridad. El estudio se basa en el índice de predisposición tecnológica (TRI) y el modelo de aceptación de tecnologías (TAM). Utilizando un modelo de investigación, los autores aplicaron una encuesta a 220 personas en Chile y

analizaron los datos mediante la técnica de mínimos cuadrados parciales. Los resultados mostraron que la utilidad percibida del reconocimiento facial como medida de seguridad está explicada en un 50% por factores como las normas sociales y la percepción de responsabilidad.

(Domingo, 2021) en su investigación abordó el reconocimiento facial como una herramienta de seguridad en espacios públicos y sus implicaciones para la privacidad individual. El objetivo fue analizar la efectividad de esta tecnología en la detección rápida de personas y evaluar el impacto que su uso tiene en la privacidad. A través de una metodología cualitativa, basada en la revisión de estudios sobre tecnologías biométricas, se exploraron los beneficios y riesgos del reconocimiento facial en estos contextos. Aunque el estudio no contó con una muestra específica, se discutieron los casos de implementación en lugares públicos. Los resultados indicaron que, aunque el reconocimiento facial es eficaz para identificar personas en grandes multitudes, su uso sin restricciones puede comprometer la privacidad. En conclusión, el estudio resaltó la necesidad de establecer una legislación que regule claramente el uso de esta tecnología para equilibrar la seguridad con la protección de los derechos individuales.

(Bastos & Esteves, 2021) se centraron en los riesgos sociales derivados del uso del reconocimiento facial en sistemas de vigilancia digital. El objetivo de su investigación fue examinar cómo la tecnología de reconocimiento facial ha transformado los mecanismos de vigilancia y los peligros que esto implica para la privacidad. Utilizando un enfoque teórico-descriptivo y cualitativo, apoyado en la investigación documental indirecta, los autores analizaron estudios previos y marcos comparativos. Aunque no trabajaron con una población específica, se enfocaron en la literatura académica existente sobre el uso de esta tecnología. Los

resultados revelaron que la modernización tecnológica ha permitido un incremento en la discreción de los sistemas de vigilancia, lo que exacerba las preocupaciones sobre la privacidad y la seguridad individual. Como conclusión, los autores señalaron la necesidad de una evaluación crítica y regulaciones más estrictas para mitigar los riesgos asociados con el uso indiscriminado de estas tecnologías.

Paulo Menino (2022) investigó los métodos de detección y reconocimiento facial, enfocándose en los algoritmos más efectivos y en la aplicación de la tecnología en imágenes térmicas y visibles. El objetivo de su investigación fue comparar la precisión de diferentes algoritmos de reconocimiento facial y evaluar su desempeño en condiciones adversas. Utilizando datos proporcionados por la Universidad de Aveiro, Menino realizó un análisis comparativo de redes neuronales convolucionales profundas y métodos tradicionales. Aunque no se especifica una población humana, se trabajó con un conjunto de datos de imágenes faciales. Los resultados mostraron que los algoritmos basados en redes neuronales ofrecen una mayor precisión en comparación con los enfoques convencionales, especialmente en imágenes térmicas, donde se logró una mejora del 30%. En conclusión, Menino destacó que las técnicas avanzadas en redes neuronales tienen un gran potencial para mejorar la detección facial en condiciones complejas, abriendo nuevas posibilidades para el uso del reconocimiento facial en diversos contextos.

En su proyecto de investigación (Orea, 2023) desarrolló un sistema de control de acceso para instituciones de nivel medio superior y superior, utilizando la detección de rostros a través de un algoritmo propietario integrado en cámaras de la marca Hikvision. Estas cámaras capturan y comparan los rostros previamente

autorizados en su biblioteca para generar reportes de asistencia. Para obtener los datos de las cámaras, fue necesario gestionar el acceso al API de Hikvision bajo un contrato de confidencialidad, lo que permitió el manejo de los metadatos mediante Python y almacenar los eventos válidos en una base de datos. La implementación logró tiempos óptimos de sincronización de aproximadamente 5 segundos, lo que garantiza un proceso eficiente y seguro. Además, el sistema notifica a los padres, tutores o personal encargado cuando el alumno es detectado en la institución, con un tiempo de respuesta de 1 segundo. Esto permite un sistema completo de registro y notificación en aproximadamente 6 segundos. La aplicación también permite a los usuarios gestionar la información y visualizar reportes en tiempo real sobre la asistencia de los alumnos, mejorando el control y el seguimiento de su presencia. Esto optimiza la gestión de asistencia y proporciona un entorno seguro, evitando demoras y permitiendo análisis detallados del tiempo de estancia de los estudiantes.

(Melo et al., 2021) desarrollaron un proyecto que implementó un sistema de reconocimiento facial para mejorar la seguridad en el control de acceso de instalaciones judiciales. El objetivo del proyecto fue aumentar la seguridad en el Tribunal de Justicia del Distrito Federal y Territorios mediante el uso de la tecnología AMON, integrada con el software SidenWeb para el control de acceso. El sistema se aplicó en la jurisdicción del tribunal, donde se empleó para verificar las identidades de los visitantes. Los resultados indicaron que la integración del reconocimiento facial mejoró significativamente el control de seguridad en el tribunal, permitiendo una verificación eficiente y añadiendo una capa adicional de protección a las instalaciones. En conclusión, el proyecto demostró que AMON

es una herramienta efectiva para mejorar la seguridad institucional, reforzando el control de acceso y mejorando la seguridad general de las instalaciones.

2.1.2. Antecedentes nacionales

(Alejo, 2021) en su investigación llevó a cabo el análisis, diseño e implementación de un algoritmo de reconocimiento facial enfocado en la gestión del control de acceso para la empresa Altoque PS S.A., la cual se especializa en servicios de *delivery*. Este estudio es de carácter aplicado, ya que busca resolver un problema específico. El objetivo principal del proyecto es evaluar el impacto de un algoritmo de reconocimiento facial en la gestión del control de acceso de la empresa. Entre los objetivos secundarios se encuentran analizar en qué medida se disminuyeron los accesos no autorizados y cómo se redujo el tiempo promedio de verificación de acceso en la organización. Para el desarrollo del sistema, se empleó la metodología XP, que se caracteriza por fomentar una comunicación constante y retroalimentación, permitiendo ajustar el producto según los requisitos del cliente. Además, esta metodología es flexible ante los cambios, facilitando respuestas rápidas frente a cualquier eventualidad. En la fase de desarrollo del software, se utilizó un lenguaje de programación específico.

(Manuel et al., 2023) llevaron a cabo un estudio cuyo objetivo general fue desarrollar un sistema de control de acceso mediante reconocimiento facial utilizando Inteligencia Artificial. Para lograr esto, se implementaron Redes Neuronales Convolucionales (CNN) como algoritmo principal, utilizando el lenguaje de programación Python y diversas librerías como OpenCV, Imutils, Numpy y Os. La metodología se centró en la creación de un sistema capaz de identificar a personas mediante el análisis de imágenes faciales. Los resultados del

estudio fueron evaluados utilizando un dataset de 450 fotos por individuo, alcanzando un 88% de precisión. Esto sugiere que el sistema basado en tecnología de reconocimiento facial es eficaz, destacando su eficiencia al aumentar el tamaño de los conjuntos de datos. Los autores concluyen que el sistema propuesto tiene gran potencial y efectividad en el ámbito del control de acceso.

(Muñoz, 2022) llevaron a cabo un proyecto de investigación cuyo propósito fue identificar el algoritmo de reconocimiento facial más efectivo para la identificación de personas en una institución educativa de Pasco en el año 2021. La investigación se desarrolló bajo un enfoque experimental, utilizando una muestra no probabilística e intencionada compuesta por 310 imágenes de 10 estudiantes de la Facultad de Ingeniería de la UNDAC. Los algoritmos evaluados fueron Eigenface, Fisherface y Local Binary Pattern (LBP), analizados a través de las métricas de exactitud y precisión propias del aprendizaje automático. El experimento incluyó tres escenarios de entrenamiento con distintas cantidades de imágenes, seguido de la prueba de cada modelo con imágenes de los estudiantes. Los resultados mostraron que el algoritmo LBP fue el más eficiente, logrando un 94.37% en la métrica de exactitud. En cuanto a la precisión, LBP también obtuvo el valor más alto, con un 97.83%, seguido por el algoritmo Fisherface. Esto sugiere que LBP es el algoritmo más efectivo para la identificación precisa de personas en este contexto.

(Asana, 2022) en su proyecto de investigación, se propuso desarrollar un sistema de control de acceso mediante reconocimiento facial en la I.E. 81585 Sagrado Corazón de Jesús, en Cartavio, La Libertad. El estudio tuvo como objetivo principal implementar un sistema tecnológico para mejorar la seguridad en la institución educativa. La investigación fue de tipo aplicada con diseño

correlacional, utilizando como muestra los estudiantes durante el segundo y tercer bimestre del año 2022. La conclusión principal del estudio fue que el sistema de reconocimiento facial propuesto es adecuado para su implementación, brindando importantes beneficios en términos de seguridad y control de acceso en la institución, mejorando así el bienestar de los estudiantes y el personal administrativo.

(Aguirre, 2021) desarrolló una tesis con el objetivo de crear un arquetipo basado en un modelo de visión computacional para optimizar el control de acceso en una empresa privada. En su investigación, se aplicó la metodología de *Design Thinking*, abordando las cinco fases principales del proceso: empatizar, definir, idear, prototipar y testear. La implementación del sistema logró mejorar la automatización y eficacia del control de acceso en la empresa, y se destacó su capacidad de escalar a medida que crece el número de usuarios. Los resultados indicaron que el sistema propuesto es exitoso en la identificación de personas, proporcionando una solución eficiente y escalable para el control de acceso en el entorno empresarial. Como conclusión, Aguirre resalta la efectividad del sistema en la mejora de la seguridad y eficiencia operativa.

Aquijes Ronny y Ampuero Lizardo (2021) en la empresa Guimartbot S.A.C., el objetivo fue fortalecer la seguridad interna mediante la implementación de un sistema de reconocimiento facial para el acceso del personal. Se evaluó el sistema en una muestra de 20 personas, observando una significativa reducción en los intentos de acceso no autorizado. La metodología empleada incluyó diversas técnicas de extracción de características faciales, logrando una identificación precisa de los empleados. Los resultados mostraron que el sistema mejoró la precisión del control de acceso en un 18%, elevando el porcentaje de acceso

autorizado del 79% al 97%. Estos hallazgos destacan el impacto positivo del sistema en la seguridad y eficiencia operativa de la empresa, cumpliendo satisfactoriamente con los objetivos propuestos.

En la Universidad Continental (Galindo et al., 2021) investigaron el problema de la suplantación de identidad durante los exámenes finales, desarrollando un sistema de escritorio para reconocimiento facial basado en la metodología Kanban. Utilizando Trello como herramienta de gestión de actividades, los investigadores recolectaron datos mediante encuestas dirigidas a estudiantes y docentes, y realizaron pruebas con una muestra de cinco estudiantes. Cada estudiante fue fotografiado en 50 imágenes bajo diferentes condiciones (con mascarilla, sin mascarilla, y con un uso incorrecto de la mascarilla). Para el reconocimiento facial, utilizaron la librería Face Recognition y evaluaron el sistema mediante una matriz de confusión. Los resultados indicaron una precisión del 93% en el reconocimiento facial, concluyendo que el sistema es altamente preciso y eficaz para abordar la problemática de la suplantación de identidad en los exámenes finales, mejorando así la seguridad académica.

Yañez Neyra (2019), en su investigación, buscó analizar el impacto de un sistema de reconocimiento facial en el control de acceso de los estudiantes a los laboratorios de la FIIS-UNAC. El estudio, de tipo aplicado y con un diseño experimental pre-experimental, se desarrolló utilizando la metodología RUP (Proceso Unificado Racional), implementando la herramienta Rational Rose para la construcción del sistema. La muestra estuvo compuesta por 75 estudiantes de la facultad. Los resultados indicaron que la implementación del sistema contribuyó significativamente a mejorar el control de acceso a los laboratorios, incrementando la seguridad y optimizando la gestión del acceso de los alumnos.

El estudio concluyó que el sistema basado en reconocimiento facial es eficaz en este tipo de entorno educativo, ofreciendo mejoras notables en la gestión de acceso.

(Chirinos & Calero, 2021) investigaron la efectividad de tres modelos de redes neuronales convolucionales en la detección de personas que usan mascarillas de manera correcta o incorrecta, o que no las utilizan. Para su estudio, adquirieron un total de 2923 imágenes y las clasificaron en tres categorías: "Con Mascarilla", "Sin Mascarilla" y "Mal Uso". Entrenaron tres modelos de redes neuronales convolucionales, variando el número de capas en cada una, desde tres hasta siete capas. Los resultados del análisis comparativo mostraron que la red de siete capas ofreció el mejor desempeño, con una precisión del 99%. El sistema fue implementado utilizando App Designer de Matlab, simulando su uso en el control de acceso a un laboratorio universitario, demostrando un correcto funcionamiento y efectividad en la detección del uso adecuado de mascarillas. Este estudio concluyó que el sistema es altamente preciso para el control de acceso y protección sanitaria.

2.1.3. Antecedentes locales

El objetivo de la investigación realizada por (Calizaya & Calsin, 2022) fue determinar el modelo más eficiente para la detección de anomalías en videos de exámenes en línea a través del uso de inteligencia artificial. La metodología empleada se basó en la extracción de características de movimiento de una muestra de 248 videos, a partir de la cual se generó un vector de características que sirvió como entrada para el desarrollo y evaluación de tres modelos: Isolation Forest, LSTM-Autoencoder y Autoencoders. La población y muestra del estudio

se centraron en los mencionados 248 videos, que fueron seleccionados para representar un amplio espectro de comportamientos en exámenes en línea. Los resultados demostraron que el modelo Autoencoders fue el más preciso, con una tasa de acierto (accuracy) del 80.08% y una precisión del 98.00%, superando a los otros dos modelos evaluados. La investigación concluyó que la implementación de este modelo contribuiría de manera significativa a la reducción de actos ilícitos en exámenes en línea, proporcionando una herramienta eficaz para mejorar la integridad y calidad de la educación virtual.

(Mamani & Canahuire, 2022) llevaron a cabo un proyecto de tesis cuyo objetivo principal fue desarrollar un prototipo de software basado en tecnología biométrica de reconocimiento facial para el control de acceso en el Colegio Aplicación de la Universidad Nacional del Altiplano. La metodología aplicada fue experimental, y la investigación se clasificó como aplicativa. La población y muestra incluyeron participantes que utilizaron el sistema para acceder a las instalaciones de la institución. Los resultados del estudio demostraron que el prototipo no solo facilitó, sino también agilizó significativamente el proceso de ingreso de los participantes, registrando un tiempo promedio de 88.60 segundos en condiciones reconocidas para el registro número 13, y 5.50 segundos en el primer reconocimiento, lo que evidencia su eficiencia. Como conclusión, se estableció que el sistema de reconocimiento facial cumplió de manera efectiva con el control de acceso, enviando y gestionando de manera precisa la información de los participantes en una base de datos, contribuyendo así a mejorar los procesos de seguridad en la institución.

2.2. MARCO TEÓRICO

2.2.1. Biometría

2.2.1.1. Definición de biometría

La biometría (López, 2023) define como una ciencia que se enfoca en analizar las distancias y posiciones entre las partes del cuerpo para identificar a una persona en relación con el resto de la población. Los rasgos biométricos combinan la anatomía y el comportamiento humano, resultando en características similares entre parientes cercanos. Estos rasgos son esenciales para la identificación de personas, ya que no se pueden compartir ni extraviar, lo que hace que los sistemas de identificación sean más cómodos y seguros.

(Vázquez, 2014) define la biometría como "la ciencia que establece la identidad de un individuo a partir del análisis de las características fisiológicas o del comportamiento del cuerpo humano".

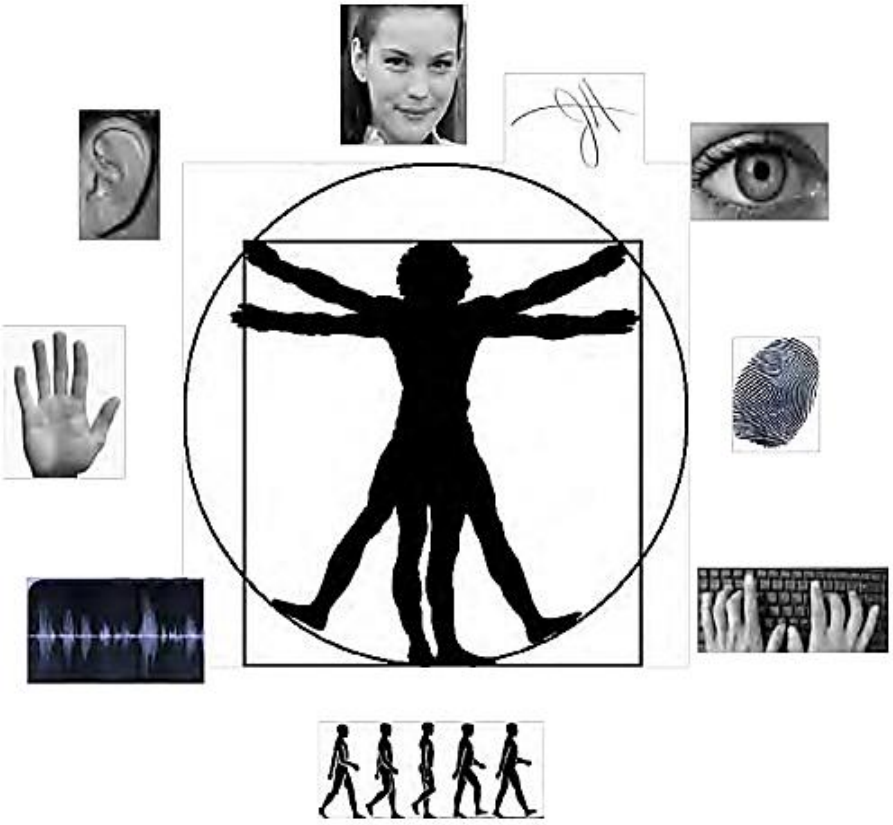
2.2.2. Control Biométrico

2.2.2.1. Definición de control biométrico

Un control biométrico es un método que puede evaluar una o varias características físicas o de comportamiento, como la huella digital, la retina, el rostro, el iris, la oreja, la voz, la firma, el olor, la vena de la mano o la información del ADN de una persona, con el propósito de confirmar su identidad (Piedra, 2019) como se puede apreciar en la siguiente figura.

Figura 1

Biometría de una persona



Fuente**:** (Vázquez, 2014)

Según (Vázquez, 2014) nos dice que un control biométrico tiene como objetivo la identificación o verificación automática de la identidad de un individuo mediante el análisis de uno o más atributos físicos o conductuales del cuerpo humano. Cada individuo registrado en este sistema es referido como usuario. Los sistemas de reconocimiento de personas se fundamentan en tres principios primarios: 1) lo que el individuo conoce, 2) lo que el individuo posee, y 3) la autenticidad del individuo. Los primeros dos principios son denominados enfoques convencionales, mientras que el tercero se relaciona con los sistemas biométricos.

El control biométrico utiliza métodos estadísticos y matemáticos aplicados a características conductuales y físicas del individuo para llevar a cabo la autenticación mediante medios electrónicos. Para realizar esta autenticación, primero es necesario almacenar los datos de las características físicas y patrones del individuo, de modo que puedan ser comparados en el dispositivo de lectura biométrica (Sullo, 2021).

(Parrales, 2024) nos dice que es importante tener en cuenta que los controles biométricos deben utilizarse con precaución y respetando la privacidad de los empleados, es importante que se cumplan las normativas de protección de datos y que se informe adecuadamente a los trabajadores sobre la recopilación y uso de sus datos biométricos.

2.2.2.2. Tipos de Control Biométrico

Hay una amplia gama de sistemas biométricos diseñados para verificar la identidad de una persona. Todos estos sistemas comparten dos pasos fundamentales para la autenticación: 1) recolección de datos, y 2) verificación. En el primer paso, se recopilan y almacenan los datos biométricos de la persona en el sistema. En el segundo paso, cuando la persona usa el sistema, éste compara los datos en tiempo real con los almacenados, determinando así el grado de precisión o error en la identificación.

(Cannatella et al., 2022) nos dice que estos pasos incluyen las siguientes fases:

- Captura: Se recogen datos físicos, biológicos o de comportamiento del usuario.

- Preprocesado: Los datos se adaptan para permitir una extracción adecuada posteriormente.
- Extracción de características: Se extraen las características esenciales de los datos recopilados.
- Comparación: Las características extraídas se comparan con los patrones previamente almacenados.

a. Huella Dactilar

"Una huella dactilar es el patrón de valles y crestas en la superficie de un dedo, que se forma durante los primeros siete meses de desarrollo fetal. Se trata de una característica única, que no se repite inclusive entre mellizos idénticos" (Valdés, 2015)

Estos sistemas permiten analizar, comparar y determinar la identidad de un individuo utilizando una base de datos. (Parrales, 2024) Las huellas dactilares tienen un alto nivel de reconocimiento fisiológico porque analizan signos únicos en los dedos, que son características permanentes de una persona. A pesar de los riesgos y causas asociados con el robo de identidad, los sistemas biométricos continúan siendo efectivos debido a los procedimientos y técnicas complejas que utilizan.

(Giraldo & Gomez, 2017) menciona que generalmente, se observan áreas oscuras que corresponden a los relieves, formados por una superficie irregular de crestas (representadas por líneas oscuras) y depresiones o valles (indicados por líneas claras), lo que genera un patrón único en cada individuo. Entre estas crestas, existen zonas en blanco que corresponden a áreas de menor relieve. Como se muestra en la figura, la identificación

mediante el patrón de huella dactilar se fundamenta en las minucias, que incluyen la ubicación y dirección de los extremos de las crestas, así como las bifurcaciones (separaciones) que ocurren a lo largo de su recorrido.

Figura 2

Reconocimiento de Huella Digital

Fuente: (Giraldo & Gomez, 2017)

b. Iris

(Valdés, 2015) nos dice que el iris es la región anular del ojo que se encuentra entre la pupila y la esclerótica. Su estructura compleja, que se forma durante el desarrollo fetal, es altamente distintiva y, por lo tanto, útil en la identificación de personas, ya que no existen dos iris idénticos.

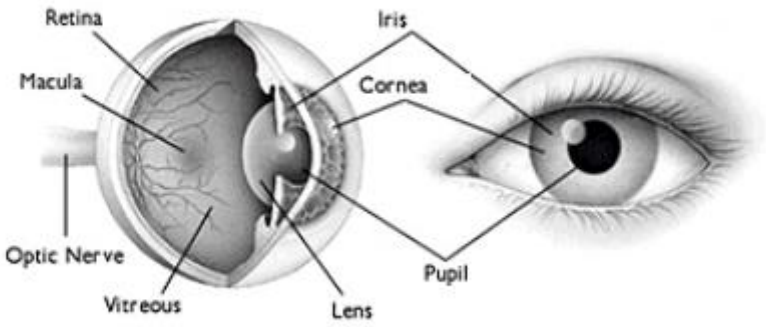
El diseño biométrico del iris se mantiene constante durante toda la vida y es exclusivo para cada persona, ya que posee un elevado número de rasgos, similar a una huella óptica (Castro, 2018)

El ojo tiene un músculo que regula el tamaño de la pupila, controlando así la cantidad de luz que penetra en el ojo. Es fundamental

mantener condiciones de iluminación constantes, ya que el tamaño del iris puede cambiar con la intensidad de la luz.

Figura 3

Reconocimiento de Iris



Fuente: (Castro, 2018)

c. Palma de la Mano

"La palma de la mano contiene patrones de valles y crestas parecidos a las huellas dactilares, pero el área de la huella de la mano es mucho mayor que la del dedo, por lo que es esperable que esta característica sea aún más distintiva. La desventaja es que por esto mismo, los sensores de captura deben ser más grandes y, por lo mismo, más costosos" (Valdés, 2015).

(Adán & Adán, n.d.) destaca que las tecnologías de sistemas biométricos que emplean la identificación de las manos están generando un considerable interés en diversas áreas de aplicación, tales como el acceso a edificaciones, aeropuertos, zonas restringidas, plantas nucleares, estadios, entre otros. Además, estos sistemas tienden a ser bien recibidos por los usuarios y son fáciles de utilizar, implementar y mantener.

Una de las desventajas destacadas por (Aguilera, 2012) es la necesidad de imágenes de alta resolución para garantizar un funcionamiento óptimo de estos sistemas, dado que se basan en la extracción y comparación de minucias y puntos singulares.

Considerando esta desventaja, otra preocupación importante sería el proceso de recolección de datos, ya que, como indica (Aglio Caballero & Belén, 2016), la recopilación de datos es fundamental en los sistemas biométricos, pero las personas tienden a resistirse cuando se les solicita un gran volumen de información.

d. Reconocimiento de la firma

Una firma es un rasgo o conjunto de rasgos realizados siempre de la misma manera que identifican a una persona y sustituyen el nombre y apellidos para aprobar o dar (Rascón, 2019).

Los diferentes métodos para la verificación de firma pueden dividirse en dos grupos principales: off-line (estáticos) y on-line (dinámicos) (Mendaza et al., 2010). Las técnicas off-line se enfocan en el análisis de una imagen digitalizada en escala de grises de la firma manuscrita sobre papel. Por otro lado, las técnicas on-line se basan en las características dinámicas del proceso de firma, como la presión ejercida, las inclinaciones, las posiciones y la velocidad del stylus durante su trazado (Mendaza et al., 2010).

El problema del reconocimiento de firmas consiste en identificar al autor de una firma. En el ámbito del reconocimiento de formas, el proceso de identificación de firmas representa uno de los desafíos más complejos

debido a la amplia diversidad en el estilo y la forma de la escritura manual de cada individuo. Además, se enfrenta a dificultades como la superposición en el trazado de la firma, la interconexión de los caracteres que componen las palabras y las particularidades del bolígrafo empleado en la escritura, entre otros factores (Jabbour et al., 2009).

Según (Cortes Osorio et al., 2010) el mayor desafío de este método radica en que "una persona nunca firma de manera idéntica dos veces"

e. Reconocimiento de la Voz

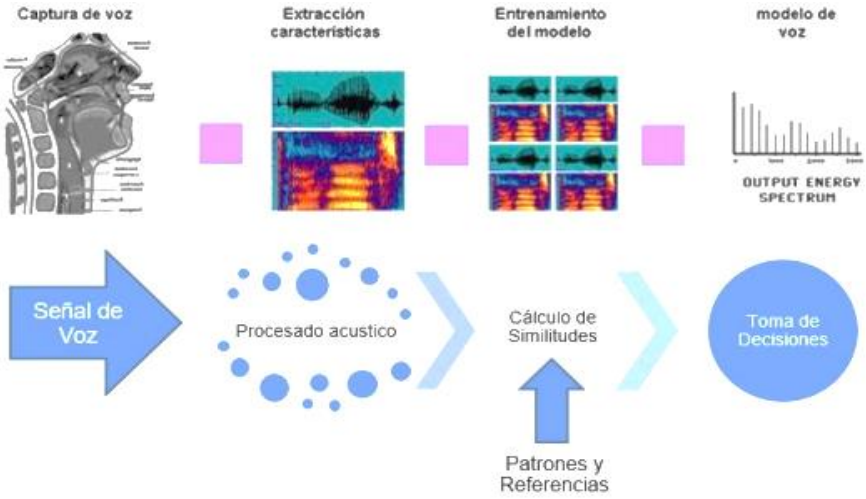
Según (Cortes Osorio et al., 2010) el reconocimiento de voz se realiza mediante la digitalización de distintas palabras de una persona. Cada palabra se descompone en segmentos, de los cuales se extraen 3 o 4 tonos predominantes que se capturan digitalmente y se almacenan en una tabla o espectro conocido como plantilla de la voz.

“Las características de la voz de un individuo se basan en la forma y tamaño de las estructuras biológicas que son usadas en la síntesis del sonido, que son particulares para cada persona” (Valdés, 2015).

En cuanto a factores ambientales, "este sistema biométrico es vulnerable a influencias externas como el ruido, el estado de ánimo, el envejecimiento y enfermedades respiratorias que puedan afectar la voz" (Giraldo & Gomez, 2017).

Figura 4

Proceso de reconocimiento de voz



Fuente: (Giraldo & Gomez, 2017)

2.2.2.3. Ventajas y desventajas de los sistemas biométricos

Los sistemas biométricos ofrecen una manera precisa y confiable de verificar la identidad de las personas mediante características únicas y medibles, como huellas dactilares, iris, voz o reconocimiento facial. A continuación, se exploran las ventajas y desventajas de estos sistemas.

Tabla 1

Ventajas y desventajas de los controles biométricos

Técnica	Ventajas	Desventajas
Reconocimiento facial	Fácil, rápido y barato	La iluminación puede alterar la autenticación
Lectura de huella dactilar	Barato y muy seguro.	Posibilidad de burla por medio de las réplicas, cortes o lastimaduras pueden alterar la autenticación.
Lectura de iris/retina	Muy seguro.	Instructivo (molesto para el usuario)
Lectura de la palma de la mano	Poca necesidad de memoria de almacenamiento de los patrones.	Lento y no muy seguro.

Técnica	Ventajas	Desventajas
Reconocimiento de la firma	Barato y muy seguro.	Puede ser alterado por el estado emocional de la persona.
Reconocimiento de la voz	Barato, útil para los accesos remotos.	Lento, puede ser alterado por el estado emocional de la persona, fácilmente reproducible.

Fuente: (Castro, 2018)

Interpretación: La tabla anterior detalla y compara diversas técnicas de control biométrico, resaltando sus ventajas y sus desventajas. El cuadro anterior nos dice que el reconocimiento facial se caracteriza por su fácil implementación y coste reducido, aunque puede ser afectado por condiciones variables de iluminación. La lectura de huella dactilar se elogia por su alta seguridad y eficiencia económica, pero existe el riesgo de comprometer la autenticación mediante réplicas o daños cutáneos. El reconocimiento de iris/retina ofrece un nivel superior de seguridad, aunque requiere instrucción precisa para el usuario. En cambio, la lectura de la palma de la mano es menos segura y más lenta, pero demanda menos espacio de almacenamiento. Además, el reconocimiento de firma es económico y útil para accesos remotos, aunque puede verse afectado por la fluctuación emocional del usuario. Por último, el reconocimiento de voz es asequible y seguro, aunque susceptible a variaciones emocionales y reproducción no autorizada.

2.2.2.4. Comparación de los sistemas biométricos

Tabla 2

Comparación de los controles biométricos

Sistemas biométricos	Fiabilidad	Facilidad de uso	Prevención de ataques	Aceptación	Estabilidad
Ojo (iris)	Muy alta	Media	Muy alta	Media	Alta
Ojo (retina)	Muy alta	Baja	Muy alta	Baja	Alta
Huellas dactilares	Muy alta	Alta	Alta	Alta	Alta
Vascular dedo	Muy alta	Muy alta	Muy alta	Alta	Alta
Vascular mano	Muy alta	Muy alta	Muy alta	Alta	Alta
Geometría de la mano	Alta	Alta	Alta	Alta	Media
Escritura y firma	Media	Media	Media	Muy alta	Baja
Voz	Alta	Alta	Media	Alta	Media
Cara 2D	Media	Media	Media	Muy alta	Media
Cara 3D	Alta	Alta	Alta	Muy alta	Alta

Fuente: (Castro, 2018)

Interpretación: La tabla anterior ofrece una comparación detallada de la fiabilidad y estabilidad de varias técnicas de control biométrico. Cada método, como el reconocimiento facial, de huella dactilar, de iris, y de voz, entre otros, se evalúa en términos de su precisión y consistencia en diversos entornos y situaciones. Este análisis proporciona una mejor comprensión de la confiabilidad de cada técnica y su idoneidad para aplicaciones específicas donde la consistencia y la precisión son fundamentales. Por ejemplo, el reconocimiento facial muestra una fiabilidad y prevención de ataques mediana, pero se destaca por su alta aceptación y una estabilidad moderada.

2.2.3. Reconocimiento Facial

2.2.3.1. Definición de Reconocimiento Facial

La revisión de la literatura indica que “el reconocimiento facial es una herramienta que permite la identificación automática de una persona a través de una imagen digital” (D. Espinoza & Jorquera, 2015). El reconocimiento facial es un método para identificar o confirmar la identidad de una persona a través de su rostro (Aquijes & Ampuero, 2021).

Por su parte, (Galindo et al., 2021) nos dice que, “El reconocimiento facial es un método biométrico de autenticación que utiliza características físicas del cuerpo para verificar la identidad de una persona. Se basa en un conjunto específico de datos biométricos que identifican al individuo mediante el análisis de la forma y estructura única de su rostro”.

(Galindo et al., 2021) señala que la finalidad principal de un sistema de reconocimiento facial consiste en obtener una imagen o una fotografía de prueba de un rostro "desconocido", y luego localizar una imagen del mismo rostro dentro de un conjunto de imágenes "conocidas" o de entrenamiento.

(Aquijes & Ampuero, 2021) nos dice que los sistemas de reconocimiento facial pueden detectar el rostro de una persona utilizando fotografías o videos en tiempo real.

Los sistemas biométricos con reconocimiento facial emplean técnicas que identifican rasgos específicos del rostro, según (Parrales, 2024) nos dice que son:

- **Orejas**: El tamaño es la característica principal que las define, aunque suelen ser excluidas del reconocimiento facial debido a variaciones indeseadas.
- **Cejas**: Ubicadas en la parte superior de la cara, su tamaño, color y grosor pueden variar, pero estas variaciones no afectan significativamente el reconocimiento.
- **Ojos**: Constituyen uno de los rasgos más distintivos del rostro, ya que su geometría es única y proporciona una gran cantidad de información.
- **Nariz**: Su tamaño puede variar, pero no altera las expresiones faciales de la persona.
- **Boca**: Proporciona información sobre una persona a través de su flexibilidad y diversidad de movimientos.

Teniendo en cuenta la definición de reconocimiento facial, (Matul, 2023) nos dice que una persona se identifica visualmente principalmente por sus rasgos faciales, los cuales proporcionan características únicas a cada individuo. Esta técnica ha experimentado un desarrollo significativo en los últimos años gracias a los avances tecnológicos.

Figura 5

Reconocimiento facial de una persona

Fuente: (Mobbeel, 2024)

2.2.3.2. Tecnologías y Algoritmos Utilizados

Según (Morcillo, 2020) se presentarán algunos de los kits de desarrollo de software (SDK), interfaces de programación de aplicaciones (API), plataformas y empresas destacadas en tecnología de reconocimiento facial en la actualidad.

a. Deep Vision AI

Según la página oficial de Deep Vision IA (Deepvisionai, 2020), la empresa se enfoca en proporcionar soluciones ágiles, innovadoras y rentables basadas en aprendizaje profundo y visión por computadora de última generación. Estas soluciones se aplican a diversas industrias aprovechando tecnologías y tendencias avanzadas. Nuestro enfoque especializado radica en descubrir el contenido visual dentro de los datos de nuestros clientes mediante el uso de tecnología avanzada de reconocimiento visual.

(Trends, 2019) nos dice que utiliza tecnología avanzada de visión por computadora para interpretar automáticamente imágenes y videos, transformando el contenido visual en análisis en tiempo real y valiosa información. Su software de reconocimiento facial vigila constantemente áreas específicas para identificar a las personas a lo largo del tiempo, comparándolas con una lista de individuos de interés con una precisión extraordinaria

b. SenseTime

“SenseTime es una empresa global dedicada al desarrollo de tecnologías innovadoras de inteligencia artificial que tienen un impacto

positivo en las economías, la sociedad y la humanidad en general. Además, es la empresa exclusiva de IA más financiada del mundo y cuenta con la valoración más alta en su campo" (Sensetime, n.d.).

Entre su software de plataforma, como nos dice (Trends, 2019) encontramos los siguientes:

- **SensePortrait-S:** Es un servidor estático de reconocimiento facial que ofrece funciones de detección facial desde una fuente de imágenes.
- **SensePortrait D:** Es un servidor dinámico de reconocimiento facial que proporciona funciones de detección facial en múltiples flujos de video de vigilancia, así como seguimiento facial, extracción y comparación de características.
- **SenseFace**: Es una plataforma de vigilancia de reconocimiento facial. Basada en tecnología de reconocimiento facial impulsado por un algoritmo de aprendizaje profundo, ofrece soluciones integradas de análisis inteligente de video, que incluyen vigilancia de objetivos, análisis de trayectorias, gestión de poblaciones y análisis de datos relevantes, entre otros.

c. Amazon Rekognition

Es un servicio de reconocimiento de imágenes con tecnología de aprendizaje profundo que detecta objetos, escenas y rostros; extrae texto, reconoce a personas famosas e identifica contenido inapropiado en imágenes. También le permite realizar búsquedas y comparar rostros (Amazon, 2023).

Rekognition es una robusta oferta de uno de los principales proveedores de servicios en la nube, AWS. Este servicio está completamente gestionado y optimizado para la plataforma AWS, lo que lo convierte en la elección preferida para aquellos que ya utilizan AWS para sus despliegues (Thakur, 2024).

