PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

FACULTAD DE INGENIERÍA



TRABAJO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULO DE MÁSTER EN TECNOLOGÍAS DE LA INFORMACIÓN MENCIÓN EN GESTIÓN Y ADMINISTRACIÓN DE TECNOLOGÍAS

TEMA:

"IMPACTO DE LA INTELIGENCIA ARTIFICIAL EN LA SEGURIDAD CIUDADANA EN AEROPUERTOS"

AUTOR:

SANDRA ELIZABETH GARROCHAMBA SÁNCHEZ

DIRECTOR:

MSC. DAMIÁN ANÍBAL NICOLALDE RODRÍGUEZ

QUITO, AGOSTO 2024

PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR FACULTAD DE INGENIERÍA

DECLARACIÓN Y AUTORIZACIÓN

Yo, **Sandra Elizabeth Garrochamba Sánchez**, con cédula de ciudadanía No. **1900743707**, autor del trabajo de graduación titulado: **"IMPACTO DE LA INTELIGENCIA ARTIFICIAL EN LA SEGURIDAD CIUDADANA EN AEROPUERTOS"**, previo a la obtención del título de **Magíster en Tecnologías de Información mención Gestión y Administración de TI**, de la Facultad de Ingeniería:

1. Declaro tener pleno conocimiento de la obligación que tiene la Pontificia Universidad Católica del Ecuador, de conformidad con el artículo 144 de la Ley Orgánica de Educación Superior, de entregar a la SENESCYT en formato digital una copia del referido trabajo de graduación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.
2. Autorizo a la Pontificia Universidad Católica del Ecuador a difundir a través de sitio web de la Biblioteca de la PUCE, el referido trabajo de graduación, respetando las políticas de propiedad intelectual de Universidad.

Quito D.M., 28 de agosto de 2024

Atentamente;

Sandra Elizabeth Garrochamba Sánchez
Autor del Trabajo de Titulación

JESUITAS ECUADOR

APROBACIÓN DEL DIRECTOR

En mi carácter de Director (a) – Tutor (a) del Trabajo de Posgrado Titulado: **"IMPACTO DE LA INTELIGENCIA ARTIFICIAL EN LA SEGURIDAD CIUDADANA EN AEROPUERTOS",** presentado por la maestrante **Sandra Elizabeth Garrochamba Sánchez**, con cédula de ciudadanía No. 1900743707, para la obtención del título de **Magíster en Tecnologías de Información mención Gestión y Administración de TI**, considero que dicho Trabajo de Investigación reúne los requisitos y méritos suficientes para ser sometido a la evaluación por parte de los Lectores – Evaluadores que se designen para tal fin por parte de las autoridades de la Facultad de Ingeniería.

En la ciudad de Quito D.M., a los 28 días de agosto de 2024.

Atentamente;

Msc. Damián Aníbal Nicolalde Rodríguez

Tutor del Trabajo de Titulación

JESUITAS ECUADOR

HOJA DE EVIDENCIA ANTIPLAGIO

TURNITIN: INCLUIR HOJA DEL INFORME CON EL PORCENTAJE

JESUITAS ECUADOR

DECLARACIÓN DE AUTENTICIDAD Y RESPONSABILIDAD

Yo, **Sandra Elizabeth Garrochamba Sánchez**, con cédula de ciudadanía No. 1900743707, declaro que los resultados obtenidos en la investigación **"IMPACTO DE LA INTELIGENCIA ARTIFICIAL EN LA SEGURIDAD CIUDADANA EN AEROPUERTOS**", como requisito previo para lo obtención del del título de **Magíster en Tecnologías de Información mención Gestión y Administración de TI** son absolutamente originales, auténticos y personales.

En tal virtud, declaro que el contenido, las conclusiones y los efectos legales y académicos, que se desprenden del trabajo de investigación, y luego de la redacción de este documento, son y serán de mi sola y exclusiva responsabilidad legal y académica.

En la ciudad de Quito D.M., a los 28 días de mes de agosto de 2024.

Atentamente;

Sandra Elizabeth Garrochamba Sánchez
Autor del Trabajo de Titulación

JESUITAS ECUADOR

DEDICATORIA

Se la dedico a mi esposo por ser incondicional y apoyarme en todas mis metas. A mi hija Melina por darme fuerzas con su ternura para seguir adelante. A mis queridos padres por su amor incondicional y apoyo constante en cada etapa de mi vida. A mi hermana, hermanos, sobrina y sobrino por su amor y sus palabras de aliento que han sido mi motivación a lo largo de este camino.

JESUITAS ECUADOR

AGRADECIMIENTO

A Dios por ser mi fortaleza en todo este proceso. A mi esposo Michael, por su amor, paciencia y apoyo durante este camino. A mi hija Melina por ser mi fuente de energía y motivación cada día. A mis padres, hermanos, hermana sobrino, sobrina y cuñado por brindarme su amor y cariño. A mi tutor Msc. Damián Aníbal Nicolalde Rodríguez por su acompañamiento y guía durante el desarrollo de mi trabajo de titulación. A mis amigos por alentarme a culminar esta meta. Y a la Empresa Pública Metropolitana de Servicios Aeroportuario por permitirme desarrollar mi trabajo de titulación.

JESUITAS ECUADOR

TABLA DE CONTENIDOS

PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR i
DECLARACIÓN Y AUTORIZACIÓN ii
APROBACIÓN DEL DIRECTOR iii
HOJA DE EVIDENCIA ANTIPLAGIO iv
DECLARACIÓN DE AUTENTICIDAD Y RESPONSABILIDAD v
DEDICATORIA vi
AGRADECIMIENTO vii
TABLA DE CONTENIDOS viii
ÍNDICE DE TABLAS ix
ÍNDICE DE FIGURAS x
RESUMEN xi
ABSTRACT xii
CAPÍTULO I: PLANTEAMIENTO DEL PROBLEMA 1
1. Introducción 1
1.1. Justificación 1
1.2. Planteamiento del problema 2
1.2.1. Formulación del problema 3
1.3. Contextualización del tema u objeto: inteligencia artificial. 4
1.4. Objetivos 5
1.4.1. Objetivo general 5
1.4.2. Objetivos específicos 5
1.5. Marco Teórico y Conceptual 5
1.5.1. Antecedentes o marco referencial 5
CAPÍTULO II: REVISIÓN DE LA LITERATURA 9
2. MARCO TEÓRICO 9
2.1. Inteligencia artificial 9
2.2. Seguridad en aeropuertos 12
2.3. Reconocimiento facial 13
2.4. Consideraciones éticas en el reconocimiento facial 26
2.5. Marco regulatorio y normativo de reconocimiento facial en aeropuertos 28
CAPÍTULO III: METODOLOGÍA 35
3. Metodología 35
3.1. Introducción a la metodología 35
3.2. Tipo de investigación 35

JESUITAS ECUADOR

3.3. Enfoque de investigación 36
3.4. Diseño de la investigación 37
3.5. Población y muestra 38
CAPÍTULO IV: RESULTADOS 40
4. RESULTADOS 40
4.1. Fase 1: Revisión Documental 40
4.2. Resultados del análisis de inclusión y exclusión 43
4.4. Fase 2: Investigación empírica 49
4.4.1. Parte Cuantitativa 58
CAPÍTULO V: ANÁLISIS DE RESULTADOS 68
5. ANÁLISIS DE RESULTADOS 68
5.1. Análisis de la entrevista aplicada al experto de seguridad 68
5.2. Análisis de los resultados de la encuesta aplicada al personal de seguridad del aeropuerto 70
CAPÍTULO VI: CONCLUSIONES Y RECOMENDACIONES 72
6. CONCLUSIONES Y RECOMENDACIONES 72
6.1. Conclusiones 72
6.2. Recomendaciones 72
CAPÍTULO VII: REFERENCIAS 74
7. REFERENCIAS BIBLIOGRÁFICAS 74
CAPÍTULO VIII: ANEXOS 77
8. ANEXOS 77
8.1. Encuesta sobre el impacto de la inteligencia artificial en la seguridad ciudadana en aeropuertos 77
8.2. Entrevista sobre el impacto de la inteligencia artificial en la seguridad ciudadana en aeropuertos 82

ÍNDICE DE TABLAS

Tabla 1: Criterios de inclusión y exclusión. 40
Tabla 2: Comparación de métodos tradicionales vs. modernos. 45
Tabla 3: Resultados pregunta 1 de la encuesta. 58
Tabla 4: Resultados pregunta 2 de la encuesta. 59
Tabla 5: Resultados pregunta 3 de la encuesta. 60
Tabla 6: Resultados pregunta 4 de la encuesta. 61
Tabla 7: Resultados pregunta 5 de la encuesta. 62
Tabla 8: Resultados pregunta 6 de la encuesta. 63
Tabla 9: Resultados pregunta 7 de la encuesta. 64
Tabla 10: Resultados pregunta 8 de la encuesta. 65

JESUITAS ECUADOR

Tabla 11: Resultados pregunta 9 de la encuesta...... 66
Tabla 12: Resultados pregunta 10 de la encuesta...... 67

ÍNDICE DE FIGURAS

Figura 2: Resultados pregunta 1 de la encuesta. 58
Figura 3: Resultados pregunta 2 de la encuesta. 59
Figura 4: Resultados pregunta 3 de la encuesta. 60
Figura 5: Resultados pregunta 4 de la encuesta. 61
Figura 6: Resultados pregunta 5 de la encuesta. 62
Figura 7: Resultados pregunta 6 de la encuesta. 63
Figura 8: Resultados pregunta 7 de la encuesta. 64
Figura 9: Resultados pregunta 8 de la encuesta. 65
Figura 10: Resultados pregunta 9 de la encuesta. 66
Figura 11: Resultados pregunta 10 de la encuesta. 67

JESUITAS ECUADOR

Tema: “Impacto de la inteligencia artificial en la seguridad ciudadana en aeropuertos.”

Autor: Sandra Elizabeth Garrochamba Sánchez

RESUMEN

La investigación aborda el impacto de la inteligencia artificial (IA) en la seguridad ciudadana en aeropuertos, destacando el uso del reconocimiento facial para detectar y prevenir amenazas. Se ha evidenciado que la implementación de sistemas de reconocimiento facial basados en IA mejora la seguridad, acelera los procesos de control de pasajeros y permite identificar a personas buscadas por las autoridades de manera más eficiente. Sin embargo, este avance también plantea preocupaciones éticas, como el riesgo de violaciones de privacidad, sesgos en la identificación y desafíos legales. La investigación realiza un análisis comparativo entre técnicas tradicionales y modernas de reconocimiento facial, evaluando su precisión y eficacia, así como sus implicaciones éticas. Al final, se proponen recomendaciones para mejorar la aceptación y funcionamiento de estas tecnologías en el ámbito aeroportuario.

Palabras clave: Inteligencia Artificial, Seguridad ciudadana**,** Aeropuertos**,** Reconocimiento facial**,** Ética**,** Privacidad**,** Tecnología**,** Análisis comparativo**,** Métodos tradicionales.

JESUITAS ECUADOR

Theme: "Impact of artificial intelligence on citizen security at airports."

Author: Sandra Elizabeth Garrochamba Sánchez

ABSTRACT

This research examines the impact of artificial intelligence (AI) on citizen security at airports, focusing on the use of facial recognition to detect and prevent threats. It has been demonstrated that the implementation of AI-based facial recognition systems enhances security, speeds up passenger control processes, and effectively identifies wanted individuals. However, this advancement also raises ethical concerns, such as potential privacy violations, biases in identification, and legal challenges. The study conducts a comparative analysis between traditional and modern facial recognition techniques, evaluating their accuracy and effectiveness along with their ethical implications. Finally, recommendations are proposed to improve the acceptance and functionality of these technologies in the airport context.

Keywords: Artificial intelligence, Citizen security, Airports, facial recognition, Ethics, Privacy, Technology, Comparative analysis, Traditional methods.

JESUITAS ECUADOR

CAPÍTULO I: PLANTEAMIENTO DEL PROBLEMA

1. Introducción

1.1. Justificación

La seguridad ciudadana es esencial para cualquier sociedad. Los gobiernos y las autoridades encargadas de mantener el orden deben garantizar la protección y el bienestar de los ciudadanos. La creciente amenaza de terrorismo, contrabando y otros delitos hace que la seguridad en los aeropuertos sea una prioridad global. Según un informe de la Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC) de 2021, el tráfico ilícito de drogas sigue siendo un problema crítico, con un aumento del 15% en el tráfico transfronterizo en los últimos cinco años. Además, el Global Terrorism Index 2022 informó que el terrorismo ha aumentado en varias regiones del mundo, destacando la necesidad de medidas de seguridad más robustas.

Los aeropuertos son partes importantes de la infraestructura de transporte global, y cualquier falla en su seguridad puede tener un impacto negativo significativo tanto en la economía como en la confianza pública en el sistema de transporte aéreo. En las últimas décadas, las amenazas a la seguridad en los aeropuertos han aumentado significativamente. Los aeropuertos se enfrentan a desafíos complejos, como el aumento de ataques terroristas y el contrabando de drogas y mercancías ilegales.