Entre las destacadas características de *Recognition* se incluyen la capacidad de realizar análisis en tiempo real al cargar imágenes o videos en S3, un amplio análisis facial que abarca género, color de cabello, expresiones faciales, y la detección de ojos abiertos, entre otros aspectos.

La principal fortaleza de Rekognition, sin embargo, también representa su mayor limitación: su integración está tan profundamente ligada a los servicios de AWS que puede resultar difícil de utilizar con otros servicios, lo que podría requerir compromisos significativos para hacerlo funcionar fuera de este entorno específico.

d. Kairos

Kairos ofrece reconocimiento facial de vanguardia y ético a desarrolladores y empresas en todo el mundo. Las personas pueden integrar el Reconocimiento Facial a través de la API en la nube de Kairos, o alojar Kairos en sus propios servidores para tener un control total sobre los datos, la seguridad y la privacidad. Esto permite crear experiencias de cliente más seguras y accesibles (Trends, 2019).

Kairos es compatible con imágenes y videos, ofreciendo todas las características avanzadas esperadas de una API moderna de reconocimiento facial, también ofrece una opción de implementación

local. El costo varía según el caso de uso y puede ser significativamente más alto dependiendo de los requerimientos específicos (Thakur, 2024).

e. Google Cloud Vision

Google ha decidido distinguir sus servicios de reconocimiento facial entre imágenes y vídeos. La API destinada a imágenes se denomina Cloud Vision (Thakur, 2024). El servicio orientado a imágenes es bastante similar a lo que AWS ofrece, el servicio de vídeo destaca por su capacidad de catalogación y búsqueda. Esto será beneficioso para empresas que gestionan grandes archivos de vídeo y necesitan analizarlos o buscar información específica.

(Resource, 2022) nos dice que la API de Google Cloud Vision incluye:

- Identificación de etiquetas y entidades para reconocer el objeto principal dentro de una imagen. Esto permite crear metadatos en el catálogo de imágenes para facilitar la búsqueda basada en imágenes.
- Reconocimiento óptico de caracteres (OCR) para interpretar el texto presente en una imagen. Google Cloud Vision puede reconocer automáticamente una amplia variedad de idiomas diferentes.
- Detección de contenido inapropiado mediante la Búsqueda Segura, útil para identificar material inadecuado en imágenes de acceso público.
- Reconocimiento facial que identifica rostros en una imagen, incluyendo características como la posición de la nariz, ojos y boca, y permite detectar emociones.

- Detección de puntos de referencia, junto con la identificación de coordenadas de latitud y longitud asociadas.
- Identificación de logotipos para reconocer marcas y productos dentro de una imagen.

f. OpenCV

"OpenCV es una biblioteca de código abierto para visión por computadora y aprendizaje automático. Diseñada para ofrecer una plataforma para aplicaciones de visión por computadora y promover la adopción de la percepción de máquinas en productos comerciales, permite a las empresas utilizar y modificar el código con facilidad" (Morcillo, 2020)**.**

Según (Aquijes & Ampuero, 2021) OpenCV es una biblioteca de código abierto que emplea inteligencia artificial y se centra en el procesamiento de imágenes, desempeñando un papel crucial en el avance de sistemas con inteligencia artificial en tiempo real.

(Aquijes & Ampuero, 2021) nos dice que OpenCV es una biblioteca que permite extraer una gran cantidad de información a partir de imágenes o vídeos en tiempo real. Es capaz de procesar e identificar patrones en imágenes utilizando operaciones y algoritmos matemáticos en lo que se conoce como espacio vectorial, lo que facilita reconocer múltiples características dentro de los datos visuales.

2.2.3.3. Face Recognition

(Morcillo, 2020) nos dice que Face Recognition es una biblioteca de reconocimiento facial, considerada la más fácil de usar en el mundo,

que permite identificar y manipular rostros desde Python o desde la línea de comandos. Esta herramienta se basa en la tecnología de reconocimiento facial de última generación de Dlib, desarrollada mediante aprendizaje profundo. Su modelo alcanza una precisión del 99.38 % en el conjunto de pruebas *Labeled Faces in the Wild* (Ageitgey, 2022). Por su parte (Galindo et al., 2021) nos dice que Face Recognition está desarrollado utilizando técnicas de aprendizaje profundo para el reconocimiento facial y se basa en características geométricas.

Según (Basil, 2023) el reconocimiento facial implica varios pasos clave para alcanzar su objetivo.

a. Detección de rostro

Proceso en el cual se identifican las caras en imágenes o videos, las tecnologías que utilizan son las siguientes.

Clasificadores de cascada de Haar

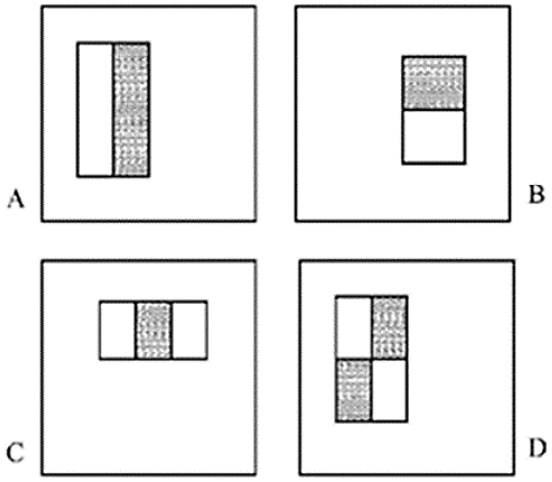
La técnica de cascada se basa en la combinación secuencial de varios clasificadores débiles, cada uno de los cuales analiza una sección específica de una imagen o de un fotograma en el caso de video (Jeremías, 2020).

El clasificador Haar en cascada se entrena utilizando cientos de muestras tanto positivas como negativas, lo que permite al sistema reconocer la forma del objeto que se desea identificar.

Las características clave del sistema de detección se basan en la suma de píxeles dentro de áreas rectangulares de la imagen.

Figura 6

Entradas de Haar Cascada



Fuente: (Jeremías, 2020)

Interpretación: El algoritmo trabaja con ventanas de tamaño uniforme que contienen 2, 3 o 4 rectángulos de igual dimensión. En cada una de estas ventanas se aplica la función Haar, que se calcula sumando los píxeles dentro de los rectángulos blancos y restando los píxeles dentro de los rectángulos sombreados.

Redes Neuronales convolucionales

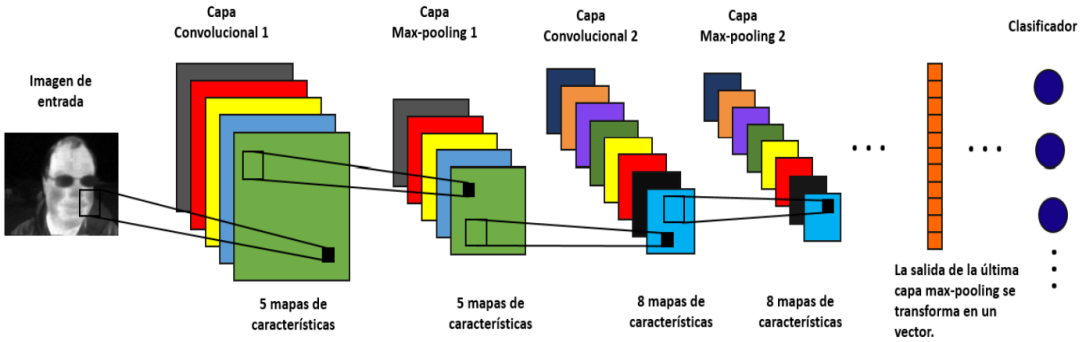
Una red neuronal se puede describir como un modelo matemático formado por numerosos elementos de procesamiento organizados en diferentes capas, que emula el comportamiento de las neuronas biológicas (Cayllahua & Suárez, 2019).

(Figuero et al., 2020) nos dicen que una red neuronal convolucional es un tipo de red especializada en aprender características locales de los datos de entrada, los cuales están estructurados en múltiples arreglos. Este tipo de algoritmo es especialmente eficiente en el reconocimiento de

patrones a partir de imágenes, comenzando con la identificación de características básicas, como líneas, para luego aprender a distinguir elementos más complejos, como figuras geométricas, objetos, animales, personas y lugares.

Figura 7

Red Neuronal Convolucional básica



Fuente: (Figuero et al., 2020)

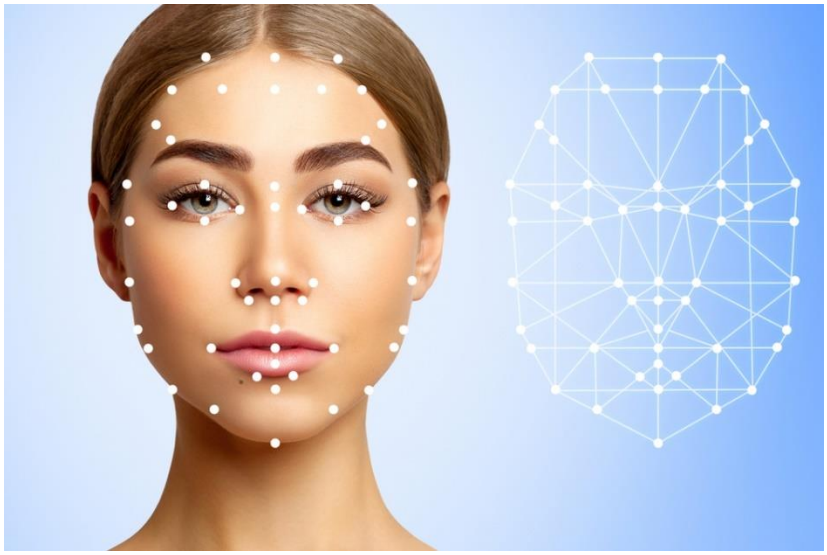
Interpretación: La red neuronal anterior comienza con una secuencia de capas convolucionales y max-pooling, donde la última capa de max-pooling genera un vector que sirve como entrada para una red neuronal completamente conectada, cuya capa final actúa como clasificador. Las capas convolucionales consisten en mapas de características formados por neuronas que comparten un filtro de pesos. Luego, las capas max-pooling reducen las dimensiones de estos mapas, seleccionando el valor máximo en regiones específicas, lo que simplifica la información sin perder las características más relevantes.

b. Extracción de puntos de referencia facial

Como nos dice (D. Ramos, 2018) este método consiste en encontrar los extremos norte, sur, oriente y occidente de cada región de interés por eje.

Figura 8

Extracción de puntos de referencia facial



Fuente: (Estudi, 2020)

c. Extracción de características faciales

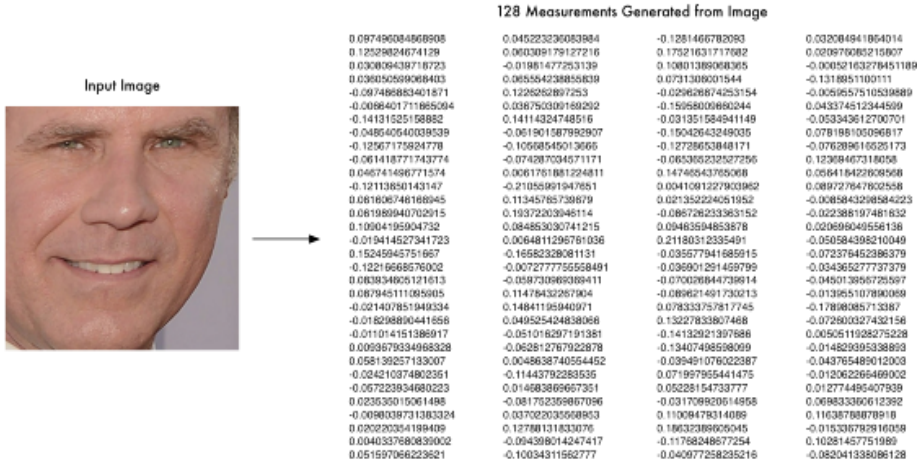
Esta es una de las fases más importantes, en donde el sistema extrae las características únicas del rostro, como la distancia entre los ojos, la forma de la nariz, y otras peculiaridades que permiten diferenciar un rostro de otro (Cadena, 2021). Estas características se convierten en un vector o embebido facial, que es una representación matemática del rostro.

Vectorización o *embeddings*

(Gallo, 2022) nos dice que, un vector es una lista de 128 valores que describen un fenómeno, es este caso, un rostro.

Figura 9

Ejemplo de vectorización de una imagen



Fuente: (Gallo, 2022)

Interpretación: Para que la computadora pueda reconocer a una persona por medio de su rostro se necesita de números, por eso se realiza la vectorización de la imagen.

d. Clasificación facial

Distancia Euclidiana

La distancia euclidiana es una métrica matemática empleada para determinar la distancia entre dos puntos en un espacio geométrico. Fundamentada en la geometría euclidiana, esta medida se calcula utilizando el teorema de Pitágoras. La distancia euclidiana representa la longitud del segmento de línea recta que une dos puntos en dicho espacio (Ríos, 2020).

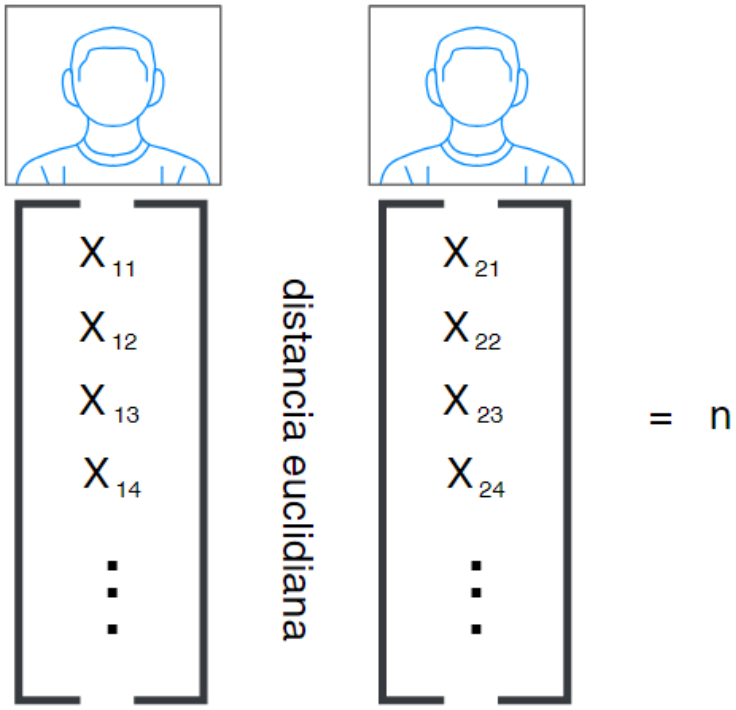
Como nos dice (Hernández, 2018) la distancia euclidiana entre x & y está dada por la fórmula.

$$d = \sqrt{\sum_{i=1}^{n} (v_{1i} - v_{2i})^2}$$

En el reconocimiento facial, la distancia euclidiana se utiliza para comparar dos vectores de características faciales. Cuanto más pequeña es la distancia entre dos vectores, más similares son los rostros.

Figura 10

Comparación de vectores



Interpretación: Se aplica la distancia euclidiana entre los dos vectores (rostros vectorizados) y se obtiene un valor n, el cual es la distancia entre ambos vectores.

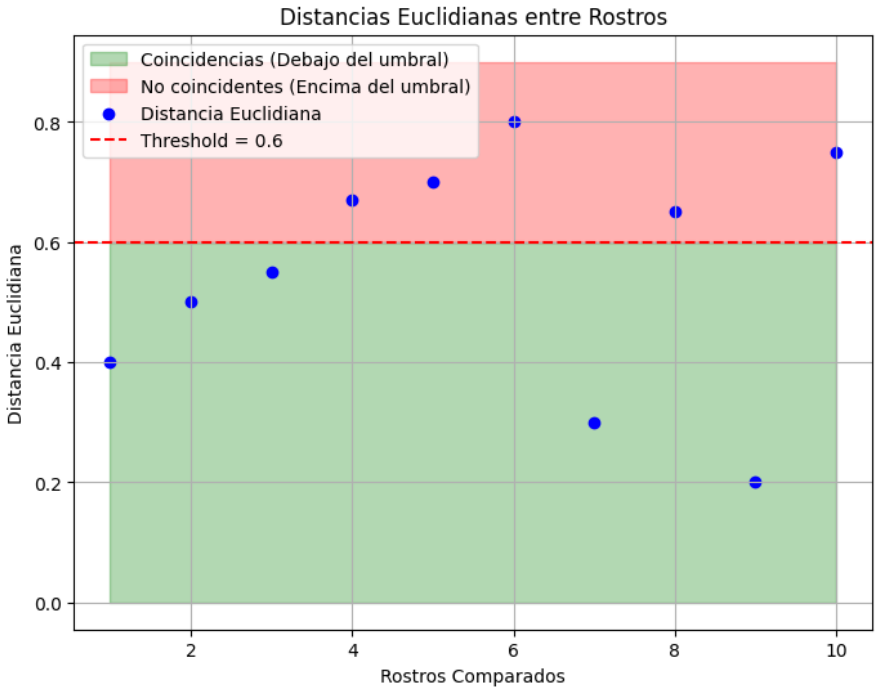
Umbral (*Threshold*) de decisión

Como nos dice (Rodríguez, 2017) los umbrales se emplean, por ejemplo, para establecer límites máximos en la concentración de

contaminantes del aire, reducir niveles de ruido, tratar el agua y mejorar la seguridad en los sistemas alimentarios.

Figura 11

Distancia euclidiana entre rostros



Interpretación: En el reconocimiento facial supongamos que tienes un umbral de decisión de 0.6 para la similitud de la distancia euclidiana. Si la similitud calculada entre dos vectores faciales es 0.7, que es mayor que el umbral, se concluye que los rostros no coinciden. Si la similitud es 0.5, que es menor que el umbral, se concluye que coinciden.

2.2.3.4. Parámetros y medidas de desempeño

a. Matriz de Confusión

Una Matriz de confusión nos muestra como se ha comportado un modelo de clasificación tras predecir un conjunto de datos (Alberto Pérez, 2014).

Las matrices de confusión son usadas para obtener los datos de precisión, sensibilidad y especificidad que tiene un modelo tras predecir un conjunto de datos.

Una matriz de consistencia es una tabla que nos permite ver qué tan "confundido" está nuestro modelo al momento de la clasificación, mostrándonos tanto los aciertos como desaciertos cometidos para cada una de las categorías.

Figura 12

Valores de la matriz de confusión

Fuente: (Barrios, 2019)

- Los verdaderos positivos (TP) son aquellos casos que han sido correctamente clasificados como pertenecientes a la clase de interés. Por ejemplo, si la clase de interés es "personas con diabetes", los TP son las personas con diabetes que han sido correctamente identificadas como tal.

- Los verdaderos negativos (TN) representan los casos que han sido clasificados correctamente como no pertenecientes a la clase de interés. En el ejemplo de la diabetes, un TN sería cualquier persona sin diabetes que ha sido correctamente identificada como tal.
- Los falsos positivos (FP) ocurren cuando una clase que no pertenece a la de interés es clasificada incorrectamente como si lo fuera. Por ejemplo, una persona sana que es erróneamente clasificada como una persona con diabetes.
- Los falsos negativos (FN) suceden cuando la clase de interés no es reconocida correctamente. Esto ocurre, por ejemplo, cuando una persona con diabetes es clasificada incorrectamente como si no tuviera la condición, cuando en realidad debería haber sido identificada como diabética.

Una vez se identifican los verdaderos positivos (TP), verdaderos negativos (TN), falsos positivos (FP) y falsos negativos (FN), es posible calcular los parámetros de precisión, sensibilidad y especificidad.

b. Precisión

La precisión es un término que se expresa como la proximidad entre las indicaciones o valores medidos de un mismo mensurando (Magnitud particular sujeta a medición), obtenidos en mediciones repetidas, bajo condiciones especificadas, se expresa numéricamente (Prieto, 2012).

Otra definición de precisión, según (Ortega, 2008) señala que la precisión se refiere a la capacidad de un instrumento para generar

resultados consistentes en mediciones repetidas bajo las mismas condiciones, sin necesariamente estar relacionado con un valor real. La precisión refleja el grado de concordancia entre los resultados obtenidos al aplicar el mismo procedimiento experimental varias veces sobre una misma muestra, manteniendo condiciones constantes.

(Moré, 2019) en su proyecto nos dice que la precisión se halla con los datos de la matriz de confusión y su fórmula es.

$$precisión = \frac{TP}{TP + FP}$$

La precisión es una métrica que indica la proporción de predicciones correctas dentro de todas las predicciones positivas realizadas por el modelo. En esta fórmula, se calcula dividiendo los verdaderos positivos (TP) entre la suma de verdaderos positivos (TP) y falsos positivos (FP). Esto significa que la precisión evalúa cuántas de las instancias clasificadas como positivas realmente pertenecen a la clase de interés, ignorando las predicciones que fueron incorrectas. Una precisión alta implica que el modelo comete pocos errores al identificar positivos. Una balanza puede ser muy precisa si al hacer varias mediciones da siempre el mismo resultado.

c. Exactitud

Se define como la proximidad entre el valor medido, y el valor verdadero del mesurando.

La exactitud se refiere a la habilidad de un instrumento para acercarse al valor físico verdadero. Cuando se realizan múltiples

mediciones, la exactitud evalúa cuán próxima está la media de esas mediciones al valor real, reflejando así el grado de calibración del dispositivo. En otras palabras, la exactitud indica la proximidad de los datos obtenidos respecto al valor verdadero.

Para hallar la exactitud citamos a (Moré, 2019) donde nos dice que la exactitud se halla de la siguiente forma.

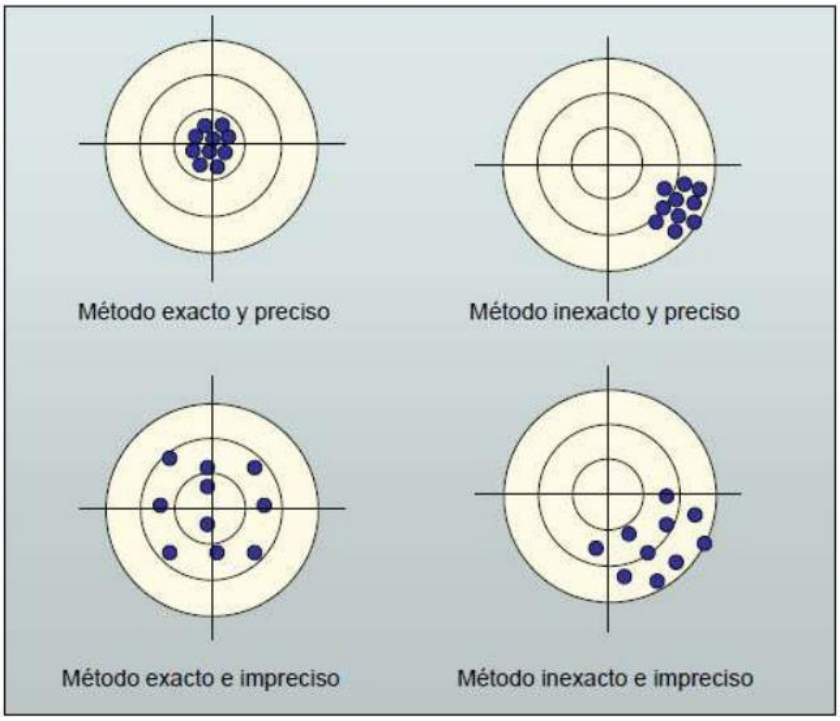
$$exactitud = \frac{TP + TN}{TP + FP + TN + FN}$$

La exactitud se calcula dividiendo la suma de verdaderos positivos (TP) y verdaderos negativos (TN) entre el total de instancias, que incluye verdaderos positivos (TP), falsos positivos (FP), verdaderos negativos (TN) y falsos negativos (FN). Esta métrica refleja la proporción de predicciones correctas, tanto positivas como negativas, respecto al total de predicciones realizadas. Un valor elevado de exactitud indica que el modelo clasifica correctamente la mayoría de los casos.

Entendiendo estos dos conceptos por la revisión de la literatura, a continuación, se presenta una comparación entre ambos, precisión y exactitud

Figura 13

Precisión y exactitud



Interpretación: En el gráfico anterior, se observa la distinción entre precisión y exactitud. Podemos afirmar que un sistema puede ser preciso sin necesariamente ser exacto, y viceversa. La precisión se refiere a la consistencia de un sistema al producir el mismo resultado en múltiples mediciones, mientras que la exactitud se refiere a qué tan cerca está el resultado del valor real o deseado.

2.2.3.5. Casos de Uso

A continuación, se muestran algunas situaciones concretas donde se puede aplicar un sistema de reconocimiento facial (AWS, 2023).

a. Control de acceso

El reconocimiento facial ofrece una mejora considerable en la seguridad y el acceso tanto en hoteles como en aeropuertos. En el contexto hotelero, permite a los huéspedes acceder a sus habitaciones de manera conveniente, eliminando la necesidad de tarjetas físicas. En los aeropuertos, esta tecnología tiene el potencial de sustituir tanto las tarjetas de embarque como los controles de pasaportes. Además, es fundamental para identificar a individuos problemáticos y abordar situaciones de seguridad críticas de manera eficaz (Barten, 2024).

(Aquijes & Ampuero, 2021) nos dicen que la importancia del sistema de reconocimiento facial para mejorar la seguridad y el control de acceso en entornos corporativos ha sido ampliamente reconocida en la actualidad. En un contexto donde la delincuencia muestra un preocupante aumento, la implementación de sistemas biométricos como el reconocimiento facial emerge como una herramienta efectiva en la lucha contra el crimen.

b. Control de aeropuertos y fronteras

En muchos aeropuertos, los datos biométricos se utilizan como sustitutos de los pasaportes, permitiendo a los viajeros evitar largas filas y acceder rápidamente a las puertas de embarque a través de terminales automatizadas. “En el aeropuerto La Guardia de Queens, recientemente se introdujo un método innovador en los controles de seguridad de la Terminal C. Durante el proceso habitual de revisión, algunos pasajeros optaron por una fila especial donde se les tomó una fotografía con un iPad

que se comparó instantáneamente con una base de datos gubernamental. Aquellos cuya imagen coincidía fueron autorizados a continuar sin necesidad de mostrar identificación física ni tarjeta de embarque, simplificando significativamente el proceso de seguridad" (Chung, 2024).

c. Banca

Las empresas destinan en promedio hasta el veinte por ciento de sus ingresos a herramientas de ciberseguridad, según la revista digital ''Financiero''. En ciertos lugares del continente Oriental, como algunos locales de KFC, es posible pagar simplemente sonriendo gracias al reconocimiento facial. Por ejemplo, en la sede de BBVA en Madrid, esta tecnología agiliza pagos seguros, donde los usuarios solo necesitan mirar hacia una cámara para completar la transacción (Spark, n.d.). Este avance fue reconocido como una de las mejores ideas del año por 'Actualidad Económica'. La autenticación mediante reconocimiento facial permite a las personas validar transacciones solo con su mirada, eliminando la necesidad de contraseñas de un solo uso o verificación en dos pasos, lo cual mejora la seguridad al evitar vulnerabilidades que podrían ser explotadas por hackers.

d. Salud

El síndrome de *DiGeorge* afecta a alrededor de 1 de cada 4,000 niños y ocasiona anomalías en múltiples partes del cuerpo (Sierra Santos et al., 2014). Esta condición representa un desafío de salud más grave en países menos desarrollados, donde los recursos para diagnósticos avanzados son limitados. Por consiguiente, el reconocimiento facial, que

muestra una precisión impresionante del 96.6%, emerge como una prometedora herramienta de esperanza para quienes sufren del síndrome de *DiGeorge* (Thakur, 2024).

e. Educación:

Como nos dice (Aznarte et al., 2022), el empleo de tecnologías biométricas ofrece varias ventajas adicionales en el ámbito educativo. Estas tecnologías optimizan el uso del tiempo al simplificar tareas como el control de asistencia, facilitando la adaptación curricular para estudiantes ausentes. Además, fortalecen la seguridad en las aulas al detectar automáticamente personas que no pertenecen al curso.

Un caso exitoso es el de la primera prueba "Exam" aplicada a postulantes de USIL, quienes completaron un examen de matemáticas y lenguaje que duró casi dos horas. Después del examen, los estudiantes llenaron una encuesta de satisfacción en la cual casi todos expresaron su acuerdo con el uso de esta plataforma para la evaluación. Además, mostraron una alta satisfacción con la facilidad de uso y la seguridad del sistema (USIL, 2022).

2.2.4. Sistemas Informáticos

2.2.4.1. Definición de Sistemas Informáticos:

“Los sistemas informáticos consisten en un conjunto integrado de software, hardware y recursos humanos que trabajan en conjunto con un propósito específico. Estos sistemas facilitan el procesamiento y

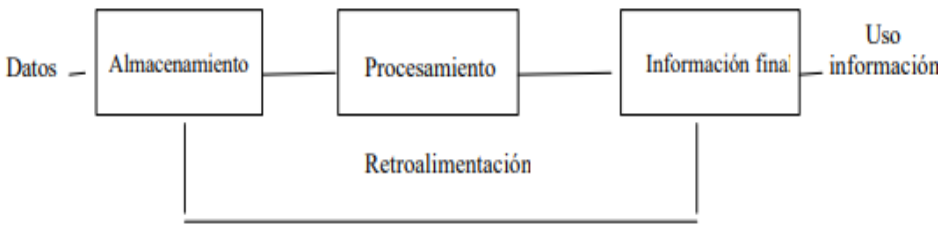
almacenamiento de información al interrelacionarse eficazmente" (Bernad & Rodriguez, 2020).

Según (Hernandez, n.d.), los sistemas informáticos se definen como un conjunto estructurado de procedimientos que, al manejar datos organizados según los requisitos específicos de una empresa, recopilan, procesan y distribuyen de manera selectiva la información fundamental para la operación empresarial, así como para las tareas de dirección y supervisión correspondientes. Este sistema, en parte, respalda los procesos críticos necesarios para llevar a cabo las funciones comerciales según la estrategia definida por la empresa.

(Chacón, 2007) Un sistema informático es un conjunto cohesionado de elementos diseñados para capturar, almacenar, procesar y distribuir información. Su propósito es apoyar la toma de decisiones, el control, el análisis y la planificación estratégica dentro de una organización.

Figura 14

Proceso de un sistema informático



Fuente: (Hernandez, n.d.)

2.2.4.2. Componentes de un sistema informático

(Gonzaga, 2020) nos dice que los sistemas informáticos tienen tres tipos de componentes, los cuales son.

a. Componente físico (Hardware)

El soporte físico se refiere al conjunto de componentes físicos que comúnmente utilizamos en los sistemas informáticos. Dentro del hardware de los sistemas informáticos, se distinguen dos partes principales: la unidad central de procesamiento (CPU) y los periféricos (Posada, n.d.). Lo conforman los ordenadores, periféricos, sistema de comunicaciones y proporcionan la capacidad y la potencia de cálculo del sistema informático (Vilcanqui, 2023).

b. Componente lógico (Software)

(Posada, n.d.) El componente lógico comprende todos los entornos, sistemas y programas utilizados para optimizar el funcionamiento de los componentes informáticos. Se pueden clasificar en dos tipos principales:

- Software de base, que abarca sistemas operativos, programas de servicios, utilidades, compiladores, intérpretes y entornos operativos.
- Software de aplicación, que engloba aplicaciones estándar, bases de datos, programas personalizados y sistemas expertos.

c. Componente humano

Este componente humano está integrado por todas las personas involucradas en cada etapa del ciclo de vida de un sistema informático

(diseño, desarrollo, implementación, operación). Es de vital importancia dado que los sistemas informáticos son creados por humanos y destinados al uso humano (Gonzaga, 2020).

2.2.4.3. Gestión y Seguridad de los sistemas informáticos

a. Gestión de la información

Según (Suárez Alfonso et al., 2015) la gestión de la información abarca todas las acciones destinadas a obtener, procesar, almacenar y posteriormente recuperar de manera efectiva la información generada o recibida por una organización, facilitando así el desarrollo de sus operaciones. Complementando a la idea (Gil et al., 2011) lo define como el proceso de obtener la información adecuada en el formato correcto, para la persona o entidad adecuada, al costo adecuado, en el momento oportuno y en el lugar apropiado, con el fin de facilitar la toma de decisiones adecuada.

b. Seguridad de la información

"La seguridad de la información se puede definir como conjunto de medidas técnicas, organizativas y legales que permiten a la organización asegurar la confidencialidad, integridad y disponibilidad de un sistema de información" (Calderon Arateco, 2019)

(Pallero & Heguiabehere, 2023) nos dice que la seguridad de la información se refiere al conjunto de prácticas diseñadas para garantizar la integridad, disponibilidad y confidencialidad de la información, sin importar el medio de almacenamiento, desde una perspectiva de procesos.

Esta visión de la seguridad de la información se incorpora en las diversas funciones de una organización, incorporando prácticas recomendadas tanto en sus procesos como en sus servicios. Por lo tanto, es crucial comprender la misión y funciones de la organización, así como las prácticas y estándares de seguridad de la información, para integrarlas de manera efectiva.

2.2.5. Arquitecturas de desarrollo de software

2.2.5.1. Definición de arquitecturas de desarrollo

"La arquitectura de software de un sistema se refiere al conjunto de estructuras necesarias para analizar y entender el sistema. Incluye los elementos de software, sus relaciones y las propiedades de estos componentes" (Velasco, 2016). En esencia, la arquitectura de software puede considerarse como la estructura organizativa del sistema, basada en la definición de los componentes y sus interacciones.

La arquitectura se define como el conjunto de decisiones cruciales sobre cómo se organiza un sistema de software. Esto incluye la selección de los elementos estructurales que conformarán el sistema y sus interfaces, así como la descripción del comportamiento de estas interfaces durante las interacciones entre los componentes del sistema. En otras palabras, una arquitectura de software es una descripción de los subsistemas y componentes del sistema y de las relaciones que existen entre ellos (Cárdenas, 2016).

2.2.5.2. Arquitectura en capas

"La arquitectura en capas es un enfoque de diseño de software que organiza las funcionalidades del sistema en distintas capas o niveles. Cada capa se especializa en un conjunto particular de tareas y se comunica con las capas adyacentes a través de interfaces claramente definidas" (Martín Durán, 2023).

"La arquitectura en capas ayuda a estructurar las aplicaciones que se pueden descomponer en grupos de subtareas en la que cada grupo de subtareas está en un nivel particular de abstracción" (Cárdenas, 2016)

Como nos define (Oscar Blancarte, 2021) alguna de las ventajas de esta arquitectura es:

- Facilita la separación de responsabilidades, dado que cada capa se enfoca en una función específica.
- Esta arquitectura es sencilla de implementar, ampliamente conocida y utilizada en muchas aplicaciones, lo que la hace accesible para la mayoría de los desarrolladores.
- Al estar organizada en capas, se puede probar cada una de manera independiente, lo que permite un análisis más detallado y controlado del sistema.
- Gracias a que cada capa cumple una función particular, es más fácil identificar el origen de los errores y corregirlos, o realizar modificaciones localizadas sin afectar el sistema completo.

- La separación por capas permite aislar los servidores en diferentes subredes, dificultando los ataques y aumentando la protección del sistema.

2.2.6. Metodologías de Desarrollo de Sistemas Informáticos

2.2.6.1. Definición de Metodologías de Desarrollo

La metodología de desarrollo puede definirse como un enfoque o forma de interpretar la realidad, y se utiliza como una estructura para planificar y controlar el proceso de creación de un sistema (MegaPractical, n.d.).

(A. Espinoza, 2013) lo define como "Conjunto de actividades, procedimientos, técnicas, herramientas y documentos estandarizados y organizados dentro de un marco de trabajo. Estos elementos son fundamentales para estructurar, planificar y controlar eficazmente la transformación de una necesidad o conjunto de necesidades en un sistema de información".

(MegaPractical, n.d.) menciona que los objetivos de una metodología de desarrollo de software son los siguientes:

- Establecer adecuadamente todos los requisitos de un sistema de software.
- Proporcionar un método sistemático para el desarrollo que permita controlar el proceso.
- Realizar la construcción de un sistema de software en un plazo y costos adecuados.

- Desarrollar un sistema que esté bien documentado y sea fácil de mantener.
- Facilitar la identificación temprana de cualquier cambio necesario durante el desarrollo.
- Garantizar que el sistema satisfaga las necesidades de las partes interesadas.