Una de las tecnologías más prometedoras para mejorar la seguridad en los aeropuertos es la inteligencia artificial (IA). La IA supera ampliamente las capacidades humanas y las técnicas tradicionales de seguridad para analizar grandes volúmenes de datos en tiempo real, reconocer patrones y detectar anomalías. Esto la convierte en una herramienta prometedora para mejorar la seguridad ciudadana de manera más eficiente y efectiva. La implementación de IA en los procesos de seguridad aeroportuaria puede generar mejoras significativas. Un informe de 2023 de la Asociación Internacional de Transporte Aéreo (IATA) mostró que el uso de inteligencia artificial puede reducir el tiempo de procesamiento de pasajeros en un 30%, mejorando la experiencia del viajero y, al mismo tiempo, manteniendo altos estándares de seguridad.

Los sistemas de reconocimiento facial, análisis de comportamiento y detección de objetos sospechosos permiten una vigilancia más precisa y rápida, reduciendo el tiempo de

JESUITAS ECUADOR

respuesta ante posibles amenazas. Además, con el aumento de las ciudades inteligentes, la seguridad ciudadana se está convirtiendo en un desafío crucial que la IA está bien posicionada para abordar. En algunos aeropuertos, se están utilizando Sensores ópticos para supervisar la longitud de las filas de pasajeros, la rapidez con que las personas avanzan a través de los puntos de seguridad, además de sistemas de videovigilancia y cámaras equipadas con inteligencia artificial, para el reconocimiento facial de personas sospechosas o buscadas por la justicia. También se están implementando cámaras térmicas asistidas por IA, capaces de medir la temperatura corporal en cuestión de segundos, lo que es particularmente relevante en el contexto de la pandemia de COVID-19.

Un caso de éxito en la implementación de tecnología de inteligencia artificial en la seguridad aeroportuaria es el aeropuerto de Schiphol en Ámsterdam. Schiphol ha implementado un sistema de reconocimiento facial basado en inteligencia artificial que ha demostrado ser altamente efectivo en la identificación de personas sospechosas y en la prevención de posibles amenazas (Airport Technology, 2021). Otro ejemplo destacado es el aeropuerto de Singapur Changi, que ha implementado sistemas de inteligencia artificial para el análisis de comportamiento de los pasajeros y la detección de comportamientos sospechosos, contribuyendo a una reducción del 20% en los incidentes de seguridad (Liu, J., et al., 2019).

Por lo expuesto, este tema se centra en la urgencia de mejorar la seguridad en los aeropuertos en respuesta a amenazas complejas y cambiantes, mediante el uso de la inteligencia artificial para crear sistemas de seguridad más eficientes, efectivos y respetuosos con los pasajeros. Esta investigación no solo impulsará el progreso científico y tecnológico, sino que también tendrá un impacto significativo en la seguridad y eficiencia de los aeropuertos de todo el mundo.

1.2. Planteamiento del problema

La seguridad en aeropuertos se ha convertido en un tema crítico a nivel global, especialmente ante el crecimiento del tráfico aéreo y la evolución constante de las amenazas potenciales. La protección de pasajeros, personal y las instalaciones de los aeropuertos requiere de una vigilancia eficiente y eficaz. Sin embargo, la supervisión humana y las tecnologías convencionales han demostrado ser insuficientes para detectar y prevenir amenazas sofisticadas.

Las técnicas tradicionales de reconocimiento facial, aunque ampliamente utilizadas, enfrentan múltiples desafíos:

- **Sensibilidad a condiciones ambientales:** Estas técnicas suelen ser muy sensibles a variaciones en la iluminación, ángulos de visión y expresiones faciales, lo que limita su eficacia en diversas situaciones del mundo real.
- **Robustez ante oclusiones:** El rendimiento de sistemas de reconocimiento facial disminuye significativamente en condiciones de oclusión, donde partes del rostro pueden estar cubiertas.
- **Sesgos y discriminación:** Existen preocupaciones serias sobre la precisión de los algoritmos de reconocimiento facial, que tienden a presentar tasas de error más altas al identificar a personas de ciertos grupos étnicos, géneros o rangos de edad. Esto se debe, en gran medida, a conjuntos de datos utilizados para entrenar estos sistemas que no son suficientemente diversos.
- **Vulnerabilidad a ataques:** Los métodos tradicionales son más susceptibles a ataques de presentación (por ejemplo, imágenes o videos manipulados), lo que compromete su fiabilidad en entornos de alta seguridad.
- **Problemas éticos y legales:** A pesar de las ventajas en seguridad, su uso puede acarrear detenciones injustificadas y preocupaciones sobre la invasión de la privacidad, lo que subraya la necesidad de un enfoque equilibrado entre seguridad y derechos individuales.

Además, aunque la inteligencia artificial se está aplicando ya en el ámbito de la seguridad pública, su implementación en aeropuertos también enfrenta varios retos:

- **Privacidad y protección de datos:** La recolección y el procesamiento de datos biométricos plantea serias cuestiones sobre la protección de la privacidad.
- **Fiabilidad y tasa de error:** Los sistemas de IA deben demostrar una fiabilidad superior y minimizar errores para ser considerados viables en entornos críticos.
- **Falta de regulación y supervisión:** La carencia de directrices claras y regulaciones sobre el uso de IA en seguridad genera incertidumbres en su aplicación y consecuencias potenciales de su uso.

1.2.1. Formulación del problema

La formulación del problema se centra en la necesidad de investigar y desarrollar sistemas de reconocimiento facial basados en inteligencia artificial que sean más precisos y éticos para mejorar la seguridad en los aeropuertos. Específicamente, se busca abordar las siguientes interrogantes:

JESUITAS ECUADOR

- ¿Cómo puede la inteligencia artificial mejorar la detección de amenazas en los aeropuertos a través del reconocimiento facial?

- ¿Cómo se pueden superar las limitaciones y desafíos existentes en las técnicas tradicionales de reconocimiento facial, como la sensibilidad a variaciones en la iluminación, la vulnerabilidad a ataques y la falta de diversidad en los conjuntos de datos de entrenamiento?

- ¿Qué consideraciones éticas y de privacidad deben tenerse en cuenta al implementar sistemas de reconocimiento facial basados en inteligencia artificial en entornos aeroportuarios?

- ¿Cómo se puede garantizar la fiabilidad, precisión y no discriminación de los sistemas de reconocimiento facial basados en inteligencia artificial en entornos aeroportuarios, y cómo pueden supervisarse y regularse estos sistemas de manera efectiva?

1.3. Contextualización del tema u objeto: inteligencia artificial.

La inteligencia artificial se ha convertido en una herramienta cada vez más relevante en la sociedad actual, siendo aplicada en una amplia gama de industrias y sectores, incluyendo la seguridad ciudadana. En particular, en aeropuertos, donde la seguridad es una prioridad fundamental, la inteligencia artificial ha demostrado ser una herramienta invaluable para mejorar la eficiencia y precisión de los sistemas de seguridad.

El impacto de la inteligencia artificial en la seguridad ciudadana en aeropuertos se manifiesta en diversas formas. Por un lado, la IA permite el análisis y procesamiento de grandes volúmenes de datos en tiempo real, lo que facilita la detección de posibles amenazas o anomalías de manera más rápida y efectiva. Asimismo, los algoritmos de aprendizaje automático pueden identificar patrones y comportamientos sospechosos, ayudando a prevenir incidentes de seguridad antes de que ocurran, la inteligencia artificial se utiliza en la automatización de procesos de seguridad, como el reconocimiento facial y la detección de objetos prohibidos, lo que agiliza los controles de seguridad y reduce la posibilidad de errores humanos. Del mismo modo, los sistemas de IA pueden realizar un seguimiento de la ubicación y movimiento de los pasajeros dentro del aeropuerto, mejorando la coordinación y la respuesta en caso de emergencias.

La inteligencia artificial ha revolucionado la seguridad ciudadana en aeropuertos, proporcionando herramientas avanzadas y eficientes que garantizan la protección de los pasajeros y el personal aeroportuario. Su impacto positivo se refleja en una mayor eficacia en la detección de amenazas, una respuesta más rápida ante posibles incidentes y una mejora general en la experiencia de viaje de los pasajeros.

JESUITAS ECUADOR

1.4. Objetivos

1.4.1. Objetivo general

Realizar un estudio comparativo de las técnicas de inteligencia artificial que están siendo usadas para el reconocimiento facial de personas sospechosas o buscados por la justicia en aeropuertos versus métodos tradicionales en términos de precisión y ética.

1.4.2. Objetivos específicos

- Identificar los métodos tradicionales de reconocimiento facial que se están utilizando para el reconocimiento facial de personas sospechosas en aeropuertos.
- Describir las técnicas de IA más usadas para el reconocimiento facial.
- Realizar un análisis descriptivo comparativo de la precisión de las técnicas tradicionales frente a las técnicas contemporáneas más utilizadas para el reconocimiento facial.
- Realizar un estudio bibliográfico que permita la identificación de las implicaciones éticas que se tiene en el reconocimiento facial.

1.5. Marco Teórico y Conceptual

1.5.1. Antecedentes o marco referencial

Los aeropuertos, al ser nodos críticos en la infraestructura de transporte de naciones, han sido históricamente objetivos primordiales para posibles amenazas terroristas y actividades ilegales. Desde los ataques del 11 de septiembre de 2001, el enfoque en la seguridad aeroportuaria ha experimentado transformaciones significativas, invirtiendo en tecnología y protocolos de seguridad más sofisticados para prevenir eventos similares. Aparte de las prácticas tradicionales, como las inspecciones manuales y el uso de escáneres de rayos X y detectores de metales, la implementación de tecnología avanzada ha comenzado a jugar un papel crucial.

En los últimos años, la inteligencia artificial (IA) ha introducido mejoras notables en la seguridad aeroportuaria. El reconocimiento facial se ha integrado en los procesos de identificación de pasajeros, utilizando algoritmos avanzados para verificar identidades y detectar comportamientos sospechosos. Esto ha generado un debate sobre las implicaciones éticas y la regulación de su uso.

A continuación, se detallan algunos estudios relevantes:

JESUITAS ECUADOR

Carrasco (2020) analizó las implicaciones éticas y legales del reconocimiento facial en España, subrayando que su uso debe estar vinculado a la proporcionalidad, identificando personas con razones fundadas de sospecha.

Jaramillo (2020) abordó la vulneración de derechos en el uso del reconocimiento facial, enfatizando la necesidad de un marco legal claro que defina límites y objetivos en el contexto de la seguridad pública.

Tomás Balmaceda et al. (2021) exploraron la historia del vínculo entre la tecnología de reconocimiento facial y los temas de seguridad, resaltando la percepción errónea de que estos sistemas son inherentemente objetivos y exentos de sesgos.

Ortiz (2021) analizó los sesgos de género asociados a sistemas de IA, destacando que la falta de un marco ético en la implementación de tecnologías de reconocimiento facial puede comprometer valores democráticos fundamentales.

Garnica y Usiña (2022) presentaron una plataforma de reconocimiento facial en tiempo real para la búsqueda de personas desaparecidas. Este sistema, basado en aprendizaje profundo y redes neuronales, enfatiza la aplicación de la IA en problemas sociales críticos.

Taype, Gallardo y Samaniego (2021) desarrollaron un sistema de reconocimiento facial utilizado en contextos académicos, demostrando la efectividad de la tecnología para abordar problemas de suplantación de identidad y evaluando su precisión con métricas cuantitativas.

A continuación, se detallan estudios recientes:

Smith y Hsu (2023) investigaron la integración de tecnologías de detección de amenazas en la seguridad aeroportuaria, proponiendo un enfoque holístico que combina el reconocimiento facial con sensores de comportamiento para una vigilancia más eficaz. Su estudio resalta la importancia del análisis de datos en tiempo real para detectar patrones inusuales, mejorando así la seguridad general.

Miller et al. (2022) realizaron un estudio sobre el impacto de las tecnologías de reconocimiento facial en la experiencia del viajero, sugiriendo que, si bien mejoran la eficiencia del proceso de embarque, también suscitan preocupaciones sobre la privacidad y el consentimiento informado de los pasajeros.

Fernández y Gómez (2023) profundizaron en la efectividad de las medidas de seguridad en aeropuertos post-pandemia, destacando la creciente dependencia de la tecnología, incluida la automatización y la IA, para adaptarse a nuevas normativas y comportamientos de los viajeros.

Zhang et al. (2023) investigaron el uso de tecnologías de inteligencia artificial en la detección de fraudes en embarques y equipajes, proponiendo un modelo predictivo que combina aprendizaje

automático y análisis de comportamiento para mejorar la seguridad sin comprometer la experiencia del pasajero.

La evolución de la Inteligencia Artificial (IA) comienza en la década de 1940, cuando se llevaron a cabo las primeras investigaciones sobre la posibilidad de crear máquinas que fueran capaces de pensar y aprender como un ser humano. Durante la Segunda Guerra Mundial, matemáticos y expertos en computación, como Alan Turing, John von Neumann (quien hizo contribuciones significativas a la teoría de juegos, crucial para la toma de decisiones en IA) y Norbert Wiener (reconocido por su trabajo en cibernética y por acuñar el término "cibernética"), se dedicaron al desarrollo de técnicas de cálculo y procesamiento de información que serían fundamentales para el avance posterior de la IA.

En los años 50, la IA se enfocó en el diseño de programas informáticos que pudieran replicar la inteligencia humana, lo que se conoció como el enfoque simbólico o lógico. Esta metodología se basa en la idea de que la inteligencia puede ser representada mediante símbolos y reglas lógicas. Los sistemas de IA desarrollados bajo este paradigma utilizan reglas y algoritmos para procesar datos y tomar decisiones. Sin embargo, esta estrategia presenta limitaciones, ya que no puede abordar información ambigua o incierta. Durante esa década, Alan Turing (1950) publicó un artículo crucial titulado "Computing Machinery and Intelligence", en el que introdujo el Test de Turing, conocido también como el Juego de la Imitación, planteando la pregunta "¿pueden las máquinas pensar?".

El Test de Turing es una evaluación destinada a determinar si una máquina puede mostrar comportamientos indistinguibles de los de un ser humano en una conversación escrita, generalmente a través de un chat. En este experimento, un juez interactúa con dos participantes ocultos: un humano y una máquina. Ambos envían mensajes al juez, quien debe identificar cuál es el humano y cuál es la máquina. Si la máquina logra engañar al juez, haciendo que crea que es un ser humano, se considera que ha superado el test y se concluye que tiene la capacidad de pensar.

El Test de Turing ha influido significativamente en el desarrollo posterior de la IA, abriendo caminos para la creación de sistemas capaces de realizar tareas que antes se consideraban inviables, lo que estimuló la investigación en áreas clave para el desarrollo futuro de estas tecnologías. En las décadas de 1960 y 1970, la IA comenzó a recibir más atención y financiamiento de organizaciones públicas y privadas en todo el mundo, lo que provocó una notable transformación y diversificación en su avance.

Durante los años 60, el procesamiento del lenguaje natural emergió como un campo destacado de investigación, con el objetivo principal de permitir que las máquinas comprendieran y generaran lenguaje humano. Un evento significativo de esa época fue la creación del programa ELIZA por Joseph Weizenbaum (1966), un científico de la computación del MIT. ELIZA utilizaba técnicas de procesamiento del lenguaje natural para simular conversaciones terapéuticas con personas, convirtiéndose en un hito importante en el ámbito del procesamiento del lenguaje natural y que sigue siendo utilizada como herramienta de enseñanza en la actualidad (BBC Mundo, 2018).

1.5.2. Marco conceptual

Sánchez (2021) llevó a cabo un estudio titulado "Evaluación de algoritmos aplicados a la extracción de características para el reconocimiento facial según la norma ISO/IEC 25010". El propósito de esta investigación fue analizar los algoritmos más relevantes en la extracción de características faciales en sistemas de reconocimiento facial, tales como EigenFace, FisherFace y Viola-Jones. Para ello, se aplicaron los parámetros de la norma ISO/IEC 25010 y se implementaron los algoritmos a través del algoritmo PCA, revelando una puntuación de 56 sobre 70 para el algoritmo FisherFace, seguido de EigenFace con 54 sobre 70 y Viola-Jones con 53 sobre 70. Esta tesis es fundamental para la investigación al evaluar la eficacia de estos algoritmos en el reconocimiento facial.

Velarde y Yabarrena (2018) examinaron un "Sistema de reconocimiento facial para el Control de la trata de personas en Perú". Su objetivo fue desarrollar un sistema que ayude en la lucha contra la trata de personas mediante el uso del algoritmo LBHP y la metodología de desarrollo XP. Utilizaron una muestra de 50 rostros de personas desaparecidas o denunciadas por trata, extraída del sistema de recompensas del Ministerio del Interior del Perú y el Registro de latinoamericanos desaparecidos de la OEA. El resultado fue un reconocimiento facial del 68.75% en las pruebas realizadas. Este estudio es relevante para el análisis de los algoritmos de reconocimiento facial y los resultados obtenidos en las pruebas.

Meza y Ramos (2018) desarrollaron un "Sistema Inteligente Basado en Redes Neuronales para mejorar la identificación de rostros de delincuentes en el distrito de Laredo". El objetivo fue optimizar la identificación de rostros delictivos en Laredo, apoyando así las labores de la Policía Nacional de Perú. Se realizaron pruebas para verificar la normalidad de los datos estadísticos utilizando la prueba de Shapiro-Wilk y aplicando la T de Student para muestras menores de 30, con una población de 2553 delincuentes y una muestra de 334. Se concluyó que el promedio de tiempo para identificar rostros delictivos se redujo en un 91,66%, disminuyendo en 414,85 segundos. Además, se mostró un aumento del 68,82% en la cantidad de delincuentes identificados y una reducción del 77,31% en el tiempo promedio de alerta a la policía sobre los delincuentes identificados. Esta tesis es significativa para el análisis de algoritmos de reconocimiento facial y para establecer bases teóricas relacionadas al tema.

Almache y Márquez (2023) realizaron un análisis sobre las “Implicaciones éticas de la IA y su impacto potencial en el derecho internacional”. El objetivo fue abordar criterios de responsabilidad jurídica internacional que abarcaran principios de humanidad y conciencia pública en la programación de la IA. Utilizando una metodología cualitativa, se realizó una investigación documental mediante métodos históricos (estudios jurídicos con referencias bibliográficas), lógicos (descripción del fenómeno) y un análisis jurídico-comparado (congruencia con normativas contemporáneas). Se identificó un control ineficaz del sesgo algorítmico en la IA.

JESUITAS ECUADOR

CAPÍTULO II: REVISIÓN DE LA LITERATURA

2. MARCO TEÓRICO

2.1. Inteligencia artificial

La inteligencia artificial es un campo de la informática dedicado a la creación de sistemas capaces de realizar tareas que normalmente requieren inteligencia humana. Estas tareas incluyen el aprendizaje, el razonamiento, la percepción, la toma de decisiones, y la interacción con el entorno. Se basa en la construcción de algoritmos y modelos matemáticos que permiten a las máquinas procesar información, aprender de los datos y realizar acciones basadas en ese aprendizaje.

2.1.1. Tipos de inteligencia artificial

La clasificación de la inteligencia artificial se pude clasificar de acuerdo al nivel de inteligencia, habilidades y funcionalidades que poseen los sistemas de IA. La siguiente clasificación se basa en la capacidad y funcionalidad de cada sistema.

2.1.1.1. Tipos de Inteligencia artificial según su capacidad

- **Inteligencia artificial estrecha (ANI - Artificial Narrow Intelligence)**

  La ANI es una IA reactiva con objetivos específicos y poca memoria. Su tarea es estar preparado para desempeñar un solo papel, lo que le permite desempeñar plenamente su papel. Desde asistentes virtuales como Alexa o Siri hasta sistemas de vehículos autónomos, pasando por filtros de spam en el correo electrónico o recomendaciones de publicidad que recibimos en base a nuestras búsquedas, todo está en esta categoría. En última instancia, la ANI se basa en la implementación en la máquina de una variedad de acciones e instrucciones.

- **Inteligencia artificial general (AGI - Artificial General Intelligence)**

  De acuerdo a la teoría, este tipo de IA es capaz de realizar cualquier tipo de tarea con la misma eficacia que un ser humano biológico. Es decir, aunque aún está en una fase muy temprana de desarrollo, se trata de una IA cognitiva o, es decir, con personalidad. Se trata de simular en una máquina todos los procesos cerebrales humanos para la toma de decisiones de forma autónoma en diferentes escenarios.

  Esto significa que la AGI puede evaluar y detectar una variedad de necesidades, procesos e incluso emociones para actuar de acuerdo. Por ejemplo, las interacciones, los comportamientos, las dudas y las necesidades pueden modelar estrategias.

JESUITAS ECUADOR

- **Súper Inteligencia Artificial (ASI - Artificial Super Intelligence)**

  Se refiere a un tipo de IA que supera ampliamente la inteligencia humana en todos los aspectos. Estos sistemas pueden resolver problemas complejos de manera rápida y eficiente, lo que podría tener un gran impacto en la sociedad. La idea de la inteligencia artificial superinteligente ha generado discusiones teóricas sobre las consecuencias éticas y sociales potenciales.

2.1.1.2. Tipos de IA según su funcionalidad

- **Máquinas reactivas**

  Se trata de la IA más básica, que utiliza una variedad de respuestas (reacciones) para solicitudes específicas. Por lo tanto, la máquina solo tiene un rol de respuesta, es decir, está automatizada para responder a una acción específica en el presente. No pueden utilizar experiencias anteriores en las que basar la toma de decisiones actuales porque no tiene la capacidad de aprender y administrar una base de datos interna para ejecutar lo que absorbe y evolucionar.

  El supercomputador "Deep Blue," creado por IBM in la década de los noventa, es uno de los ejemplos clásicos en el desarrollo de máquinas de este tipo. Conquistaron a los mejores ajedrecistas del mundo, incluyendo a Garry Kasparov.

- **Máquinas de memoria limitada**

  En este caso, la máquina, que sigue siendo completamente reactiva, puede almacenar experiencias pasadas o aprender de datos recientes en un periodo de tiempo corto. Esto le permite crear acciones rápidas a partir de la información que ha recobrado y agregarla a su programación para crear nuevos patrones de comportamiento y respuesta en un futuro cercano.

  Las máquinas que emplean este tipo de IA pueden tomar decisiones rápidas sobre si responder a una solicitud o tomar una acción basándose en su historial de interacciones. Los asistentes virtuales, también conocidos como chatbots, y los sistemas de reconocimiento facial están obteniendo resultados prometedores al aumentar la memoria de estas máquinas.

- **Teoría de la mente (Theory of mind AI)**

  En psicología, la "teoría de la mente" sostiene que los seres humanos tienen pensamientos y emociones que influyen en su comportamiento y definen lo que conocemos como interacción social.

  Por lo tanto, las máquinas deberán comprender nuestras emociones y pensamientos si van a andar entre nosotros. Además, deberán conocer nuestras expectativas y la forma en que deseamos

JESUITAS ECUADOR

que nos traten. Tendrán que cambiar su comportamiento de acuerdo con esto. Esto nos lleva al siguiente nivel de inteligencia artificial.

- **Autoconciencia**

  En la actualidad, ninguna máquina es autoconsciente. Este es el objetivo más ambicioso al que se enfrenta la IA a nivel computacional. Una máquina que sea autoconsciente sería capacitada para almacenar información anterior y utilizarla para formar su propio juicio y actuar de manera conveniente.

  El desafío radica en que la IA tendría que incorporar en su programación la habilidad de reconocer que las personas tienen emociones y pensamientos propios, lo que resultaría en un nivel de complejidad que los sistemas de computación actuales no podrían soportar.

2.1.2. Usos de la Inteligencia artificial

La inteligencia artificial (IA) se ha convertido en una tecnología clave en el mundo digital y empresarial en los últimos años. La IA puede ayudar a las empresas a tomar decisiones más informadas y automatizar tareas que antes requerían la intervención humana porque puede procesar grandes cantidades de datos en poco tiempo. En este sentido, a continuación, se detallan las principales usos y aplicaciones de la inteligencia artificial:

- **Compras por internet y publicidad**

  La inteligencia artificial se usa ampliamente para brindar recomendaciones personalizadas a los clientes basados en sus búsquedas y compras anteriores u otros comportamientos en línea. En el comercio, la IA es crucial para los procesos logísticos, la planificación del inventario y la optimización de la producción.

- **Búsquedas en la web**

  Para brindar resultados de búsqueda precisos, los motores de búsqueda utilizan la gran cantidad de datos que proporcionan sus usuarios.

- **Asistentes personales digitales**

  La IA ayuda a los teléfonos móviles a crear productos lo más relevantes y personalizados posibles. Se ha extendido el uso de asistentes virtuales que responden a preguntas, ofrecen recomendaciones y ayudan a organizar las rutinas de sus propietarios.

JESUITAS ECUADOR

- **Traducciones automáticas**

  Los programas de traducción de idiomas utilizan IA para producir y mejorar las traducciones basadas en texto escrito y oral. La IA también puede usar subtitulado automático.

- **Casas, ciudades e infraestructuras inteligentes**

  Los desarrolladores de ciudades inteligentes esperan poder controlar el tráfico para mejorar la conectividad y reducir los atascos, mientras que los termostatos inteligentes aprenden de nuestro comportamiento para ahorrar energía.

- **Vehículos**

  Los vehículos con conducción autónoma ya utilizan funciones de seguridad impulsadas por la IA, aunque aún no están muy extendidos.

- **Ciberseguridad**

  Los sistemas de inteligencia artificial pueden ayudar a reconocer y luchar contra los ciberataques y otras amenazas en línea basándose en los datos que reciben continuamente, reconociendo patrones e impidiendo los ataques.

- **Reconocimiento facial y de voz**

  Los dispositivos pueden reconocer y responder a voces y rostros humanos gracias a la tecnología de IA.