Teniendo en cuenta las definiciones anteriores y la (Maida & Pacienzia, 2015) “La metodología representa una fase específica en un trabajo o proyecto, que parte de una base teórica y conduce a la selección de técnicas concretas o métodos para alcanzar los objetivos establecidos”. Podemos decir que es fundamental elegir una metodología adecuada que se ajuste a nuestros requisitos específicos”. Complementando a este argumento (Montesino, 2018) menciona que “no todos los sistemas de la información son compatibles con todas las metodologías, pues el ciclo de vida del software puede ser variable. Por esta razón, es importante que dependiendo del tipo de software que se vaya a desarrollar, se identifique la metodología para el diseño de software idónea”

2.2.6.2. Tipos de Metodologías de Desarrollo

2.2.6.2.1. Metodologías Tradicionales

“Las metodologías tradicionales aplican una estricta disciplina al proceso de desarrollo de software para lograr un producto más eficiente. Estas metodologías se enfocan en una planificación exhaustiva de todas las tareas necesarias; una vez que se ha detallado completamente el trabajo, se inicia el ciclo de desarrollo del software” (Maida & Pacienzia, 2015).

a. Cascada

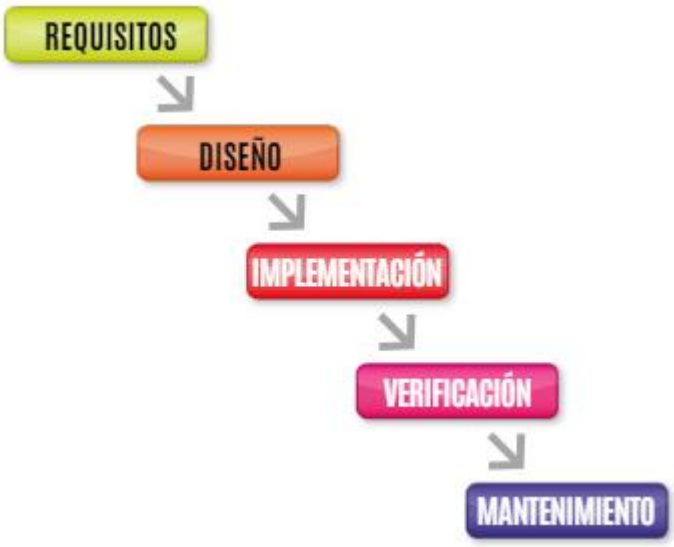
(Talent, 2021) nos dice que la metodología cascada es un enfoque secuencial utilizado comúnmente en el desarrollo de software. Este método organiza el trabajo en una serie de fases que deben completarse de manera secuencial, una después de otra. Su nombre proviene de la analogía con las cascadas, donde cada fase debe colocarse una encima de otra en un orden estricto, siguiendo una dirección descendente desde la concepción del proyecto hasta su implementación final.

"Es un enfoque metodológico que estructura meticulosamente las etapas del proceso de desarrollo de software, de manera que cada fase debe completarse antes de comenzar la siguiente. Al finalizar cada etapa, el modelo prevé una revisión exhaustiva para evaluar si el proyecto está preparado para avanzar a la fase siguiente" (Montesino, 2018).

La metodología en cascada es denominada así por la posición de las fases en el desarrollo de sistemas, que parecen caer en cascada hacia la siguiente fse.

Figura 15

Etapas de la metodología cascada



Fuente**:** (Talent, 2021)

"Es considerado como el método tradicional de explicar el proceso de desarrollo de software, por lo que actualmente es visto como anticuado" (MegaPractical, n.d.).

2.2.6.2.2. Metodologías Ágiles

(A. Espinoza, 2013) nos dice que son el resultado de un nuevo enfoque que se basa en la pronta entrega de software incremental, proveniente de un desarrollo iterativo durante todo el ciclo de vida del software"

(Maida & Pacienzia, 2015) nos dice que "Este enfoque nace como respuesta a los problemas que puedan ocasionar las metodologías tradicionales"

a. Scrum

"Es un enfoque bastante flexible que ayuda al equipo a reaccionar rápidamente en los diferentes cambios en los requisitos, además provee la gran ventaja de que puede ser aplicado consecutivamente a todos los proyectos" (MegaPractical, n.d.).

(Maida & Pacienzia, 2015) "Scrum es un proceso que aplica de forma regular un conjunto de buenas prácticas para facilitar el trabajo colaborativo en equipo, con el objetivo de lograr el mejor resultado posible en un proyecto".

Roles en Scrum

(Schwaber & Sutherland, 2020) nos dice que el equipo Scrum consta de:

- Desarrolladores: Son los miembros del equipo Scrum que se comprometen a crear cualquier parte del Incremento funcional en cada Sprint.
- Propietario del Producto (*Product Owner*): Responsable de maximizar el valor del producto resultante del trabajo del equipo Scrum. Esto puede variar según la organización, equipos Scrum e individuos.
- Scrum Master: Encargado de establecer Scrum según la Guía de Scrum. Facilita la comprensión de la teoría y la práctica de Scrum, tanto dentro del equipo como en toda la organización.

Eventos de Scrum

Scrum se estructura alrededor de varios elementos fundamentales que aseguran su efectividad, como nos dice (Schwaber & Sutherland, 2020).

- Sprint: Es la unidad básica de tiempo en Scrum donde se ejecuta el trabajo y se entrega valor.
- Planificación de Sprint: Al inicio de cada Sprint, el equipo colabora para definir qué trabajo realizará durante ese período.
- Scrum Diario (*Daily Scrum*): Reunión diaria breve donde el equipo revisa el progreso hacia el objetivo del Sprint y ajusta el plan de trabajo según sea necesario.
- Revisión del Sprint (*Sprint Review*): Al finalizar el Sprint, el equipo presenta los resultados a las partes interesadas para recibir retroalimentación y determinar los ajustes futuros.
- Retrospectiva del Sprint (Sprint Retrospective): Reunión para reflexionar sobre el Sprint y mejorar continuamente los procesos y la calidad del trabajo.

Figura 16

Metodología Scrum

Fuente**:** (MegaPractical, n.d.)

b. Extreme Programming (XP)

Es una metodología ágil de desarrollo de software que se caracteriza por un conjunto de prácticas y reglas diseñadas para adaptarse a entornos cambiantes. En lugar de enfocarse en la planificación, análisis y diseño a largo plazo, se centra en abordar múltiples aspectos simultáneamente durante todo el proceso de desarrollo (Mariscal & Cecilia, 2015).

(Dayana & Jean, 2014) nos dice que la programación extrema, también conocida como *Extreme Programming* (XP), es una metodología de desarrollo de software. Se destaca como uno de los procesos ágiles más prominentes en la ingeniería de software, diferenciándose de las metodologías tradicionales al poner un mayor énfasis en la adaptabilidad sobre la previsibilidad, enfatizando más en esta idea (Meléndez et al., 2016) menciona que "…se considera el más destacado de los procesos ágiles de desarrollo de software y presenta más énfasis en la adaptabilidad"

"La metodología XP (*Extreme Programming*) se fundamenta en la retroalimentación constante entre el cliente y el equipo de desarrollo, promoviendo una comunicación abierta y continua entre todos los involucrados. Además, se enfoca en la simplicidad de las soluciones implementadas y en el valor del coraje para adaptarse y gestionar los cambios a medida que surgen" (Letelier & Penadés, 2015).

Características de la metodología XP

(Dayana & Jean, 2014) nos dice que la metodología de programación extrema tiene las siguientes características:

- Prioriza la adaptabilidad por encima de la previsibilidad, marcando una diferencia notable con las metodologías tradicionales.
- Se implementa dinámicamente a lo largo del ciclo de vida del software.
- Es capaz de ajustarse a cambios en los requisitos del proyecto.
- Enfatiza la importancia de los individuos y sus interacciones por sobre los procesos y herramientas.
- Da prioridad al individuo y las interacciones dentro del equipo de desarrollo frente al énfasis en el proceso y las herramientas.

Roles de XP

(Letelier & Penadés, 2015) basándose en la propuesta original de Beck, nos dice que existen los siguientes roles:

- **Programador**

(Meléndez et al., 2016) nos dice que el programador implementa las historias de usuario según las necesidades del cliente, estimando el

tiempo requerido para cada una y permitiendo al cliente establecer prioridades dentro de la iteración. Además, se encarga del diseño y la ejecución de pruebas unitarias para el código desarrollado o modificado.

- **Cliente**

"El cliente escribe las historias de usuario y las pruebas funcionales para validar su implementación" (Letelier & Penadés, 2015). En cada iteración, el cliente especifica las funcionalidades deseadas y establece las prioridades para su implementación.

- **Encargado de pruebas**

Colabora con el cliente en la redacción de pruebas funcionales, realiza ejecuciones periódicas de estas pruebas, comunica los resultados al equipo y gestiona las herramientas de apoyo para las pruebas.

- **Encargado de seguimiento**

Implica monitorear continuamente las estimaciones hechas por los programadores y contrastarlas con el tiempo real de desarrollo. De este modo, se proporciona información estadística sobre la precisión de las estimaciones para facilitar su mejora.

- **Entrenador**

Líder del proceso en su totalidad. Encargado de iniciar y guiar al equipo en la implementación de todas las prácticas de la metodología XP.

- **Consultor**

Es un miembro externo con experiencia fundamental para el proyecto, que guía al equipo en la resolución de problemas específicos.

- **Gestor**

Actúa como el enlace entre el cliente y los desarrolladores. Posee conocimientos avanzados en tecnología y gestión. Se encarga de formar el equipo, adquirir los recursos necesarios y resolver los problemas que surgen. También dirige las reuniones, incluyendo la planificación de iteraciones y la gestión de compromisos. Su función principal es la coordinación.

Fases de la metodología XP

(Mariscal & Cecilia, 2015) nos dice que las fases que componen esta metodología son las siguientes:

- **Planificación**

(Meléndez et al., 2016) menciona que en esta fase se comienza recopilando historias de usuarios, que equivalen a los casos de uso tradicionales. Una vez recopiladas, los programadores evalúan rápidamente el tiempo necesario para desarrollar cada historia. Los conceptos fundamentales de la planificación incluyen las historias de usuario, el plan de entregas, el plan de iteraciones y las reuniones diarias de seguimiento.

- **Diseño**

"En este paso, se enfocará en desarrollar un código simple y directo, implementando únicamente lo necesario para que funcione el prototipo. Se buscará obtener un diseño fácil de entender y ejecutar, siguiendo las prácticas de la metodología XP que promueven la simplicidad y la eficiencia en el desarrollo" (Dayana & Jean, 2014).

- **Codificación**

En esta fase el cliente es parte integral del equipo de desarrollo en todas las fases de XP. Su participación es crucial especialmente al codificar historias de usuario. Los clientes son responsables de crear estas historias y de negociar los plazos de implementación. “Antes del desarrollo de cada historia de usuario el cliente debe especificar detalladamente lo que ésta hará y también tendrá que estar presente cuando se realicen las pruebas que verifiquen que la historia implementada cumple la funcionalidad especificada” (Dayana & Jean, 2014).

- **Pruebas**

“En la metodología XP, uno de los fundamentos es la utilización de pruebas para verificar el funcionamiento de los códigos implementados” (Dayana & Jean, 2014).

(Meléndez et al., 2016) nos dice que existen las siguientes pruebas:

Pruebas unitarias: Antes de su lanzamiento o publicación, todos los módulos deben superar las pruebas unitarias. Garantizar que todo código liberado pase las pruebas unitarias es crucial para asegurar la funcionalidad integrada del código.

Identificación y corrección de errores: Cuando se detecta un error, debe ser corregido de inmediato, implementando medidas preventivas para evitar la repetición de errores similares.

Pruebas de aceptación: Se desarrollan en cada ciclo de iteración del desarrollo, basadas en las historias de usuario.

(Dayana & Jean, 2014) nos dice que el uso de las pruebas en XP es el siguiente:

Es crucial desarrollar las aplicaciones destinadas a las pruebas en un entorno de desarrollo específico para pruebas.

Se deben someter a pruebas las diferentes clases del sistema.

Es necesario crear pruebas que validen el código antes de su implementación; como se mencionó anteriormente, es esencial crear las pruebas antes que el propio código.

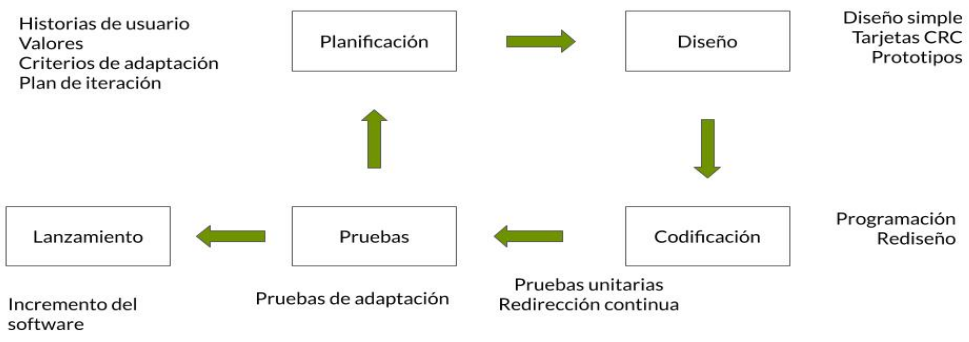
Las pruebas de aceptación son fundamentales para evaluar las diversas tareas en las que se divide una historia de usuario.

- **Lanzamiento**

En esta fase se probó todas las historias de usuario o versiones parciales con éxito, cumpliendo con los requisitos del cliente. Ahora se dispone de un software funcional que podemos integrar en el producto final.

Figura 17

Fases de la metodología XP



Fuente: (Sinnaps, 2020)

c. Kanban

(Figuerola, 2011) es una metodología de tipo *pull*, donde los recursos determinan cuándo y cuánto trabajo se comprometen a realizar. En este enfoque, los recursos toman el trabajo según su disponibilidad, en lugar de recibirlo de manera forzada desde fuera *push.*

"Kanban se fundamenta en el desarrollo incremental, desglosando el trabajo en partes manejables. El término 'Kanban' se refiere a una tarjeta de señal que simboliza una unidad de trabajo. Esta tarjeta se desplaza a través del flujo de la organización únicamente cuando hay capacidad disponible para abordar la tarea en la siguiente fase del proceso" (Cabrera, n.d.)**.**

Principios de Kanban

Según (Arango et al., 2015) los principios promovidos en la metodología Kanban son los siguientes:

- Es crucial abordar cada tarea correctamente desde el inicio, dado que corregirla después de realizarla rápidamente consume más tiempo.
- Enfocarse en realizar únicamente lo necesario, evitando distracciones con tareas secundarias o superfluas.
- Perfeccionar continuamente los procesos de desarrollo en línea con los objetivos establecidos y futuros.
- Determinar las tareas a ejecutar según las necesidades actuales o pendientes. Las tareas entrantes pueden ser priorizadas y ajustadas según requisitos específicos.

- Establecer relaciones duraderas con proveedores y mantenerlas a largo plazo.

Roles de Kanban

Según (Yépez Llerena & Armijos Guillen, 2020) Kanban no prescribe roles específicos en absoluto. Esto significa que no se limita a la posibilidad de tener un dueño del producto u otros roles adicionales. La introducción de roles puede ser beneficiosa, especialmente en proyectos de gran escala, permitiendo coordinar múltiples equipos de trabajo con el o los dueños del producto. Es fundamental seguir el principio general de Kanban de menos es más y comenzar con un enfoque minimalista.

Fases de Kanban

Según (Arango et al., 2015) nos dice que existen las siguientes fases:

- Fase 1: Capacitar a todo el personal en los principios y beneficios de Kanban.
- Fase 2: Implementar Kanban en los componentes con mayores problemas para mejorar su manufactura y detectar problemas ocultos. El entrenamiento del personal continúa en la línea de producción.
- Fase 3: Extender la implementación de Kanban al resto de los componentes. Se debe considerar las opiniones de los operadores, quienes tienen un conocimiento profundo del sistema. Es crucial informarles sobre cualquier actividad que afecte su área de responsabilidad.

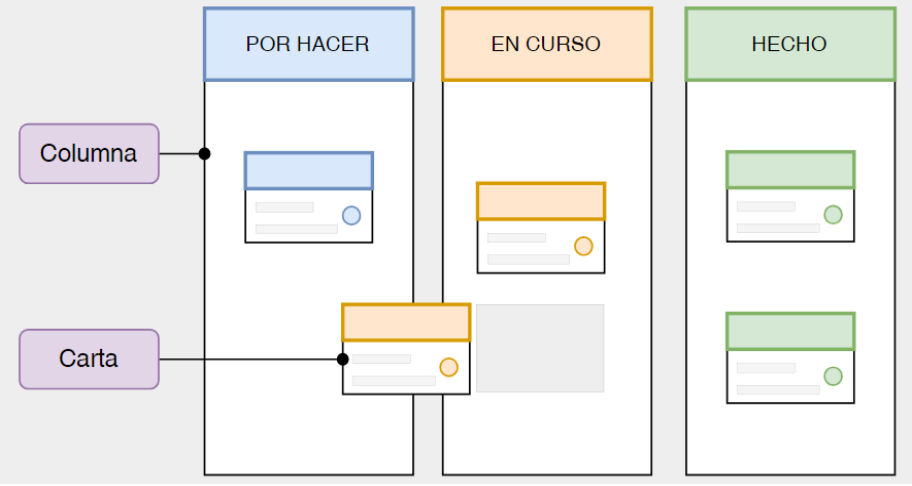
- Fase 4: Realizar una revisión del sistema Kanban, incluyendo los puntos de reorden y los niveles de stock. Es esencial seguir estas recomendaciones para garantizar el correcto funcionamiento del sistema.

Tablero Kanban

"Un tablero Kanban es una herramienta ágil de gestión de proyectos que facilita la visualización del trabajo, limita la cantidad de trabajo en curso y busca maximizar la eficiencia del proceso" (Rehkopf, n.d.).

Figura 18

Tablero Kanban



Como se puede apreciar en la imagen anterior el tablero Kanban cuenta con los siguientes elementos:

- Carta: Representan proyectos y elementos de trabajo, con una tarjeta por proyecto o tarea. Cada tarjeta puede simbolizar una historia de usuario.

- Columnas: Las columnas representan etapas específicas del flujo de trabajo global, pueden ser desde simples, como "Por hacer", "En curso" y "Terminado".

2.2.6.3. Comparación entre Metodología Tradicional Ágil

Según (Maida & Pacienzia, 2015) los métodos ágiles son atractivos debido a su flexibilidad y capacidad de adaptación, lo cual los hace preferidos por quienes evitan seguir procedimientos rigurosos. Por su parte, (Trigas & Domingo, 2012) indican que, en las metodologías tradicionales, las entregas al final del proyecto pueden resultar en productos que no cumplen con los requisitos establecidos, lo cual puede implicar cambios que comprometen los recursos de coste y tiempo. (Maida & Pacienzia, 2015) también señalan que las metodologías tradicionales tienden a tener altos costos al implementar cambios y carecen de flexibilidad en proyectos con entornos volátiles.

(Meléndez et al., 2016) destacan que las metodologías ágiles están más orientadas a procesos de desarrollo de software con ciclos cortos y niveles reducidos de formalización en la documentación requerida. A continuación, se presenta una tabla que compara las metodologías ágiles y tradicionales.

Tabla 3

Diferencias entre metodologías ágiles y tradicionales

Metodologías Ágiles	Metodologías Tradicionales
Basadas en heurísticas provenientes de prácticas de producción de código.	Basadas en normas provenientes de estándares seguidos por el entorno de desarrollo.
Especialmente preparados para cambios durante el proyecto	Cierta resistencia a los cambios.
Impuestas internamente (por el equipo de desarrollo)	Impuestas externamente
Proceso menos controlado, con pocos principios	Proceso mucho más controlado, con numerosas políticas/normas
No existe contrato tradicional o al menos es bastante flexible.	Existe un contrato prefijado
El cliente es parte del equipo de desarrollo	El cliente interactúa con el equipo de desarrollo mediante reuniones
Grupos pequeños (menores a 10 integrantes) y trabajando en el mismo sitio	Grupos grandes y posiblemente distribuidos
Pocos artefactos	Más artefactos
Pocos roles	Más roles
Menos énfasis en la arquitectura del software	La arquitectura del software es esencial y se expresa mediante modelos

Fuente: (Letelier & Penadés, 2015)

CAPÍTULO III

MATERIALES Y MÉTODOS

3.1. UBICACIÓN GEOGRÁFICA DEL PROYECTO

El proyecto se desarrolló en la ciudad de Puno y se implementó en la Universidad Nacional del Altiplano de la misma ciudad – Av. Floral 1153.

Figura 19

Ubicación geográfica del estudio

Fuente: (Google, n.d.)

3.2. OPERACIONALIZACIÓN DE VARIABLES

Tabla 4

Operacionalización de variables

VARIABLE	DEFINICIÓN	DIMENSIONES	DESCRIPCIÓN	INDICADORES	TÉCNICA	INSTRUMENTO	UNIDAD DE MEDIDA	FÓRMULA
V.I: Sistema informático con reconocimiento facial	Método de identificación que utiliza características faciales únicas para verificar o identificar a individuos. Se basa en el análisis de patrones faciales, como la distancia entre los ojos, la forma de la nariz y la boca.	Usabilidad	Según Ramos Dina y Ramos Flor (2018) la usabilidad es la forma como los profesionales interpretan la funcionabilidad del software y la calidad en uso se puede asumir como la forma que lo asimila o maneja el usuario final.	Satisfacción del usuario final	Cuestionario	Cuestionario	Escala	Escala de Likert (1 - 5)
				Confianza en el uso del sistema informático	Cuestionario	Cuestionario	Escala	Escala de Likert (1 - 5)
V.D: Control biométrico en el examen de admisión extraordinario de la UNAP.	Sistema de seguridad que utiliza características físicas o comportamientos únicos de los individuos para autenticar su identidad.	Precisión	Según Aquijes Ronny y Ampuero Lizardo (2021), la precisión es utilizada para evaluar el rendimiento de un sistema de inteligencia artificial, ya que refleja la tasa de respuestas correctas.	Porcentaje de precisión	Observación directa	Ficha de medición	Porcentaje	Fórmula propuesta por (Aquijes & Ampuero, 2021) **Precisión(P) = VP/(VP+FP)** - VP son los verdaderos positivos (predicciones correctas), - FP son los falsos positivos (predicciones incorrectas).
		Tiempo de control	Según Castro (2021), la dimensión tiempo se	Tiempo promedio	Observación directa	Ficha de registro	Segundos	

VARIABLE	DEFINICIÓN	DIMENSIONES	DESCRIPCIÓN	INDICADORES	TÉCNICA	INSTRUMENTO	UNIDAD DE MEDIDA	FÓRMULA
			utiliza para identificar el retraso y calcular el tiempo perdido por cada persona.					Fórmula descrita en el documento de (Alex Bernal, 2018). $T.P.R = \frac{\sum_{i=n}^{n} t_i}{n}$ - t es el valor de cada prueba - n es el total de datos
		Seguridad	Yañez (2019) define la seguridad como una actitud que deben adoptar tanto las empresas y sus empleados en todos los niveles, como las Administraciones Públicas, para establecer una política rigurosa de prevención de riesgos.	Nivel de seguridad	Observación directa	Ficha de evaluación	Nivel	Máximo Alto Moderado Básico Mínimo

3.3. DISEÑO Y MÉTODO DE LA INVESTIGACIÓN

3.3.1. Enfoque de la investigación

En esta investigación se ha seguido un enfoque cuantitativo, debido a que los datos obtenidos se basan en mediciones objetivas del rendimiento del sistema de reconocimiento facial en el control biométrico. El enfoque cuantitativo permite realizar un análisis estadístico para evaluar la precisión, el tiempo de respuesta y el nivel de seguridad del sistema, tal como se establece en los objetivos específicos del estudio.

Enfoque cuantitativo

Según (Sampieri et al., 2014) el enfoque cuantitativo se caracteriza por la recolección de datos numéricos, los cuales son analizados estadísticamente para encontrar patrones y relaciones. En el presente estudio, se utilizaron métricas como el porcentaje de precisión del reconocimiento facial y el tiempo de respuesta, lo cual permite una evaluación objetiva y replicable del sistema. Este enfoque es el más adecuado para validar las hipótesis planteadas y para realizar comparaciones con investigaciones previas en el campo de la biometría.

3.3.2. Tipo de investigación

De acuerdo con los objetivos formulados y propósito de la investigación, el presente proyecto reúne las condiciones para ser una investigación de tipo aplicada.

Investigación aplicada

Este tipo de investigación tiene como objetivo encontrar soluciones a problemas que tienen fenómeno utilizando el conocimiento de la investigación básica (H. Sánchez et al., 2018).

3.3.3. Diseño de investigación

El diseño de la presente investigación es cuasiexperimental con corte transversal.

Diseño cuasiexperimental

El diseño utilizado en la presente investigación es cuasiexperimental, que se caracteriza por la diferenciación de dos subniveles de la variable independiente: un grupo experimental que recibe la intervención y un grupo control que no la recibe (C. Ramos, 2021). Una característica clave de este diseño es que la asignación a los grupos no se realiza de manera aleatoria En este caso, se evaluó el rendimiento de un sistema de reconocimiento facial en el control biométrico de los postulantes al examen extraordinario de la Universidad Nacional del Altiplano Puno en 2024.

Dado que no se realizó una asignación aleatoria, los grupos se formaron con postulantes ya existentes. El objetivo principal de este diseño es medir el impacto de la implementación del sistema de reconocimiento facial en tres dimensiones: precisión, tiempo de respuesta y nivel de seguridad. Los resultados obtenidos se compararán con los datos del control biométrico basado en huellas dactilares, utilizados previamente por la universidad.

Diseño corte transversal

Este enfoque implica la recopilación de datos en un solo punto en el tiempo (H. Sánchez et al., 2018). En el presente estudio, se recopilaron datos de postulantes al examen de admisión extraordinario de la Universidad Nacional del Altiplano en el año 2024.

3.4. POBLACIÓN Y MUESTRA

3.4.1. Población

Según (Carrasco, 2005), un conjunto de elementos que se integra para formar un grupo que se relaciona con el área de interés de la investigación. Este grupo no solo abarca los componentes pertinentes, sino que también se configura de manera precisa.

En el presente estudio, la población está compuesta por los 422 postulantes que realizaron el examen de admisión extraordinario en la Universidad Nacional del Altiplano Puno durante el año 2024.

3.4.2. Muestra

Es una parte del grupo de la población para lograr recolectar datos, y que se conceptualiza y delimita con precisión, también debe ser el representativo de la población (Sampieri et al., 2014).

Debido a que la investigación busca evaluar el sistema en condiciones reales, la muestra estuvo compuesta por 100 postulantes seleccionados en el momento de la aplicación del sistema, siguiendo indicaciones de las autoridades responsables del proceso de admisión. Estas autoridades determinaron qué

postulantes pasarían por el control biométrico basado en reconocimiento facial, tomando en cuenta situaciones específicas, como inconvenientes detectados en el control previo por huella dactilar, u otros factores que, a su juicio, requerían una evaluación adicional.

3.4.3. Muestreo

En esta investigación, se empleó un muestreo no probabilístico por conveniencia. Según (Paul Diaz, 2020), esta técnica selecciona a los participantes según la accesibilidad, la aproximación y las circunstancias del investigador, mientras que (Osvaldo Hernández, 2021) señala que permite determinar de manera arbitraria cuántos participantes serán incluidos en el estudio.

Este enfoque de muestreo fue necesario debido a las condiciones operativas del examen de admisión extraordinario y a la naturaleza aplicada de la investigación, donde el investigador no tuvo control directo sobre la selección de los participantes.

3.5. MATERIALES Y EQUIPOS UTILIZADOS

3.5.1. Desarrollo del sistema

En el desarrollo de este proyecto, se utilizó una diversidad de materiales y equipos técnicos con el fin de implementar el control biométrico durante el examen extraordinario de admisión, haciendo uso de la tecnología de reconocimiento facial. A continuación, se describen en detalle los materiales y equipos empleados.

Infraestructura:

- Espacios de prueba: Se estableció un área específica para el desarrollo del sistema.
- Espacios de prueba: Inicialmente, las pruebas se realizaron en un entorno controlado. Posteriormente, se llevaron a cabo el día del examen en la Escuela Profesional de Educación, donde se realizó el examen extraordinario.

Equipos tecnológicos:

- Laptop: Se empleó una laptop con procesador Ryzen 5 3200U, 8 GB de RAM, gráficos integrados y pantalla de 14 pulgadas.
- Cámara: Se utilizó una cámara HP de 720p para la captura de imágenes faciales

Tecnología y software:

- Python: Se trabajó con Python 3.9, aprovechando las bibliotecas como OpenCV, Tkinter, Face_recognition, entre otros para el desarrollo del sistema.
- Datos: Se utilizó un archivo csv para almacenar los datos de los postulantes.
- Windows 10: Se utilizó el sistema operativo Windows 10 para asegurar la compatibilidad con las herramientas y recursos necesarios en el proyecto.

Recursos humanos:

- Investigador: El investigador lideró la recopilación de datos, supervisó las pruebas y analizó los resultados.
- Desarrollador de sistemas: Responsable de la implementación y desarrollo de los algoritmos de reconocimiento facial, asegurando su correcto funcionamiento y optimización dentro del sistema.

3.6. TÉCNICAS E INSTRUMENTOS UTILIZADOS PARA LA RECOLECCIÓN DE DATOS

Los métodos para la recopilación de datos que se utilizaron fueron los siguientes.

3.6.1. Solicitud de información

Se solicitó a la Dirección de Admisión de la Universidad Nacional del Altiplano de Puno la información de los postulantes, con el objetivo de evaluar el sistema de reconocimiento facial en el control biométrico. Esta solicitud se dividió en dos fases.

Fase de desarrollo: Se obtuvo la información de 5000 imágenes y datos de postulantes anteriores, utilizados para el entrenamiento y desarrollo del sistema.

Fase de pruebas: La información se recopiló el día del examen de admisión extraordinario, incluyendo los datos de los 422 postulantes.

Los instrumentos utilizados en esta técnica fueron:

Formato de solicitud de datos: Documento oficial presentado a la Dirección de Admisión para obtener la información.

Base de datos del sistema de admisión: La información fue proporcionada en formato digital (imágenes y datos personales).

La información solicitada incluyó:

- Documento Nacional de Identidad (DNI)
- Apellidos
- Nombres

- Escuela Profesional a la que postulan
- Imagen del rostro

Esta información fue utilizada para implementar y evaluar la efectividad del sistema de reconocimiento facial. A continuación, se presenta una tabla resumen.

Tabla 5

Resumen de los datos obtenidos para el estudio

Información de los postulantes	Cantidad fase de desarrollo	Cantidad día examen
Documento Nacional de Identidad (DNI)	5000	422
Apellidos	5000	422
Nombres	5000	422
Escuela Profesional a la cual postula	5000	422
Imagen del rostro	5000	422

3.6.2. Observación directa

(Medina et. al, 2023) nos dice que la observación es un método fundamental de investigación que involucra el registro y análisis del comportamiento y las acciones del objeto de estudio, proporcionando información detallada y objetiva sobre sujetos y situaciones. En este estudio, la observación directa se utilizó para analizar la interacción de los usuarios con el sistema de reconocimiento facial durante el examen de admisión.

Instrumentos utilizados

- **Medición de la precisión**

Para calcular la precisión en el control biométrico, se adaptó la ficha de registro (Anexo 4) elaborada por (Yañez, 2019) la cual fue validada por un panel de tres expertos.

- **Medición del tiempo de respuesta**

Para medir el tiempo requerido para llevar a cabo el control biométrico, se adaptó la ficha de medición de tiempo (Anexo 5) desarrollada por (Alejo, 2021), la cual fue validada por un panel de tres expertos.

- **Medición de la seguridad**

Para evaluar el nivel de seguridad del sistema desarrollado en este proyecto de investigación se adaptó la ficha de evaluación de seguridad (Anexo 6) que nos describe (Valdivieso, 2016), la cual cuenta con la validación de expertos.

La observación permitió obtener datos cuantitativos sobre el rendimiento del sistema en un entorno real.

3.6.3. Revisión de documentos, registros y materiales

Según (Alegría, 2020) nos dice que estos métodos de recolección de datos permiten comprender el fenómeno central de estudio y son útiles para conocer los antecedentes del entorno, las experiencias, vivencias y el funcionamiento cotidiano de las situaciones. En este estudio se realizó una revisión del Reglamento General de Admisión mediante un análisis documental para obtener un mejor entendimiento de los procesos de admisión.

3.6.4. Cuestionario

De acuerdo con (DINA & FLOR, 2019) este instrumento facilita la recolección de datos directamente de los trabajadores, a través de la respuesta a una serie de preguntas relacionadas con las variables de estudio. Se aplicó un cuestionario a los trabajadores de la Dirección de Admisión, encargados del control biométrico y otras tareas relacionadas.

3.7. MÉTODO PARA EL TRATAMIENTO DE DATOS

En este estudio, se llevaron a cabo los siguientes cálculos para el tratamiento de datos.

3.7.1. Prueba de proporciones

Estas pruebas se caracterizan por utilizar una estadística de prueba que sigue una distribución binomial, donde cada observación puede resultar en un "éxito" o un "fracaso" (Alondra Sierra, 2024). Este enfoque es fundamental para evaluar la relación entre variables categóricas y permite determinar la significancia de los resultados obtenidos.

Fórmula para la prueba de proporciones

$$Z = \frac{\hat{p} - p_0}{\sqrt{\frac{p_0(1 - p_0)}{n}}}$$

Donde:

- $\hat{p}$ = proporción muestral
- p_0 = proporción poblacional
- n = tamaño de la muestra

3.7.2. Prueba t para muestras pareadas

Se aplicó una prueba t para muestras pareadas, como describe (Shier, 2024). Este método es común en investigaciones experimentales que analizan una variable dependiente antes y después de una intervención. En este estudio, se evaluó el tiempo requerido para el control biométrico, comparando los resultados antes y después de la implementación del sistema de reconocimiento facial. Este análisis proporciona una visión clara de la efectividad de la nueva tecnología en el proceso de verificación de identidad.

Fórmula para la prueba t en muestras pareadas

$$t = \frac{\bar{X}_D}{\frac{S_D}{\sqrt{n}}}$$

Donde:

- $\bar{X}_D$= media de las diferencias
- S_D = la desviación estándar de las diferencias
- n = número de pares de observaciones.

CAPÍTULO IV

RESULTADOS Y DISCUSIÓN

4.1. DESARROLLO DEL SISTEMA INFORMÁTICO CON RECONOCIMIENTO FACIAL

Para el desarrollo del sistema de reconocimiento facial, se utilizó la metodología XP (*Extreme Programming*), que es ampliamente empleada en el desarrollo de aplicaciones de escritorio. Esta metodología se adaptó de manera óptima a los requerimientos del presente trabajo de investigación. El proceso se llevó a cabo siguiendo las fases establecidas por la metodología XP, asegurando un enfoque ágil y flexible en el diseño y la implementación del sistema. Se aplicaron las siguientes fases para el desarrollo del sistema.

4.1.1. Fase de planificación

En esta fase de la investigación, el usuario cumple un rol fundamental, su función es dar a conocer los requerimientos necesarios del sistema y estos se presentan a continuación

4.1.1.1. Usuarios que intervienen en el sistema

A continuación, se identifican y definen los principales usuarios que estarán involucrados en el sistema.

Tabla 6

Usuarios que intervienen en el sistema

Usuario	Descripción
Encargado del control biométrico	Es la persona que se encargara de realizar el control biométrico a cada uno de los postulantes al proceso de admisión.
Postulante	Persona que está postulando a la universidad, a la cual se le pasará control biométrico facial.

4.1.1.2. Historias de usuario

Las historias de usuario fueron fundamentales para dar a conocer las expectativas del usuario final.

Tabla 7

Historia de usuario desarrollo del reconocimiento facial

Nombre de historia: Desarrollo del reconocimiento facial			
Indicador	HU01	**Prioridad**	Alta
Descripción	El sistema debe capturar una imagen facial y analizar el rostro para determinar si está registrado en la base de datos. Basado en el análisis, el sistema debe proporcionar un veredicto sobre la coincidencia o falta de coincidencia del rostro.		

Tabla 8.

Historia de usuario desarrollo del sistema

Nombre de historia: Desarrollo del sistema			
Indicador	HU02	**Prioridad**	Alta
Descripción	Desarrollar y elaborar las diferentes vistas y perspectivas que compondrán la interfaz de usuario de la aplicación para garantizar una experiencia de usuario clara y funcional.		

Tabla 9

Historia de usuario incorporar el reconocimiento facial en el sistema

Nombre de historia: Incorporar el reconocimiento facial en el sistema			
Indicador	HU03	**Prioridad**	Alta
Descripción	Integrar la funcionalidad de reconocimiento facial en el sistema.		

Tabla 10

Historia de usuario capturar imágenes en tiempo real

Nombre de historia: Capturar imágenes en tiempo real			
Indicador	HU04	**Prioridad**	Alta
Descripción	Reconocer y comparar rostros en tiempo real.		

Tabla 11

Historia de usuario mostrar datos del postulante

Nombre de historia: Mostrar datos del postulante			
Indicador	HU05	**Prioridad**	Alta
Descripción	El sistema debe verificar si el rostro capturado está registrado en la base de datos. Si hay una coincidencia, debe mostrar la identificación del postulante y los datos asociados. En caso contrario, el sistema debe informar que la identificación no fue posible.		