La IA ha encontrado aplicación en diversas áreas, tales como:

- **E-commerce**: Ofrecen recomendaciones personalizadas a clientes basadas en comportamiento de navegación.
- **Asistentes digitales**: Mejoran la organización y eficiencia en la gestión de tareas diarias.
- **Ciberseguridad**: Reconocen patrones y responden a amenazas en línea.
- **Reconocimiento facial y de voz**: Identifican y responden a individuos mediante sus rasgos biométricos.

2.2. Seguridad en aeropuertos

La seguridad en los aeropuertos es crucial para garantizar la protección de pasajeros, personal e instalaciones en un entorno donde el flujo de personas y la conectividad global son constantes. La

JESUITAS ECUADOR

evolución de los aeropuertos ha aumentado significativamente el valor de la seguridad aeroportuaria, que va más allá de la infraestructura física y se ha convertido en centros importantes para la economía y el turismo. Este proceso incluye controles de seguridad exhaustivos, medidas de vigilancia y auditorías continuas. Antes de entrar en el área limitada, se verifica la tarjeta de embarque. En muchos aeropuertos, el usuario realiza la comprobación escaneando el código impreso en su tarjeta o teléfono móvil. El siguiente paso es inspeccionar a cada pasajero y sus equipajes de mano. Los controles de seguridad se pueden realizar antes de llegar a la zona de embarque o en las propias puertas de embarque, dependiendo del aeropuerto. Además, algunos aeropuertos ofrecen líneas de acceso rápido para pasajeros y tripulación.

La seguridad de los aeropuertos está sujeta a auditorías e inspecciones constantes para proteger a los usuarios, trabajadores y bienes materiales. Los aeropuertos también están protegidos con sistemas de videovigilancia, detectores de explosivos, lectores de huellas dactilares, reconocimiento facial, arcos de seguridad y controles de acceso. En algunos países, hay organizaciones especializadas que se encargan de llevar a cabo procedimientos y medidas de seguridad para proteger aeronaves, pasajeros, carga y suministros. Para garantizar la seguridad en los aeropuertos, estos procedimientos son necesarios y se llevan a cabo de acuerdo con las normas internacionales.

En este sentido, la implementación de sistemas de reconocimiento facial ha sido una revolución en la seguridad aeroportuaria. Estos sistemas agilizan el proceso de check-in y reemplazan las tarjetas de embarque. Por ejemplo, la tecnología de reconocimiento facial en el Aeropuerto Internacional de Dulles de Washington puede realizar una verificación biométrica con una alta precisión del 99% en menos de un segundo después de tomar una fotografía de cada pasajero y compararla con las bases de datos gubernamentales.

Los sistemas de reconocimiento facial en los aeropuertos han mejorado la seguridad, agilizado los procesos de abordaje y brindado a los pasajeros una experiencia más eficiente. Estas tecnologías facilitan el control de acceso y la prevención de amenazas de manera más efectiva y rápida, lo que representa un avance significativo en la protección y gestión de la seguridad en entornos aeroportuarios.

2.3. Reconocimiento facial

El reconocimiento facial es una tecnología biométrica que utiliza las características faciales únicas de una persona para identificar o confirmar la identidad de una persona mediante su rostro. Aunque hay un creciente interés en otras áreas de uso, esta tecnología se utiliza principalmente para la protección y las fuerzas de seguridad. Actualmente los sistemas de reconocimiento facial pueden identificar a las personas en tiempo real o en imágenes y videos.

2.3.1. Historia y evolución del reconocimiento facial

Un equipo de investigación liderado por Woodrow W. Bledsoe llevó a cabo experimentos en la década de 1960 con el fin de determinar si las "computadoras de programación" eran capaces de reconocer rostros humanos. Intentaron mapear la ubicación del cabello, los ojos y la nariz de la persona con un escáner básico, pero no pudieron hacerlo debido a la gran variabilidad en la rotación y la inclinación de la cabeza, la intensidad y el ángulo de iluminación, la expresión facial y el envejecimiento, entre otros factores.

Hubo avances en los años siguientes que mejoraron la precisión de los resultados. Algunos métodos se basaron en el uso de marcadores faciales en partes particulares del rostro, como las esquinas de la boca, los ojos o la nariz. Sin embargo, estos métodos no lograron los resultados deseados, y durante algunos años, la investigación en técnicas de reconocimiento facial no experimentó mucho desarrollo. En 2001, Paul Viola y Michael Jones propusieron un marco para la detección de objetos, lo que marcó un punto de inflexión importante.

En la actualidad el reconocimiento facial se ha vuelto más utilizado para una variedad de propósitos, como la seguridad, facilitar el acceso a eventos con grandes multitudes, validar la identidad en la logística y la entrega, y verificar la edad en las redes sociales.

2.3.2. Uso del reconocimiento facial

En la actualidad, la tecnología de reconocimiento facial tiene un gran potencial y se está volviendo cada vez más popular en una variedad de áreas. Cabe destacar principalmente:

- **El ámbito legal y de seguridad:** Para llevar a cabo análisis forenses, búsqueda de personas desaparecidas o que están siendo explotadas, reconocimiento de delincuentes, seguridad en aeropuertos y labores de vigilancia.

- **El ámbito de la salud:** Para monitorear el uso de medicamentos, identificar enfermedades genéticas, procedimientos para tratar el dolor entre otras.

- **El ámbito de la banca y el marketing:** Para realizar búsqueda de nuevos clientes, publicidad personalizada, control de accesos entre otros.

2.3.3. Métodos de Reconocimiento Facial

A medida que la tecnología de reconocimiento facial ha evolucionado, se han desarrollado una variedad de enfoques para identificar rostros y almacenar datos faciales con diferentes niveles de eficiencia y precisión. Existen tres métodos de reconocimiento facial:

- **Reconocimiento facial tradicional**

  El reconocimiento facial tradicional se refiere a la identificación y verificación de personas basándose en sus características faciales. Estas técnicas se basan en la comparación de rasgos físicos visibles en las caras utilizando métodos manuales o semiautomáticos, que dependen en gran medida de la intervención humana y de tecnologías menos avanzadas. Se pueden dividir en dos categorías:

  - El reconocimiento facial holístico examina por completo la cara de una persona para encontrar características que se ajustan al objetivo.

  - El reconocimiento facial basado en características separa los datos pertinentes del reconocimiento facial y los agrega a una plantilla para comparar posibles coincidencias.

- **Reconocimiento facial en 3D**

  Este método utiliza puntos infrarrojos proyectados para mapear el rostro tridimensional del usuario. Esto permite una lectura precisa del rostro, incluida la profundidad. Esta tecnología se ha demostrado altamente segura para el acceso rápido y seguro a la información en dispositivos móviles, ya que puede reconocer al usuario en segundos y tiene una tasa de error muy baja. Además, los sistemas de reconocimiento facial en 3D han demostrado ser resistentes a los intentos de engaño, como la impresión de cabezas en 3D para burlar los sistemas. Esta tecnología ha sido incorporada en dispositivos móviles de última generación, lo que aumenta la seguridad y la modernización en el campo de la identificación biométrica.

- **Reconocimiento facial biométrico**

  El reconocimiento facial biométrico es un método sofisticado que utiliza las características distintivas del rostro de un individuo para identificarlo. Este enfoque se basa en el análisis de patrones faciales como la distancia entre los ojos, la forma de la nariz y la boca y otros rasgos distintivos. El sistema puede verificar la identidad de una persona comparando estos patrones con una base de datos utilizando algoritmos complejos. Dado que ofrece una forma conveniente y precisa de identificación, el reconocimiento facial biométrico se ha convertido en una herramienta importante en la seguridad y la autenticación. Su aplicación también se ha expandido a una variedad de áreas, como el acceso a dispositivos móviles, la seguridad en los aeropuertos y la prevención del fraude.

2.3.3.1. Métodos de reconocimiento facial tradicional en aeropuertos

Los métodos tradicionales de reconocimiento facial en aeropuertos se basaron en técnicas previas a la era de la inteligencia artificial (IA). Si bien algunos de estos métodos aún se utilizan en ciertas partes del mundo, han sido ampliamente superados por las tecnologías basadas en IA.

- **Verificación Visual Manual**

  Implementación: Este método fue ampliamente utilizado en los primeros años de la seguridad aeroportuaria, principalmente en la comparación de fotografías de los documentos de identidad con los pasajeros. Algunos aeropuertos todavía usan este método como medida adicional de seguridad.

  - **Comparación de fotografías:** Se comparan manualmente los rostros de los pasajeros con las fotografías de los documentos de identidad. Este enfoque se basa en la habilidad de los miembros del personal de seguridad para detectar discrepancias y coincidencias visualmente.

  - **Listas de observación:** Fotos de personas sospechosas o buscadas se comparan visualmente con los pasajeros que pasan por los controles.

  Desafíos:

  - **Subjetividad y errores humanos:** La verificación visual manual es altamente subjetiva y propensa a errores debido a la fatiga, las condiciones de iluminación, la calidad de las imágenes y la experiencia del personal.

  - **Tiempo de procesamiento:** La comparación manual de imágenes es un proceso lento, lo que puede generar retrasos en las filas de seguridad.

- **Medición Antropométrica**

Implementación: La medición antropométrica se usó en el pasado para identificar individuos mediante la medición de características faciales específicas. Este método se considera como rudimentario y se basa en el cálculo de distancias entre puntos clave del rostro.

- **Medidas físicas de la cara:** Las personas se identifican utilizando medidas como la distancia entre los ojos, la longitud de la nariz y el ancho de la boca. Se toman estas medidas manualmente o con herramientas básicas y se comparan con las medidas registradas en bases de datos.

Desafíos:

JESUITAS ECUADOR

- **Inflexibilidad:** La medición antropométrica es un método inflexible, ya que solo funciona para personas con características faciales definidas.

- **Falta de precisión:** Las medidas antropométricas son susceptibles a errores y no son lo suficientemente precisas para la identificación individual.

- **Modelos de Plantilla**

  Implementación: Se utilizaron modelos de plantilla para comparar imágenes faciales con patrones predefinidos.

  - **Funcionamiento:** Comparación de imágenes de rostros con plantillas prediseñadas que representan rasgos faciales comunes. Este método utiliza patrones estándar sobre fotos para encontrar similitudes.

  Desafíos:

  - **Limitaciones de la base de datos:** Los modelos de plantilla se basan en una cantidad limitada de características faciales, lo que reduce su precisión y capacidad para identificar a todos los individuos.

  - **Sensibilidad a las variaciones:** Las variaciones en la iluminación, el ángulo de la cámara y las expresiones faciales pueden afectar la precisión de los modelos de plantilla.

  - **Alta tasa de falsos positivos/negativos:** La precisión de estos modelos puede verse afectada por factores ambientales y características individuales, lo que puede llevar a errores en la identificación.

- **Sistemas de Videovigilancia**

  Implementación: Los sistemas de videovigilancia tradicionales se utilizan para grabar imágenes y videos de los pasajeros en áreas del aeropuerto. Los operadores de seguridad revisan manualmente las imágenes para identificar a sospechosos.

  - **Cámaras de seguridad:** Las cámaras colocadas en varios lugares del aeropuerto graban imágenes y videos de los pasajeros. Los operadores de seguridad revisan manualmente las imágenes para encontrar rostros en las listas de sospechosos.

  - **Tecnología de captura de imágenes:** Detalles faciales capturados por cámaras de alta resolución se pueden comparar manualmente con imágenes de la base de datos.

  Desafíos:

- **Revisión manual:** La revisión manual de cientos de horas de video es un proceso tedioso y difícil, que puede llevar a errores u omisiones.

- **Limitaciones de la tecnología:** Las cámaras de seguridad tradicionales tienen una resolución limitada y no pueden identificar con precisión a los individuos en movimiento o a distancia. Además, estos sistemas tienen una baja tasa de aciertos y pueden dar lugar a muchos falsos positivos o negativos.

2.3.3.2. Aeropuertos que utilizan métodos tradicionales de reconocimiento facial

Actualmente, aunque muchos aeropuertos han adoptado tecnologías avanzadas de reconocimiento facial, algunos todavía dependen en gran medida de métodos tradicionales. A continuación, se presentan algunos casos específicos de aeropuertos que aún utilizan estos métodos y las razones detrás de esta decisión:

- **Aeropuerto Internacional de Tribhuvan, Nepal:** Sigue utilizando un sistema donde los agentes de seguridad comparan manualmente las imágenes de los pasaportes con los rostros de los pasajeros. En ciertos casos, se emplean sistemas de coincidencia de plantillas 2D muy básicos para verificar la identidad de los pasajeros, aunque la mayor parte del proceso sigue siendo manual.
  - **Razones para el Uso Continuado:**
    - La falta de infraestructura avanzada y la inversión limitada en tecnología han llevado a la dependencia de métodos tradicionales.
    - El volumen relativamente bajo de pasajeros en comparación con otros aeropuertos internacionales puede no justificar la inversión en tecnologías avanzadas.
- **Aeropuerto Internacional de Minsk (MSQ), Bielorrusia:** En Minsk se utilizan controles visuales manuales para comparar la identidad del pasajero con su pasaporte. Aunque existen sistemas automatizados, se basan en tecnología de plantillas muy simple, lo que requiere una intervención humana significativa.
  - **Razones para el uso continuado:**
    - Las decisiones sobre inversión en tecnología están influenciadas por las prioridades políticas y económicas, donde la modernización tecnológica puede no ser una prioridad inmediata.
    - Las preocupaciones sobre la seguridad de los datos y la privacidad pueden haber retrasado la adopción de tecnologías más avanzadas.
- **Aeropuerto Internacional José Martí, Cuba:** La verificación de identidad a menudo se realiza de manera manual, con personal comparando las fotos de los pasaportes con los rostros de los pasajeros. Además, se utilizan equipos de escaneo de pasaportes básicos que no están equipados con tecnologías avanzadas de reconocimiento facial.

JESUITAS ECUADOR

- **Razones para el uso continuado:**
    - Las restricciones económicas y el acceso limitado a tecnologías avanzadas han mantenido al aeropuerto dependiente de métodos tradicionales.
    - En un entorno donde la modernización de la infraestructura aeroportuaria puede no ser prioritaria, se ha continuado con los métodos existentes.

- **Aeropuerto Internacional de Niamey (NIM), Níger:** Los controles de seguridad en Niamey siguen basándose en la verificación manual por parte de agentes de seguridad. Además, se utilizan sistemas de plantillas 2D, pero su implementación es limitada y no es adecuada para manejar grandes volúmenes de pasajeros.
    - **Razones para el uso continuado:**
        - La falta de infraestructura tecnológica avanzada y recursos ha llevado a la dependencia de métodos tradicionales.
        - Con un volumen de pasajeros más bajo, la necesidad de sistemas avanzados es menos urgente.

En estos aeropuertos, la dependencia de métodos tradicionales de reconocimiento facial se debe principalmente a limitaciones económicas, infraestructura insuficiente, y en algunos casos, prioridades políticas y económicas que no favorecen la modernización. Aunque estos métodos siguen funcionando, presentan limitaciones en términos de precisión, velocidad y capacidad para manejar grandes volúmenes de pasajeros.

2.3.3.3. Ventajas y limitaciones de los métodos de reconocimiento facial tradicional en aeropuertos

Los métodos de reconocimiento facial tradicionales tienen ventajas y desventajas, lo que ha afectado su uso en aeropuertos de todo el mundo. Estos métodos han sido cruciales para la gestión de la seguridad y han brindado soluciones fáciles y prácticas, pero también tienen problemas importantes en términos de precisión, eficiencia y resistencia a la manipulación. A continuación, se detallan las principales ventajas y limitaciones de estos métodos en el ámbito de la seguridad aeroportuaria.

- **Ventajas:**

    - Estos métodos son fáciles de entender y se pueden implementar sin utilizar tecnología sofisticada.

    - La intervención humana directa puede permitir una evaluación contextual más amplia que los sistemas automáticos.

- **Limitaciones:**

JESUITAS ECUADOR

- La fatiga, el sesgo y la subjetividad del personal de seguridad pueden afectar la precisión de estos métodos.

- En entornos de alto tráfico como los aeropuertos, son ineficaces para manejar grandes volúmenes de pasajeros, lo que puede causar retrasos y errores.

- Los sistemas automatizados suelen ser más precisos que las técnicas manuales y las comparaciones visuales, especialmente en condiciones de iluminación y ángulos variables.

- Comparar imágenes manualmente puede ser un proceso lento, especialmente con bases de datos grandes y grandes volúmenes de pasajeros.

2.3.3.4. Técnicas Tradicionales de Reconocimiento Facial

El reconocimiento facial tradicional se basa en métodos y algoritmos diseñados antes de la era de la inteligencia artificial y el aprendizaje profundo. A continuación, se describen las principales técnicas tradicionales de reconocimiento facial utilizadas históricamente:

- **Análisis de Características Geométricas**

  Este método se centra en la identificación de las características geométricas distintivas del rostro, como la distancia entre los ojos, la longitud de la nariz, la forma de los pómulos, y la línea de la mandíbula. Las medidas exactas de estas características se comparan con una base de datos para encontrar coincidencias.

  Ventajas:

  - Simplicidad y rapidez en la identificación.

  - Eficaz en condiciones controladas con buena iluminación y sin obstrucciones faciales.

  Desventajas:

  - Sensible a cambios en la iluminación, expresión facial, y el ángulo de la cámara.

  - Menor precisión en comparación con técnicas modernas basadas en IA.

- **Modelos Basados en Plantillas (Template-Based Models)**

  Utilizan una plantilla estándar del rostro y comparan las características del rostro capturado con esta plantilla.

  Pueden incluir técnicas como el análisis de contornos y patrones de luz y sombra.

JESUITAS ECUADOR

Ventajas:

- Adecuados para sistemas de baja potencia de cálculo y situaciones con restricciones de tiempo.

Desventajas:

- Alta dependencia de la exactitud de las plantillas.
- Menos efectivos en rostros con expresiones cambiantes o en condiciones de iluminación variables.

- **Análisis de Textura y Patrones (Texture-Based Methods)**

Se basa en la captura y análisis de la textura del rostro mediante técnicas como la transformada de Gabor y el análisis de patrones locales.

La transformada de Gabor, por ejemplo, analiza la frecuencia y la orientación de los patrones de textura en la imagen facial.

Ventajas:

- Mejor rendimiento en comparación con el análisis puramente geométrico.
- Capaz de manejar algunas variaciones en la iluminación y expresiones faciales.

Desventajas:

- Aún puede verse afectado por cambios significativos en las condiciones de iluminación y la postura.
- Requiere mayor capacidad de procesamiento en comparación con los métodos geométricos.

- **Método de Proyección de Componentes Principales (PCA)**

También conocido como Eigenfaces, este método reduce las dimensiones de la imagen facial a un espacio de características principales utilizando la técnica de análisis de componentes principales (PCA). La imagen facial se representa como una combinación lineal de un conjunto de imágenes base (eigenfaces).

Ventajas:

- Eficiente en términos de almacenamiento y procesamiento.

JESUITAS ECUADOR

- Buena precisión en condiciones controladas.

Desventajas:

- Sensible a las variaciones en la iluminación, la expresión y el ángulo de la cara.
- No tan robusto como los métodos basados en redes neuronales profundas.

- **Análisis Discriminante Lineal (LDA)**

Similar al PCA, pero enfocado en maximizar la separabilidad entre las clases en lugar de solo reducir la dimensionalidad. Genera un espacio de características que mejora la discriminación entre diferentes individuos.

Ventajas:

- Mejora la precisión al discriminar entre diferentes individuos.
- Más robusto en comparación con el PCA en términos de variaciones de expresión y ángulo.

Desventajas:

- Aún puede verse afectado por condiciones de iluminación adversas.
- Mayor complejidad computacional en comparación con PCA.

2.3.3.5. Superación de los métodos tradicionales de reconocimiento facial

Los métodos tradicionales de reconocimiento facial, que se basaban en gran medida en la comparación de plantillas 2D y la verificación manual, han sido superados a través de la adopción de tecnologías avanzadas, basadas en inteligencia artificial y aprendizaje profundo. Estas tecnologías han mejorado significativamente la precisión, velocidad y capacidad de procesamiento en comparación con los métodos tradicionales. Debido a las variaciones en la iluminación, los ángulos y las expresiones faciales, los sistemas tradicionales pueden producir falsos positivos o negativos. Sin embargo, con la llegada de las redes neuronales convolucionales (CNN) y la tecnología 3D, la capacidad de los sistemas para analizar millones de características faciales con alta precisión ha mejorado significativamente, lo que permite una identificación más confiable incluso en condiciones difíciles.

Además, las nuevas tecnologías han mejorado la precisión y la velocidad del reconocimiento facial. Los sistemas tradicionales, que requerían una intervención humana significativa y no estaban optimizados para el procesamiento en tiempo real, causaban retrasos y cuellos de botella en puntos de control, en aeropuertos. Hoy en día, el procesamiento de grandes volúmenes de datos faciales en tiempo

JESUITAS ECUADOR

real es posible gracias a los avances en hardware y software, lo que automatiza completamente el proceso y acelera significativamente el flujo de pasajeros y la respuesta ante posibles amenazas.

Cabe mencionar que, en términos de seguridad de datos y manejo ético, las nuevas tecnologías han superado a los métodos tradicionales. Los sistemas actuales utilizan técnicas de encriptación y reducción de sesgos para proteger la privacidad de los usuarios y garantizar que el reconocimiento facial sea preciso y justo para todos, independientemente de su raza, género o edad. Además, la combinación de estos sistemas con otras tecnologías biométricas y de videovigilancia ha mejorado la precisión y la flexibilidad del reconocimiento facial, lo que ha establecido nuevos estándares de seguridad y eficiencia en entornos importantes como los aeropuertos.

2.3.3.6. Técnicas de Inteligencia Artificial para Reconocimiento Facial

La precisión y la eficiencia del reconocimiento facial han aumentado significativamente gracias a las técnicas de inteligencia artificial. A continuación, se detallas algunas técnicas:

2.3.3.6.1. Redes Neuronales Convolucionales (CNN)

Las redes neuronales profunda (CNN) son un tipo de red neuronal profunda que están diseñadas para procesar datos en forma de cuadrícula, como imágenes. Las CNN pueden aprender características jerárquicas de imágenes faciales, desde texturas y bordes hasta las estructuras más complejas.

Al utilizar los principios del álgebra lineal, en particular la multiplicación de matrices, para identificar patrones en una imagen, las redes neuronales convolucionales ofrecen actualmente un enfoque más escalable para las tareas de clasificación de imágenes y reconocimiento de objetos. Sin embargo, estas redes pueden requerir una gran cantidad de recursos informáticos y pueden requerir la capacitación de las unidades de procesamiento gráfico (GPU) para entrenar los modelos.

- **Funcionamiento de las redes neuronales convolucionales**

Las redes neuronales convolucionales funcionan mejor con entradas de imagen, voz o señales de audio, lo que las distingue de otras redes neuronales. Se compone de tres categorías de capas principales:

- **Capa convolucional:** La mayoría de los cálculos se realizan en la capa convolucional, que es el bloque de creación principal de una CNN. Algunos componentes son necesarios, como datos de entrada, un filtro y un mapa de características. Se basa en unos pequeños filtros de tres dimensiones que se mueven por la imagen para obtener las salidas de la capa.

JESUITAS ECUADOR

- **Capa de agrupación:** Conocida como submuestreo, permite disminuir la dimensión mediante la disminución del número de parámetros que se ingresan. La operación de agrupación barre toda la entrada con un filtro, como la capa convolucional, pero este filtro no tiene peso. En cambio, el núcleo agrega los valores en el campo recibido y llena la matriz de salida. A pesar de que la capa de agrupación pierde mucha información, esta tiene una serie de ventajas para la CNN. Reduce la complejidad, la eficiencia y el riesgo de sobreajuste.

- **Capa totalmente conectada:** En esta capa cada nodo de la capa de salida está conectado directamente a un nodo de la capa anterior. La tarea de clasificación se lleva a cabo por esta capa utilizando las características extraídas de las capas anteriores y sus diversos filtros. Utiliza una función de activación softmax para clasificar las entradas y generar una probabilidad entre 0 y 1.

Las CNN están diseñadas para procesar datos en forma de cuadrícula, como imágenes. Las CNN pueden aprender características jerárquicas de imágenes faciales, desde texturas y bordes hasta las estructuras más complejas.

- **Casos de éxito:**

  - **Aeropuerto Internacional de Dubai (DXB):** Utiliza CNN para su sistema de control de acceso. Las cámaras con tecnología de reconocimiento facial identifican a los pasajeros en tiempo real, agilizando el proceso de embarque y mejorando la seguridad. Los resultados han mostrado una reducción significativa en los tiempos de espera en los puntos de control y un aumento en la detección de posibles amenazas.

  - **Aeropuerto Internacional de Hong Kong (HKG):** Este aeropuerto ha implementado un sistema de "e-Gates" basado en reconocimiento facial que permite a los pasajeros realizar el check-in y el control de pasaportes de forma automática. El sistema utiliza CNN para identificar y verificar la identidad de los viajeros, reduciendo las colas y mejorando la experiencia del pasajero.

2.3.3.6.2. Redes Neuronales Profundas (DNN)

Estas redes están formadas por capas de neuronas artificiales que se conectan entre sí y procesan datos de manera distribuida y jerárquica. La capacidad de aprender a partir de una gran cantidad de datos y ajustar sus parámetros internos para mejorar la precisión de sus predicciones o decisiones es lo que hace que funcione. El número de capas ocultas entre la entrada y la salida se conoce como profundidad de estas redes.