Tabla 12

Historia de usuario generación de reportes

Nombre de historia: Generación de reportes			
Indicador	HU06	**Prioridad**	Alta
Descripción	El sistema debe generar reportes de los postulantes reconocidos por el sistema, con la hora, fecha exacta.		

Tabla 13

Historia de usuario sistema local

Nombre de historia: Sistema local			
Indicador	HU07	**Prioridad**	Alta
Descripción	El sistema debe funcionar de manera completamente local, sin necesidad de acceso a la red ni a otras computadoras.		

4.1.1.3. Estimación de historias de usuario

A continuación, se detalla el tiempo estimado para completar cada historia de usuario.

Tabla 14

Estimación del tiempo en las historias de usuario

Historia de Usuario	**Denominación**	**Semanas estimadas**	**Días estimados**
HU01	Desarrollo del reconocimiento facial	3	12
HU02	Desarrollo del sistema	3	12
HU03	Incorporar el reconocimiento facial en el sistema	2	8
HU04	Capturar imágenes en tiempo real	2	4

Historia de Usuario	Denominación	Semanas estimadas	Días estimados
HU05	Mostrar datos del postulante	2	4
HU06	Generar reportes	1	3
HU07	Sistema local	1	1
Tiempo total estimado		14	44

4.1.2. Fase de diseño

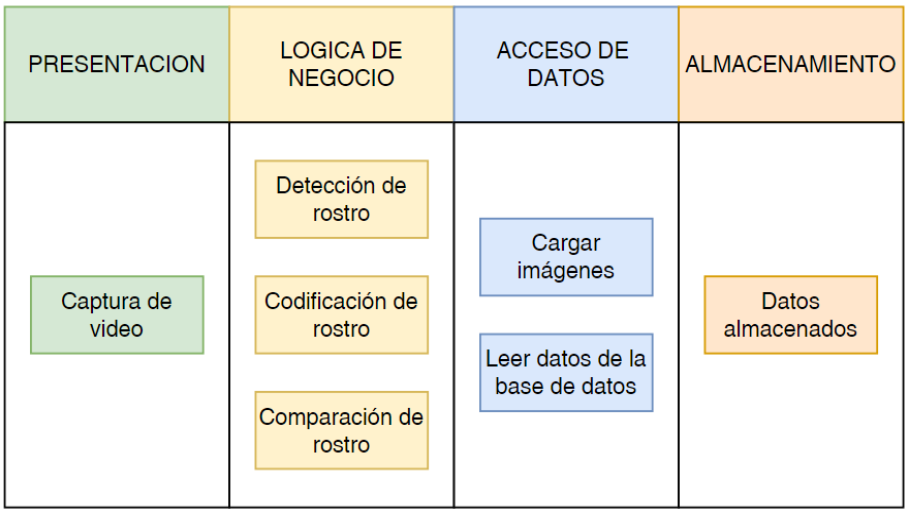
En esta etapa, el objetivo es desarrollar una estructura de software que funcione de manera eficiente y cumpla con los requisitos previamente definidos.

4.1.2.1. Arquitectura del sistema

Para el desarrollo del sistema de reconocimiento facial, se empleó una arquitectura en capas. Según se indica en el documento de (Acosta et al., 2006), una arquitectura de una sola capa es un programa sencillo que no requiere acceso a la red durante su ejecución. Esta característica resulta fundamental, ya que cumple con uno de los requisitos establecidos por el cliente. Según lo mencionado por (Emmanuel Palacio, 2023) en su artículo sobre las ventajas de la arquitectura en capas, este enfoque permite que los cambios en la base de datos o en archivos de texto utilizados como base de datos no afecten el producto final. Para su implementación, se utilizó el siguiente diagrama como referencia.

Figura 20

Diagrama de arquitectura de software



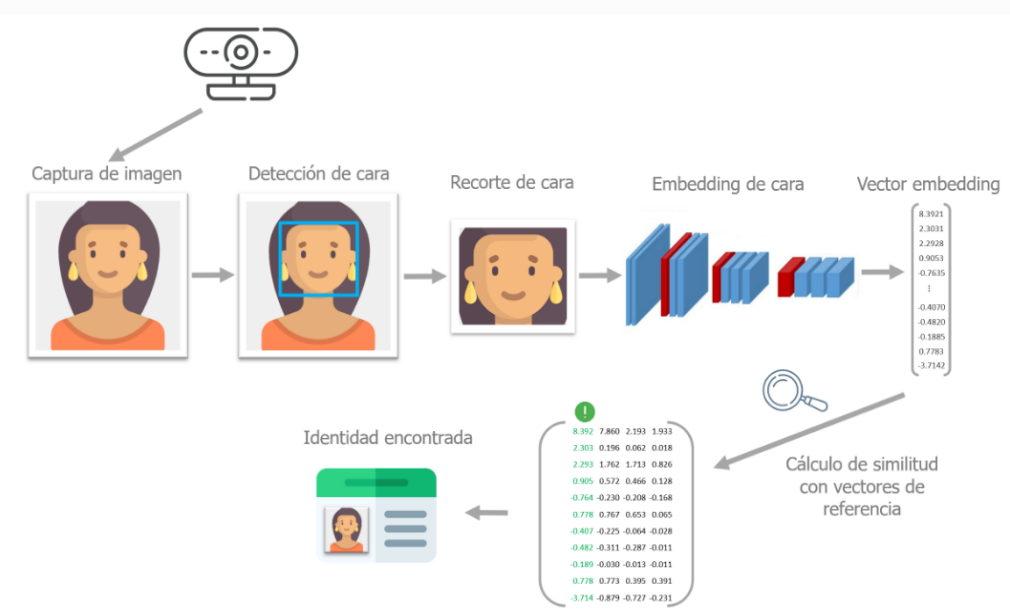
Interpretación: El sistema de reconocimiento facial se organiza en cuatro capas. La capa de presentación se encarga de capturar video en tiempo real y mostrar las coincidencias de rostros detectados a través de la interfaz. La capa de lógica de negocio utiliza la biblioteca *face_recognition* para detectar y codificar los rostros, comparándolos con los previamente almacenados para identificar coincidencias. La capa de acceso a datos carga las imágenes desde una carpeta y lee la información de los postulantes desde un archivo CSV. Finalmente, la capa de almacenamiento guarda tanto las imágenes como los datos en archivos CSV, garantizando el acceso adecuado a los recursos necesarios.

4.1.2.2. Diseño del reconocimiento facial

A continuación, se presenta un diagrama que ilustra el proceso de reconocimiento facial, detallando los componentes clave y su interacción.

Figura 21

Proceso de reconocimiento facial



Fuente: (Amat, 2021)

Interpretación: El diagrama anterior ilustra el proceso de reconocimiento facial utilizado en el examen. El primer paso consiste en capturar la imagen del postulante. A continuación, el sistema detecta el rostro, recorta la imagen para centrarse únicamente en el rostro del postulante y realiza el *embedding* facial, que implica vectorizar la imagen. Posteriormente, se calcula la similitud entre el vector de la imagen actual y los vectores de referencia previamente almacenados. Finalmente, se determina si el postulante es reconocido o no.

4.1.2.3. Diseño de la interfaz del sistema

El diseño se centra en crear una arquitectura robusta y adaptable que garantice el rendimiento óptimo del sistema. Para el diseño de la interfaz del sistema, se adoptó el siguiente modelo, que define la disposición y funcionalidad de los elementos de la interfaz de usuario.

Figura 22

Prototipo de la interfaz del sistema

Interpretación: Como se observa en la imagen anterior, el prototipo del sistema está diseñado para cumplir con los requisitos establecidos por el usuario. En el lado izquierdo de la interfaz, se muestran los datos de los postulantes. La pantalla incluye una visualización en tiempo real de la cámara para la captura de imágenes durante el examen, así como una foto de referencia tomada en el momento de la inscripción. Además, se ha incorporado un cuadro de búsqueda por DNI para prevenir cualquier posible incidente.

4.1.3. Fase de desarrollo

4.1.3.1. Tecnologías empleadas para el desarrollo

El desarrollo de este sistema con reconocimiento facial para el examen de admisión utilizó diversas tecnologías avanzadas para su creación, las cuales se detalla a continuación.

- **Python:** Utilizado como lenguaje de programación principal, es elegido por su flexibilidad y la amplia gama de bibliotecas disponibles.
- **face_recognition:** Algoritmo utilizado para la identificación de **rostros** mediante el análisis de características geométricas.
- **OpenCV:** Biblioteca de visión por computadora que se centra en el procesamiento de **imágenes** y videos en tiempo real, permite gestionar la captura y el análisis de imágenes.
- **Dlib:** Esta biblioteca **proporciona** herramientas para la detección y extracción de puntos faciales, identificando aproximadamente 68 puntos clave en el rostro.
- **NumPy:** Una biblioteca fundamental para el manejo de operaciones matemáticas y el procesamiento de arrays.
- **Tkinter:** Esta librería proporciona herramientas para construir interfaces gráficas de usuario (GUI).
- **ProcessPoolExecutor:** Permite ejecutar tareas en paralelo utilizando múltiples procesos. Esto es especialmente útil cuando tienes tareas que son CPU intensivas y pueden beneficiarse de la ejecución en múltiples núcleos del procesador.
- **JSON:** Es un formato de intercambio de datos ligero que resulta sencillo de leer y escribir para los seres humanos, y que las máquinas pueden analizar y generar con facilidad.
- **auto-py-to-exe:** Convierte scripts de Python en archivos ejecutables para Windows.

4.1.3.2. Distribución de las carpetas

Para el desarrollo del sistema se siguió el siguiente diagrama de distribución de carpetas.

Figura 23

Distribución de las carpetas del sistema

```
RECONOCIMIENTO_FACIAL_UNAP/
│
├── data/                              # Carpeta principal para almacenar datos
│   ├── rostros_vectorizados/          # Subcarpeta para almacenar los rostros vectorizados
│   │   └── rostros_vectorizados.json  # Archivo JSON con los rostros vectorizados
│   └── estudiantes/                   # Subcarpeta con los datos de los estudiantes
│       └── datos.xlsx                 # Archivo Excel con los datos de los estudiantes
│
├── scripts/                           # Carpeta para scripts de procesamiento
│   ├── crear_base_datos.py            # Script para vectorizar los rostros
│   └── sistema_reconocimiento.py      # Script principal para realizar el reconocimiento facial
│
├── reports/                           # Carpeta para almacenar los reportes generados
│   └── reporte.xlsx                   # Archivo Excel con los reportes del sistema
│
├── README.md                          # Archivo de documentación del proyecto
```

Interpretación: La carpeta raíz contiene dos subcarpetas principales una que almacena las imágenes de los rostros de los estudiantes y otra carpeta llamada scripts, que guarda los scripts de Python. El script crear_base_datos.py procesa y prepara las imágenes para la base de datos, mientras que sistema_reconocimiento.py realiza el reconocimiento facial en tiempo real. Además, se incluye un archivo README.md para documentar el proyecto y proporcionar instrucciones de uso. Esta disposición facilita el mantenimiento, la escalabilidad y la colaboración en el proyecto.

4.1.3.3. Creación de la base de datos

Con los datos proporcionados por la Dirección de Admisión, transferimos la información a nuestra carpeta de rostros, que sirve como nuestra base de datos para la comparación con los rostros a reconocer. El

sistema emplea la vectorización para comparar los rostros de nuestra base de datos con los rostros detectados por la cámara. En esta etapa, vectorizamos las imágenes utilizando tecnología de multiprocesos para optimizar y agilizar el proceso.

Figura 24

Código para la creación de la base de datos de los rostros

```python
import cv2
import os
import face_recognition
import numpy as np
from concurrent.futures import ProcessPoolExecutor
import json

def cargar_y_codificar(image_path):
    imgdb = cv2.imread(image_path)
    img = cv2.cvtColor(imgdb, cv2.COLOR_BGR2RGB)

    # Reducir el tamaño de la imagen (ajusta el valor según sea necesario)
    img = cv2.resize(img, (0, 0), fx=0.5, fy=0.5)

    # Obtener las codificaciones de los rostros
    face_encodings = face_recognition.face_encodings(img, model="cnn")

    if face_encodings:
        # Si hay al menos un rostro, devolver la codificación del primer rostro
        cod = face_encodings[0].tolist()
        return cod
    else:
        # Si no se encontraron rostros en la imagen, puedes manejar este caso de alguna manera
        print("-----------------------------------------------")
        print(image_path)
        print("-----------------------------------------------")
        return None

if __name__ == "__main__":
    # accedemos a la carpeta
    path = "bd_Images500"  # Nombre de la carpeta de nuestras imgs
    images = [f"{path}/{i}" for i in os.listdir(path)]

    with ProcessPoolExecutor() as executor:
        #lista_cod = list(executor.map(cargar_y_codificar, images))
        lista_cod = list(executor.map(cargar_y_codificar, images, chunksize=10))

    # Filtrar None (imágenes sin rostros detectados)
    lista_cod = [cod for cod in lista_cod if cod is not None]

    with open('exportacion_Images500.json', 'w') as archivo:
        json.dump(lista_cod, archivo)
```

Interpretación: El código anterior procesa las imágenes de nuestra base de datos reduciendo su tamaño para facilitar el análisis y convirtiéndolas a un formato adecuado para el reconocimiento facial.

Luego, utiliza una herramienta para detectar y codificar los rostros en cada imagen. Para mejorar la eficiencia, procesa varias imágenes en paralelo. Al finalizar, filtra las imágenes sin rostros detectados y guarda las codificaciones en un archivo JSON, que se usará posteriormente en nuestra aplicación de reconocimiento facial.

4.1.3.4. Desarrollo del reconocimiento facial

Para desarrollar el reconocimiento facial, se emplearon las tecnologías *dlib* y *face_recognition*. La tecnología dlib se utilizó para la detección y alineación de rostros, así como para la extracción de características faciales precisas, mientras que *face_recognition* se encargó de comparar estas características y realizar la identificación de los rostros mediante codificaciones faciales.

Figura 25

Código del reconocimiento facial

```
def actualizar_video():
    ret, frame = vid.read()
    if ret:

        # Buscamos los rostros
        faces = face_recognition.face_locations(frame)
        facecod = face_recognition.face_encodings(frame, faces)

        for facecod, faceloc in zip(facecod, faces):

            # Comparamos rostros de DB con rostro en tiempo real
            comparacion = face_recognition.compare_faces(rostroscod, facecod)

            #calculamos la similitud
            similitud = face_recognition.face_distance(rostroscod, facecod)

            # Buscamos el valor mas bajo
            min = np.argmin(similitud)

            if comparacion[min]:

                nombre = clases[min].upper() ## MAYUSCULAS
                print(nombre)
                yi, xf, yf, xi = faceloc
                yi, xf, yf, xi = yi+4, xf+4, yf+4, xi+4

                indice = comparacion.index(True)
                global comp1
                r = None
                g = None
                b = None
                if comp1 != indice:
                    r = random.randrange(0,255,50)
                    g = random.randrange(0,255,50)
                    b = random.randrange(0,255,50)

                    comp1 = indice

                if comp1 == indice:
                    # ------------ Capturamos el rostro y lo mostramos en captura_img
                    rostro_capturado = frame
                    rostro_capturado = cv2.cvtColor(rostro_capturado, cv2.COLOR_BGR2RGB)
                    rostro_capturado = Image.fromarray(rostro_capturado)
                    rostro_capturado = rostro_capturado.resize((640, 480), Image.ANTIALIAS)
                    rostro_capturado_tk = ImageTk.PhotoImage(rostro_capturado)

                    # Mostramos el rostro en captura_img
                    rostro_reconocido.configure(image=rostro_capturado_tk)
                    rostro_reconocido.image = rostro_capturado_tk

                    # ----------------------- MOSTRAR DATOS EN PANTALLA (VIDEO) ----------------------------------------------
                    cv2.rectangle(frame, (faceloc[3], faceloc[0]), (faceloc[1], faceloc[2]), (0, 255, 0), 2) # MOSTRAR RECTANGULO VERDE

                    buscar_img_en_bd(nombre)
                    hora_entrada(nombre)
                else:
                    #Extraemos coordenadas
                    yi, xf, yf, xi = faceloc
                    yi, xf, yf, xi = yi+4, xf+4, yf+4, xi+4
                    cv2.rectangle(frame, (faceloc[3], faceloc[0]), (faceloc[1], faceloc[2]), (0, 255, 0), 2) # MOSTRAR RECTANGULO VERDE
                    cv2.putText(frame, "DESCONOCIDO", (xi+6, yf-6), cv2.FONT_HERSHEY_SIMPLEX, 1, (0, 0, 255), 2) # MOSTRAR DNI

        actualizar_imagen(frame)
        detener_captura.id_captura = ventana.after(10, actualizar_video)
```

Interpretación: El código desarrollado para el reconocimiento facial emplea las librerías *dlib* y *face_recognition* para identificar rostros en tiempo real desde un video. La función actualizar video lee el *frame* del video, detecta y codifica los rostros presentes, luego los compara con una base de datos de rostros predefinidos. Calcula la similitud entre el rostro detectado y los rostros almacenados, y selecciona el más cercano para

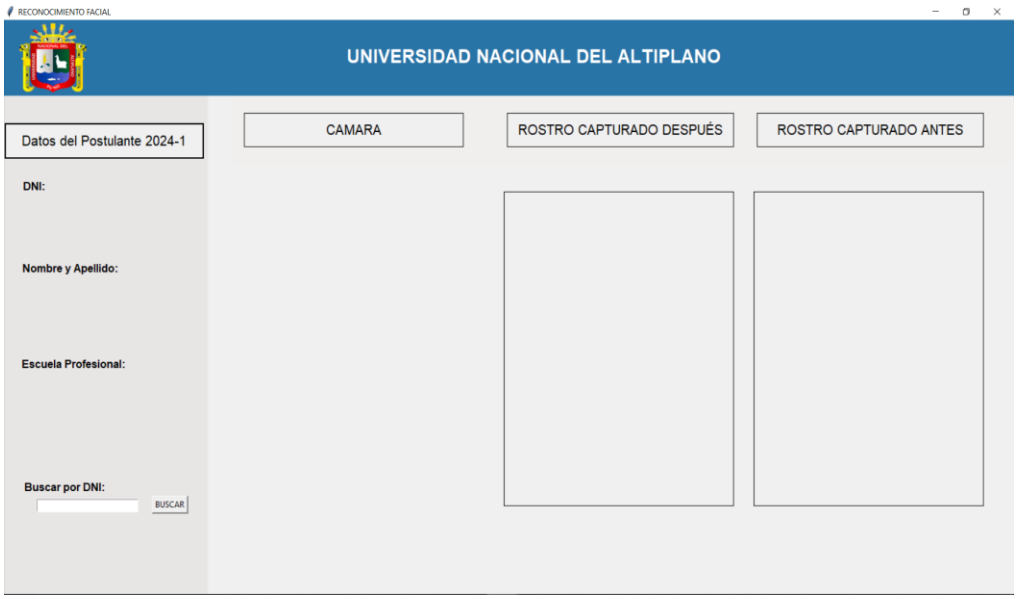
realizar la identificación. Si se encuentra una coincidencia, muestra el nombre de la persona en pantalla, resalta el rostro con un rectángulo verde en el video, y captura una imagen del rostro. Si no se identifica a la persona, marca el rostro como "DESCONOCIDO". El sistema también actualiza la imagen en la interfaz de usuario y gestiona el ciclo de captura de video.

4.1.3.5. Desarrollo de la interfaz del sistema

Para desarrollar la interfaz del sistema, se empleó Tkinter, lo cual permitió cumplir con las especificaciones proporcionadas por el usuario.

Figura 26

Desarrollo de la interfaz del sistema



4.1.4. Fase de pruebas

Después de haber concluido el desarrollo del sistema con reconocimiento facial, se procedió a hacer las pruebas respectivas. En este sistema, se llevaron a

cabo pruebas de validación de usuario y validación operativa para asegurar que el sistema funcione correctamente y cumpla con los requisitos establecidos.

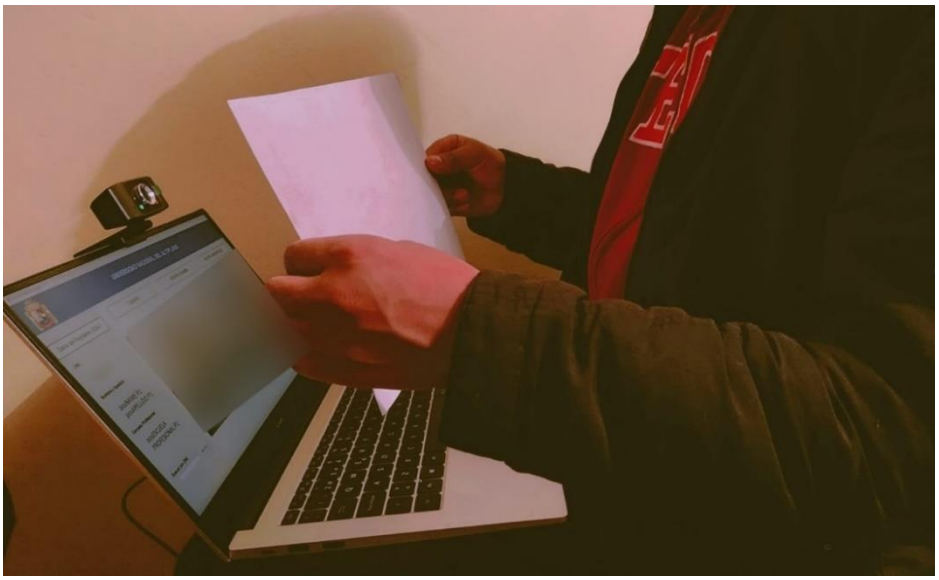
4.1.4.1. Pruebas de refinamiento

Durante estas pruebas, se evaluaron distintos valores de *tolerance* o *threshold* para encontrar el umbral óptimo. Los resultados obtenidos fueron analizados exhaustivamente, lo que permitió ajustar el sistema y mejorar su capacidad para identificar correctamente a las personas en el conjunto de imágenes.

a) Reconocimiento por medio de fotos

Figura 27

Pruebas con las fotos de los postulantes



Interpretación: En esta prueba, se utilizaron las mismas imágenes de los postulantes debido a la imposibilidad de contactar a los postulantes directamente. Como alternativa, se llevaron a cabo las pruebas utilizando las imágenes impresas de los postulantes.

Tabla 15

Pruebas con fotos para los distintos valores de threshold

N	Precisión con Valor de *threshold*				
	0.7	0.6	0.5	0.4	0.3
1	0.75	0.80	0.88	0.94	0.82

Interpretación: Después de realizar todas las pruebas necesarias, el umbral de 0.7 arrojó resultados poco precisos, ya que el sistema identificaba erróneamente a personas, es decir, fallaba al determinar si alguien era o no reconocido correctamente. Por otro lado, con un umbral de 0.3, el sistema se volvió más estricto al comparar, pero factores como la iluminación o pequeñas variaciones en las imágenes provocaban errores en los resultados. Por lo tanto, podemos concluir que el umbral que ofreció los mejores resultados fue el de 0.4, con una precisión del 0.94.

4.1.4.2. Pruebas de validación

Las pruebas de validación se realizan antes de que el programa entre en funcionamiento y debe cumplir con las expectativas del cliente (J. Sánchez, 2015).

a) Pruebas de aceptación de usuario

Con el objetivo de verificar y validar el correcto funcionamiento del sistema de reconocimiento facial en un entorno real, se llevaron a cabo pruebas de aceptación de usuario en entornos controlados. Estas pruebas se realizaron bajo estrictas condiciones supervisadas y contaron con la

participación de empleados de la Dirección de Admisión de la Universidad Nacional del Altiplano Puno, quienes colaboraron en la simulación de los diferentes escenarios a evaluar.

Objetivo de la prueba

El principal objetivo de estas pruebas fue garantizar que el sistema cumpla con los requerimientos especificados, tanto en términos de precisión como de usabilidad, para así asegurar la credibilidad y confiabilidad del sistema.

Escenarios de simulación

Se diseñaron escenarios controlados en los que los empleados de la Dirección de Admisión fueron registrados en la base de datos del sistema con imágenes y datos completos y pusieron a prueba el sistema.

Figura 28

Trabajador de la Dirección de Admisión realizando pruebas de validación del sistema

Tabla 16

Resultados de la aceptación del sistema

Escenario	Descripción	Resultados esperados	Resultados obtenidos
Verificación de identidad	Identificación de empleados registrados en el sistema.	El sistema debe reconocer al empleado correctamente.	De 5 personas, no reconoció a 1.
Tiempo de respuesta	Tiempo que tarda el sistema en procesar la verificación desde la captura del rostro hasta la confirmación.	Inferior a 5 segundos.	2 segundos.
Rechazo de personas no registradas	Intentos de verificación de personas que no están en la base de datos del sistema.	El sistema debe rechazar la verificación con un mensaje de "usuario desconocido"	100% de rechazo.

Interpretación: El sistema de verificación de identidad presentó algunas dificultades durante las pruebas. Aunque reconoció correctamente al 80% de los empleados registrados, falló en 1 de 5 casos debido a problemas con la inclinación de la cámara y la iluminación, lo que sugiere que el sistema es sensible a estos factores. Sin embargo, fue eficiente en cuanto al tiempo de respuesta, procesando las verificaciones en un promedio de 2 segundos, mejorando la expectativa de menos de 5 segundos. Además, rechazó al 100% de las personas no registradas, lo que confirma su eficacia en cuanto a seguridad al impedir accesos no autorizados.

b) Pruebas de validación operativa

La finalidad de las pruebas de validación operativa es asegurar que el sistema esté listo para su uso en un entorno real, comprobando que todas sus funcionalidades clave funcionen correctamente y sin problemas.

Objetivo de la prueba

El objetivo de las pruebas de validación operativa es garantizar que el sistema funcione correctamente de acuerdo con los requisitos establecidos

Escenario de simulación

En estas pruebas, se asegura que el sistema funcione correctamente y que cumpla con los requisitos establecidos, como la generación de reportes. Se verifica la ausencia de problemas y se confirma que todas las funcionalidades requeridas operen según lo esperado.

Figura 29

Validando los reportes y el uso correcto de datos de postulantes

Tabla 17

Resumen de las pruebas de sistemas

HU	Denominación	Resultado esperado	Resultado obtenido
HU01	Desarrollo del reconocimiento facial	Reconocimiento facial creado exitosamente	Exitoso
HU02	Desarrollo del sistema	Sistema de reconocimiento facial creado exitosamente	Exitoso
HU03	Incorporar el reconocimiento facial en el sistema	Incorporación exitosa del reconocimiento facial y el sistema	Exitoso
HU04	Capturar imágenes en tiempo real	Captura exitosa de imágenes en tiempo real	Exitoso
HU05	Mostrar datos del postulante	Se muestra datos exitosamente	Exitoso
HU06	Generar reportes	Se genera reportes exitosamente	Exitoso
HU07	Sistema local	El sistema debe funcionar en una máquina, sin necesidad de conexión a internet.	Exitoso

4.1.5. Fase de lanzamiento

El lanzamiento oficial del sistema de reconocimiento facial se realizó el 23 de febrero de 2024, día del examen de admisión extraordinario de la Universidad Nacional del Altiplano (UNA). Este despliegue se llevó a cabo tras meses de desarrollo y pruebas exhaustivas, asegurando que el sistema cumpliera con todas las normativas de seguridad y protección de datos vigentes en el marco de las regulaciones universitarias y nacionales.

Durante el examen, el uso del sistema fue supervisado rigurosamente por un equipo multidisciplinario, incluyendo representantes de la Dirección de Admisión, autoridades académicas de la UNA, y el personal encargado tanto del examen de admisión como del control biométrico. Estos actores clave se encargaron de monitorear la correcta ejecución del sistema, asegurando que cada postulante fuera identificado de manera precisa y sin interrupciones.

Tras el examen, se recogió retroalimentación de las autoridades universitarias y del personal involucrado, quienes destacaron la eficiencia del sistema y su impacto positivo en la agilidad del proceso de control biométrico. Asimismo, se identificaron áreas de mejora menor que serán abordadas en futuras actualizaciones del sistema para optimizar aún más su rendimiento.

4.2. RESULTADOS CORRESPONDIENTES AL OBJETIVO ESPECÍFICO 01

Objetivo específico 01: Calcular la precisión del sistema informático con reconocimiento facial en el control biométrico del examen extraordinario de la Universidad Nacional del Altiplano Puno en el año 2024.

4.2.1. Descripción

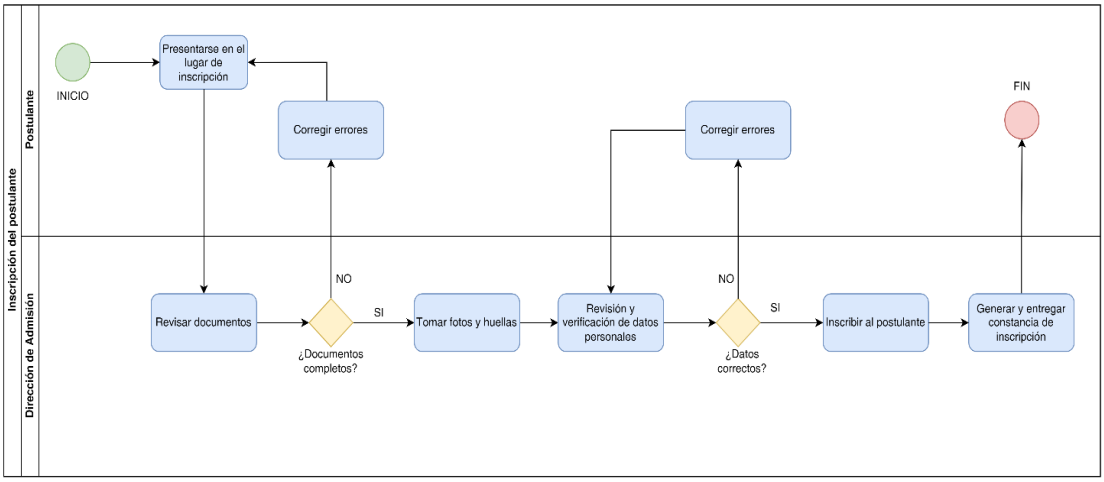
La Universidad Nacional del Altiplano (UNA) ofrece un total de cinco procesos de admisión para aspirantes, diseñados para atender a diversas necesidades y perfiles de estudiantes. Entre estos, dos procesos son realizados a través del Centro Preuniversitario CEPREUNA, dos corresponden al Examen General de Admisión, y el último es el Examen Extraordinario, el cual fue el escenario seleccionado para llevar a cabo el experimento de este estudio.

El Examen Extraordinario es un proceso exclusivo que se realiza solo una vez al año y está dirigido a grupos selectos de postulantes. Entre los participantes se incluyen egresados de educación secundaria que hayan obtenido los primeros puestos en sus respectivas instituciones, deportistas destacados que han representado a su institución o país en competiciones reconocidas, y profesionales en formación que desean realizar traslados internos o externos hacia nuevas carreras. Asimismo, este proceso es una oportunidad para personas tituladas que buscan cursar una segunda carrera o especialización dentro de esta casa superior de estudios.

Para el proceso de admisión extraordinario 2024-I, se presentaron un total de 422 postulantes en las diversas modalidades previamente mencionadas. La Universidad Nacional del Altiplano ofreció 93 vacantes para este proceso, según lo establecido en el reglamento general de admisión 2024. Para este proceso los postulantes siguieron una serie de pasos, los cuales se detallan en el siguiente gráfico.

Figura 30

Diagrama de procesos del objetivo 1



Interpretación: El gráfico anterior ilustra el proceso de inscripción que debe seguir el postulante. Como primer paso, el postulante debe presentarse personalmente en el lugar de inscripción, el cual, para el proceso de admisión extraordinario 2024-I, se ubicó en el edificio de 15 pisos. A continuación, la oficina encargada procede con la revisión de los documentos, la toma de huellas dactilares y captura del rostro del postulante, para después realizar la verificación de los datos personales. En caso de que se detecten errores en alguno de estos pasos, el postulante deberá corregirlos antes de continuar. Finalmente, se realiza la inscripción formal y se entrega al postulante la constancia de inscripción, completando así el proceso. Este flujo garantiza que toda la información presentada sea precisa y que el postulante cumpla con los requisitos establecidos por la universidad.

Una vez comprendido el proceso de inscripción, la Universidad Nacional del Altiplano (UNA) Puno procedió a ofrecer el examen de admisión extraordinario. En esta etapa, se implementó el sistema de reconocimiento facial para asegurar un control biométrico eficiente. El primer paso en esta fase fue la

evaluación de la precisión del sistema desarrollado, un aspecto crítico para garantizar la correcta identificación de los postulantes.

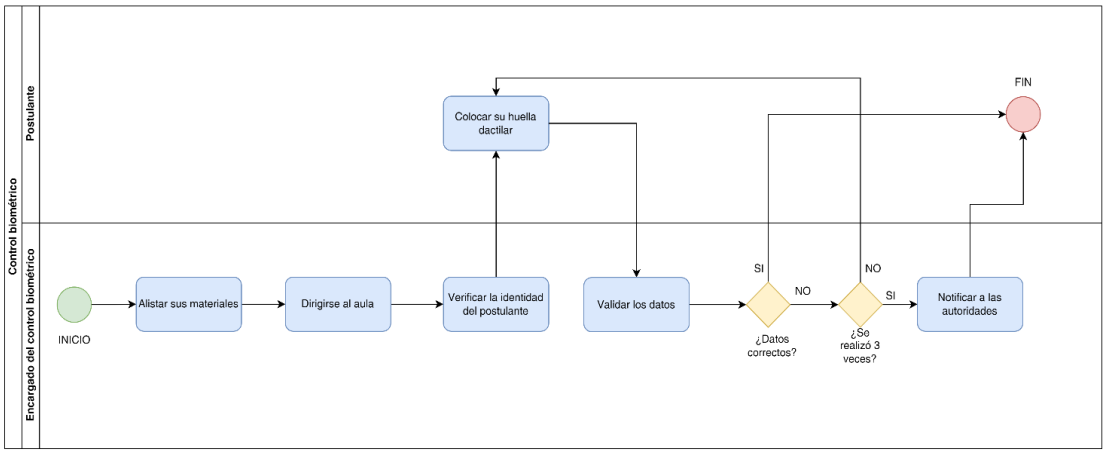
Para realizar esta evaluación, se llevaron a cabo pruebas en condiciones controladas antes y después de la implementación del sistema de reconocimiento facial. El objetivo de este proceso fue medir el rendimiento del sistema al comparar las imágenes capturadas en tiempo real con la base de datos previamente establecida. A través de estas pruebas, se evaluó la capacidad del sistema para identificar correctamente los rostros registrados y para diferenciar aquellos que no coincidían con la información almacenada.

4.2.2. Desarrollo

Para el desarrollo de esta hipótesis, se llevó a cabo una serie de pasos cuidadosamente planificados y ejecutados, luego de haber finalizado la implementación del sistema de reconocimiento facial y revisado los procedimientos involucrados en el proceso de admisión extraordinario seleccionado. Cada uno de estos pasos fue esencial para asegurar que el sistema se ajustara adecuadamente a los requerimientos específicos de la Universidad Nacional del Altiplano Puno y ofreciera un control biométrico fiable. En primer lugar, se realizó una revisión de los procesos y tecnológicos que forman parte del control biométrico en el proceso de admisión extraordinario, los cuales se muestran a continuación.

Figura 31

Proceso de control biométrico por huella digital



Interpretación: El diagrama muestra de manera clara y estructurada el proceso que se sigue para llevar a cabo el control biométrico en los procesos de admisión. En primer lugar, una persona designada de la Dirección de Admisión es responsable de gestionar este control. Esta persona es quien verifica la identidad de los postulantes utilizando un dispositivo biométrico, en este caso, un lector de huellas dactilares. Cada postulante coloca su dedo en el lector, permitiendo que el sistema compare las huellas con la base de datos previamente cargada para confirmar su identidad.

Tabla 18

Equipos utilizados en la verificación biométrica

Equipo	Características	Descripción
Laptop	Intel I7 de 9na, 8 GB de RAM.	La laptop se utiliza como unidad central para ejecutar el sistema de control biométrico, procesar los datos y realizar las verificaciones.
Lector biométrico	Sensor de huellas.	Permite a los postulantes colocar

	sus huellas dactilares para que el sistema las verifique.

Una vez comprendido en detalle el proceso de control biométrico tradicional, se procedió a realizar la medición de este proceso empleando la tecnología de reconocimiento facial, con el objetivo de calcular su precisión en comparación con el método convencional. Para llevar a cabo esta evaluación de manera rigurosa, se siguieron los pasos detallados a continuación.

Medición antes de implementar el sistema (pretest)

Para la recolección de datos en el pretest, se emplearon las fichas de medición previamente definidas en la sección de instrumentos. Este enfoque nos permitió recopilar información precisa sobre el desempeño del sistema de reconocimiento facial en condiciones controladas. A continuación, se presentan los resultados obtenidos.

Tabla 19

Medición de la precisión pretest

Métrica	Valor
Reconocimientos correctos	81
Reconocimientos incorrectos	19
Total	100

De los datos recolectados, se observa que de un total de 100 mediciones, el sistema logró identificar correctamente a 81 postulantes, lo que representa un porcentaje de aciertos del 81%. Este nivel de precisión indica que el control biométrico mediante huellas digitales es efectivo para el reconocimiento de

individuos en el contexto del examen, pero comete errores. Por otro lado, los 19 casos de reconocimiento incorrecto sugieren áreas de mejora en el sistema, ya que es fundamental minimizar la tasa de falsos negativos y positivos para asegurar la fiabilidad del proceso. Este análisis inicial es crucial para implementar mejoras en la tecnología para garantizar experiencias más robustas y precisas durante el examen.

Medición después de implementar el sistema (postest)

Preparación del entorno

Se configuró todo el equipo necesario para llevar a cabo el experimento, tal como se describe en el cuadro siguiente.

Tabla 20

Equipo utilizado para la medición de la precisión

Equipo	Características	Descripción
Laptop	AMD Ryzen 5 3500u, 8 GB de RAM, gráficos integrados.	La laptop se utiliza como unidad central para ejecutar el sistema de reconocimiento facial, procesar los datos y realizar las verificaciones.
Cámara web	720p de resolución.	Permite capturar y detectar el rostro del postulante.

Otra información clave en este proceso fue la base de datos de los postulantes, que incluía tanto las imágenes de sus rostros como todos los datos relacionados con su postulación. Esta base de datos fue esencial para garantizar que el sistema de reconocimiento facial pudiera realizar comparaciones precisas

y eficaces. Con esta información a disposición, se procedió a realizar una serie de pasos para la manipulación y preparación del dataset, asegurando que estuviera correctamente estructurado para el análisis y el funcionamiento del sistema.

Manipulación del dataset

En esta etapa, se realizó la preparación y tratamiento del dataset proporcionado por la Dirección de Admisión. Se obtuvieron dos conjuntos de datos, el primero consistía en una base de datos que contenía información detallada de los postulantes, como nombres, apellidos, y documentos de identidad. El segundo correspondía a una carpeta con las fotografías de los rostros de los candidatos, donde cada imagen estaba claramente etiquetada con el número de DNI del respectivo postulante, facilitando su identificación.

Para garantizar el cumplimiento de los protocolos de seguridad y confidencialidad establecidos por la universidad, ambos archivos fueron entregados minutos antes del inicio del examen de admisión extraordinario. Esto minimizó el riesgo de acceso no autorizado o manipulación de los datos, asegurando así la integridad de la información utilizada en el sistema de reconocimiento facial. Una vez recibido el dataset, se procedió a su integración en el sistema, asegurando que las imágenes y datos personales se almacenaran de forma local y segura.

Creación del dataset

Se llevó a cabo la vectorización de las imágenes proporcionadas por la Dirección de Admisión, lo que consistió en transformar cada fotografía en un conjunto de características numéricas que el sistema de reconocimiento facial pudiera interpretar y procesar eficientemente. Para optimizar este procedimiento,

se utilizó multiprocesamiento, lo que permitió dividir la tarea en múltiples hilos y así acelerar significativamente el proceso de vectorización.

Durante este paso, uno de los principales problemas que se presentó fue el tiempo requerido para generar los *embeddings* de las imágenes. El proceso de creación de la base de datos, que consistía en convertir las imágenes faciales en representaciones numéricas (*embeddings*) para que pudieran ser reconocidas por el sistema, resultó ser más lento de lo anticipado. Esto se debió a la alta demanda computacional que implica el procesamiento de cada imagen, ya que cada una debe ser vectorizada y almacenada en la base de datos del sistema. La demora en este paso afectó temporalmente la eficiencia del flujo de trabajo, lo que puso en evidencia la necesidad de optimizar este proceso o emplear hardware más potente para reducir los tiempos de espera y mejorar la velocidad general del sistema.

Dado que no se disponía de un hardware más potente, se decidió optar por la primera opción la cual consistía en optimizar el proceso de creación de *embeddings* mediante el uso de multiprocesamiento y aprovechamiento de los hilos disponibles en la laptop. Esta solución permitió distribuir la carga de trabajo entre varios núcleos de la CPU, acelerando el procesamiento de las imágenes faciales y reduciendo significativamente el tiempo necesario para generar los *embeddings*. Con esta estrategia, se logró una mejora notable en la eficiencia del sistema sin necesidad de recurrir a equipos más avanzados, optimizando los recursos disponibles.

Tabla 21

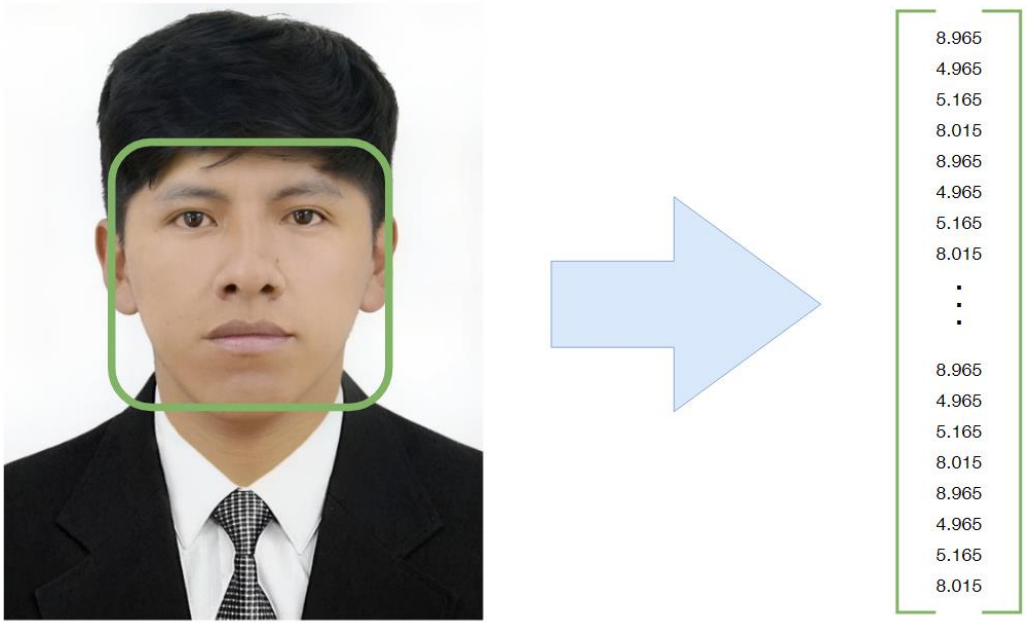
Tiempos para realizar embeddings

N	Descripción	Tiempo total por las 422 imágenes
1	Tiempo tomado antes de usar multiprocesos.	20 minutos
2	Tiempo tomado después de usar multiprocesos.	5 minutos

La implementación de la técnica de multiprocesamiento permitió reducir drásticamente el tiempo necesario para generar los *embeddings* de las 422 imágenes, pasando de 20 minutos a solo 5 minutos. Esta optimización fue clave, considerando el tiempo limitado disponible antes del examen de admisión. Gracias a esta mejora, el sistema pudo procesar un volumen elevado de datos de manera eficiente, asegurando que el *dataset* estuviera listo con la precisión requerida y sin comprometer la calidad ni la seguridad de la información manejada. Además, este enfoque demostró la capacidad del sistema para adaptarse a condiciones de hardware limitadas, manteniendo un rendimiento óptimo.

Figura 32

Vectorización de un rostro



Interpretación: La imagen anterior ilustra el proceso de vectorización aplicado a una fotografía. En primer lugar, el sistema detecta el rostro dentro de la imagen, destacándolo mediante un cuadro verde que delimita su contorno. Esta detección es fundamental, ya que permite al sistema enfocarse únicamente en la región relevante, ignorando el fondo u otras áreas no necesarias. Una vez identificado el rostro, se realiza la vectorización exclusivamente de esa sección. El sistema convierte los rasgos faciales en un conjunto de vectores numéricos que representan características como la distancia entre los ojos, la forma de la mandíbula, y otros patrones únicos. Estos vectores son utilizados posteriormente para realizar comparaciones y reconocer a los postulantes durante el examen, optimizando tanto la precisión como el tiempo de respuesta del sistema.

4.2.3. Evaluación

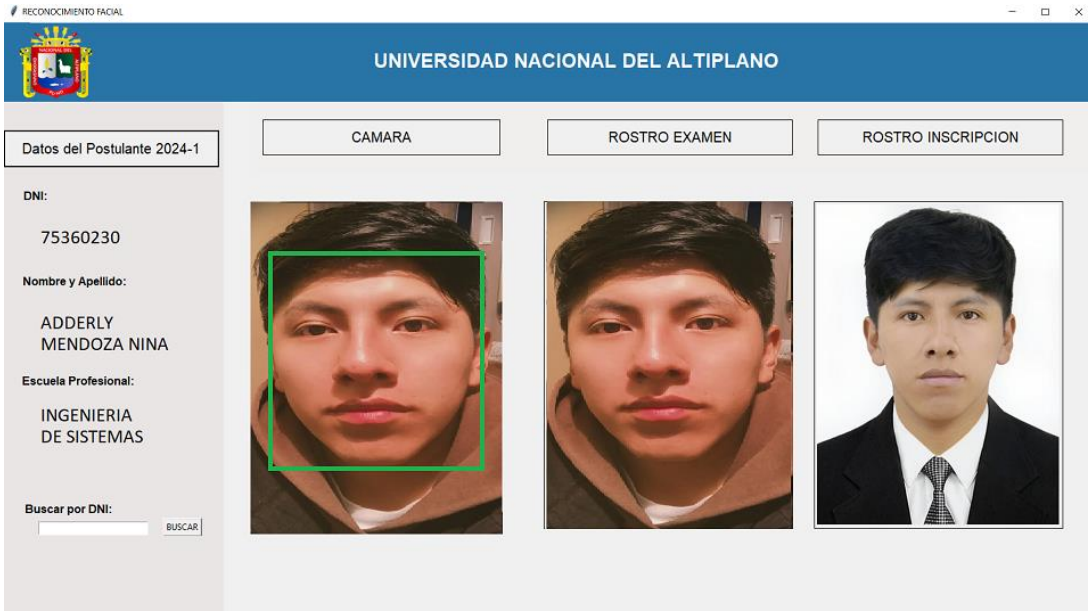
Una vez realizado la preparación del sistema y la creación de la base de datos se procedió a evaluar la precisión del sistema, la cual se describe a continuación.

Durante la fase de desarrollo, las pruebas en entornos controlados lograron una precisión del 93%, lo cual fue un resultado alentador. Posteriormente, esta evaluación se llevó a cabo en un contexto real durante el examen de admisión extraordinario, donde se capturaron imágenes de 100 postulantes pertenecientes a la población previamente definida.

El control biométrico mediante el sistema de reconocimiento facial se implementó pocos minutos después del inicio del examen de admisión, bajo la estricta supervisión de las autoridades universitarias. Estas autoridades seleccionaban de manera aleatoria a los postulantes que debían someterse al control biométrico mediante el sistema de reconocimiento facial, garantizando la imparcialidad y el rigor en el proceso. Este procedimiento no solo buscaba validar la identidad de los estudiantes de manera rápida y eficiente, sino también evaluar la capacidad del sistema en un entorno controlado, pero con la presión del tiempo real de la prueba. El proceso de reconocimiento facial se detalla a continuación, destacando las fases clave que permitieron la verificación de la identidad de los postulantes sin generar interrupciones significativas en el desarrollo del examen.

Figura 33

Reconocimiento facial de una persona



Interpretación: La imagen anterior muestra el proceso de reconocimiento facial realizado por el sistema. Por motivos de seguridad y confidencialidad, no puedo mostrar los resultados obtenidos con los postulantes reales. No obstante, la imagen ilustra claramente cómo el sistema detecta un rostro en tiempo real desde la columna de la cámara, captura la imagen, y la coloca en la columna correspondiente al examen. El sistema compara la imagen capturada con las fotos almacenadas previamente en la base de datos. Si encuentra una coincidencia, muestra la fotografía correspondiente con la que se realizó la comparación. En la parte izquierda de la aplicación, se visualizan los datos personales del postulante reconocido, tales como el nombre, apellido y número de DNI. En los casos en los que el sistema no encuentra una coincidencia en la base de datos, se indica el resultado como "desconocido", lo que garantiza que el sistema identifica tanto a los postulantes reconocidos como a los que no tienen registro en el sistema.

4.2.4. Resultados

Luego de llevar a cabo la evaluación y el control biométrico de los postulantes a través del análisis de sus rostros, se procede a presentar la tabla con los resultados obtenidos, estos resultados se obtuvieron por el sistema y anotando a los postulantes que reconocía. Esta tabla detalla de manera exhaustiva cada uno de los datos recopilados durante el proceso, proporcionando una visión clara y precisa de los resultados.

Tabla 22

Medición de la precisión en el reconocimiento

Nº	Reconocimiento	Nº	Reconocimiento	Nº	Reconocimiento
1	Correcto	35	Correcto	69	Correcto
2	Correcto	36	Correcto	70	Correcto
3	Correcto	37	Correcto	71	Correcto
4	Correcto	38	Correcto	72	Correcto
5	Correcto	39	Correcto	73	Incorrecto
6	Correcto	40	Correcto	74	Correcto
7	Correcto	41	Correcto	75	Correcto
8	Correcto	42	Correcto	76	Correcto
9	Incorrecto	43	Correcto	77	Correcto
10	Correcto	44	Correcto	78	Correcto
11	Correcto	45	Correcto	79	Correcto
12	Correcto	46	Correcto	80	Correcto
13	Correcto	47	Correcto	81	Correcto
14	Correcto	48	Correcto	82	Correcto
15	Correcto	49	Correcto	83	Correcto
16	Correcto	50	Correcto	84	Correcto

17	Correcto	51	Correcto	85	Correcto
18	Correcto	52	Correcto	86	Correcto
19	Correcto	53	Correcto	87	Incorrecto
20	Correcto	54	Correcto	88	Correcto
21	Correcto	55	Correcto	89	Correcto
22	Incorrecto	56	Correcto	90	Correcto
23	Correcto	57	Incorrecto	91	Correcto
24	Correcto	58	Correcto	92	Correcto
25	Correcto	59	Correcto	93	Correcto
26	Correcto	60	Correcto	94	Correcto
27	Correcto	61	Correcto	95	Correcto
28	Correcto	62	Correcto	96	Correcto
29	Correcto	63	Correcto	97	Correcto
30	Incorrecto	64	Correcto	98	Incorrecto
31	Correcto	65	Correcto	99	Correcto
32	Correcto	66	Correcto	100	Correcto
33	Correcto	67	Correcto		
34	Correcto	68	Correcto		
		Total			100

Interpretación: De los 100 postulantes evaluados mediante el sistema de reconocimiento facial, el sistema logró identificar correctamente a 93 de ellos, alcanzando una tasa de éxito del 93%. Los 7 casos en los que el sistema falló se debieron a problemas con la iluminación, lo que afectó la calidad del reconocimiento. Este problema se resolvió ajustando el ángulo de la cámara para mejorar la iluminación y obtener una imagen más clara del postulante. Estos ajustes garantizaron que la precisión del sistema fuera óptima, y se recomienda continuar optimizando las condiciones de captura para minimizar futuros errores.

Según Aquijes Ronny y Ampuero Lizardo (2021), la precisión es la métrica más comúnmente utilizada para evaluar el rendimiento de un sistema de inteligencia artificial, ya que refleja la tasa de respuestas correctas. Esta métrica se expresa generalmente como un porcentaje o una fracción que indica la proporción de predicciones exactas realizadas por el sistema.

Para medir la precisión del sistema de reconocimiento facial desarrollado en este trabajo, se utilizó una matriz de confusión, la cual permite comparar las predicciones realizadas por el sistema con los resultados reales, diferenciando entre verdaderos positivos, verdaderos negativos, falsos positivos y falsos negativos. Esto ofrece una visión más detallada del rendimiento del sistema en términos de su capacidad para reconocer correctamente a los postulantes, así como para identificar posibles errores o falsos reconocimientos. La matriz de confusión se presenta a continuación como parte del análisis de precisión realizado.

Tabla 23

Matriz de confusión del sistema con reconocimiento facial

	Valores reales	
Valores predicción	**Verdaderos positivos**	**Falsos positivos**
	93	7
	Falsos negativos	**Verdaderos negativos**
	0	0

Siguiendo la fórmula propuesta por (Aquijes & Ampuero, 2021)

$$Precisión(P) = \frac{VP}{VP + FP}$$

Donde,

- VP son los verdaderos positivos (predicciones correctas)
- FP son los falsos positivos (predicciones incorrectas).

Aplicando esta fórmula a los resultados obtenidos:

$$Precisión(P) = \frac{VP}{VP + FP} = \frac{93}{93 + 6} = \frac{93}{100} = 0.93$$

En la evaluación realizada con 100 postulantes, el sistema logró una precisión del 93%, reconociendo correctamente a 93 de los postulantes y cometiendo errores en 7 casos. Este resultado demuestra que el sistema fue capaz de identificar correctamente a la gran mayoría de los participantes, con solo un pequeño margen de error, lo que confirma la eficacia del modelo para el reconocimiento facial en el contexto del examen de admisión.

4.2.5. Discusión

Las pruebas del sistema se llevaron a cabo en un entorno realista utilizando los equipos informáticos previamente especificados. A pesar de las limitaciones del hardware, como la capacidad de procesamiento y la resolución de la cámara, el sistema demostró un rendimiento eficiente, lo que permitió evaluar la robustez del algoritmo de reconocimiento facial en condiciones típicas del examen. Estas condiciones incluyeron variaciones en la iluminación, la distancia a la cámara y la calidad de las imágenes capturadas en tiempo real.

Durante la evaluación del sistema de reconocimiento facial para el control biométrico en el examen extraordinario de la Universidad Nacional del Altiplano Puno en 2024, se logró una precisión del 93%, identificando correctamente a 93

de 100 postulantes. Los 7 errores detectados se debieron a problemas de iluminación, que fueron corregidos posteriormente.

Comparando con otros estudios, Mateo Jiménez (2020) alcanzó una precisión del 85% en un sistema de reconocimiento facial para vehículos, lo que es inferior al 93% obtenido en esta investigación. Esto indica que una combinación eficaz de algoritmos y una muestra amplia pueden mejorar la precisión. Velloso Bastos y Barros Esteves (2021) enfatizan la necesidad de evaluar críticamente los sistemas de reconocimiento facial, subrayando la importancia de considerar los impactos en la privacidad y la sociedad. Este enfoque es relevante para la implementación responsable de tecnologías de vigilancia.

Paulo Menino (2022) demostró que las redes neuronales convolucionales profundas ofrecen una mayor precisión en el reconocimiento facial, lo cual es consistente con el enfoque avanzado adoptado en esta investigación para mejorar los resultados, por su parte Reyes Campos et al. (2023) obtuvieron una precisión del 88% en un sistema de reconocimiento facial basado en Redes Neuronales Convolucionales, mostrando la efectividad de esta tecnología en contextos específicos, similar a los resultados obtenidos en nuestra evaluación.

Asana Raymundo (2022) halló que el reconocimiento facial mejoró significativamente la seguridad en una institución educativa, destacando la aplicabilidad de la tecnología en entornos similares al examen extraordinario, mientras que Galindo et al. (2021) lograron una precisión del 93% en la identificación de estudiantes para prevenir la suplantación de identidad en

exámenes finales, evidenciando la robustez y efectividad de los sistemas de reconocimiento facial en contextos educativos.

4.3. RESULTADOS CORRESPONDIENTES AL OBJETIVO ESPECÍFICO 02

Objetivo específico 02: Medir el tiempo de respuesta del sistema informático con reconocimiento facial en el control biométrico del examen extraordinario de la Universidad Nacional del Altiplano Puno en el año 2024.

4.3.1. Descripción

El segundo objetivo específico está centrado en la medición del tiempo de respuesta del sistema informático con reconocimiento facial aplicado al examen extraordinario de la UNA Puno. El tiempo de respuesta se define como el intervalo transcurrido desde el momento en que el postulante se presenta ante la cámara hasta que el sistema identifica su rostro y genera un resultado de coincidencia o no coincidencia en la base de datos. Este proceso es crítico para garantizar una verificación rápida y precisa en un entorno real de examen, donde el flujo constante de postulantes demanda un sistema ágil y eficiente.

Para esta evaluación, se utilizaron los mismos equipos previamente mencionados en el objetivo específico anterior. Estos equipos fueron configurados para simular las condiciones del examen, donde los postulantes debían presentarse frente a la cámara para que el sistema realizara la verificación facial en tiempo real.

4.3.2. Evaluación

Evaluar el tiempo de respuesta del sistema de reconocimiento facial es crucial para medir su rendimiento en condiciones reales, ya que debe ser lo

suficientemente ágil para no interrumpir el flujo del examen de admisión. Un sistema de respuesta ágil es fundamental para asegurar que el proceso de validación se lleve a cabo de manera eficaz, evitando retrasos que puedan impactar negativamente la experiencia de los postulantes y la elaboración del examen de admisión. En este proceso se hizo la medición del antes y el después de aplicar el sistema.

Obtención de los datos de tiempo pretest

Para la recolección de datos relacionados con el tiempo en el pretest, se utilizaron las fichas de medición definidas anteriormente en la sección de instrumentos. Este enfoque nos permitió obtener información precisa y objetiva sobre el rendimiento del sistema tradicional utilizado en los procesos de admisión. La medición del tiempo es fundamental, ya que no solo evalúa la eficiencia del sistema, sino que también impacta directamente en la experiencia del usuario durante el proceso de identificación. A continuación, se presentan los resultados obtenidos.

Tabla 24

Obtención de los datos de tiempo pretest

Métrica	Valor
Total	100 mediciones
Tiempo promedio	10 segundos

Los resultados muestran que, en promedio, el sistema de reconocimiento facial logró completar el proceso de identificación en 10 segundos. Este tiempo promedio es un indicador importante de la velocidad y eficiencia del sistema, lo

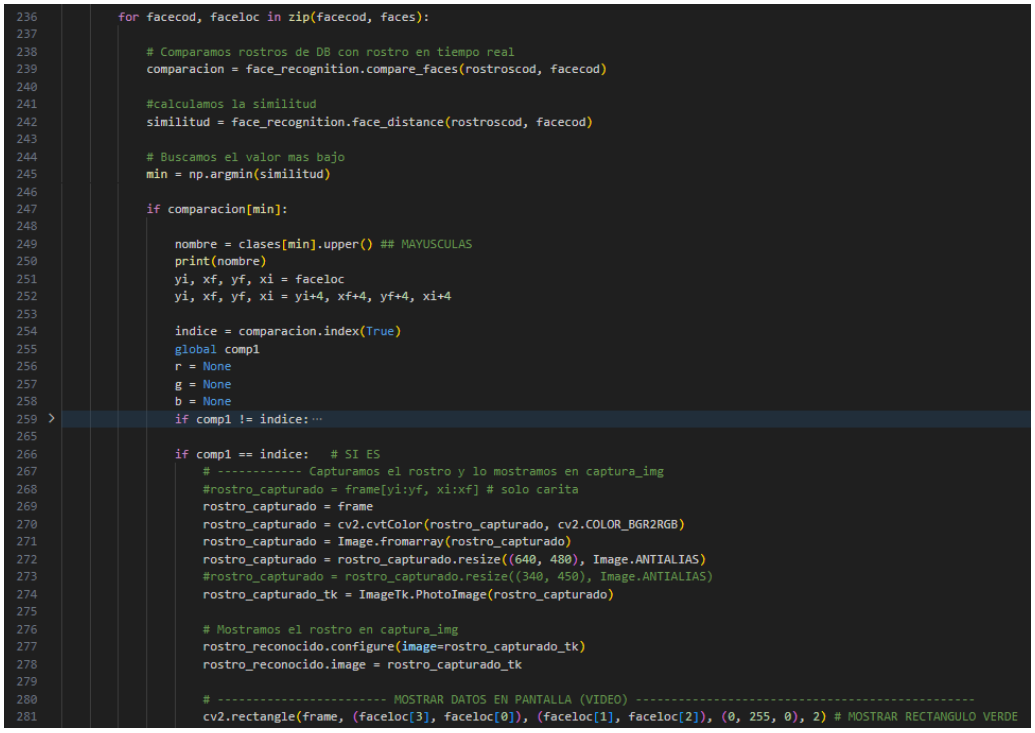
cual es crítico en situaciones donde el tiempo de respuesta puede influir en la experiencia del usuario, como durante la realización de un examen. El hecho de que el tiempo promedio de reconocimiento se mantenga en 10 segundos sugiere que el sistema no está optimizado para proporcionar respuestas rápidas, lo que puede contribuir a una mala satisfacción del usuario y un flujo de trabajo menos ágil.

Obtención de los datos de tiempo postest

Para obtener los datos sobre el tiempo de respuesta del sistema en el postest, se utilizaron los reportes generados por el sistema. El sistema cuenta con una funcionalidad específica para la generación de reportes, que registra y proporciona información detallada sobre el tiempo de respuesta en cada instancia de verificación. Estos reportes fueron fundamentales para analizar y evaluar el rendimiento del sistema durante el proceso de examen.

Figura 34

Código para la obtención del tiempo de reconocimiento



```
for facecod, faceloc in zip(facecod, faces):

    # Comparamos rostros de DB con rostro en tiempo real
    comparacion = face_recognition.compare_faces(rostroscod, facecod)

    #calculamos la similitud
    similitud = face_recognition.face_distance(rostroscod, facecod)

    # Buscamos el valor mas bajo
    min = np.argmin(similitud)

    if comparacion[min]:

        nombre = clases[min].upper() ## MAYUSCULAS
        print(nombre)
        yi, xf, yf, xi = faceloc
        yi, xf, yf, xi = yi+4, xf+4, yf+4, xi+4

        indice = comparacion.index(True)
        global comp1
        r = None
        g = None
        b = None
        if comp1 != indice:···

        if comp1 == indice:   # SI ES
            # ------------ Capturamos el rostro y lo mostramos en captura_img
            #rostro_capturado = frame[yi:yf, xi:xf] # solo carita
            rostro_capturado = frame
            rostro_capturado = cv2.cvtColor(rostro_capturado, cv2.COLOR_BGR2RGB)
            rostro_capturado = Image.fromarray(rostro_capturado)
            rostro_capturado = rostro_capturado.resize((640, 480), Image.ANTIALIAS)
            #rostro_capturado = rostro_capturado.resize((340, 450), Image.ANTIALIAS)
            rostro_capturado_tk = ImageTk.PhotoImage(rostro_capturado)

            # Mostramos el rostro en captura_img
            rostro_reconocido.configure(image=rostro_capturado_tk)
            rostro_reconocido.image = rostro_capturado_tk

            # ------------------------ MOSTRAR DATOS EN PANTALLA (VIDEO) ----------------------------------------------
            cv2.rectangle(frame, (faceloc[3], faceloc[0]), (faceloc[1], faceloc[2]), (0, 255, 0), 2) # MOSTRAR RECTANGULO VERDE
```

Interpretación: El sistema inicia evaluando los fotogramas del video que se está capturando en tiempo real, buscando detectar rostros. Una vez identificado un rostro, procede a compararlo con las imágenes almacenadas en la base de datos. Finalmente, el sistema genera una respuesta, indicando si el rostro detectado coincide o no con alguno en la base de datos.

A continuación, se presenta una tabla con los tiempos de respuesta registrados para cada prueba, mostrando cuánto tardó el sistema en identificar a cada postulante. Esta métrica permite analizar la eficiencia del sistema y determinar si cumple con los requerimientos de rapidez establecidos para su implementación.

Tabla 25

Medición del tiempo de reconocimiento

Nº	Tiempo (seg)	Nº	Tiempo (seg)	Nº	Tiempo (seg)
1	2	35	2	69	2
2	1	36	1	70	2
3	3	37	2	71	3
4	3	38	3	72	2
5	2	39	3	73	-
6	2	40	2	74	3
7	1	41	3	75	3
8	2	42	2	76	1
9	-	43	3	77	3
10	1	44	3	78	2
11	1	45	3	79	2
12	2	46	1	80	2
13	2	47	1	81	1
14	2	48	1	82	1
15	3	49	1	83	1
16	2	50	3	84	3
17	2	51	2	85	2
18	2	52	3	86	2
19	3	53	2	87	-
20	2	54	3	88	1
21	1	55	1	89	2
22	-	56	3	90	1
23	2	57	-	91	3
24	2	58	3	92	2
25	1	59	1	93	2

Nº	Tiempo (seg)	Nº	Tiempo (seg)	Nº	Tiempo (seg)
26	1	60	1	94	3
27	3	61	2	95	2
28	3	62	1	96	2
29	3	63	3	97	1
30	-	64	3	98	2
31	2	65	1	99	3
32	1	66	2	100	2
33	1	67	3		
34	2	68	1		
		Total			100

Interpretación: La tabla anterior muestra la medición del tiempo de reconocimiento facial del sistema en segundos para 100 postulantes. La mayoría de los tiempos se distribuyen entre 1 y 3 segundos, con algunos postulantes siendo reconocidos en 1 segundo, mientras que otros tardaron hasta 3 segundos. Los tiempos de respuesta son cruciales para evaluar la eficiencia del sistema. Las entradas marcadas con - indican que el sistema no pudo identificar a esos postulantes, registrando así su estatus como desconocidos y, por lo tanto, esos datos no se incluyeron en los reportes. Esto sugiere que, aunque el sistema mostró un rendimiento general eficiente, existieron casos donde no logró realizar la identificación.

4.3.3. Resultados

Para calcular el tiempo de respuesta promedio de los 93 postulantes cuyos rostros fueron reconocidos, se aplicará la fórmula descrita en el documento de (Bernal, 2021).

$$Tiempo\ Promedio\ de\ Respuesta = \frac{\sum_{i=n}^{n} t_i}{n}$$

Tabla 26

Valor de las variables en el tiempo de respuesta

Variable	Valor
t	Valor de cada prueba
n	93

Reemplazamos en la ecuación y nos queda:

$$Tiempo\ Promedio\ de\ Respuesta = \frac{\sum_{i=n}^{n} t_i}{n} = 2\ segundos$$

Este tiempo promedio indica que, en promedio, el sistema de reconocimiento facial tarda 2 segundos en identificar a cada postulante desde el momento en que se presenta frente a la cámara hasta que se realiza la comparación con la base de datos. Este rendimiento es relevante en el contexto del examen de admisión, ya que un tiempo de respuesta de 2 segundos por postulante asegura una rápida identificación sin causar demoras significativas en el proceso del examen. La eficiencia del sistema en términos de tiempo de respuesta contribuye a una experiencia más fluida y efectiva para los postulantes, permitiendo una gestión más eficiente del examen de admisión.

4.3.4. Discusión

La medición del tiempo de respuesta es esencial para determinar la eficiencia del sistema en un entorno de alta demanda, donde es necesario que el proceso de reconocimiento facial no cause interrupciones ni demoras significativas en el desarrollo del examen. Un tiempo de respuesta rápido no solo

optimiza la rapidez del proceso de verificación, sino que también mejora la experiencia del postulante y facilita una gestión eficiente del tiempo durante la admisión.

La aceptación del sistema de reconocimiento facial en el control biométrico del examen extraordinario de la Universidad Nacional del Altiplano Puno está en línea con investigaciones anteriores. Por ejemplo, Aquijes y Ampuero (2021) también hallaron una alta aceptación de sistemas biométricos en entornos de seguridad, destacando la rapidez y la reducción de errores humanos como las principales ventajas. En nuestro caso, el rápido tiempo de respuesta del sistema ha contribuido significativamente a la eficiencia del proceso de admisión, reduciendo demoras y mejorando la experiencia del usuario.

La evaluación del tiempo de respuesta del sistema en 2024 reveló un promedio de 2 segundos, un resultado notablemente favorable en comparación con estudios previos. Paulo Menino (2022) demostró que las redes neuronales convolucionales profundas pueden mejorar la precisión del reconocimiento facial. Nuestro sistema, con un tiempo de respuesta de 2 segundos, combina efectivamente rapidez y precisión.

Santana Melo et al. (2021) subrayaron cómo el reconocimiento facial mejora la seguridad en instalaciones judiciales, destacando la importancia de sistemas rápidos y confiables, cualidades que nuestro sistema también presenta.

A nivel nacional, Reyes Campos et al. (2023) implementaron redes neuronales convolucionales con un 88% de precisión, mientras que Mamani Aquino & Canahuire Quispe (2022) observaron variaciones en los tiempos de

respuesta. Estos estudios refuerzan la relevancia de nuestro tiempo promedio de 2 segundos, situándolo favorablemente en comparación con estos resultados.

4.4. RESULTADOS CORRESPONDIENTES AL OBJETIVO ESPECÍFICO 03

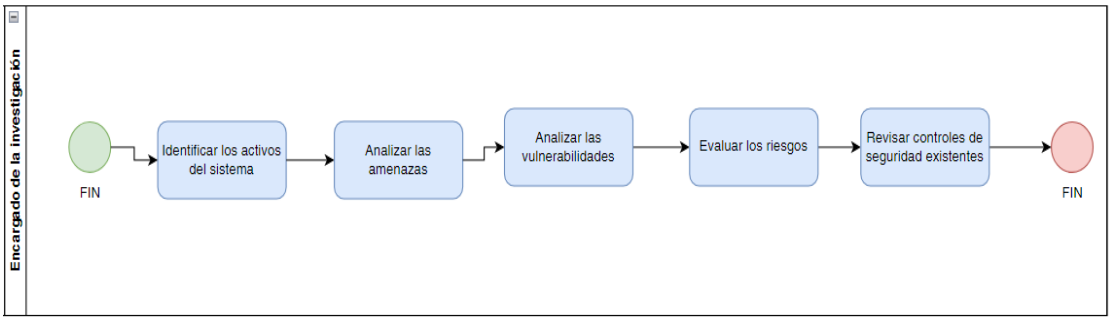
Objetivo específico 03: Evaluar el nivel de seguridad del sistema informático con reconocimiento facial en el control biométrico del examen extraordinario de la Universidad Nacional del Altiplano Puno en el año 2024.

4.4.1. Descripción

El tercer objetivo específico se centra en evaluar el nivel de seguridad del sistema informático con reconocimiento facial implementado para el control biométrico del proceso de admisión. Este análisis es crucial para garantizar que el sistema no solo funcione correctamente en términos de precisión y tiempo de respuesta, sino que también ofrezca un alto nivel de seguridad para proteger la integridad de los datos y la privacidad de los postulantes.

Figura 35

Diagrama de procesos del objetivo 3



Este proceso comprende varias etapas esenciales, en primer lugar, se realiza la identificación y valoración de los activos de información. A

continuación, se procede a identificar las amenazas y vulnerabilidades presentes en el entorno. Finalmente, se evalúan los riesgos asociados con estas amenazas.

4.4.2. Evaluación

Para la evaluación de esta hipótesis, se tomó como referencia el trabajo realizado por Valdivieso (2016), quien llevó a cabo un exhaustivo análisis de riesgos. En su estudio, utilizó diversos instrumentos, como fichas de registro, cuestionarios y fichas de observación. Muchos de estos instrumentos son proporcionados por la metodología aplicada (MAGERIT), pero fueron adaptados a las necesidades específicas de la organización en cuestión. En este proyecto, se decidió adoptar la ficha de registro desarrollada por Valdivieso, lo que garantiza un enfoque coherente y ajustado a los requerimientos del estudio. A continuación, se presentan los pasos llevados a cabo en el proceso de evaluación.

Identificación de los activos

En primer lugar, es crucial tener un inventario detallado de todos los activos que utiliza el sistema de reconocimiento facial. Estos activos incluyen tanto componentes de hardware y software, como también la información generada y procesada por el sistema. Posteriormente, se deben identificar las amenazas y vulnerabilidades que puedan afectar a estos activos.

Tabla 27

Activos que utiliza el sistema con reconocimiento facial

Hardware	Software	Otros
Laptop	Sistema con reconocimiento facial.	Reportes del sistema
Cámara	Antivirus	-

Una vez se han identificado los activos involucrados en el sistema de reconocimiento facial, el siguiente paso es analizar las amenazas que podrían comprometer estos elementos. Estas amenazas pueden incluir desde ataques externos, fallos en los componentes o errores humanos. Es necesario considerar las vulnerabilidades que se encuentran en el hardware, software y manejo de la información.

Análisis de amenazas y vulnerabilidades

Se identificaron las siguientes amenazas y vulnerabilidades en el sistema de reconocimiento facial.

Tabla 28

Amenazas y vulnerabilidades en la seguridad

Amenazas externas	Amenazas internas	Vulnerabilidades
Ciberataques	Fallas del sistema	Mal manejo de la base de datos
Robo de dispositivo	Fallos en la laptop	Software desactualizado
Acceso no autorizado a la base de datos	Fallos en la cámara	Presencia de malware en la laptop

Evaluación de riesgos

Una vez identificadas las amenazas y vulnerabilidades, se procede con el análisis de riesgos, una fase crucial para determinar el nivel de exposición del sistema a posibles incidentes de seguridad. Este análisis consiste en evaluar la probabilidad de que una amenaza logre explotar una vulnerabilidad en alguno de los activos del sistema.