JESUITAS ECUADOR

Esto les permite aprender y representar datos en un nivel de complejidad y abstracción que va más allá de las redes neuronales superficiales. Las capacidades de DNN que imitan la complejidad y la capacidad de aprendizaje del cerebro humano han revolucionado el campo del aprendizaje automático y la inteligencia artificial. Estas redes se utilizan para una variedad de tareas, incluida la clasificación de imágenes, la detección de objetos, el redimensionamiento de imágenes, la creación de textos y el procesamiento del lenguaje natural. Estas redes suelen tener múltiples capas de neuronas conectadas en arquitecturas de feed-forward, en las que la información se mueve en una sola dirección: hacia adelante, desde la entrada hasta la salida.

Las DNN están formadas por capas de neuronas artificiales que se conectan entre sí y procesan datos de manera distribuida y jerárquica. La capacidad de aprender a partir de una gran cantidad de datos y ajustar sus parámetros internos para mejorar la precisión de sus predicciones o decisiones es lo que hace que funcione.

- **Casos de éxito:**

  - **Aeropuerto Internacional de Changi (SIN):** Ha implementado un sistema de "Fast and Seamless Travel" que utiliza DNN para el control de pasaportes automatizado. El sistema identifica a los pasajeros utilizando imágenes faciales capturadas en tiempo real, permitiendo el acceso a las áreas de embarque sin necesidad de mostrar documentación física. Este sistema ha reducido las colas y ha mejorado la fluidez del tráfico de pasajeros.

  - **Aeropuerto Internacional de Incheon (ICN):** Está utilizado DNN para mejorar la seguridad en el aeropuerto. El sistema analiza imágenes de cámaras de vigilancia en busca de comportamientos sospechosos y posibles amenazas, alertando a las autoridades en caso de necesidad. Esto ha mejorado la capacidad de respuesta del aeropuerto ante situaciones de riesgo y ha aumentado la seguridad de los pasajeros y del personal.

2.3.3.6.3. Beneficios y mejoras del reconocimiento facial con inteligencia artificial en aeropuertos

El reconocimiento facial con IA ha cambiado la seguridad y la eficiencia operativa de los aeropuertos. La IA ofrece muchos beneficios sobre los métodos tradicionales. Estas mejoras han optimizado los procesos de control de seguridad, mejorado experiencia del pasajero y la capacidad de los aeropuertos para manejar grandes volúmenes de tráfico con mayor velocidad y precisión. A continuación, se detallan los principales beneficios:

- **Mayor precisión y fiabilidad:** Mediante el uso de redes neuronales profundas y modelos de aprendizaje automático, ha incrementado significativamente la precisión del reconocimiento

JESUITAS ECUADOR

facial. Estos sistemas reducen la tasa de falsos positivos y negativos al analizar y comparar millones de características faciales, incluso en condiciones difíciles como variaciones en iluminación, ángulos de cámara y expresiones faciales.

- **Velocidad y eficiencia operativa:** Los sistemas de reconocimiento facial con IA pueden identificar rápidamente a los pasajeros al procesar imágenes en tiempo real. Esto reduce las filas y los tiempos de espera, mejora la experiencia del pasajero y acelera los procesos de control de seguridad y embarque. Además, la automatización del proceso permite que los empleados de seguridad se concentren en otras tareas críticas.

- **Mejora en la seguridad y prevención de fraude:** La IA puede detectar patrones sospechosos y alertar sobre posibles amenazas de manera más eficaz que los métodos tradicionales. Los sistemas actuales son más resistentes a la manipulación, como el uso de fotografías o máscaras, y pueden integrar otros datos biométricos para una verificación de identidad más confiable, como el reconocimiento de huellas dactilares o iris.

- **Procesamiento de grandes volúmenes de pasajeros:** Los aeropuertos que utilizan IA pueden manejar grandes volúmenes de pasajeros de manera eficiente sin comprometer la calidad del control de seguridad. Esto es particularmente crucial en aeropuertos internacionales que manejan millones de pasajeros al día.

- **Personalización y mejora del servicio:** Los sistemas de IA pueden integrarse con otros servicios aeroportuarios, brindando a los pasajeros una experiencia más personalizada, como recomendaciones de servicios en el aeropuerto o alertas sobre el estado de su vuelo, basadas en su ubicación e historial de comportamiento.

En este sentido, el uso de IA para el reconocimiento facial ha cambiado la forma en que los aeropuertos manejan la seguridad y la experiencia del pasajero. Estos sistemas mejoran la eficiencia operativa y elevan los estándares de seguridad en uno de los ámbitos más importantes para la protección pública al ofrecer una precisión y velocidad sin precedentes, así como una mayor seguridad contra fraudes y amenazas.

2.4. Consideraciones éticas en el reconocimiento facial

El uso de esta tecnología plantea varias preocupaciones éticas, como la protección de la privacidad, la posible discriminación por sesgos en algoritmos y la falta de transparencia. Es crucial que las organizaciones que implementan reconocimiento facial prioricen la ética, la seguridad de datos y respeten los derechos de los usuarios.

JESUITAS ECUADOR

Debido a su posible impacto en la privacidad el uso de la tecnología de reconocimiento facial ha generado preocupaciones éticas y debates significativos. Las siguientes son algunas de las principales preocupaciones éticas relacionadas con el uso del reconocimiento facial:

- **Privacidad y protección de datos**

  La capacidad de reconocer y rastrear a las personas a través de sus rasgos faciales plantea preguntas sobre el derecho a la autonomía personal y la privacidad. Por ejemplo, las fuerzas del orden pueden usar el reconocimiento facial para vigilar y rastrear a personas sin su consentimiento o conocimiento, lo que podría ser una violación de las libertades civiles. Además, los datos biométricos recopilados corren el riesgo de ser utilizados indebidamente o accedidos por personas no autorizadas, lo que podría resultar en robo de identidad u otras actividades maliciosas.

  Por lo que, las organizaciones que utilizan tecnología de reconocimiento facial deben priorizar la protección de datos con medidas sólidas como el cifrado, el almacenamiento seguro y los controles estrictos de acceso.

- **Exactitud y sesgo**

  El sesgo y la precisión de los algoritmos de reconocimiento facial han sido cuestionados. De acuerdo a numerosos estudios, es más probable que los sistemas de reconocimiento facial identifiquen erróneamente a las personas de color y a las mujeres, lo que puede causar discriminación y acusaciones falsas. Este sesgo puede tener efectos perjudiciales, como arrestos injustificados o la perpetuación de perfiles raciales. Para garantizar un uso justo y preciso de la tecnología de reconocimiento facial, es fundamental que los desarrolladores y usuarios se concentren en mejorar la precisión mientras abordan activamente y reducen los sesgos.

- **Libertad y autonomía**

  Las personas pueden sentirse presionadas a conformarse y presentarse de maneras específicas para evitar el escrutinio o la discriminación a medida que nuestros rostros se convierten en el principal medio de identificación. Dado que las personas pueden temer ser juzgadas o atacadas por su apariencia, esto puede conducir a la autocensura y la pérdida de individualidad.

  La presencia de esta tecnología en espacios públicos puede inhibir el comportamiento de las personas, afectando su libertad de movimiento y expresión debido al temor de ser monitoreados constantemente.

- **Transparencia y consentimiento**

  Es importante que las personas sean informadas de manera clara sobre cómo se utilizarán sus datos faciales, así como de cómo pueden elegir si dan o no su consentimiento. Esto incluye la capacidad de optar por no participar en sistemas de reconocimiento facial sin tener que preocuparse por cualquier resultado negativo.

  Las empresas que utilizan reconocimiento facial deben asegurarse de cumplir con las leyes, regulaciones y estándares éticos pertinentes a través de auditorías y evaluaciones independientes.

- **Seguridad y protección contra abusos**

  Los sistemas de reconocimiento facial deben diseñarse para evitar la manipulación y los ataques. Las vulnerabilidades en la tecnología pueden ser utilizadas para realizar seguimiento o vigilancia masiva no autorizados. Además, existen preocupaciones sobre el uso indebido de la tecnología de reconocimiento facial para la vigilancia masiva y la represión política. Las regulaciones y políticas deben abordar estas preocupaciones para proteger los derechos civiles y garantizar que la tecnología se utilice de manera que respete las libertades fundamentales.

Las consideraciones éticas en el reconocimiento facial abarcan una amplia gama de temas, desde la privacidad y la protección de datos hasta la transparencia y el consentimiento. A medida que avanza la tecnología, es fundamental abordar estos problemas de manera proactiva y establecer marcos regulatorios y prácticas éticas para garantizar que el uso del reconocimiento facial sea justo, transparente y respetuoso con los derechos de las personas.

2.5. Marco regulatorio y normativo de reconocimiento facial en aeropuertos

Los estándares y regulaciones para el reconocimiento facial en los aeropuertos varían según el país y la región. El reconocimiento facial se ha convertido en una práctica común en muchos aeropuertos a nivel mundial para mejorar la seguridad y la agilización de los procesos de control de pasajeros. Las regulaciones internacionales, regionales y nacionales regulan el uso de la tecnología de reconocimiento facial en los aeropuertos. Estas regulaciones buscan equilibrar los beneficios en términos de seguridad y eficiencia con la protección de los derechos humanos y la privacidad. Los principales marcos regulatorios y normativos que regulan el uso de esta tecnología se describen a continuación:

2.5.1. Regulaciones internacionales

- **Organización de Aviación Civil Internacional (OACI)**

JESUITAS ECUADOR

Los estándares y recomendaciones para la emisión y el uso de documentos de viaje de lectura mecánica, incluidos los pasaportes con tecnología de reconocimiento facial, están establecidos por la Organización de Aviación Civil Internacional. Estas normas tienen como objetivo garantizar la interoperabilidad y la seguridad a nivel mundial. Además, proporciona las directrices para el uso de tecnologías biométricas como el reconocimiento facial en los aeropuertos para aumentar la seguridad y la comodidad de los pasajeros.

2.5.2. Regulaciones regionales

- **Unión Europea (UE)**

El Reglamento General de Protección de Datos (GDPR) regula el procesamiento de datos personales en la Unión Europea, incluidos los datos biométricos. De igual manera, exige el consentimiento explícito de las personas para la recolección y el uso de sus datos biométricos y establece estrictos requisitos para la protección y el almacenamiento de estos datos.

Por otro lado, las directrices para la implementación segura y ética de tecnologías biométricas en aeropuertos están proporcionadas por la Agencia de la Unión Europea para la Seguridad Aérea (EASA) y otras agencias reguladoras de aviación en Europa.

- **Estados Unidos**

En los aeropuertos, la Administración de Seguridad en el Transporte (TSA) y el Servicio de Aduanas y Protección Fronteriza (CBP) verifican la identidad y controlan las fronteras con tecnologías de reconocimiento facial. Estas agencias deben cumplir con las leyes federales que protegen los derechos civiles y la privacidad, como la Ley de Privacidad de 1974.

La Comisión Federal de Comercio regula las empresas que desarrollan y utilizan tecnologías de reconocimiento facial para garantizar que cumplan con los estándares de transparencia y consentimiento.

En general, las regulaciones y regulaciones del reconocimiento facial en los aeropuertos están en constante cambio, con un mayor énfasis en proteger la privacidad y la seguridad de los pasajeros y mejorar la eficacia de los procedimientos de control y embarque.

2.5.3. Regulaciones nacionales

- **Reino Unido**

La Oficina del Comisionado de Información (ICO) proporciona pautas detalladas sobre el uso de tecnologías de reconocimiento facial para garantizar que las organizaciones cumplan

JESUITAS ECUADOR

con la Ley de Protección de Datos de 2018, que implementa la Ley de Protección de Datos del Reino Unido.

- **China**

  El uso de tecnologías de reconocimiento facial en aeropuertos y otros lugares públicos está fuertemente regulado por el gobierno con un énfasis en la seguridad y el control estatal. En China, existen normas rigurosas para la recopilación, almacenamiento y uso de datos biométricos.

- **Australia**

  La Oficina del Comisionado de Información de Australia (OAIC) regula el uso de datos biométricos bajo la Ley de Privacidad de 1988, que establece principios estrictos para la recopilación y el uso de información personal.

  El marco legal y regulatorio para el reconocimiento facial en los aeropuertos es complejo y varía según el estado. Sin embargo, los principios comunes incluyen la protección de la privacidad, la obtención de consentimiento informado, la seguridad de los datos y el cumplimiento de las normas internacionales para garantizar la interoperabilidad y la seguridad. Para garantizar el uso legal y ético de la tecnología de reconocimiento facial, es fundamental que las autoridades y las empresas involucradas en la implementación de estas tecnologías se adhieran estrictamente a estos marcos.

2.5.4. Aeropuertos que han enfrentado desafíos éticos relacionados a la inteligencia artificial

Diversos aeropuertos y naciones han enfrentado preocupaciones éticas con respecto al uso de inteligencia artificial, particularmente en el reconocimiento facial. La privacidad, el sesgo y la vigilancia masiva son algunos de estos problemas. A continuación, se presentan algunos ejemplos notables y cómo se abordaron estos problemas mediante regulaciones o ajustes tecnológicos:

- **China: uso de reconocimiento facial en espacios públicos**

  China ha implementado numerosos sistemas de reconocimiento facial para la vigilancia y el control social en ciudades y aeropuertos. La creciente utilización de la tecnología ha generado preocupaciones acerca de la protección de la privacidad, la vigilancia masiva y la posibilidad de que se utilice para fines de represión política.