Para llevar a cabo este análisis, se utilizó el instrumento de Valdiviezo (2016), que ofrece una estructura para la gestión de riesgos de seguridad de la información. Este instrumento, validado por expertos en el área, permite identificar, evaluar y clasificar los riesgos más críticos, proporcionando resultados precisos y confiables.

Paso 1: Identificación de activos, amenazas y vulnerabilidades

A continuación, se detallan los activos, las amenazas asociadas a cada uno y las vulnerabilidades identificadas.

Tabla 29

Relación entre activo, amenaza, vulnerabilidad

Activo	Amenaza	Vulnerabilidad
Laptop	Robo de dispositivo	Ausencia de cifrado de datos
Laptop	Ciberataque	Software desactualizado
Cámara	Fallos en la cámara	Calidad de hardware deficiente.
Sistema de reconocimiento facial	Acceso no autorizado	Fallos en la configuración de seguridad
Reportes del sistema	Ciberataque o acceso no autorizado	Mala gestión de la base de datos
Antivirus	Presencia de malware	Antivirus no actualizado

Paso 2: Matriz de riesgos

En este paso, se realiza una matriz de evaluación de riesgos basada en dos criterios fundamentales: probabilidad (baja, media, alta) e impacto (bajo, medio, alto). Esto permite priorizar las amenazas más críticas.

Tabla 30

Identificación de la matriz de riesgos

Riesgo	Probabilidad	Impacto
Robo de la laptop	Medio	Alto
Fallos del sistema	Bajo	Crítico
Fallos en la cámara	Bajo	Medio
Ciberataque a la laptop	Alto	Alto
Acceso no autorizado al sistema	Medio	Alto
Fallos en la configuración de la base de datos	Bajo	Alto
Presencia de malware	Medio	Medio

Una vez que se hizo la identificación de los riesgos, sus probabilidades y el impacto que tendrían, se realiza la revisión de los controles existentes en el sistema.

Revisión de controles de seguridad existentes.

Una vez realizada la identificación y evaluación de los riesgos, es necesario revisar los controles de seguridad implementados en el sistema de reconocimiento facial para determinar si son suficientes para mitigar las amenazas y vulnerabilidades detectadas. A continuación, se describe el estado actual de los controles implementados y su efectividad en la seguridad del sistema.

Tabla 31

Controles de seguridad existentes en el sistema

Riesgo	Control existente
Robo de la laptop	Se realizaron copias de seguridad del sistema en un USB y en la nube (Drive), asegurando la disponibilidad de los datos en caso de pérdida o robo del equipo.
Fallos del sistema	Se han llevado a cabo pruebas en entornos controlados, lo que minimiza la probabilidad de fallos. Además, el objetivo específico 1 ha demostrado resultados positivos en la detección y prevención de errores.
Fallos en la cámara	La cámara utilizada es nueva, lo que reduce significativamente la probabilidad de fallos, otro método para mitigar este posible riesgo es usar la cámara de la laptop.
Ciberataque a la laptop	La laptop está protegida mediante un antivirus actualizado y un firewall, lo que ofrece una defensa básica contra ataques cibernéticos.
Acceso no autorizado	El equipo cuenta con autenticación de usuario para restringir el acceso.
Fallos en la base de datos	La base de datos de los rostros está almacenada en un entorno seguro, y para mejorar la privacidad se utiliza la vectorización de rostros en lugar de imágenes completas.
Presencia de malware	Se ejecutaron análisis de virus y amenazas con un antivirus actualizado tanto antes del desarrollo como antes del lanzamiento del sistema.

4.4.3. Resultados

Los resultados obtenidos del análisis del sistema de reconocimiento facial indican un desempeño destacado en términos de seguridad. A continuación, se detallan los hallazgos principales.

- En cuanto a los fallos del sistema, el objetivo específico 1 demuestra que el sistema funciona eficazmente en un entorno real como el del examen de admisión extraordinario, con una precisión destacada del 93%.
- Robo de la laptop: Se han implementado controles efectivos, como las copias de seguridad en USB y en la nube, garantizando la recuperación de datos en caso de pérdida o robo del equipo. Este control disminuye el impacto de la pérdida física de la laptop, aunque el riesgo de robo aún existe.
- Fallos en la cámara: Dado que la cámara es nueva, la probabilidad de fallos es baja. Sin embargo, un mecanismo de respaldo está presente al poder utilizar la cámara integrada de la laptop, lo que mejora la capacidad del sistema ante este tipo de fallos.
- Ciberataque a la laptop: El uso de un antivirus actualizado y un firewall proporciona una defensa básica contra ataques cibernéticos. Sin embargo, esta protección debería complementarse con otros controles más avanzados para mitigar posibles ataques sofisticados.
- Acceso no autorizado: La autenticación de usuario en la laptop es un control estándar que ayuda a prevenir accesos no autorizados. Aunque es una medida adecuada, podría mejorarse con autenticaciones de varios pasos o cifrado de datos sensibles.
- Fallos en la base de datos: Al almacenar la base de datos en un entorno seguro y utilizar la vectorización de los rostros en lugar de imágenes completas, se ha fortalecido la seguridad y privacidad de la información. Esto mitiga significativamente el riesgo de exposición de datos sensibles.
- Presencia de malware: El sistema está protegido mediante análisis de virus y amenazas previos al desarrollo y lanzamiento. La actualización constante del

antivirus asegura que el sistema esté defendido contra las amenazas más recientes, aunque se podría reforzar con medidas adicionales como un sistema de monitoreo continuo.

El análisis de los datos confirma que el sistema de reconocimiento facial implementado cumple con los requisitos de seguridad establecidos, proporcionando un rendimiento robusto y fiable para el control biométrico del examen.

4.4.4. Discusión

Los resultados obtenidos del análisis indican que el sistema ha alcanzado una precisión del 93%, lo que demuestra un rendimiento destacado en la identificación de postulantes en un entorno real. Esto se alinea con estudios previos que también han mostrado altos niveles de precisión en sistemas similares, como los que se mencionaron en el primer objetivo específico.

En cuanto a la protección contra robos, el sistema ha implementado controles efectivos como copias de seguridad en USB y en la nube. Esta estrategia disminuye el impacto de la pérdida física del equipo, aunque el riesgo de robo aún persiste. Este enfoque es coherente con las prácticas recomendadas en la literatura, como la de Pico Yépez y Cordero Ynga (2019), quienes destacaron la importancia de medidas de seguridad para proteger la información en sistemas con reconocimiento facial. Sin embargo, se observa que la protección contra ciberataques en el sistema actual podría beneficiarse de controles más avanzados, ya que solo se utilizan un antivirus actualizado y un firewall, similar a lo que sugirió la investigación de Camara (2021) sobre la necesidad de una regulación robusta y medidas adicionales en la protección de datos biométricos.

En relación a los fallos de la cámara, el sistema ha incorporado un mecanismo de respaldo que utiliza la cámara integrada de la laptop, lo que mejora la capacidad del sistema para manejar fallos de hardware. Este enfoque es comparable a la investigación de Santana Melo, Arruda Neves y Oliveira Neto (2021), que mostró cómo la implementación de tecnologías de reconocimiento facial puede mejorar la seguridad, destacando la importancia de contar con sistemas de respaldo.

En cuanto al acceso no autorizado, el sistema emplea autenticación estándar de usuario en la laptop, aunque podría beneficiarse de métodos adicionales como autenticación de varios pasos. Esto es consistente con las observaciones de Domingo Jaramillo (2021), quien subrayó la necesidad de legislación específica para el uso de tecnología de reconocimiento facial para proteger la privacidad individual.

Finalmente, la base de datos está almacenada en un entorno seguro y se utiliza la vectorización de rostros para proteger la información. Esto se alinea con los hallazgos de Mamani Aquino y Canahuire Quispe (2022), quienes destacaron la eficacia del reconocimiento facial en la gestión de accesos en instituciones educativas, así como con la investigación de Calizaya Bobadilla y Calsin Cari (2023), que resaltó la importancia de minimizar el riesgo de fraude en entornos en línea. Además, la protección contra malware mediante análisis de virus y amenazas previos al desarrollo es una medida adecuada, pero se podría fortalecer con un sistema de monitoreo continuo, en línea con las recomendaciones de Velloso Bastos y Barros Esteves (2021) para realizar evaluaciones críticas sobre el uso de tecnologías de vigilancia.

4.5. APORTE DE LA INVESTIGACIÓN

El desarrollo de este sistema informático con reconocimiento facial para el control biométrico en el examen de admisión extraordinario de la Universidad Nacional del Altiplano en el año 2024, no solo se limita a la implementación de algoritmos conocidos, sino que presenta varios aportes científicos relevantes en el campo de la biometría educativa.

En primer lugar, este trabajo destaca por su novedad al adaptar algoritmos de reconocimiento facial, como *face_recognition* y *dlib*, en un contexto educativo, específicamente para la verificación de identidad en exámenes de admisión. Estos algoritmos han sido ampliamente utilizados en otras áreas, como la seguridad y la vigilancia, la aplicación en el ámbito educativo, y en particular en procesos de admisión, representa un avance importante. La adaptación de este tipo de tecnología a contextos que requieren una alta presión y se trabaja con un gran volumen de personas, como el examen de admisión, no solo mejora la precisión del control biométrico, sino que también sienta precedentes para su implementación en otras instituciones educativas que enfrentan retos similares en términos de suplantación de identidad y seguridad en sus procesos de admisión.

Los resultados obtenidos en este proyecto muestran una mejora notable en la precisión y el tiempo de respuesta del sistema, abordando eficazmente varios problemas críticos del examen de admisión de la Universidad Nacional del Altiplano. Se identificaron dos desafíos principales: el tiempo de toma de control biométrico y la precisión en la evaluación de los postulantes. Estos inconvenientes surgían del uso de un sistema basado en huellas dactilares, que no siempre lograba reconocer al postulante, generando retrasos y errores en la verificación de identidad. Esto impactaba

negativamente tanto en la experiencia de los postulantes como en la integridad del proceso de admisión. Para solucionar esto, se implementó un sistema de reconocimiento facial, lo que permitió alcanzar un 93% de precisión en la identificación, un logro significativo, especialmente considerando las condiciones desafiantes, como la variación en la iluminación y la calidad de las cámaras utilizadas.

El tiempo de respuesta de 2 segundos representa una optimización considerable en comparación con otros sistemas biométricos, garantizando que la verificación de identidad se realice de manera ágil y sin interrumpir el desarrollo normal del examen. Esto asegura una experiencia fluida y eficiente para los postulantes. Este trabajo destaca la aplicación de un modelo en un problema de la vida real, contribuyendo significativamente a la mejora de procesos en contextos educativos y estableciendo un referente para futuras implementaciones en instituciones similares.

Otro aporte relevante del proyecto es el enfoque en la seguridad biométrica, ya que el sistema se basa en la vectorización de los rostros. Esta técnica no solo reduce el espacio de almacenamiento, sino que también mejora la privacidad y seguridad de los datos. Además, cumple con estándares de seguridad, lo que lo distingue de otros sistemas que no consideran adecuadamente la protección de información sensible. La implementación de estas medidas de seguridad refuerza la confianza tanto de los postulantes como de la institución en la transparencia y equidad del proceso de admisión.

Es fundamental resaltar la escalabilidad y aplicabilidad del sistema desarrollado. Su diseño modular, basado en la metodología XP, permite que el sistema no solo se implemente en otros exámenes de admisión, sino también en diversos entornos institucionales que requieran un control biométrico eficiente y seguro. La flexibilidad de la arquitectura facilita su replicación y mejora, abriendo oportunidades para su uso en

contextos más allá del ámbito universitario, lo que potencia su impacto en múltiples sectores.

El enfoque adoptado en este proyecto y las tecnologías utilizadas no solo mitigan los inconvenientes identificados, sino que también demuestran que, mediante ajustes adecuados en los parámetros del algoritmo, se puede optimizar el rendimiento del sistema, incluso en situaciones de recursos limitados. Estos aportes evidencian que el trabajo realizado va más allá del uso de algoritmos existentes, contribuyendo con mejoras significativas en precisión, tiempo de respuesta, seguridad y aplicabilidad. Esto convierte al sistema en una solución innovadora para el control biométrico en entornos educativos.

4.6. PRUEBA DE HIPÓTESIS

4.6.1. Hipótesis específica 01

Hipótesis Nula (H0): La precisión del sistema informático con reconocimiento facial es menor que la de los métodos tradicionales en el control biométrico de los postulantes al examen de admisión extraordinario.

Hipótesis Alternativa (H1): La precisión del sistema informático con reconocimiento facial es mayor que la de los métodos tradicionales en el control biométrico de los postulantes al examen de admisión extraordinario.

4.6.1.1. Metodología de prueba

Para llevar a cabo este análisis, utilizaremos una prueba de proporciones. Según lo define (Sierra, 2024), estas pruebas se caracterizan por tener una estadística de prueba con distribución binomial, en la que cada observación resulta en un “éxito” o “fracaso”.

4.6.1.2. Análisis estadístico

Para empezar con el análisis estadístico comenzamos por definir las métricas que utilizaremos en la prueba.

- Reconocimientos satisfactorios: 93
- Casos no reconocidos: 7

Vamos a llevar a cabo una prueba de proporciones para comparar la precisión del nuevo sistema con un umbral de éxito predefinido. Establecemos el umbral en 81% (p0 = 0.81), valor establecido con base en la precisión del sistema antes de su implementación. La prueba se desarrollará de la siguiente manera.

Calculamos la proporción observada y el valor Z:

Proporción observada ($\hat{p}$)

$$(\hat{p}) = \frac{93}{100} = 0.9$$

Calcular el valor de Z

$$Z = \frac{\hat{p} - p_0}{\sqrt{\frac{p_0(1 - p_0)}{n}}}$$

Donde,

- $\hat{\boldsymbol{p}} = 0.93$
- $\boldsymbol{p_0} = 0.81$
- $\boldsymbol{n} = 100$

Sustituyendo en la fórmula, tenemos:

$$Z = \frac{0.93 - 0.81}{\sqrt{\frac{0.81 * (1 - 0.81)}{100}}} = \frac{0.12}{\sqrt{\frac{0.1539}{100}}} = \frac{0.12}{0.0392} = 3.06$$

Determinamos el valor crítico para un nivel de significancia α típico de 0.05 (prueba unilateral), el valor crítico Z es aproximadamente 1.645 (valor sacado del diagrama *t-student*).

4.6.1.3. Decisión

Los resultados indican que el valor de Z es 3.06, que supera el valor crítico de 1.645. Por lo tanto, se rechaza la hipótesis nula y se acepta la hipótesis alternativa. Esto demuestra que la precisión del sistema, que es 0.93, es significativamente mayor al umbral de 0.81, superándolo en 0.12.

4.6.2. Hipótesis específica 02

Hipótesis Nula (H0): El tiempo de respuesta del sistema informático con reconocimiento facial es mayor que los métodos tradicionales en el control biométrico de los postulantes al examen de admisión extraordinario.

Hipótesis Alternativa (H1): El tiempo de respuesta del sistema informático con reconocimiento facial es menor que los métodos tradicionales en el control biométrico de los postulantes al examen de admisión extraordinario.

4.6.2.1. Metodología de prueba

Se recopilaron datos sobre el tiempo que tomaba realizar el control biométrico a través del método de la observación utilizando una ficha de medición, previa a la implementación del sistema de reconocimiento

facial. Posteriormente, se compararon con los tiempos obtenidos tras la aplicación del nuevo sistema.

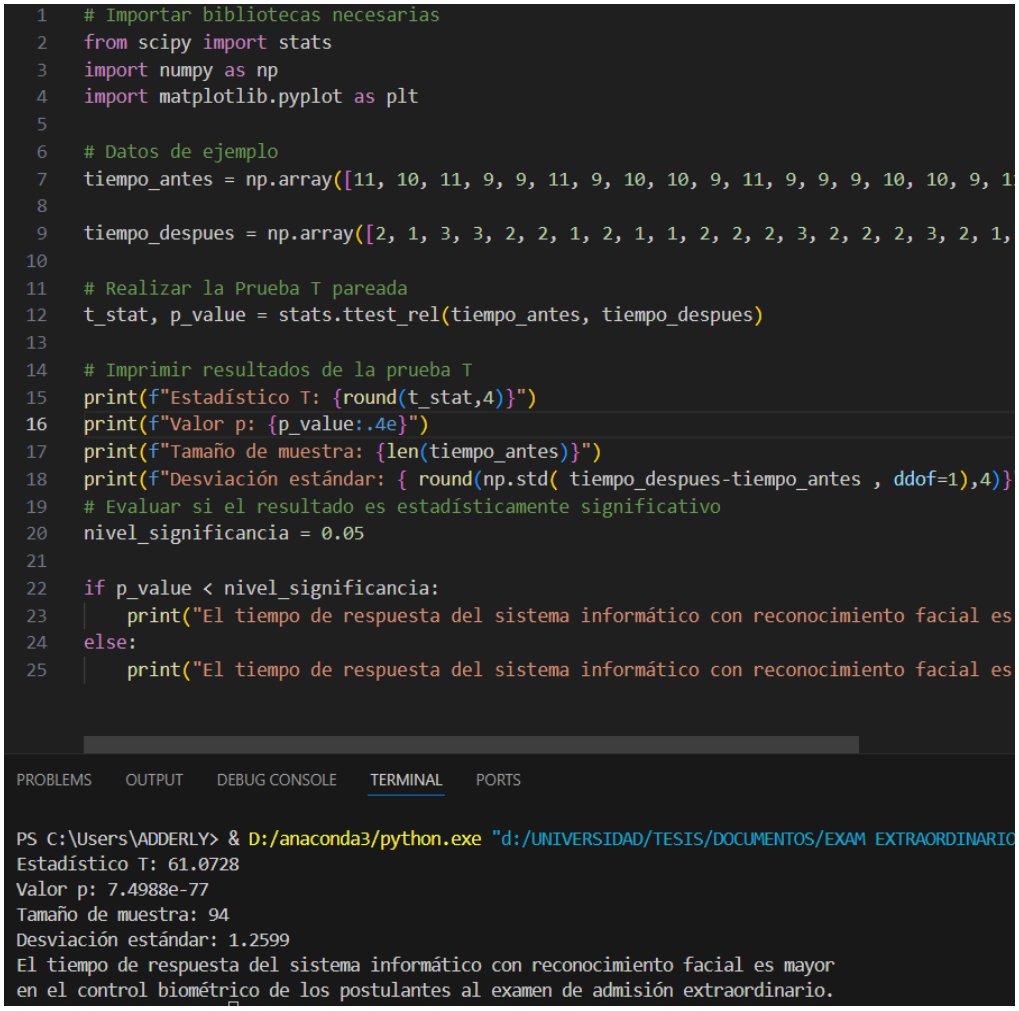
4.6.2.2. Análisis estadístico

Para evaluar la hipótesis planteada, se empleó una prueba t para muestras pareadas, como describe (Rosie Shir, 2004), este enfoque es común en investigaciones experimentales donde se mide la variable dependiente antes y después de la intervención. En esta investigación se mide el tiempo que toma el control biométrico antes y después del sistema con reconocimiento facial.

El nivel de significancia (α) se fijó en 0.05, lo que implica que se acepta un riesgo del 5% de cometer un error tipo I, es decir, de rechazar la hipótesis nula cuando en realidad es verdadera.

Figura 36

Código para analizar el tiempo de respuesta del sistema



```
# Importar bibliotecas necesarias
from scipy import stats
import numpy as np
import matplotlib.pyplot as plt

# Datos de ejemplo
tiempo_antes = np.array([11, 10, 11, 9, 9, 11, 9, 10, 10, 9, 11, 9, 9, 9, 10, 10, 9, 1

tiempo_despues = np.array([2, 1, 3, 3, 2, 2, 1, 2, 1, 1, 2, 2, 2, 3, 2, 2, 2, 3, 2, 1,

# Realizar la Prueba T pareada
t_stat, p_value = stats.ttest_rel(tiempo_antes, tiempo_despues)

# Imprimir resultados de la prueba T
print(f"Estadístico T: {round(t_stat,4)}")
print(f"Valor p: {p_value:.4e}")
print(f"Tamaño de muestra: {len(tiempo_antes)}")
print(f"Desviación estándar: { round(np.std( tiempo_despues-tiempo_antes , ddof=1),4)}
# Evaluar si el resultado es estadísticamente significativo
nivel_significancia = 0.05

if p_value < nivel_significancia:
    print("El tiempo de respuesta del sistema informático con reconocimiento facial es
else:
    print("El tiempo de respuesta del sistema informático con reconocimiento facial es
```

```
PROBLEMS  OUTPUT  DEBUG CONSOLE  TERMINAL  PORTS

PS C:\Users\ADDERLY> & D:/anaconda3/python.exe "d:/UNIVERSIDAD/TESIS/DOCUMENTOS/EXAM EXTRAORDINARIO
Estadístico T: 61.0728
Valor p: 7.4988e-77
Tamaño de muestra: 94
Desviación estándar: 1.2599
El tiempo de respuesta del sistema informático con reconocimiento facial es mayor
en el control biométrico de los postulantes al examen de admisión extraordinario.
```

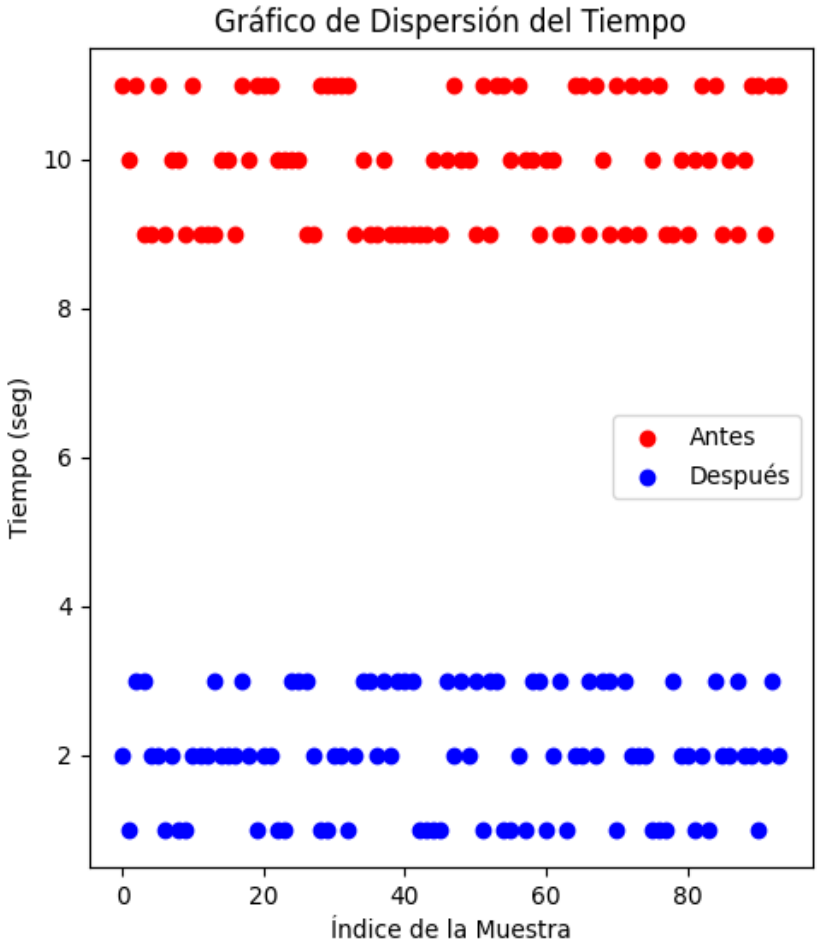
De la imagen anterior podemos decir que:

- **Estadístico T:** 61.0721
- **Valor p:** $7.4988 * 10^{-77}$
- **Tamaño de muestra:** 94
- **Desviación estándar:** 1.2599

Podemos visualizar los datos anteriores mediante gráficos, lo que facilita una mejor comprensión de la optimización en el tiempo de reconocimiento lograda con el sistema de reconocimiento facial.

Figura 37

Gráfico del tiempo antes y después



Interpretación: El gráfico de dispersión ilustra la diferencia en el tiempo de reconocimiento. Los puntos rojos representan los tiempos de evaluación antes de implementar el sistema de reconocimiento facial, mientras que los puntos azules corresponden a los tiempos registrados después de su implementación.

4.6.2.3. Decisión

Los resultados muestran que el valor de p es extremadamente pequeño ($7.4988 * 10^{-77}$), lo que nos permite rechazar la hipótesis nula.

Esto sugiere que existe una diferencia significativa en el tiempo de reconocimiento de una persona antes y después de la implementación del sistema de reconocimiento facial.

4.6.3. Hipótesis específica 03

Hipótesis Nula (H0): El nivel de seguridad del sistema es menor que el de los métodos tradicionales en el control biométrico de los postulantes al examen de admisión.

Hipótesis Alternativa (H1): El nivel de seguridad del sistema es mayor que el de los métodos tradicionales en el control biométrico de los postulantes al examen de admisión.

4.6.3.1. Metodología de prueba

Para evaluar la seguridad del sistema de reconocimiento facial, se han revisado varios aspectos importantes. Primero, el sistema muestra una alta precisión del 93% en la identificación de postulantes, destacándose por su eficacia en un entorno real.

Se han implementado medidas para proteger contra el robo de la laptop, como copias de seguridad en USB y en la nube, lo que asegura la recuperación de datos en caso de pérdida o robo. Además, el sistema dispone de una cámara de respaldo en la laptop para continuar funcionando si la cámara principal falla, aumentando su resiliencia.

Para contrarrestar ciberataques, se utiliza un antivirus actualizado y un firewall, aunque se recomienda añadir medidas de seguridad adicionales para enfrentar amenazas más sofisticadas. En términos de

acceso no autorizado, el sistema emplea autenticación de usuario, pero se sugiere mejorar esta seguridad con autenticaciones adicionales o cifrado de datos.

La seguridad de la base de datos se refuerza mediante la vectorización de rostros en lugar de almacenar imágenes completas, lo que disminuye el riesgo de exposición de datos sensibles. Finalmente, el sistema está protegido contra malware con un análisis de virus previo y actualizaciones constantes, aunque se aconseja añadir un sistema de monitoreo continuo para mejorar la protección.

4.6.3.2. Análisis

El análisis de los datos muestra que las medidas de seguridad implementadas, como copias de seguridad, protección contra ciberataques y manejo de fallos, contribuyen significativamente a la seguridad general del sistema. La alta precisión del sistema y las medidas preventivas en caso de robo o fallos refuerzan la robustez del sistema, lo que indica un cumplimiento sólido con los requisitos de seguridad.

4.6.3.3. Decisión

Con base en los resultados obtenidos y el análisis de las medidas de seguridad implementadas, se rechaza la hipótesis nula (H_0). La evidencia sugiere que el sistema de reconocimiento facial cumple con los requisitos de seguridad establecidos para el control biométrico del examen extraordinario. Por lo tanto, se acepta la hipótesis alternativa (H_1), concluyendo que el sistema proporciona un rendimiento robusto y fiable en términos de seguridad.

V. CONCLUSIONES

- El desarrollo e implementación del sistema de reconocimiento facial en el examen de admisión extraordinario ha demostrado ser una solución precisa, eficiente y segura para el control biométrico. Este sistema ha permitido no solo la optimización en la identificación de posibles suplantadores de identidad, reduciendo drásticamente el margen de error, sino que también ha incrementado la eficiencia operativa al acortar considerablemente el tiempo necesario para verificar a cada postulante. La incorporación de esta avanzada tecnología biométrica garantiza un control más riguroso y transparente del proceso de admisión y cumple con las expectativas de los usuarios, quienes han señalado que el sistema es fácil de usar y accesible. Este aspecto es fundamental, ya que facilita la adopción del sistema por parte del personal encargado y mejora la experiencia de los usuarios. Además, la implementación de este sistema establece un modelo de referencia para otras instituciones educativas que deseen optimizar sus propios mecanismos de control, impulsando estándares más elevados de seguridad y eficiencia en los procesos de admisión. Este enfoque no solo refuerza la confianza en la tecnología como un aliado en la protección de la integridad académica, sino que también sienta las bases para futuras innovaciones en sistemas biométricos en contextos educativos.
- La precisión del sistema, con una tasa de reconocimiento del 93%, demuestra que es extremadamente confiable y eficaz en condiciones normales de operación. Este nivel de precisión asegura que la identificación de los postulantes se realice con un margen de error mínimo, lo cual es fundamental en procesos donde la exactitud es clave. Sin embargo, para mantener y, en lo posible, optimizar aún más esta precisión, es esencial tomar en cuenta factores externos, como la iluminación, los

ángulos de las cámaras y las variaciones en las características faciales, que pueden influir en el rendimiento del sistema. En este sentido, la mejora continua del sistema, a través del ajuste de los parámetros de reconocimiento y el uso de tecnologías complementarias, será clave para alcanzar niveles de precisión superiores y garantizar un funcionamiento óptimo en todo tipo de entornos.

– El tiempo de respuesta del sistema es otro de sus puntos fuertes, procesando la identificación de los 93 postulantes reconocidos en un promedio de 2 segundos. Este rendimiento eficiente no solo cumple, sino que supera las expectativas al reducir significativamente los tiempos de espera. En comparación con métodos menos sofisticados, este tiempo de respuesta ágil refleja una mejora sustancial en la eficiencia operativa del sistema, lo cual es crucial en contextos de alta demanda como los procesos de admisión. Además, la rapidez en el reconocimiento facial minimiza la posibilidad de errores humanos y permite que el sistema funcione de manera fluida, mejorando la experiencia tanto para los usuarios como para los administradores del proceso. Esta agilidad se traduce en un flujo continuo de identificación y una reducción de posibles cuellos de botella, lo que es especialmente valioso en situaciones de estrés o cuando se manejan grandes volúmenes de datos.

– La seguridad del sistema ha sido diseñada de manera integral para abordar y mitigar posibles riesgos y amenazas, garantizando la protección y confidencialidad de la información biométrica. El cumplimiento con los estándares más rigurosos en protección de datos refuerza la confianza en el sistema, asegurando que las identidades de los postulantes estén bien protegidas frente a posibles vulneraciones o intentos de suplantación. Estas características de seguridad no solo refuerzan la integridad del proceso, sino que también establecen

un marco de protección robusto y confiable, adecuado para su implementación no solo en entornos educativos, sino también en otros contextos que requieran altos niveles de seguridad, como sectores gubernamentales o corporativos. La capacidad del sistema para prevenir amenazas potenciales garantiza su eficacia y durabilidad en el tiempo, haciendo que sea una solución sostenible y escalable en el futuro.

VI. RECOMENDACIONES

- Se recomienda mejorar la calidad de la cámara utilizada para la captura de imágenes, una cámara de mayor resolución y mejor capacidad para manejar condiciones de iluminación podría aumentar significativamente la precisión del sistema de reconocimiento facial. Una cámara con características avanzadas, como una mayor tasa de cuadros por segundo (fps) y un sensor con alta sensibilidad a la luz, facilitaría la captura de imágenes, incluso en entornos con iluminación desfavorable, asegurando un rendimiento más confiable en diversas condiciones.
- Se sugiere evaluar la posibilidad de emplear hardware más potente, como procesadores con mayor capacidad de cómputo o servidores dedicados en lugar de una laptop. Esto reduciría significativamente los tiempos de procesamiento, especialmente cuando se maneja un gran volumen de datos. La integración de tecnologías complementarias, como la computación paralela o el uso de GPU (Unidad de Procesamiento Gráfico), podría acelerar aún más la velocidad del reconocimiento facial, garantizando un rendimiento eficiente incluso en escenarios de alta demanda.
- Para mejorar la seguridad del sistema, se sugiere la implementación de cámaras con tecnología de detección de vida, las cuales permiten verificar si el rostro capturado corresponde a una persona real y no a una imagen o video, reduciendo así el riesgo de suplantación por métodos fraudulentos. Finalmente, se recomienda realizar auditorías de seguridad periódicas y pruebas de penetración para identificar y corregir posibles vulnerabilidades, manteniendo un sistema seguro y confiable a largo plazo.

VII. REFERENCIAS BIBLIOGRÁFICAS

Adán, A., & Adán, M. (n.d.). *RECONOCIMIENTO A TRAVÉS DE MANOS*. Retrieved July 20, 2024, from https://www.academia.edu/1631683/RECONOCIMIENTO_A_TRAVÉS_DE_MANOS

Ageitgey. (2022). *face_recognition*. Github. https://github.com/ageitgey/face_recognition

Aglio Caballero, A., & Belén, R. S. (2016). IMPLEMENTACIÓN Y EVALUACIÓN DE UN SISTEMA BIOMÉTRICO DE RECONOCIMIENTO DE VENAS DE LAS MANOS MEDIANTE DESCRIPTORES LOCALES DE TEXTURA. *Universidad Politécnica de Madrid*, 1–79. https://zaguan.unizar.es/record/112622/files/TAZ-TFG-2022-641.pdf

Aguilera, M. (2012). *Reconocimiento biométrico basado en imágenes de huellas palmares* [Universidad Autónoma de Madrid]. http://www.jcee.upc.es/JCEE2001/PDFs 2000/13ESPINOSA.pdf

Aguirre, J. (2021). Desarrollo de un Sistema basado en Deep Learning y visión computacional de reconocimiento facial para mejorar el control de acceso a una empresa privada. *Universidad Tecnológica Del Perú*, 6.

Alberto Pérez. (2014). *Diseño De Un Sistemas Basado En Bosques Aleatorios Para La Detección De Tumores Cerebrales Mediante Imágenes Hiperespectrales.* 133.

Alegría, R. F. D. (2020). Métodos cualitativos para la obtención de la información. *Universidad Salazar Virtual*, 103–184.

Alejo, P. (2021). Algoritmo de reconocimiento facial para la gestión del control de acceso de la empresa Altoque PS S.A. *Universidad Cesar Vallejo*, 1–71.

https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/50737/Cusma_GM-SD.pdf?sequence=1&isAllowed=y

Amat, J. (2021). *Reconocimiento facial con deep learning y python*. Ciencia de Datos. https://cienciadedatos.net/documentos/py34-reconocimiento-facial-deeplearning-python

Amazon. (2023). *Amazon Rekognition Image*. Aws. https://aws.amazon.com/es/rekognition/image-features/

Aquijes, R., & Ampuero, L. (2021). Implementación de un Sistema de Reconocimiento Facial para el control de acceso del personal en la empresa GUIMARTBOT S.A.C". *Universidad Cesar Vallejo*, 1–71. https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/50737/Cusma_GM-SD.pdf?sequence=1&isAllowed=y

Arango, S. M. D., Campuzano, Z. L. F., & Zapata, C. J. A. (2015). Manufacturing process improvement using the Kanban. *Revista Ingenierías Universidad de Medellín*, *14*(27), 221–234. http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S1692-33242015000200014&lng=en&nrm=iso&tlng=es

Asana, R. (2022). Sistema de reconocimiento facial para el control de acceso en la I.E. 81585 Sagrado Corazón de Jesús de Cartavio - Ascope - La Libertad en el segundo y tercer bimestre del año lectivo 2022. *UNIVERSIDAD PRIVADA ANTENOR ORREGO*, 1–60. http://www.gonzalezcabeza.com/documentos/CRECIMIENTO_MICROBIANO.pdf

AWS. (2023). *¿Qué es el reconocimiento facial?* Amazon. https://aws.amazon.com/es/what-is/facial-recognition/

Aznarte, J. L., Pardos, M. M., & Lacruz López, J. M. (2022). Sobre el uso de

tecnologías de reconocimiento facial en la universidad: el caso de la UNED. *RIED-Revista Iberoamericana de Educacion a Distancia*, *25*(1), 261–277. https://doi.org/10.5944/ried.25.1.31533

Barrios, J. (2019). *La matriz de confusión y sus métricas*. BIG DATA. https://www.juanbarrios.com/la-matriz-de-confusion-y-sus-metricas/

Barten, M. (2024). *4 casos de uso de reconocimiento facial en la industria hotelera*. REVFINE. https://www.revfine.com/es/reconocimiento-facial-industria-hotelera/#:~:text=Los usos más comunes del,de acceso a las habitaciones

Basil. (2023). *Face Recognition in Python: A Comprehensive Guide*. Medium. https://basilchackomathew.medium.com/face-recognition-in-python-a-comprehensive-guide-960a48436d0f

Bastos, E. A. V., & Esteves, V. B. (2021). Tecnologias de reconhecimento facial. *Direitos Democráticos & Estado Moderno*, *3*, 216–240. https://doi.org/10.23925/ddem.i3.53875

Bernad, M., & Rodriguez, M. (2020). *Sistemas Informáticos, tipos y clasificación*.

Bernal, A. (2021). Facultad De Ingeniería, Arquitectura Y Urbanismo. *Universidad Señor de Sipán*, 141.

Bravo, C. J., Ramírez, P. E., & Arenas, J. (2018). Aceptación del Reconocimiento Facial Como Medida de Vigilancia y Seguridad: Un Estudio Empírico en Chile. *Información Tecnológica*, *29*(2), 115–122. https://doi.org/10.4067/s0718-07642018000200115

Cabrera, F. (n.d.). Kanban : Metodología ágil de desarrollo de Software. *Universidad Nacional Del Sur*.

Cadena, J. (2021). Técnica eficiente para reconocimiento facial global utilizando wavelets y máquinas de vectores de soporte en imágenes 3D. *Universidad Nacional Mayor de San Marcos*, 258.

Calderon Arateco, L. L. (2019). Seguridad informática y seguridad de la informacion. *Universidad Piloto de Colombia*. http://repository.unipiloto.edu.co/handle/20.500.12277/2821

Calizaya, M., & Calsin, F. (2022). MODELO PARA LA DETECCIÓN DE ANOMALÍAS EN SECUENCIAS DE VIDEOS DE EXÁMENES EN LÍNEA MEDIANTE INTELIGENCIA ARTIFICIAL CASO DE ESTUDIO: UNIVERSIDAD NACIONAL DEL ALTIPLANO. *Universidad Nacional Del Altiplano*, 1–168. http://repositorio.unap.edu.pe/bitstream/handle/UNAP/7104/Molleapaza_Mamani_Joel_Neftali.pdf?sequence=1&isAllowed=y

Cannatella, T., Méndez, M., & Sández, P. (2022). Identificación de Personas en Sistemas de Videovigilancia sin uso de Reconocimiento Facial. *XXVIII Congreso Argentino de Ciencias de La Computación - CACIC 2022*, 957–961. http://sedici.unlp.edu.ar/bitstream/handle/10915/149626/Documento_completo.pdf?sequence=1&isAllowed=y%0Ahttp://sedici.unlp.edu.ar/handle/10915/149626

Cárdenas, L. (2016). El patrón de arquitectura n-capas con orientación al dominio como solución en el diseño de aplicaciones empresariales. *Revista Tecnología & Desarrollo*, *11*(1), 59–66. https://doi.org/10.18050/td.v11i1.679

Carrasco, S. (2005). Metodología de la investigación científica: Pautas metodológicas para diseñar y elaborar el proyecto de investigación. : Aplicaciones en educación y otras ciencias sociales. In *Lima [Perú] : San Marcos*.

Castro, P. (2018). Implementación de un sistema de control de acceso biométrico zk-x7 por medio de huella dactilar en el laboratorio de hardware de la carrera de

ingeniería en computación y redes. *Universidad Estatal Del Sur de Manabí*, *05*. http://repositorio.unesum.edu.ec/handle/53000/2305

Cayllahua, N., & Suárez, J. (2019). Redes neuronales de aprendizaje profundo para el reconocimiento facial y control de acceso de estudiantes a un laboratorio. *Universidad Ricardo Palma*, 149. http://repositorio.urp.edu.pe/handle/urp/1040

Chacón, J. (2007). Sistemas informáticos: Estructura y funciones. Elementos de "Hardware". elementos de "Software." *Preparadores de Oposiciones Para La Enseñanza*, *7*(2), 1–22. https://www.preparadores.eu/temamuestra/PTecnicos/PComerciales.pdf

Chirinos, X., & Calero, P. (2021). Detección Del Uso Correcto De Mascarillas Utilizando Una Red Neuronal Convolucional Para El Ingreso De Personas a Un Laboratorio De Una Universidad. *Universidad Ricardo Palma*, 1–72. https://repositorio.urp.edu.pe/bitstream/handle/URP/4864/T030_47584611_T CHIRINOS CARRANZA XAVIER ALEXANDER.pdf?sequence=1&isAllowed=y

Chung, C. (2024). *El reconocimiento facial llegará pronto a tu aeropuerto más cercano*. The New York Times. https://www.nytimes.com/es/2024/02/21/espanol/reconocimiento-facial-aeropuertos.html

Cortes Osorio, J. A., Medina Aguirre, F. A., & Muriel Escobar, J. A. (2010). Sistemas de seguridad basados en Biometría. *Scientia et Technica*, *17*, 98–102. http://www.redalyc.org/pdf/849/84920977016.pdf

Cristián Bravo, Ramirez, P., & Arenas, J. (2018). Aceptación del Reconocimiento Facial Como Medida de Vigilancia y Seguridad: Un Estudio Empírico en Chile. *Información Tecnológica*. https://doi.org/10.4067/S0718-07642018000200115

Dayana, B., & Jean, R. (2014). Metodología Actual Metodología XP. *Universidad*

Nacional Experimental de Los Llanos Occidentales Ezequiel Zamora, *August*, 1–43.

Deepvisionai. (2020). *Información sobre nosotros*. DeepVisionIA. https://deepvisionai.in

DINA, R. C., & FLOR, R. C. (2019). Implementación De Un Sistema Informático Para La Mejora De La Productividad Del Área De Secretaría Académica En El I.E.S.T.P. Señor De Acoria – Huancavelica. *Repositorio Institucional - UNH*, 80. http://repositorio.unh.edu.pe/handle/UNH/2755

Domingo, C. (2021). Utilización del sistema de reconocimiento facial para preservar la seguridad ciudadana. Use of the facial recognition system to preserve public safety. *El Criminalista Digital*, *2*, 18. https://revistaseug.ugr.es/index.php/cridi/article/view/20899/20280

Espinoza, A. (2013). MANUAL PARA ELEGIR UNA METODOLOGÍA DE DESARROLLO DE SOFTWARE DENTRO DE UN PROYECTO INFORMÁTICO. In *Universidad de Piura*. Universidad de Piura.

Espinoza, D., & Jorquera, P. (2015). Reconocimiento Facial. *Pontificia Universidad Católica de Valparaíso*, 63. http://opac.pucv.cl/pucv_txt/txt-1000/UCD1453_01.pdf

Estudi. (2020). *EL ANÁLISIS FACIAL, ¿EN QUÉ CONSISTE Y PARA QUÉ SIRVE?* Estudi Dental Barcelono. https://estudidentalbarcelona.com/el-analisis-facial-en-que-consiste-y-para-que-sirve/

Figuero, R., Gonzáles, G., & Moreno, C. (2020). Reconocimiento de objetos del hogar, usando redes neuronales convolucionales. *Polo Del Conocimiento*, *5*(01), 563–580.

Figuerola, N. (2011). Kanban, Su Uso en el Desarrollo de Software. In *Journal of Personality*. http://www.ghbook.ir/index.php?name=های رسانه و فرهنگ نوین&option=com_dbook&task=readonline&book_id=13650&page=73&chkhashk=ED9C9491B4&Itemid=218&lang=fa&tmpl=component%0Ahttps://articulositit.files.wordpress.com/2011/11/kanban.pdf

Galindo, D., Huaringa, S., & Samaniego, G. (2021). *Reconocimiento facial para la identificación de los alumnos en exámenes finales en la modalidad presencial de la Universidad Continental – Huancayo, 2021*. Universidad Continental.

Gallo, A. (2022). *Reconocimiento facial ¿Cómo la compu sabe que tú, eres tú?* Medium. https://agustingallof.medium.com/reconocimiento-facial-cómo-la-compu-sabes-que-tú-eres-tú-f8baab6d6e35

Gil, M., López, G., Molina, C., & Bolio, C. (2011). LA GESTIÓN DE LA INFORMACIÓN COMO BASE DE UNA INICIATIVA DE GESTIÓN DEL CONOCIMIENTO. In *Ingeniería Industrial*. Instituto Superior Politécnico José Antonio Echevarría.

Giraldo, A., & Gomez, D. (2017). ESTADO DEL ARTE DE LA SEGURIDAD EN SISTEMAS BIOMETRICOS. *UNIVERSIDAD ABIERTA Y A DISTANCIA*, 94. https://repository.unad.edu.co/bitstream/handle/10596/14348/52752700.pdf?sequence=1&isAllowed=y

Gonzaga, S. L. (2020). Componentes de un sistema informático. *Componente de Un Sistema Informático*. https://repository.uaeh.edu.mx/revistas/index.php/ixtlahuaco/article/view/10403

Google. (n.d.). *Universidad Nacional del Altiplano*. Retrieved July 26, 2024, from https://www.google.com/maps/search/unap/@-15.8286999,-70.0235837,16z/data=!3m1!4b1?entry=ttu&g_ep=EgoyMDI0MDkxMS4wIKXMDSoASAFQAw%3D%3D

Guzmán, P. (2023). EVALUACION DE METODOS DE RECONOCIMIENTO FACIAL PARA ANALISIS AUTOMATICO DE REPORTES DE PREY. *Universidad De Chile*.

Hernandez, A. (n.d.). Los Sistemas de Información: Evolución y Desarrollo. *Universidad de Zaragoza*, 14. https://dialnet.unirioja.es/descarga/articulo/793097.pdf

Hernández, F. (2018). El Concepto de Distancia y su Aplicación en Estadística Multivariada. *Amai*.

Jabbour, G., Márquez, R., Ruiz, L., & Maldonado, L. (2009). Reconocimiento de firmas off-line mediante máquinas de vectores de soporte. *Ciencia e Ingeniería*, *31*(1).

Jeremías, E. (2020). Reconocimiento de objetos a través de la metodología Haar Cascades. *Radi*, *16*(2314–0925), 1–7.

Jiménez, M. (2020). Reconocimiento facial como medida de seguridad para alertar el robo de automoviles. *Universidad Autónoma Del Estado de México*, 106. http://hdl.handle.net/20.500.11799/109601

LaRepública. (2021). *Detienen a sujeto acusado de suplantación en examen de admisión*. Diario La República. https://larepublica.pe/sociedad/2021/10/28/detienen-a-sujeto-acusado-de-suplantacion-en-examen-de-admision-universidad-lrnd

Letelier, P., & Penadés, M. C. (2015). Métodologías ágiles para el desarrollo de software: eXtreme Programming (XP). *Universidad Politécnica de Valencia*, *5*(26), 17. http://www.jstor.org/stable/3541599?origin=crossref

López, G. E. C. (2023). DISEÑO DE UN SISTEMA BIOMÉTRICO PARA EL CONTROL DE ASISTENCIA DEL PERSONAL ADMINISTRATIVO DE LA

ESCUELA SUPERIOR DE ARTE DE LA UNIVERSIDAD DE SAN CARLOS DE GUATEMALA. *Universidad de San Carlos de Guatemala*, *4*, 75. http://emecanica.ingenieria.usac.edu.gt/sitio/wp-content/subidas/6ARTÍCULO-III-INDESA-SIE.pdf

Maida, G., & Pacienzia, J. (2015). Metodologías de desarrollo de software [Universidad Católica Argentina]. In *Biblioteca Digital de la Universidad Católica Argentina*. http://bibliotecadigital.uca.edu.ar/repositorio/tesis/metodologias-desarrollo-software.pdf

Mamani, A. B., & Canahuire, R. C. (2022). Prototipo De Un Sistema De Reconocimiento Facial Para El Control Biométrico En El Colegio Aplicación De La Universidad Nacional Del Altiplano Puno -2019. *Universidad Nacional Del Altiplano*, 1–111. http://repositorio.unap.edu.pe/bitstream/handle/UNAP/7104/Molleapaza_Mamani_Joel_Neftali.pdf?sequence=1&isAllowed=y

Manuel, J. E., Campos, R., Daniel, L., & Luján, A. (2023). Artificial Facial recognition system for access control through Artificial Intelligence. *Revista Innovación y Software*, *4*(1).

Mariscal, F., & Cecilia, R. (2015). *Metodología de Análisis y Diseño de Sistemas de Información*. https://es.slideshare.net/slideshow/metodologia-xp-tarea-msmad/53522681

Matul, M. (2023). DISEÑO DE INVESTIGACIÓN DE UN SISTEMA BIOMÉTRICO DE RECONOCIMIENTO Y VERIFICACIÓN DE IDENTIDAD DE PACIENTES EN HOSPITAL DEL ÁREA METROPOLITANA A TRAVÉS DE REDES DE TELECOMUNICACIONES [Universidad de San Carlos de Guatemala]. In *Universidad de San Carlos de Guatemala* (Vol. 4). http://emecanica.ingenieria.usac.edu.gt/sitio/wp-content/subidas/6ARTÍCULO-III-INDESA-SIE.pdf

MegaPractical. (n.d.). *Metodologías de desarrollo de software* (p. 19).

Meléndez, S., Gaitan, E., & Pérez, N. (2016). Metologia Agil de desarrollo de software programacion extrema [Universidad Nacional Autonoma de Nicaragua, Managua]. In *Universidad Nacional Autonoma de Nicaragua, Managua*. https://repositorio.unan.edu.ni/1365/1/62161.pdf

Mendaza, A., Sanchez, R., Valverde, F., & Hurtado, O. (2010). *Estudio de un sistema de reconocimiento biométrico mediante firma manuscrita online basado en SVM usando Análisis Formal de Conceptos*. ResearchGate. https://www.researchgate.net/publication/47528726_Estudio_de_un_sistema_de_reconocimiento_biometrico_mediante_firma_manuscrita_online_basado_en_SVM_usando_Analisis_Formal_de_Conceptos

Mobbeel. (2024). *¿Qué es el reconocimiento facial? Usos y evolución*. MOBBEEL. https://www.mobbeel.com/reconocimiento-facial/

Montesino, R. Y. (2018). *METODOLOGIAS DE DESARROLLO DE SOFTWARE Y LOS DESARROLLADORES DE LAS MYPES EN TINGO MARÍA, 2017*. Universidad Nacional Hermilio Valdizán.

Morcillo, F. (2020). *Desarrollo de un sistema de reconocimiento facial utilizando Deep Learning con OpenCV* [Universidad Politécnica de Valencia]. https://riunet.upv.es/bitstream/handle/10251/156694/Morcillo - Desarrollo de un sistema de reconocimiento facial utilizando Deep Learning con OpenCV.pdf?sequence=1&isAllowed=y

Moré, J. (2019). *Evaluación de la calidad de los sistemas de reconocimiento de sentimientos*. 7–10.

Muñoz, C. B. (2022). Algoritmos de reconocimiento facial mediante aprendizaje automático para la identificación de personas en una institución educativa de Pasco - 2021. *Tesis de Grado*, 1–135.

Orea, A. (2023). SISTEMA DE CONTROL DE ACCESO A INSTITUCIONES DE EDUCACION SUPERIOR Y MEDIA SUPERIOR A TRAVÉS DE TÉCNICAS DE RECONOCIMIENTO FACIAL. *INSTITUTO TECNOLÓGICO SUPERIOR DE TEZIUTLÁN*.

Ortega, I. (2008). Precisión y Exactitud. *Biodiversidad*, 25–26.

Osvaldo Hernández. (2021). Aproximación a los distintos tipos de muestreo no probabilístico que existen. *SCIELO*. http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S0864-21252021000300002#:~:text=Muestreo por conveniencia%3A La muestra,que establecen criterios a seguir.

Pallero, M., & Heguiabehere, J. (2023). Seguridad de la información y ciberseguridad. In *Ministerio de Ciencia, Tecnología e Innovación* (p. 25). https://fundacionsadosky.org.ar/wp-content/uploads/2023/12/Seguridad-de-la-informacion-y-ciberseguridad.pdf

Panamericana. (2023). *DETIENEN A SUJETOS QUE SUPLANTABAN IDENTIDAD DE POSTULANTES PARA DAR EXAMEN DE ADMISIÓN*. https://panamericana.pe/nacionales/374839-detienen-sujetos-suplantaban-identidad-postulantes-dar-examen-admision

Parrales, J. (2024). DESARROLLO DE UN SOFTWARE PARA EL CONTROL DE PERSONAL MEDIANTE SISTEMA BIOMÉTRICO EN LA UNIDAD EDUCATIVA FISCAL ALEJO LASCANO [Universidad Estatal del Sur de Manabí]. In *Universidad Estatal Del Sur De Manabí*. http://repositorio.unesum.edu.ec/bitstream/53000/3558/1/PONCE ROBLES GABRIELA NICOLE.pdf

Paul Diaz. (2020). *SISTEMA WEB UTILIZANDO OOHDM PARA LA GESTIÓN DE PROCESOS EN EL ÁREA DE ATENCIÓN AL CLIENTE DE LA EMPRESA ELECTRO PUNO S.A.A. - JULIACA 2017* [Universidad Nacional del Altiplano

Puno].
https://repositorio.unap.edu.pe/bitstream/handle/20.500.14082/16245/Diaz_Gomez_Saddam_Paul.pdf?sequence=1&isAllowed=y

Pérez, N. (2021). Los sistemas de reconocimiento facial: una mirada a la luz del examen de proporcionalidad. *Revista Internacional de Derecho Humanos*, *12*(01), 55–88. https://doi.org/10.26422/ridh.2022.1201.per

Pico, M., & Cordero, B. (2019). ANÁLISIS DEL MODELO DE VOTO ELECTRÓNICO CON RECONOCIMIENTO FACIAL PARA LA UNIVERSIDAD ESTATAL DE MILAGRO. *UNIVERSIDAD ESTATAL DE MILAGRO*, 1–23.

Piedra, L. A. Z. (2019). *Control Biométrico para relevo de Conductores con RPI Zero W y GPS Ruptela* (Issue 112). Universidad Tecnológica del Perú.

Posada, P. (n.d.). *SISTEMAS INFORMÁTICOS: ESTRUCTURA, ELEMENTOS, COMPONENTES Y SU FUNCIÓN EN EL CONJUNTO. PROGRAMAS TIPOS Y CARACTERISTICAS.* 18.

Prieto, E. (2012). ¿Sabías que Exactitud no es lo mismo que Precisión? *E-Medida. La Revista Española de Metrologia*, *Febrero*, 2. http://materias.df.uba.ar/f1qa2017c1/files/2012/07/exactitud-precision.pdf

Ramos, C. (2021). Editorial: Diseños de investigación experimental. *CienciAmérica*, *10*(1), 1–7. https://doi.org/10.33210/ca.v10i1.356

Ramos, D. (2018). Detección Automática De Puntos Faciales. *Universidad Militar Nueva Granada*.

Rascón, R. (2019). USO DE DATOS BIOMÉTRICOS COMO MÉTODO PARA OTORGAR EL CONSENTIMIENTO EN LA CONTRATACIÓN

ELECTRÓNICA. ALGUNOS ASPECTOS A CONSIDERAR. *INFOTEC POSGRADOS*, 51.

Rehkopf, M. (n.d.). *¿Qué es un tablero de kanban?* ATLASSIAN. Retrieved August 7, 2024, from https://www.atlassian.com/es/agile/kanban/boards

Resource, S. (2022). *What is Google Cloud Vision?* ResourceSpace. https://www.resourcespace.com/blog/what-is-google-vision

Ríos, R. (2020). INTRODUCCIÓN A LOS MÉTODOS DEL ANÁLISIS DE REDES SOCIALES. *Universidad de California Riverside*.

Rodríguez, Y. M. (2017). Determinación de los umbrales sensoriales de detección, de identificación, de diferenciación y el umbral máximo en el sabor ácido, mediante metodología de elección forzada entre tres alternativas (3- AFC). *Universidad Nacional de Colombia*, *1*, 1–53. https://acortar.link/X5HZR4

Sampieri, R., Collado, C., & Baptista, M. (2014). *Metodología de la Investigación*. McGRAW-HILL. https://apiperiodico.jalisco.gob.mx/api/sites/periodicooficial.jalisco.gob.mx/files/metodologia_de_la_investigacion_-_roberto_hernandez_sampieri.pdf

Sánchez, H., Reyes, C., & Mejía, K. (2018). *Manual de términos en investigación científica, tecnológica y humanística*. Universidad Ricardo Palma.

Sánchez, J. (2015). Pruebas de Software. Fundamentos y Técnicas. *Universidad Politécnica de Madrid*, 130. https://oa.upm.es/40012/1/PFC_JOSE_MANUEL_SANCHEZ_PENO_3.pdf

Schwaber, K., & Sutherland, J. (2020). *La Guía Scrum*.

Sensetime. (n.d.). Face Recognition All-in-one Device. *SensePass*.

Shier, R. (2024). Paired t-test. *Evidence-Based Obstetrics and Gynecology*, *5*(3), 105–106. https://doi.org/10.1016/j.ebobgyn.2003.09.001

Sierra, A. (2024). *Estadística No Paramétrica: Pruebas para proporciones*. El Blog de Leo. https://blog.nekomath.com/estadistica-no-parametrica-pruebas-para-proporciones/

Sierra Santos, L., Casaseca García, P., García Moreno, A., & Martín Gutiérrez, V. (2014). Síndrome de Di George. *Revista Clínica de Medicina de Familia*, *7*(2), 141–143. https://doi.org/10.4321/s1699-695x2014000200010

Sinnaps. (2020). *METODOLOGÍA XP O PROGRAMACIÓN EXTREMA*. SINNAPS. https://www.sinnaps.com/blog-gestion-proyectos/metodologia-xp#google_vignette

Spark, J. (n.d.). *Cinco casos de uso del reconocimiento facial*. Jaak. https://blog.jaak.ai/5-casos-de-uso-del-reconocimiento-facial

Suárez Alfonso, A., Cruz Rodríguez, I., & Pérez Macías, Y. (2015). La gestión de la información: Herramienta esencial para el desarrollo de habilidades en la comunidad estudiantil universitaria. *Revista Universidad y Sociedad*, *7*(3), 72–79. http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S2218-36202015000200011&lang=pt%0Ahttp://scielo.sld.cu/pdf/rus/v7n2/rus10215.pdf

Sullo, P. (2021). PROPUESTA DE IMPLEMENTACIÓN DEL SISTEMA BIOMÉTRICO PARA EL CONTROL DE ASISTENCIA ADMINISTRATIVA DE LA GERENCIA REGIONAL DE EDUCACION MOQUEGUA-2019 [Universidad Autónoma del Perú]. In *Universidad Autónoma del Perú*. https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/50737/Cusma_GM-SD.pdf?sequence=1&isAllowed=y

Talent, D. (2021). *Metodologías de Gestión de Proyectos* (Vol. 2014, Issue 1106).

Tapia, A. (2024). *El detalle que permitió la captura de La Kena en una tienda departamental de San Pedro Garza García*. Infobae. https://www.infobae.com/mexico/2024/01/19/el-detalle-que-permitio-la-captura-de-la-kena-en-una-tienda-departamental-de-san-pedro-garza-garcia/

Thakur, A. (2024). *All About Facial Recognition for Businesses*. GEEKFLARE. https://geekflare.com/facial-recognition-for-business/

Trends, M. (2019). *Best Facial Recognition Software*. Analytics Insight. https://www.analyticsinsight.net/faceimage-recognition/best-facial-recognition-software

Trigas, M., & Domingo, A. (2012). Gestión de Proyectos Informáticos. Metodología Scrum. *Openaccess.Uoc.Edu*, 56. http://www.quimbiotec.gob.ve/sistem/auditoria/pdf/ciudadano/mtrigasTFC0612memoria.pdf%5Cnhttp://openaccess.uoc.edu/webapps/o2/bitstream/10609/17885/1/mtrigasTFC0612memoria.pdf

UPC. (2019). *UPC implementa avanzado sistema de reconocimiento facial para exámenes online*. Innovación Educativa. https://innovacioneducativa.upc.edu.pe/2019/02/14/upc-implementa-avanzado-sistema-de-reconocimiento-facial-para-examenes-online/

USIL. (2022). *USIL implementa nueva plataforma "Exam" de reconocimiento facial para exámenes de admisión y conocimiento a distancia*. USIL. https://blogs.usil.edu.pe/novedades/usil-implementa-nueva-plataforma-exam-de-reconocimiento-facial-para-examenes-de-admision-y-conocimiento-distancia

Valdés, F. (2015). *Reconocimiento de huellas dactilares usando la cámara de un dispositivo móvil* [Universidad de Chile]. https://repositorio.uchile.cl/handle/2250/137108

Valdivieso, Y. (2016). Análisis de Riesgos de los activos de información de la Clínica

Internacional – Piura aplicando la metodología MAGERIT. *Journal of Chemical Information and Modeling*, *53*(9), 1689–1699.

Vázquez, M. Á. (2014). Sistema de Reconocimiento Facial Mediante Técnicas de Visión Tridimensional. In *Centro de Investigación en Optica, A.C.* Centro de Investigación en Optica, A.C.

Velasco, P. (2016). Arquitectura de Software - Conceptos y ciclo de desarrollo. In *Cengage Learning Editores* (Issue April).

Vera, C. A. H. (2015). *Software de control de acceso y registro personal a través de reconocimiento facial para la agencia de turismo CITEFTOURING de la ciudad de Tulcán*. Universidad Regional Autónoma de los Andes "UNIANDES."

Vilcanqui, J. (2023). *Componentes de Un Sistema Informatico - Evaluacion*. SCRIBD. https://es.scribd.com/presentation/617290823/Componentes-de-Un-Sistema-Informatico-Evaluacion

Voces. (2023). *Detectan tres casos de suplantación en Examen de Admisión 2023-2*. Voces. https://diariovoces.com.pe/detectan-tres-casos-de-suplantacion-en-examen-de-admision-2023-2/

Yañez, L. (2019). Sistema de reconocimiento facial para el control de acceso de estudiantes a los laboratorios de la FIIS-UNAC, 2019. In *Repositorio Institucional - UCV*. Universidad César Vallejo.

Yépez Llerena, E. D., & Armijos Guillen, K. F. (2020). Aplicación de la metodología kanban en el desarrollo del software para generación, validación y actualización de reactivos, integrado al sistema informático de control académico unach. [Universidad Nacional de Chimborazo]. In *Universidad Nacional de Chimborazo*. http://dspace.uazuay.edu.ec/bitstream/datos/7646/1/06678.pdf

Adán, A., & Adán, M. (n.d.). *RECONOCIMIENTO A TRAVÉS DE MANOS*. Retrieved July 20, 2024, from https://www.academia.edu/1631683/RECONOCIMIENTO_A_TRAVÉS_DE_MANOS

Ageitgey. (2022). *face_recognition*. Github. https://github.com/ageitgey/face_recognition

Aglio Caballero, A., & Belén, R. S. (2016). IMPLEMENTACIÓN Y EVALUACIÓN DE UN SISTEMA BIOMÉTRICO DE RECONOCIMIENTO DE VENAS DE LAS MANOS MEDIANTE DESCRIPTORES LOCALES DE TEXTURA. *Universidad Politécnica de Madrid*, 1–79. https://zaguan.unizar.es/record/112622/files/TAZ-TFG-2022-641.pdf

Aguilera, M. (2012). *Reconocimiento biométrico basado en imágenes de huellas palmares* [Universidad Autónoma de Madrid]. http://www.jcee.upc.es/JCEE2001/PDFs 2000/13ESPINOSA.pdf

Aguirre, J. (2021). Desarrollo de un Sistema basado en Deep Learning y visión computacional de reconocimiento facial para mejorar el control de acceso a una empresa privada. *Universidad Tecnológica Del Perú*, 6.

Alberto Pérez. (2014). *Diseño De Un Sistemas Basado En Bosques Aleatorios Para La Detección De Tumores Cerebrales Mediante Imágenes Hiperespectrales.* 133.

Alegría, R. F. D. (2020). Métodos cualitativos para la obtención de la información. *Universidad Salazar Virtual*, 103–184.

Alejo, P. (2021). Algoritmo de reconocimiento facial para la gestión del control de acceso de la empresa Altoque PS S.A. *Universidad Cesar Vallejo*, 1–71. https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/50737/Cusma_GM-SD.pdf?sequence=1&isAllowed=y

Amat, J. (2021). *Reconocimiento facial con deep learning y python*. Ciencia de Datos. https://cienciadedatos.net/documentos/py34-reconocimiento-facial-deeplearning-python

Amazon. (2023). *Amazon Rekognition Image*. Aws. https://aws.amazon.com/es/rekognition/image-features/

Aquijes, R., & Ampuero, L. (2021). Implementación de un Sistema de Reconocimiento Facial para el control de acceso del personal en la empresa GUIMARTBOT S.A.C". *Universidad Cesar Vallejo*, 1–71. https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/50737/Cusma_GM-SD.pdf?sequence=1&isAllowed=y

Arango, S. M. D., Campuzano, Z. L. F., & Zapata, C. J. A. (2015). Manufacturing process improvement using the Kanban. *Revista Ingenierías Universidad de Medellín*, *14*(27), 221–234. http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S1692-33242015000200014&lng=en&nrm=iso&tlng=es

Asana, R. (2022). Sistema de reconocimiento facial para el control de acceso en la I.E. 81585 Sagrado Corazón de Jesús de Cartavio - Ascope - La Libertad en el segundo y tercer bimestre del año lectivo 2022. *UNIVERSIDAD PRIVADA ANTENOR ORREGO*, 1–60. http://www.gonzalezcabeza.com/documentos/CRECIMIENTO_MICROBIANO.pdf

AWS. (2023). *¿Qué es el reconocimiento facial?* Amazon. https://aws.amazon.com/es/what-is/facial-recognition/

Aznarte, J. L., Pardos, M. M., & Lacruz López, J. M. (2022). Sobre el uso de tecnologías de reconocimiento facial en la universidad: el caso de la UNED. *RIED-Revista Iberoamericana de Educacion a Distancia*, *25*(1), 261–277. https://doi.org/10.5944/ried.25.1.31533

Barrios, J. (2019). *La matriz de confusión y sus métricas*. BIG DATA. https://www.juanbarrios.com/la-matriz-de-confusion-y-sus-metricas/

Barten, M. (2024). *4 casos de uso de reconocimiento facial en la industria hotelera*. REVFINE. https://www.revfine.com/es/reconocimiento-facial-industria-hotelera/#:~:text=Los usos más comunes del,de acceso a las habitaciones

Basil. (2023). *Face Recognition in Python: A Comprehensive Guide*. Medium. https://basilchackomathew.medium.com/face-recognition-in-python-a-comprehensive-guide-960a48436d0f

Bastos, E. A. V., & Esteves, V. B. (2021). Tecnologias de reconhecimento facial. *Direitos Democráticos & Estado Moderno*, *3*, 216–240. https://doi.org/10.23925/ddem.i3.53875

Bernad, M., & Rodriguez, M. (2020). *Sistemas Informáticos, tipos y clasificación*.

Bernal, A. (2021). Facultad De Ingeniería, Arquitectura Y Urbanismo. *Universidad Señor de Sipán*, 141.

Bravo, C. J., Ramírez, P. E., & Arenas, J. (2018). Aceptación del Reconocimiento Facial Como Medida de Vigilancia y Seguridad: Un Estudio Empírico en Chile. *Información Tecnológica*, *29*(2), 115–122. https://doi.org/10.4067/s0718-07642018000200115

Cabrera, F. (n.d.). Kanban : Metodología ágil de desarrollo de Software. *Universidad Nacional Del Sur*.

Cadena, J. (2021). Técnica eficiente para reconocimiento facial global utilizando wavelets y máquinas de vectores de soporte en imágenes 3D. *Universidad Nacional Mayor de San Marcos*, 258.

Calderon Arateco, L. L. (2019). Seguridad informática y seguridad de la informacion. *Universidad Piloto de Colombia.* http://repository.unipiloto.edu.co/handle/20.500.12277/2821

Calizaya, M., & Calsin, F. (2022). MODELO PARA LA DETECCIÓN DE ANOMALÍAS EN SECUENCIAS DE VIDEOS DE EXÁMENES EN LÍNEA MEDIANTE INTELIGENCIA ARTIFICIAL CASO DE ESTUDIO: UNIVERSIDAD NACIONAL DEL ALTIPLANO. *Universidad Nacional Del Altiplano*, 1–168. http://repositorio.unap.edu.pe/bitstream/handle/UNAP/7104/Molleapaza_Mamani_Joel_Neftali.pdf?sequence=1&isAllowed=y

Cannatella, T., Méndez, M., & Sández, P. (2022). Identificación de Personas en Sistemas de Videovigilancia sin uso de Reconocimiento Facial. *XXVIII Congreso Argentino de Ciencias de La Computación - CACIC 2022*, 957–961. http://sedici.unlp.edu.ar/bitstream/handle/10915/149626/Documento_completo.pdf?sequence=1&isAllowed=y%0Ahttp://sedici.unlp.edu.ar/handle/10915/149626

Cárdenas, L. (2016). El patrón de arquitectura n-capas con orientación al dominio como solución en el diseño de aplicaciones empresariales. *Revista Tecnología & Desarrollo*, *11*(1), 59–66. https://doi.org/10.18050/td.v11i1.679

Carrasco, S. (2005). Metodología de la investigación científica: Pautas metodológicas para diseñar y elaborar el proyecto de investigación. : Aplicaciones en educación y otras ciencias sociales. In *Lima [Perú] : San Marcos*.

Castro, P. (2018). Implementación de un sistema de control de acceso biométrico zk-x7 por medio de huella dactilar en el laboratorio de hardware de la carrera de ingeniería en computación y redes. *Universidad Estatal Del Sur de Manabí*, *05*. http://repositorio.unesum.edu.ec/handle/53000/2305

Cayllahua, N., & Suárez, J. (2019). Redes neuronales de aprendizaje profundo para el

reconocimiento facial y control de acceso de estudiantes a un laboratorio. *Universidad Ricardo Palma*, 149. http://repositorio.urp.edu.pe/handle/urp/1040

Chacón, J. (2007). Sistemas informáticos: Estructura y funciones. Elementos de "Hardware". elementos de "Software." *Preparadores de Oposiciones Para La Enseñanza*, *7*(2), 1–22. https://www.preparadores.eu/temamuestra/PTecnicos/PComerciales.pdf

Chirinos, X., & Calero, P. (2021). Detección Del Uso Correcto De Mascarillas Utilizando Una Red Neuronal Convolucional Para El Ingreso De Personas a Un Laboratorio De Una Universidad. *Universidad Ricardo Palma*, 1–72. https://repositorio.urp.edu.pe/bitstream/handle/URP/4864/T030_47584611_T CHIRINOS CARRANZA XAVIER ALEXANDER.pdf?sequence=1&isAllowed=y

Chung, C. (2024). *El reconocimiento facial llegará pronto a tu aeropuerto más cercano*. The New York Times. https://www.nytimes.com/es/2024/02/21/espanol/reconocimiento-facial-aeropuertos.html

Cortes Osorio, J. A., Medina Aguirre, F. A., & Muriel Escobar, J. A. (2010). Sistemas de seguridad basados en Biometría. *Scientia et Technica*, *17*, 98–102. http://www.redalyc.org/pdf/849/84920977016.pdf

Cristián Bravo, Ramirez, P., & Arenas, J. (2018). Aceptación del Reconocimiento Facial Como Medida de Vigilancia y Seguridad: Un Estudio Empírico en Chile. *Información Tecnológica*. https://doi.org/10.4067/S0718-07642018000200115

Dayana, B., & Jean, R. (2014). Metodología Actual Metodología XP. *Universidad Nacional Experimental de Los Llanos Occidentales Ezequiel Zamora*, *August*, 1–43.

Deepvisionai. (2020). *Información sobre nosotros*. DeepVisionIA.

https://deepvisionai.in

DINA, R. C., & FLOR, R. C. (2019). Implementación De Un Sistema Informático Para La Mejora De La Productividad Del Área De Secretaría Académica En El I.E.S.T.P. Señor De Acoria – Huancavelica. *Repositorio Institucional - UNH*, 80. http://repositorio.unh.edu.pe/handle/UNH/2755

Domingo, C. (2021). Utilización del sistema de reconocimiento facial para preservar la seguridad ciudadana. Use of the facial recognition system to preserve public safety. *El Criminalista Digital*, *2*, 18. https://revistaseug.ugr.es/index.php/cridi/article/view/20899/20280

Espinoza, A. (2013). MANUAL PARA ELEGIR UNA METODOLOGÍA DE DESARROLLO DE SOFTWARE DENTRO DE UN PROYECTO INFORMÁTICO. In *Universidad de Piura*. Universidad de Piura.

Espinoza, D., & Jorquera, P. (2015). Reconocimiento Facial. *Pontificia Universidad Católica de Valparaíso*, 63. http://opac.pucv.cl/pucv_txt/txt-1000/UCD1453_01.pdf

Estudi. (2020). *EL ANÁLISIS FACIAL, ¿EN QUÉ CONSISTE Y PARA QUÉ SIRVE?* Estudi Dental Barcelono. https://estudidentalbarcelona.com/el-analisis-facial-en-que-consiste-y-para-que-sirve/

Figuero, R., Gonzáles, G., & Moreno, C. (2020). Reconocimiento de objetos del hogar, usando redes neuronales convolucionales. *Polo Del Conocimiento*, *5*(01), 563–580.

Figuerola, N. (2011). Kanban, Su Uso en el Desarrollo de Software. In *Journal of Personality*. http://www.ghbook.ir/index.php?name=های رسانه و فرهنگ نوین&option=com_dbook&task=readonline&book_id=13650&page=73&chkhashk=ED9C9491B4&Itemid=218&lang=fa&tmpl=component%0Ahttps://articulositfiles.wordpress.com/2011/11/kanban.pdf

Galindo, D., Huaringa, S., & Samaniego, G. (2021). *Reconocimiento facial para la identificación de los alumnos en exámenes finales en la modalidad presencial de la Universidad Continental – Huancayo, 2021*. Universidad Continental.