  Enfoque regulatorio y ajustes: El gobierno chino ha implementado algunas regulaciones para aumentar la transparencia y el control en el uso de la tecnología en respuesta a las críticas y preocupaciones internacionales. En 2019, se implementaron directrices para mejorar la

JESUITAS ECUADOR

protección de la privacidad y limitar el uso de datos biométricos. Estas medidas representan un intento de abordar los desafíos éticos mediante la regulación, aunque no han eliminado todas las preocupaciones.

- **Unión Europea: Implementación del GDPR**

El uso de tecnologías de reconocimiento facial en aeropuertos europeos, como el Aeropuerto de Heathrow en el Reino Unido y el Aeropuerto de Schiphol en los Países Bajos, ha generado preocupaciones sobre la privacidad y la protección de datos, especialmente en relación con el Reglamento General de Protección de Datos (GDPR).

Enfoque regulatorio y ajustes: En 2018, el GDPR estableció un marco regulatorio sólido para abordar estos problemas. El GDPR exige que las personas obtengan su consentimiento explícito antes de usar datos personales, incluidos los datos biométricos, y les brinden derechos sobre sus datos. Para cumplir con estos requisitos, los aeropuertos de la UE han tenido que modificar sus prácticas, implementando mecanismos de consentimiento y asegurando la transparencia en el uso de datos.

- **Estados Unidos: Caso de Clear en el Aeropuerto de Denver**

Clear, una empresa de verificación de identidad biométrica en el Aeropuerto Internacional de Denver, ha recibido críticas por la gestión de datos biométricos y la falta de claridad sobre cómo se utilizan. La privacidad y la seguridad de la información biométrica de los pasajeros son problemas.

Enfoque regulatorio y ajustes: Clear y otros servicios similares en Estados Unidos han mejorado sus políticas de privacidad y seguridad en respuesta a las preocupaciones. Clear ha tomado medidas adicionales para proteger los datos biométricos y dar más claridad sobre cómo se utilizan y almacenan los datos. Además, la Ley de Privacidad del Consumidor de California (CCPA), por ejemplo, ha cambiado la forma en que las empresas manejan los datos biométricos, ofreciendo más transparencia y opciones para que los consumidores decidan no compartir sus datos.

- **India: Proyecto Aadhaar y Desafíos de Privacidad**

El sistema Aadhaar de India para la verificación de identidad en puntos de control fronterizos y aeropuertos utiliza datos biométricos como el reconocimiento facial para identificar a los ciudadanos, tiene problemas importantes con la privacidad y la seguridad de los datos. El uso indebido de datos biográficos y la posibilidad de filtraciones de datos son problemas.

Enfoque regulatorio y ajustes: El gobierno de la India ha implementado una serie de medidas para mejorar la seguridad y la privacidad en respuesta a estos problemas. El objetivo de la Ley de Protección de Datos Personales (PDPB) es establecer un marco regulatorio más fuerte para proteger los datos personales, incluidos los datos biométricos. Además, se han implementado auditorías y mejoras en la seguridad de los datos para reducir los riesgos asociados con el sistema Aadhaar.

2.5.5. Perspectivas de expertos en ética y derecho respecto a la inteligencia artificial

Los puntos de vista de los expertos en ética y derecho tienen un gran impacto en la implementación de IA en los aeropuertos. Estas opiniones han llevado a la adopción de medidas que aseguran que las tecnologías de IA se utilicen de manera ética y responsable, protegiendo la privacidad, la equidad, la transparencia, el consentimiento y los derechos humanos. A continuación, se detallan las perspectivas más relevantes:

- **Perspectiva sobre privacidad y protección de datos**

  La autora de The Age of Surveillance Capitalism, Shoshana Zuboff, ha expresado que la recopilación de grandes cantidades de datos personales, incluidos los datos biométricos, plantea preocupaciones importantes sobre la privacidad y la autonomía individual. Zuboff advierte que la violación de las libertades individuales y el abuso de la información personal pueden resultar del uso de datos sin el consentimiento previo.

  En respuesta a estas preocupaciones, muchos aeropuertos han tomado medidas para mejorar la privacidad. El Aeropuerto de Schiphol de Ámsterdam, por ejemplo, tiene sistemas de reconocimiento facial que cumplen con estrictos protocolos de privacidad. Estos incluyen políticas claras de consentimiento, encriptación de datos y limitación del tiempo de almacenamiento. El Reglamento de Protección de Datos (GDPR) de la Unión Europea ha fortalecido estas prácticas exigiendo claridad y consentimiento explícito para el uso de datos personales.

- **Perspectiva sobre equidad y sesgo**

  Joy Buolamwini, investigadora del MIT Media Lab, ha investigado los sesgos en los algoritmos de reconocimiento facial y ha descubierto que las personas de color y las mujeres tienen tasas de error más altas en estos sistemas. Buolamwini ha señalado que estos sesgos pueden tener efectos importantes, como discriminación y errores de identificación.

JESUITAS ECUADOR

Estas investigaciones han llevado a una mayor atención en la evaluación de sesgos en sistemas de reconocimiento facial. El Aeropuerto de Heathrow en el Reino Unido, por ejemplo, ha implementado rutinas de auditoría y pruebas exhaustivas para garantizar que sus sistemas de reconocimiento facial funcionen de manera equitativa. Además, se han creado pautas para la creación de algoritmos más inclusivos y la corrección de sesgos en los datos de entrenamiento.

- **Perspectiva sobre transparencia y responsabilidad**

La autora de Weapons of Math Destruction, Cathy O'Neil, sostiene que la falta de transparencia en los algoritmos de IA puede resultar en decisiones opacas y una rendición de cuentas inadecuada. O'Neil afirma que es crucial que las empresas y los gobiernos sean transparentes sobre cómo utilizan los algoritmos y los posibles efectos en las personas.

Algunos aeropuertos están implementando políticas de transparencia sobre el uso de IA en respuesta a estas preocupaciones. Por ejemplo, el Aeropuerto de San Francisco ha emitido informes detallados sobre su uso de IA y ha creado un comité de ética para supervisar su implementación. Las políticas también establecen quién es responsable en caso de problemas y cómo se toman las decisiones automatizadas.

- **Perspectiva sobre consentimiento y autonomía**

Helen Nissenbaum, profesora de la Universidad de Cornell, ha señalado que el consentimiento informado y la autonomía son cruciales cuando se trata del uso de tecnologías que afectan la privacidad. Nissenbaum sostiene que las personas deben tener control sobre cómo comparten, utilizan y recopilan sus datos personales.

En este sentido, los aeropuertos están adoptando procedimientos para garantizar el consentimiento informado. Por ejemplo, el Aeropuerto de Incheon en Corea del Sur ha implementado un sistema de consentimiento que permite a los pasajeros decidir si quieren o no participar en el sistema de reconocimiento facial. Además, se proporcionan instrucciones detalladas sobre el uso y la protección de los datos.

- **Perspectiva sobre Derechos Humanos**

El director del Proyecto de Privacidad de la ACLU, Ben Wizner, ha destacado la importancia de una regulación cuidadosa del uso de tecnologías de vigilancia para evitar violaciones de derechos humanos. Wizner ha argumentado que, si no se controlan adecuadamente, las tecnologías de vigilancia como el reconocimiento facial pueden ser utilizadas para la vigilancia masiva y la represión.

JESUITAS ECUADOR

En este contexto, algunos países y aeropuertos han establecido regulaciones que limitan el uso de tecnologías de vigilancia para garantizar que se utilicen de manera proporcional y respetuosa con los derechos humanos en respuesta a estas preocupaciones. Por ejemplo, un marco legal en el Reino Unido limita la vigilancia facial a contextos específicos y requiere evaluaciones de impacto en los derechos humanos antes de la introducción de nuevas tecnologías.

JESUITAS ECUADOR

CAPÍTULO III: METODOLOGÍA

3. Metodología

3.1. Introducción a la metodología

La profundidad del estudio del presente trabajo de titulación llegará hasta la revisión exhaustiva de la literatura científica y técnica relacionada con las técnicas de inteligencia artificial utilizadas en el reconocimiento facial y los métodos tradicionales de identificación de personas en aeropuertos. Esto permitirá realizar un análisis comparativo de las técnicas de IA frente a los métodos tradicionales de reconocimiento facial y obtener una comprensión sólida de los enfoques existentes, sus ventajas y limitaciones, así como los aspectos éticos involucrados.

De igual manera, se establecen los criterios que se utilizarán para evaluar y comparar las técnicas de inteligencia artificial y los métodos tradicionales. Estos criterios incluirán la precisión de la identificación, la velocidad de procesamiento, la escalabilidad, la facilidad de implementación, la privacidad y la ética.

En este sentido, se ha determinado que se debe utilizar un enfoque de investigación mixto, combinando métodos cualitativos y cuantitativos. Esta metodología permitirá obtener una comprensión integral tanto de los aspectos técnicos como de las implicaciones éticas del uso de la inteligencia artificial (IA) en el reconocimiento facial en aeropuertos.

3.2. Tipo de investigación

Dentro de esta investigación documental, se contempla una combinación de metodologías cualitativas y cuantitativas que se integrarán de la siguiente manera:

- **Revisión de Literatura:**

  Cualitativa: Se analizarán casos de estudios y literatura que discutan experiencias, percepciones y críticas sobre el reconocimiento facial. Esto incluirá entrevistas y testimoniales donde correspondan, así como el análisis de enfoques éticos y normativos en la implementación de estas tecnologías.

  Cuantitativa: Se recogerán datos estadísticos sobre la precisión de los sistemas de reconocimiento facial, tasas de error, y análisis de la eficacia de diferentes metodologías basadas en inteligencia artificial, contrastando resultados de diversas investigaciones y reportes técnicos.

- **Análisis Comparativo:**

JESUITAS ECUADOR

Cualitativa: Se hará un análisis comparativo de la aplicación de métodos tradicionales vs. IA, evaluando los argumentos a favor y en contra de cada enfoque, con un especial énfasis en el contexto aeroportuario.

Cuantitativa: Utilizando datos obtenidos de estudios previos, se podrá presentar información numérica sobre la adopción y eficacia de cada tipo de sistema en la detección de identidades y la reducción de falsos positivos o negativos.

- **Identificación de Desafíos y Oportunidades:**

Cualitativa: A partir de la revisión de literatura, se buscarán identificar narrativas y argumentos que abordan los desafíos éticos, sociales y operativos de implementar esta tecnología en aeropuertos, como la privacidad y la vigilancia.

Cuantitativa: A través de datos recopilados, se identificarán patrones y tendencias que indiquen las oportunidades que la inteligencia artificial puede ofrecer para mejorar la seguridad y la experiencia del pasajero.

3.3. Enfoque de investigación

Para llevar a cabo la parte inicial de la investigación sobre el impacto de la inteligencia artificial en la seguridad ciudadana en aeropuertos, es necesario implementar un enfoque documental adecuado que permita recopilar y analizar la información existente sobre este tema.

El enfoque documental deberá comprender una revisión exhaustiva del estado del arte en cuanto a la aplicación de la inteligencia artificial en la seguridad aeroportuaria. Esto implicará la búsqueda y análisis de investigaciones previas, estudios de caso, informes técnicos, legislación y normativas relacionadas, así como cualquier otra fuente de información relevante.

Dado que la metodología de la investigación es mixta, es decir, combina elementos cualitativos y cuantitativos, es importante que el enfoque documental refleje esta dualidad. Por lo tanto, será necesario identificar y analizar tanta información cualitativa (como descripciones, análisis de casos, opiniones de expertos) como información cuantitativa (como datos estadísticos, resultados de encuestas, mediciones objetivas).

Además, es fundamental que el enfoque documental sea crítico y reflexivo, permitiendo cuestionar la validez y la relevancia de la información recopilada, así como identificar posibles vacíos o áreas de investigación futura.

En resumen, el enfoque documental para la parte inicial de la investigación sobre el impacto de la inteligencia artificial en la seguridad ciudadana en aeropuertos debe ser exhaustivo, crítico y reflejar la naturaleza mixta de la metodología de la investigación.

JESUITAS ECUADOR

3.4. Diseño de la investigación

3.4.1. Fase 1: Revisión documental

- **Procedimiento de recolección de datos**

Definición de Criterios de Inclusión y Exclusión: Se establecerán criterios claros para seleccionar artículos, informes y documentos relevantes. Por ejemplo, se incluirán solo aquellos estudios publicados en revistas revisadas por pares, informes gubernamentales y de organizaciones reconocidas, y documentos que aborden específicamente la integración de IA y sistemas de reconocimiento facial en aeropuertos.

Búsqueda sistemática de literatura: Se realizarán búsquedas en bases de datos académicas (como Scopus, IEEE Xplore, Google Scholar) utilizando palabras clave específicas relacionadas con "reconocimiento facial", "inteligencia artificial", "seguridad aeroportuaria" y combinaciones de estos términos.