Gallo, A. (2022). *Reconocimiento facial ¿Cómo la compu sabe que tú, eres tú?* Medium. https://agustingallof.medium.com/reconocimiento-facial-cómo-la-compu-sabes-que-tú-eres-tú-f8baab6d6e35

Gil, M., López, G., Molina, C., & Bolio, C. (2011). LA GESTIÓN DE LA INFORMACIÓN COMO BASE DE UNA INICIATIVA DE GESTIÓN DEL CONOCIMIENTO. In *Ingeniería Industrial*. Instituto Superior Politécnico José Antonio Echevarría.

Giraldo, A., & Gomez, D. (2017). ESTADO DEL ARTE DE LA SEGURIDAD EN SISTEMAS BIOMETRICOS. *UNIVERSIDAD ABIERTA Y A DISTANCIA*, 94. https://repository.unad.edu.co/bitstream/handle/10596/14348/52752700.pdf?sequence=1&isAllowed=y

Gonzaga, S. L. (2020). Componentes de un sistema informático. *Componente de Un Sistema Informático*. https://repository.uaeh.edu.mx/revistas/index.php/ixtlahuaco/article/view/10403

Google. (n.d.). *Universidad Nacional del Altiplano*. Retrieved July 26, 2024, from https://www.google.com/maps/search/unap/@-15.8286999,-70.0235837,16z/data=!3m1!4b1?entry=ttu&g_ep=EgoyMDI0MDkxMS4wIKXMDSoASAFQAw%3D%3D

Guzmán, P. (2023). EVALUACION DE METODOS DE RECONOCIMIENTO FACIAL PARA ANALISIS AUTOMATICO DE REPORTES DE PREY. *Universidad De Chile*.

Hernandez, A. (n.d.). Los Sistemas de Información: Evolución y Desarrollo. *Universidad de Zaragoza*, 14.

https://dialnet.unirioja.es/descarga/articulo/793097.pdf

Hernández, F. (2018). El Concepto de Distancia y su Aplicación en Estadística Multivariada. *Amai*.

Jabbour, G., Márquez, R., Ruiz, L., & Maldonado, L. (2009). Reconocimiento de firmas off-line mediante máquinas de vectores de soporte. *Ciencia e Ingeniería*, *31*(1).

Jeremías, E. (2020). Reconocimiento de objetos a través de la metodología Haar Cascades. *Radi*, *16*(2314–0925), 1–7.

Jiménez, M. (2020). Reconocimiento facial como medida de seguridad para alertar el robo de automoviles. *Universidad Autónoma Del Estado de México*, 106. http://hdl.handle.net/20.500.11799/109601

LaRepública. (2021). *Detienen a sujeto acusado de suplantación en examen de admisión*. Diario La República. https://larepublica.pe/sociedad/2021/10/28/detienen-a-sujeto-acusado-de-suplantacion-en-examen-de-admision-universidad-lrnd

Letelier, P., & Penadés, M. C. (2015). Métodologías ágiles para el desarrollo de software: eXtreme Programming (XP). *Universidad Politécnica de Valencia*, *5*(26), 17. http://www.jstor.org/stable/3541599?origin=crossref

López, G. E. C. (2023). DISEÑO DE UN SISTEMA BIOMÉTRICO PARA EL CONTROL DE ASISTENCIA DEL PERSONAL ADMINISTRATIVO DE LA ESCUELA SUPERIOR DE ARTE DE LA UNIVERSIDAD DE SAN CARLOS DE GUATEMALA. *Universidad de San Carlos de Guatemala*, *4*, 75. http://emecanica.ingenieria.usac.edu.gt/sitio/wp-content/subidas/6ARTÍCULO-III-INDESA-SIE.pdf

Maida, G., & Pacienzia, J. (2015). Metodologías de desarrollo de software [Universidad

Católica Argentina]. In *Biblioteca Digital de la Universidad Católica Argentina*. http://bibliotecadigital.uca.edu.ar/repositorio/tesis/metodologias-desarrollo-software.pdf

Mamani, A. B., & Canahuire, R. C. (2022). Prototipo De Un Sistema De Reconocimiento Facial Para El Control Biométrico En El Colegio Aplicación De La Universidad Nacional Del Altiplano Puno -2019. *Universidad Nacional Del Altiplano*, 1–111. http://repositorio.unap.edu.pe/bitstream/handle/UNAP/7104/Molleapaza_Mamani_Joel_Neftali.pdf?sequence=1&isAllowed=y

Manuel, J. E., Campos, R., Daniel, L., & Luján, A. (2023). Artificial Facial recognition system for access control through Artificial Intelligence. *Revista Innovación y Software*, *4*(1).

Mariscal, F., & Cecilia, R. (2015). *Metodología de Análisis y Diseño de Sistemas de Información*. https://es.slideshare.net/slideshow/metodologia-xp-tarea-msmad/53522681

Matul, M. (2023). DISEÑO DE INVESTIGACIÓN DE UN SISTEMA BIOMÉTRICO DE RECONOCIMIENTO Y VERIFICACIÓN DE IDENTIDAD DE PACIENTES EN HOSPITAL DEL ÁREA METROPOLITANA A TRAVÉS DE REDES DE TELECOMUNICACIONES [Universidad de San Carlos de Guatemala]. In *Universidad de San Carlos de Guatemala* (Vol. 4). http://emecanica.ingenieria.usac.edu.gt/sitio/wp-content/subidas/6ARTÍCULO-III-INDESA-SIE.pdf

MegaPractical. (n.d.). *Metodologías de desarrollo de software* (p. 19).

Meléndez, S., Gaitan, E., & Pérez, N. (2016). Metologia Agil de desarrollo de software programacion extrema [Universidad Nacional Autonoma de Nicaragua, Managua]. In *Universidad Nacional Autonoma de Nicaragua, Managua*. https://repositorio.unan.edu.ni/1365/1/62161.pdf

Mendaza, A., Sanchez, R., Valverde, F., & Hurtado, O. (2010). *Estudio de un sistema de reconocimiento biométrico mediante firma manuscrita online basado en SVM usando Análisis Formal de Conceptos*. ResearchGate. https://www.researchgate.net/publication/47528726_Estudio_de_un_sistema_de_reconocimiento_biometrico_mediante_firma_manuscrita_online_basado_en_SVM_usando_Analisis_Formal_de_Conceptos

Mobbeel. (2024). *¿Qué es el reconocimiento facial? Usos y evolución*. MOBBEEL. https://www.mobbeel.com/reconocimiento-facial/

Montesino, R. Y. (2018). *METODOLOGIAS DE DESARROLLO DE SOFTWARE Y LOS DESARROLLADORES DE LAS MYPES EN TINGO MARÍA, 2017*. Universidad Nacional Hermilio Valdizán.

Morcillo, F. (2020). *Desarrollo de un sistema de reconocimiento facial utilizando Deep Learning con OpenCV* [Universidad Politécnica de Valencia]. https://riunet.upv.es/bitstream/handle/10251/156694/Morcillo - Desarrollo de un sistema de reconocimiento facial utilizando Deep Learning con OpenCV.pdf?sequence=1&isAllowed=y

Moré, J. (2019). *Evaluación de la calidad de los sistemas de reconocimiento de sentimientos*. 7–10.

Muñoz, C. B. (2022). Algoritmos de reconocimiento facial mediante aprendizaje automático para la identificación de personas en una institución educativa de Pasco - 2021. *Tesis de Grado*, 1–135.

Orea, A. (2023). SISTEMA DE CONTROL DE ACCESO A INSTITUCIONES DE EDUCACION SUPERIOR Y MEDIA SUPERIOR A TRAVÉS DE TÉCNICAS DE RECONOCIMIENTO FACIAL. *INSTITUTO TECNOLÓGICO SUPERIOR DE TEZIUTLÁN*.

Ortega, I. (2008). Precisión y Exactitud. *Biodiversidad*, 25–26.

Osvaldo Hernández. (2021). Aproximación a los distintos tipos de muestreo no probabilístico que existen. *SCIELO*. http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S0864-21252021000300002#:~:text=Muestreo por conveniencia%3A La muestra,que establecen criterios a seguir.

Pallero, M., & Heguiabehere, J. (2023). Seguridad de la información y ciberseguridad. In *Ministerio de Ciencia, Tecnología e Innovación* (p. 25). https://fundacionsadosky.org.ar/wp-content/uploads/2023/12/Seguridad-de-la-informacion-y-ciberseguridad.pdf

Panamericana. (2023). *DETIENEN A SUJETOS QUE SUPLANTABAN IDENTIDAD DE POSTULANTES PARA DAR EXAMEN DE ADMISIÓN*. https://panamericana.pe/nacionales/374839-detienen-sujetos-suplantaban-identidad-postulantes-dar-examen-admision

Parrales, J. (2024). DESARROLLO DE UN SOFTWARE PARA EL CONTROL DE PERSONAL MEDIANTE SISTEMA BIOMÉTRICO EN LA UNIDAD EDUCATIVA FISCAL ALEJO LASCANO [Universidad Estatal del Sur de Manabí]. In *Universidad Estatal Del Sur De Manabí*. http://repositorio.unesum.edu.ec/bitstream/53000/3558/1/PONCE ROBLES GABRIELA NICOLE.pdf

Paul Diaz. (2020). *SISTEMA WEB UTILIZANDO OOHDM PARA LA GESTIÓN DE PROCESOS EN EL ÁREA DE ATENCIÓN AL CLIENTE DE LA EMPRESA ELECTRO PUNO S.A.A. - JULIACA 2017* [Universidad Nacional del Altiplano Puno]. https://repositorio.unap.edu.pe/bitstream/handle/20.500.14082/16245/Diaz_Gomez_Saddam_Paul.pdf?sequence=1&isAllowed=y

Pérez, N. (2021). Los sistemas de reconocimiento facial: una mirada a la luz del examen de proporcionalidad. *Revista Internacional de Derecho Humanos*, *12*(01), 55–88. https://doi.org/10.26422/ridh.2022.1201.per

Pico, M., & Cordero, B. (2019). ANÁLISIS DEL MODELO DE VOTO ELECTRÓNICO CON RECONOCIMIENTO FACIAL PARA LA UNIVERSIDAD ESTATAL DE MILAGRO. *UNIVERSIDAD ESTATAL DE MILAGRO*, 1–23.

Piedra, L. A. Z. (2019). *Control Biométrico para relevo de Conductores con RPI Zero W y GPS Ruptela* (Issue 112). Universidad Tecnológica del Perú.

Posada, P. (n.d.). *SISTEMAS INFORMÁTICOS: ESTRUCTURA, ELEMENTOS, COMPONENTES Y SU FUNCIÓN EN EL CONJUNTO. PROGRAMAS TIPOS Y CARACTERISTICAS.* 18.

Prieto, E. (2012). ¿Sabías que Exactitud no es lo mismo que Precisión? *E-Medida. La Revista Española de Metrologia*, *Febrero*, 2. http://materias.df.uba.ar/f1qa2017c1/files/2012/07/exactitud-precision.pdf

Ramos, C. (2021). Editorial: Diseños de investigación experimental. *CienciAmérica*, *10*(1), 1–7. https://doi.org/10.33210/ca.v10i1.356

Ramos, D. (2018). Detección Automática De Puntos Faciales. *Universidad Militar Nueva Granada*.

Rascón, R. (2019). USO DE DATOS BIOMÉTRICOS COMO MÉTODO PARA OTORGAR EL CONSENTIMIENTO EN LA CONTRATACIÓN ELECTRÓNICA. ALGUNOS ASPECTOS A CONSIDERAR. *INFOTEC POSGRADOS*, 51.

Rehkopf, M. (n.d.). *¿Qué es un tablero de kanban?* ATLASSIAN. Retrieved August 7, 2024, from https://www.atlassian.com/es/agile/kanban/boards

Resource, S. (2022). *What is Google Cloud Vision?* ResourceSpace. https://www.resourcespace.com/blog/what-is-google-vision

Ríos, R. (2020). INTRODUCCIÓN A LOS MÉTODOS DEL ANÁLISIS DE REDES SOCIALES. *Universidad de California Riverside*.

Rodríguez, Y. M. (2017). Determinación de los umbrales sensoriales de detección, de identificación, de diferenciación y el umbral máximo en el sabor ácido, mediante metodología de elección forzada entre tres alternativas (3- AFC). *Universidad Nacional de Colombia*, *1*, 1–53. https://acortar.link/X5HZR4

Sampieri, R., Collado, C., & Baptista, M. (2014). *Metodología de la Investigación*. McGRAW-HILL. https://apiperiodico.jalisco.gob.mx/api/sites/periodicooficial.jalisco.gob.mx/files/metodologia_de_la_investigacion_-_roberto_hernandez_sampieri.pdf

Sánchez, H., Reyes, C., & Mejía, K. (2018). *Manual de términos en investigación científica, tecnológica y humanística*. Universidad Ricardo Palma.

Sánchez, J. (2015). Pruebas de Software. Fundamentos y Técnicas. *Universidad Politécnica de Madrid*, 130. https://oa.upm.es/40012/1/PFC_JOSE_MANUEL_SANCHEZ_PENO_3.pdf

Schwaber, K., & Sutherland, J. (2020). *La Guía Scrum*.

Sensetime. (n.d.). Face Recognition All-in-one Device. *SensePass*.

Shier, R. (2024). Paired t-test. *Evidence-Based Obstetrics and Gynecology*, *5*(3), 105–106. https://doi.org/10.1016/j.ebobgyn.2003.09.001

Sierra, A. (2024). *Estadística No Paramétrica: Pruebas para proporciones*. El Blog de Leo. https://blog.nekomath.com/estadistica-no-parametrica-pruebas-para-proporciones/

Sierra Santos, L., Casaseca García, P., García Moreno, A., & Martín Gutiérrez, V.

(2014). Síndrome de Di George. *Revista Clínica de Medicina de Familia*, *7*(2), 141–143. https://doi.org/10.4321/s1699-695x2014000200010

Sinnaps. (2020). *METODOLOGÍA XP O PROGRAMACIÓN EXTREMA*. SINNAPS. https://www.sinnaps.com/blog-gestion-proyectos/metodologia-xp#google_vignette

Spark, J. (n.d.). *Cinco casos de uso del reconocimiento facial*. Jaak. https://blog.jaak.ai/5-casos-de-uso-del-reconocimiento-facial

Suárez Alfonso, A., Cruz Rodríguez, I., & Pérez Macías, Y. (2015). La gestión de la información: Herramienta esencial para el desarrollo de habilidades en la comunidad estudiantil universitaria. *Revista Universidad y Sociedad*, *7*(3), 72–79. http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S2218-36202015000200011&lang=pt%0Ahttp://scielo.sld.cu/pdf/rus/v7n2/rus10215.pdf

Sullo, P. (2021). PROPUESTA DE IMPLEMENTACIÓN DEL SISTEMA BIOMÉTRICO PARA EL CONTROL DE ASISTENCIA ADMINISTRATIVA DE LA GERENCIA REGIONAL DE EDUCACION MOQUEGUA-2019 [Universidad Autónoma del Perú]. In *Universidad Autónoma del Perú*. https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/50737/Cusma_GM-SD.pdf?sequence=1&isAllowed=y

Talent, D. (2021). *Metodologías de Gestión de Proyectos* (Vol. 2014, Issue 1106).

Tapia, A. (2024). *El detalle que permitió la captura de La Kena en una tienda departamental de San Pedro Garza García*. Infobae. https://www.infobae.com/mexico/2024/01/19/el-detalle-que-permitio-la-captura-de-la-kena-en-una-tienda-departamental-de-san-pedro-garza-garcia/

Thakur, A. (2024). *All About Facial Recognition for Businesses*. GEEKFLARE. https://geekflare.com/facial-recognition-for-business/

Trends, M. (2019). *Best Facial Recognition Software*. Analytics Insight. https://www.analyticsinsight.net/faceimage-recognition/best-facial-recognition-software

Trigas, M., & Domingo, A. (2012). Gestión de Proyectos Informáticos. Metodología Scrum. *Openaccess.Uoc.Edu*, 56. http://www.quimbiotec.gob.ve/sistem/auditoria/pdf/ciudadano/mtrigasTFC0612memoria.pdf%5Cnhttp://openaccess.uoc.edu/webapps/o2/bitstream/10609/17885/1/mtrigasTFC0612memoria.pdf

UPC. (2019). *UPC implementa avanzado sistema de reconocimiento facial para exámenes online*. Innovación Educativa. https://innovacioneducativa.upc.edu.pe/2019/02/14/upc-implementa-avanzado-sistema-de-reconocimiento-facial-para-examenes-online/

USIL. (2022). *USIL implementa nueva plataforma "Exam" de reconocimiento facial para exámenes de admisión y conocimiento a distancia*. USIL. https://blogs.usil.edu.pe/novedades/usil-implementa-nueva-plataforma-exam-de-reconocimiento-facial-para-examenes-de-admision-y-conocimiento-distancia

Valdés, F. (2015). *Reconocimiento de huellas dactilares usando la cámara de un dispositivo móvil* [Universidad de Chile]. https://repositorio.uchile.cl/handle/2250/137108

Valdivieso, Y. (2016). Análisis de Riesgos de los activos de información de la Clínica Internacional – Piura aplicando la metodología MAGERIT. *Journal of Chemical Information and Modeling*, *53*(9), 1689–1699.

Vázquez, M. Á. (2014). Sistema de Reconocimiento Facial Mediante Técnicas de Visión Tridimensional. In *Centro de Investigación en Optica, A.C.* Centro de Investigación en Optica, A.C.

Velasco, P. (2016). Arquitectura de Software - Conceptos y ciclo de desarrollo. In

Cengage Learning Editores (Issue April).

Vera, C. A. H. (2015). *Software de control de acceso y registro personal a través de reconocimiento facial para la agencia de turismo CITEFTOURING de la ciudad de Tulcán*. Universidad Regional Autónoma de los Andes "UNIANDES."

Vilcanqui, J. (2023). *Componentes de Un Sistema Informatico - Evaluacion*. SCRIBD. https://es.scribd.com/presentation/617290823/Componentes-de-Un-Sistema-Informatico-Evaluacion

Voces. (2023). *Detectan tres casos de suplantación en Examen de Admisión 2023-2*. Voces. https://diariovoces.com.pe/detectan-tres-casos-de-suplantacion-en-examen-de-admision-2023-2/

Yañez, L. (2019). Sistema de reconocimiento facial para el control de acceso de estudiantes a los laboratorios de la FIIS-UNAC, 2019. In *Repositorio Institucional - UCV*. Universidad César Vallejo.

Yépez Llerena, E. D., & Armijos Guillen, K. F. (2020). Aplicación de la metodología kanban en el desarrollo del software para generación, validación y actualización de reactivos, integrado al sistema informático de control académico unach. [Universidad Nacional de Chimborazo]. In *Universidad Nacional de Chimborazo*. http://dspace.uazuay.edu.ec/bitstream/datos/7646/1/06678.pdf

ANEXOS

ANEXO 1: Solicitud de autorización y recolección de datos

SOLICITO: AUTORIZACIÓN PARA REALIZAR TRABAJO DE INVESTIGACIÓN

Estimado Dr. JUAN CARLOS BENAVIDES HUANCA
DIRECTOR DE LA DIRECCIÓN DE ADMISIÓN DE LA UNA PUNO.

Yo, Mendoza Nina Adderly, identificado con número de DNI: 75360230. Me dirijo a usted con el propósito de solicitar su autorización para implementar y aplicar un sistema de reconocimiento facial en el proceso de control biométrico durante el examen de admisión extraordinario de la Universidad Nacional del Altiplano de Puno, programado para el año 2024. Esta iniciativa forma parte de mi tesis titulada **"Sistema informático con reconocimiento facial para mejorar el control biométrico en el examen de admisión extraordinario"**.

Para llevar a cabo esta implementación de manera efectiva, es esencial contar con información precisa y actualizada sobre los postulantes.

Cabe destacar que la información recopilada será utilizada exclusivamente para fines académicos y de investigación, garantizando en todo momento la confidencialidad y la protección de los datos personales de los postulantes.

Agradezco de antemano su atención a esta solicitud y quedo a la espera de su pronta respuesta. Estoy a su disposición para proporcionar cualquier información adicional que considere necesaria.

Atentamente,

Mendoza Nina Adderly
DNI: 75360230

ANEXO 2: Cuestionario para la usabilidad del sistema con reconocimiento facial

CUESTIONARIO PARA EVALUAR LA USABILIDAD DEL SISTEMA CON RECONOCIMIENTO FACIAL EN EL EXAMEN DE ADMISIÓN EXTRAORDINARIO DE LA UNIVERSIDAD NACIONAL DEL ALTIPLANO PUNO, 2024

Instrucciones: Estimado(a) participante, a continuación, se presentan 8 preguntas sobre su experiencia con el sistema de reconocimiento facial. Le solicitamos que indique su nivel de satisfacción marcando con una "X" la opción que mejor refleje su opinión.

Escala de medición:

Muy insatisfecho	Insatisfecho	Indiferente	Satisfecho	Muy satisfecho
1	2	3	4	5

Nº	Pregunta	1	2	3	4	5
1	¿Qué tan satisfecho está con el rendimiento general del sistema de reconocimiento facial?					
2	¿Considera que el sistema cumple con sus expectativas para realizar el control biométrico?					
3	¿Cómo calificaría la facilidad de uso del sistema?					
4	¿Recomendaría este sistema para su uso en otros procesos de control biométrico?					
5	¿Qué tan confiable considera que es el sistema para reconocer correctamente a las personas registradas?					
6	¿Ha experimentado algún error en el reconocimiento facial que le haga desconfiar del sistema?					
7	¿Se siente seguro utilizando el sistema de reconocimiento facial en un entorno de trabajo?					
8	¿Considera que el sistema de reconocimiento facial protege adecuadamente los datos y la privacidad de los usuarios?					

ANEXO 3: Validación del cuestionario por el Alfa de Cronbach

	ITEMS (PREGUNTAS)								
ENCUESTADOS	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**SUMA**
E1	4	4	5	4	3	2	3	3	28
E2	5	4	5	4	5	3	5	5	36
E3	4	3	3	3	4	3	4	4	28
E4	4	4	3	2	2	2	3	3	23
E5	5	4	5	5	4	2	4	3	32
E6	4	5	4	4	3	2	4	4	30
E7	4	4	5	4	3	3	5	4	32
E8	3	5	5	2	3	3	3	4	28
E9	5	4	5	4	5	2	5	4	34
E10	3	4	5	5	2	2	4	5	30
E11	3	2	3	2	4	3	3	5	25
E12	3	3	3	4	4	2	4	4	27
E13	4	5	5	4	4	3	5	5	35
E14	3	3	4	3	4	2	3	4	26
VARIANZA	**0,55102**	**0,693878**	**0,77551**	**0,959184**	**0,816327**	**0,244898**	**0,637755**	**0,494898**	
SUMATORIA DE VARIANZAS	**5,173469388**								
VARIANZA DE LA SUMA DE LAS PREGUNTAS	**13,81632653**								

Reemplazando en la fórmula para hallar α:

$$\alpha = \frac{K}{K-1}\left[1 - \frac{\sum V_i}{Vt}\right] = \frac{8}{8-1}\left[1 - \frac{5.17346}{13.81632}\right] = 0.71$$

De acuerdo con la tabla de clasificación de fiabilidad basada en el Alfa de Cronbach, un valor de 0.71 se considera aceptable.

Índice	Nivel de fiabilidad	Valor de Alfa de Cronbach
1	Excelente	]0.9, 1]
2	Muy bueno	]0.7, 0.9]
3	Bueno	]0.5, 0.7]
4	Regular	]0.3, 0.5]
5	Deficiente [	0, 0.3]

Por lo tanto, podemos concluir que el cuestionario presenta un buen nivel de fiabilidad para el propósito de nuestra investigación.

ANEXO 4: Ficha de registro para la precisión

FICHA DE REGISTRO				
INVESTIGADOR		Mendoza Nina Adderly		
OBJETIVO		Calcular la precisión del sistema en el control biométrico		
Lugar de estudio		Universidad Nacional del Altiplano		
Ubicación		Av. Floral 1153, Puno		
DATOS TÉCNICOS				
TIPO DE PRUEBA		PRE-TEST		
		POST-TEST		
DIMENSIÓN		**MEDIDA**	Porcentual (%)	
Indicador	Precisión			
PRECISIÓN(P) = VP/(VP+FP)		**VP:** Predicciones correctas **FP:** Predicciones incorrectas		
Nº	**Ubicación**	**Fecha**	**Correcto**	**Incorrecto**

ANEXO 5: Ficha de medición para el tiempo

FICHA DE MEDICIÓN				Nº
Lugar de estudio		Universidad Nacional del Altiplano		
Ubicación		Av. Floral 1153, Puno		
Variable dependiente		Control biométrico	**Dimensión**	Tiempo de control
Fórmula		$\frac{\sum_{i=n}^{n} t_i}{n}$	**Indicador**	Tiempo (s)
TIPO DE PRUEBA		PRE-TEST		
		POST-TEST		
Nº	**Fecha**	**Tiempo**	**Observación**	

ANEXO 6: Ficha de medición para la seguridad

IDENTIFICACIÓN DE ACTIVOS			
Nombre:			
Puesto:			
ACTIVO POR TIPO			**(X) = SI**
D	**Data/Información**		
[backup]	Copias de respaldo		
[password]	Credenciales (contraseñas)		
[auth]	Datos de validación de credenciales		
[source]	Codigo fuente		
[exe]	Codigo ejecutable		
SW	**Aplicacioness/Software**		
[prp]	Desarrollo propio		
[sub]	Desarrollo a medida		
HW	**Equipos informáticos**		
[pc]	Computadora personal		
[vhost]	Equipos virtuales		
[peripheral]	Periféricos		
[camera]		Cámara	
[print]		Medios de impresión	
[firewall]	Cortafuegos		
SI	**Soporte de información**		
[electronic]	Electrónicos		
[disk]		Discos	
[vdisk]		Discos virtuales	
[san]		Almacenamiento en red	
[usb]		Dispositivos de UB	

IDENTIFICACIÓN DE AMENAZAS		
Nombre:		
Puesto:		
AMENAZAS		**(X) = SI**
N	**Amenazas Naturales**	
[N.1]	Daños por fuego	
[N.2]	Daños por agua	
[N.3]	Desastres Naturales	
E	**Errores y fallos no intecionales**	
[E.1]	Errores de usuario	
[E.2]	Errores de configuración	
[E.3]	Pérdida de equipos	
[E.4]	Vulnerabilidad del sistema	
[E.5]	Errores de actualización de software	
A	**Ataques malintecionados**	
[A.1]	Abuso de privilegios	
[A.2]	Destrucción de información	
[A.3]	Destrucción de equipos	

ANEXO 7: Matriz de consistencia

Sistema informático con reconocimiento facial para mejorar el control biométrico en el examen de admisión extraordinario de la Universidad Nacional del Altiplano Puno, 2024

<table>
<tr><th>FORMULACIÓN DEL PROBLEMA</th><th>OBJETIVOS</th><th>HIPÓTESIS</th><th>VARIABLES</th><th>DIMENSIONES</th><th>INDICADORES</th><th>METODOLOGÍA DE LA INVESTIGACIÓN</th></tr>
<tr><td>PROBLEMA GENERAL:</td><td>OBJETIVO GENERAL:</td><td>HIPÓTESIS PRINCIPAL:</td><td>VARIABLE INDEPENDIENTE:</td><td>PARA LA VARIABLE INDEPENDIENTE</td><td>PARA LA VARIABLE INDEPENDIENTE</td><td>TIPO DE INVESTIGACIÓN</td></tr>
<tr><td rowspan="3">¿Es posible mejorar el control biométrico en el examen de admisión extraordinario de la Universidad Nacional del Altiplano mediante un sistema informático con reconocimiento facial?</td><td rowspan="3">Desarrollar un sistema informático de reconocimiento facial para mejorar el control biométrico en el examen de admisión extraordinario de la Universidad Nacional del Altiplano en el año 2024.</td><td rowspan="3">El sistema informático con reconocimiento facial incidirá positivamente en el control biométrico del examen extraordinario de la Universidad Nacional del Altiplano Puno en el año 2024.</td><td rowspan="3">Sistema informático con reconocimiento facial</td><td rowspan="3">Usabilidad</td><td>Satisfacción del usuario final</td><td rowspan="3">De acuerdo a los objetivos formulados y propósito de la investigación, el presente proyecto reúne las condiciones para ser una investigación de tipo aplicada.</td></tr>
<tr><td>Facilidad de uso</td></tr>
<tr><td></td><td>ENFOQUE DE INVESTIGACIÓN</td></tr>
</table>

<table>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td>En esta investigación se ha seguido un enfoque cuantitativo.</td></tr>
<tr><td>PROBLEMAS ESPECÍFICOS:</td><td>OBJETIVOS ESPECÍFICOS:</td><td>HIPÓTESIS ESPECÍFICAS:</td><td>VARIABLE DEPENDIENTE:</td><td>PARA LA VARIABLE DEPENDIENTE</td><td>PARA LA VARIABLE DEPENDIENTE</td><td>DISEÑO DE INVESTIGACIÓN</td></tr>
<tr><td rowspan="2">¿Cuál es la precisión del sistema informático con reconocimiento facial en el control biométrico de los postulantes al examen de admisión extraordinario de la Universidad Nacional del Altiplano?</td><td rowspan="2">Calcular la precisión del sistema informático de reconocimiento facial en el control biométrico del examen extraordinario de la Universidad Nacional del Altiplano Puno en el año 2024.</td><td rowspan="2">La precisión del sistema informático con reconocimiento facial es mayor que la de los métodos tradicionales en el control biométrico de los postulantes.</td><td rowspan="3">Control biométrico en el examen de admisión extraordinario de la UNAP.</td><td rowspan="2">Precisión</td><td rowspan="2">Porcentaje de precisión</td><td>El diseño del presente proyecto de investigación es cuasiexperimental con corte transversal.</td></tr>
<tr><td>POBIACIÓN, MUESTRA Y MUESTREO</td></tr>
<tr><td>¿Qué tiempo de respuesta tiene el sistema informático con reconocimiento facial en el control biométrico de los postulantes al examen de admisión extraordinario de la Universidad Nacional del Altiplano?</td><td>Medir el tiempo de respuesta del sistema informático de reconocimiento facial en el control biométrico del examen extraordinario de la Universidad Nacional del Altiplano Puno en el año 2024.</td><td>El tiempo de respuesta del sistema informático con reconocimiento facial es menor que el de los métodos tradicionales en el control biométrico de los postulantes.</td><td>Tiempo de control</td><td>Tiempo promedio</td><td>Población:
422 postulantes al examen de admisión extraordinario de la UNAP, año 2024.

Muestra:
100 postulantes al examen de admisión extraordinario de la UNAP, año 2024

Muestreo:
No probabilístico por conveniencia</td></tr>
</table>

						TÉCNICAS E INSTRUMENTOS DE RECOLECCIÓN DE DATOS
¿Cuál es el nivel de seguridad del sistema informático con reconocimiento facial en el control biométrico de los postulantes al examen de admisión extraordinario de la Universidad Nacional del Altiplano?	Evaluar el nivel de seguridad del sistema informático de reconocimiento facial en el control biométrico del examen extraordinario de la Universidad Nacional del Altiplano Puno en el año 2024.	El nivel de seguridad del sistema informático con reconocimiento facial es mayor que el de los métodos tradicionales en el control biométrico de los postulantes.		Seguridad	Nivel de seguridad	**Técnica:** - Fichaje - Solicitud - Cuestionario - Revisión documentaria **Instrumento:** - Solicitud - Ficha de registro - Ficha de medición - Ficha de evaluación - Cuestionario - Análisis documental

ANEXO 8: Declaración jurada de autenticidad de tesis

Universidad Nacional del Altiplano Puno | VRI Vicerrectorado de Investigación | Repositorio Institucional

DECLARACIÓN JURADA DE AUTENTICIDAD DE TESIS

Por el presente documento, Yo Adderly Mendoza Nina,
identificado con DNI 75360230 en mi condición de egresado de:

☒ **Escuela Profesional,** ☐ **Programa de Segunda Especialidad,** ☐ **Programa de Maestría o Doctorado**
INGENIERÍA DE SISTEMAS,
informo que he elaborado el/la ☒ **Tesis** o ☐ **Trabajo de Investigación** denominada:
"Sistema informático con reconocimiento facial para mejorar el control biométrico en el examen de admisión extraordinario de la Universidad Nacional del Altiplano Puno, 2024"

Es un tema original.

Declaro que el presente trabajo de tesis es elaborado por mi persona y **no existe plagio/copia** de ninguna naturaleza, en especial de otro documento de investigación (tesis, revista, texto, congreso, o similar) presentado por persona natural o jurídica alguna ante instituciones académicas, profesionales, de investigación o similares, en el país o en el extranjero.

Dejo constancia que las citas de otros autores han sido debidamente identificadas en el trabajo de investigación, por lo que no asumiré como suyas las opiniones vertidas por terceros, ya sea de fuentes encontradas en medios escritos, digitales o Internet.

Asimismo, ratifico que soy plenamente consciente de todo el contenido de la tesis y asumo la responsabilidad de cualquier error u omisión en el documento, así como de las connotaciones éticas y legales involucradas.

En caso de incumplimiento de esta declaración, me someto a las disposiciones legales vigentes y a las sanciones correspondientes de igual forma me someto a las sanciones establecidas en las Directivas y otras normas internas, así como las que me alcancen del Código Civil y Normas Legales conexas por el incumplimiento del presente compromiso

Puno 19 de Noviembre del 2024

FIRMA (obligatoria)

Huella

ANEXO 9: Autorización para el depósito de tesis en el Repositorio Institucional

Universidad Nacional del Altiplano Puno | VRI Vicerrectorado de Investigación | Repositorio Institucional

AUTORIZACIÓN PARA EL DEPÓSITO DE TESIS O TRABAJO DE INVESTIGACIÓN EN EL REPOSITORIO INSTITUCIONAL

Por el presente documento, Yo ADDERLY MENDOZA NINA,
identificado con DNI 75360230 en mi condición de egresado de:

☒ **Escuela Profesional,** ☐ **Programa de Segunda Especialidad,** ☐ **Programa de Maestría o Doctorado**

INGENIERÍA DE SISTEMAS,

informo que he elaborado el/la ☒ **Tesis** o ☐ **Trabajo de Investigación** denominada:

"Sistema informático con reconocimiento facial para mejorar el control biométrico en el examen de admisión extraordinario de la Universidad Nacional del Altiplano Puno, 2024"

para la obtención de ☐ **Grado,** ☒ **Título Profesional** o ☐ **Segunda Especialidad.**

Por medio del presente documento, afirmo y garantizo ser el legítimo, único y exclusivo titular de todos los derechos de propiedad intelectual sobre los documentos arriba mencionados, las obras, los contenidos, los productos y/o las creaciones en general (en adelante, los "Contenidos") que serán incluidos en el repositorio institucional de la Universidad Nacional del Altiplano de Puno.

También, doy seguridad de que los contenidos entregados se encuentran libres de toda contraseña, restricción o medida tecnológica de protección, con la finalidad de permitir que se puedan leer, descargar, reproducir, distribuir, imprimir, buscar y enlazar los textos completos, sin limitación alguna.

Autorizo a la Universidad Nacional del Altiplano de Puno a publicar los Contenidos en el Repositorio Institucional y, en consecuencia, en el Repositorio Nacional Digital de Ciencia, Tecnología e Innovación de Acceso Abierto, sobre la base de lo establecido en la Ley N° 30035, sus normas reglamentarias, modificatorias, sustitutorias y conexas, y de acuerdo con las políticas de acceso abierto que la Universidad aplique en relación con sus Repositorios Institucionales. Autorizo expresamente toda consulta y uso de los Contenidos, por parte de cualquier persona, por el tiempo de duración de los derechos patrimoniales de autor y derechos conexos, a título gratuito y a nivel mundial.

En consecuencia, la Universidad tendrá la posibilidad de divulgar y difundir los Contenidos, de manera total o parcial, sin limitación alguna y sin derecho a pago de contraprestación, remuneración ni regalía alguna a favor mío; en los medios, canales y plataformas que la Universidad y/o el Estado de la República del Perú determinen, a nivel mundial, sin restricción geográfica alguna y de manera indefinida, pudiendo crear y/o extraer los metadatos sobre los Contenidos, e incluir los Contenidos en los índices y buscadores que estimen necesarios para promover su difusión.

Autorizo que los Contenidos sean puestos a disposición del público a través de la siguiente licencia:

Creative Commons Reconocimiento-NoComercial-CompartirIgual 4.0 Internacional. Para ver una copia de esta licencia, visita: https://creativecommons.org/licenses/by-nc-sa/4.0/

En señal de conformidad, suscribo el presente documento.

Puno 19 de Noviembre del 2024

FIRMA (obligatoria)

Huella