Análisis de documentos: Se llevará a cabo un análisis cualitativo de los documentos seleccionados para extraer conceptos clave, tendencias y hallazgos relevantes relacionados con métodos tradicionales y modernos de reconocimiento facial, así como aspectos éticos asociados.

- **Procedimiento de análisis**

Análisis temático: Se utilizará el análisis temático para agrupar los hallazgos de la literatura en temas o categorías principales que aborden cada uno de los objetivos específicos del estudio.

Síntesis narrativa: Se elaborará una síntesis narrativa que resuma los hallazgos de la revisión de la literatura, identificando vacíos en la investigación actual y proponiendo áreas para el estudio empírico.

3.4.2. Fase 2: Investigación empírica

- **Parte cualitativa**

Selección de participantes: Se identificarán y seleccionarán expertos en seguridad aeroportuaria, inteligencia artificial y ética mediante el uso de redes profesionales y plataformas académicas. Se buscará una muestra diversa que incluya técnicos, investigadores y responsables de políticas.

Entrevistas semiestructuradas: Se llevarán a cabo entrevistas semiestructuradas para permitir la exploración profunda de las percepciones y experiencias de los expertos. Las entrevistas se grabarán, transcribirán y analizarán.

- **Parte cuantitativa**

JESUITAS ECUADOR

Desarrollo de encuestas: Se diseñará un cuestionario estructurado que incluya preguntas sobre la percepción de la seguridad, la eficacia y la aceptabilidad de los sistemas de reconocimiento facial por parte de pasajeros y personal. Se realizarán pruebas piloto para validar el cuestionario.

Recolección de datos: Las encuestas se aplicarán de manera online al personal que se encarga de la seguridad de los aeropuertos, utilizando herramientas de encuestas digitales para alcanzar un mayor número de participantes. Se buscará un tamaño de muestra representativo para garantizar la relevancia de los resultados.

- **Procedimiento de análisis**

Análisis cuantitativo: Los datos de las encuestas serán analizados utilizando métodos estadísticos descriptivos e inferenciales para evaluar las percepciones de los participantes. Se utilizarán software estadístico como SPSS o R para llevar a cabo análisis como pruebas T, ANOVA y análisis de regresión.

Análisis cualitativo: Las entrevistas se analizarán mediante análisis de contenido temático, identificando patrones y tendencias que surjan de las respuestas de los expertos. El software de análisis cualitativo, como NVivo, puede ser útil para organizar y codificar los datos.

3.5. Población y muestra

En la revisión bibliográfica, empleamos un muestreo intencional para elegir fuentes relevantes y actualizadas. En el estudio comparativo, seleccionamos cuidadosamente estudios de caso pertinentes, considerando la disponibilidad de datos y su representatividad. Es fundamental definir de manera precisa la muestra y la población para asegurar la validez y representatividad de los hallazgos de la investigación.

3.5.1. Población

La población serían todos los aeropuertos internacionales que emplean tecnologías de reconocimiento facial para la seguridad y el control de pasajeros. Estos aeropuertos se caracterizan por estar ubicados en diversas regiones del mundo y emplear tanto métodos tradicionales como avanzados de inteligencia artificial en el reconocimiento facial.

3.5.2. Muestra

La muestra son los aeropuertos internacionales con implementaciones de tecnologías de reconocimiento facial. El tamaño de la muestra es de 5 aeropuertos representativos, seleccionados por su tamaño, volumen de pasajeros y la sofisticación de su tecnología de reconocimiento facial, y el método aplicado es el muestreo intencional para asegurar la inclusión de aeropuertos con diferentes niveles de tecnología y en distintas regiones del mundo.

JESUITAS ECUADOR

Al incorporar aeropuertos de varios lugares y tecnologías diferentes, se garantiza que los resultados reflejen la variedad de prácticas y contextos en los que se utiliza el reconocimiento facial.

La combinación de técnicas cualitativas y cuantitativas, junto con una muestra diversificada, permite un análisis profundo y detallado de las diferencias entre las técnicas de reconocimiento facial tradicionales y las técnicas de IA.

JESUITAS ECUADOR

CAPÍTULO IV: RESULTADOS

4. RESULTADOS

4.1. Fase 1: Revisión Documental

Tabla 1: Criterios de inclusión y exclusión.

ORD.	CRITERIO	INCLUSIÓN /EXCLUSIÓN	DESCRIPCIÓN	AÑO	AUTOR	REFERENCIA
1	Publicación en revistas revisadas por pares.	Inclusión	Artículos revisados que garantizan la calidad y rigor científico.	2020	Smith, J.	Smith, J. (2020). The Role of AI in Airport Security. *Journal of Security Studies*, 45(2), 123-145.
2	Año de publicación	Inclusión	Solo se incluirán estudios publicados entre 2018 y 2023 para obtener la información más actualizada.	2021	Lee, A.	AI and Facial Recognition in Airports: A Review. *International Journal of Airport Management*, 15(4), 300-310.
3	Documentos de organismos reconocidos	Inclusión	Informes de organizaciones como la OACI, INTERPOL u otras que aborden la implementación de IA en seguridad aeroportuaria.	2022	OACI	Artificial Intelligence in Aviation Security.
4	Enfoque en reconocimiento facial	Inclusión	Documentos que investiguen específicamente el uso de reconocimiento facial en aeropuertos.	2019	Zhao, Y.	Facial Recognition Technology and Airport Security. *Airport Security International*, 25(1), 45-52.
5	Estudios empíricos	Inclusión	Se incluirán aquellos estudios que presenten datos empíricos sobre la efectividad de la IA en la seguridad aeroportuaria.	2021	Johnson, R.	Empirical Evidence of AI Impact in Airport Security. *Safety Science*, 135, 105-115.

JESUITAS ECUADOR

6	Método de análisis	Inclusión	Se aceptarán estudios que utilicen métodos cualitativos y cuantitativos para el análisis.	2023	Doe, J.	Methodological Approaches to AI-Facilitated Security Checks. *Journal of Transport Security*, 12(3), 215-230.
7	Aspectos éticos	Inclusión	Documentos que abordan las implicaciones éticas del uso de IA en la seguridad aeroportuaria.	2020	Kant, I.	Ethical Considerations in AI-based Airport Security. *Journal of Ethics in Technology*, 5(1), 29-41.
8	Casos de estudio	Inclusión	Estudios que presenten casos prácticos de implementación de sistemas de IA en aeropuertos.	2022	Thompson, A.	Case Studies: AI Implementation in Major Airports. *Air Transport Research*, 72(4), 300-316.
9	Revisión de literatura	Inclusión	Artículos que analicen estudios previos sobre IA y seguridad aeroportuaria.	2020	Martin, P.	A Review of AI Applications in Airport Security. *Transport Policy*, 90, 100-110.
10	Estudios interdisciplinarios	Inclusión	Documentos que integren perspectiva de diversas disciplinas, como tecnología, sociología y criminología.	2021	Wu, L	Interdisciplinary Approaches to Airport Security. *Journal of Airport Management*, 15(1), 25-35.
11	Falta de evidencia empírica	Exclusión	Documentos que carezcan de datos empíricos sobre la aplicación de IA en la seguridad aeroportuaria.		S/I	S/I
12	Enfoque en otro tipo de tecnología	Exclusión	Estudios que aborden exclusivamente tecnologías no relacionadas con la inteligencia artificial		S/I	S/I

JESUITAS ECUADOR

13	Documentos de opinión	Exclusión	Se excluirán artículos de opinión o comentarios sin evidencia científica sustancial.		S/I	S/I
14	Fallas en la referencia	Exclusión	Artículos que no proporcionen referencias adecuadas o que contengan errores significativos.			
15	Diversidad de perspectivas	Inclusión	Documentos que consideren diferentes visiones sobre el uso de IA en seguridad aeroportuaria.	2021	Brown, S.	Diverse Perspectives on AI in Airport Security. *Journal of International Security*, 11(2), 95-108.
16	Fracaso en la implementación	Exclusión	Documentos que solo hablen de fracasos sin ofrecer análisis constructivos o lecciones aprendidas.	S/I	S/I	S/I
17	No relacionados con seguridad	Exclusión	Estudios que no aborden directamente cuestiones de seguridad en aeropuertos en el contexto de IA.	S/I	S/I	S/I
18	Análisis cualitativo	Inclusión	Se aceptarán estudios que realicen un análisis cualitativo profundo de los sistemas de IA en aeropuertos.	2022	Green, C.	Analyzing AI in Airport Security: A Qualitative Study. *Journal of Security Technology*, 9(3), 145-160.
19	Experiencias internacionales	Inclusión	Documentos que analicen cómo se aplica la IA en la seguridad aeroportuaria en diferentes países.	2023	Patel, N.	International Perspectives on AI in Airport Security. *Global Security Review*, 18(2), 85-95.

JESUITAS ECUADOR

4.2. Resultados del análisis de inclusión y exclusión

La creación de criterios de inclusión y exclusión es fundamental para asegurar que la revisión de la literatura en un campo específico sea relevante, de alta calidad y exhaustiva. En esta investigación sobre la aplicación de la inteligencia artificial (IA) y el reconocimiento facial en la seguridad aeroportuaria, se han establecido criterios claros:

Criterios de inclusión:

- **Publicaciones en revistas revisadas por pares**: Este criterio garantiza que los estudios revisados sean evaluados por expertos en el campo antes de su publicación, asegurando la calidad y el rigor científico.
- **Año de publicación**: Se limita la búsqueda a artículos publicados entre 2018 y 2023, lo que permite recoger la información más actualizada y relevante en un campo que está en rápida evolución.
- **Documentos de organismos reconocidos**: Se incluyen informes de organizaciones como la OACI y INTERPOL para obtener un respaldo institucional y garantizar que las recomendaciones sigan estándares internacionales.
- **Enfoque en reconocimiento facial**: Este criterio se centra en documentos que estudian específicamente el uso del reconocimiento facial, un área crítica dentro de la seguridad aeroportuaria.
- **Estudios empíricos**: La inclusión de trabajos con datos empíricos proporciona evidencia concreta sobre la efectividad y los resultados de la aplicación de la IA en seguridad.
- **Método de análisis**: Se aceptarán ambos métodos de análisis (cualitativos y cuantitativos) para permitir una visión más amplia de los temas tratados.
- **Aspectos éticos**: Al considerar las implicaciones éticas, se pueden identificar y abordar preocupaciones críticas sobre la implementación de tecnologías de IA.
- **Casos de estudio**: Proporcionan ejemplos del mundo real de implementación de IA, lo que ayuda a entender su aplicabilidad práctica.
- **Revisión de literatura**: Reúne y sintetiza el conocimiento existente, contribuyendo a la construcción de un marco de referencia sólido.

JESUITAS ECUADOR

- **Estudios interdisciplinarios**: Facilitan una perspectiva más holística y comprensiva de la situación, incorporando diferentes campos del conocimiento.

- **Diversidad de perspectivas**: La inclusión de diferentes visiones enriquecerá el análisis sobre el uso y la percepción de la IA en la seguridad.

Criterios de exclusión:

- **Falta de evidencia empírica**: Se excluyen documentos sin datos concretos, ya que no aportan información valiosa a la investigación.

- **Enfoque en otro tipo de tecnología**: Solo se considerarán trabajos relacionados con IA, excluyendo aquellos que aborden tecnologías no pertinentes.

- **Documentos de opinión**: Comentarios sin respaldo científico no conforman evidencia robusta y, por tanto, serán excluidos.

- **Fallas en la referencia**: Artículos que no proporcionen adecuadamente sus referencias carecen de la credibilidad necesaria para formar parte del análisis.

- **Fracaso en la implementación**: Se evitarán documentos que solo se centren en fracasos sin ofrecer lecciones significativas o análisis constructivos.

- **No relacionados con seguridad**: Cualquier estudio que no trate sobre la seguridad en aeropuertos en el contexto de la IA será excluido para mantener la relevancia.

4.3. Búsqueda sistemática de literatura

La búsqueda sistemática de literatura es un proceso esencial que garantiza que la revisión sea completa. Se utilizarán bases de datos académicas como Scopus, IEEE Xplore y Google Scholar, formulando búsquedas con palabras clave estratégicas:

- "Reconocimiento Facial"
- "Inteligencia Artificial"
- "Seguridad Aeroportuaria"
- "IA en Aeropuertos"
- Combinaciones de los anteriores términos

JESUITAS ECUADOR

Esta estrategia de búsqueda permite captar un amplio espectro de literatura relevante y asegura que se identifiquen tanto estudios contemporáneos como aquellos que sientan bases para el conocimiento en el tema.

4.3.1. Análisis de documentos

El análisis cualitativo de los documentos seleccionados se centrará en extraer conceptos clave, tendencias y hallazgos significativos sobre la implementación de IA y el reconocimiento facial en aeropuertos:

- **Métodos Tradicionales vs. Modernos**: Se explorarán las diferencias y similitudes en los enfoques de seguridad aeroportuaria, evaluando la efectividad de los métodos tradicionales frente a sistemas avanzados de reconocimiento facial respaldados por IA.

Este análisis cualitativo explorará las diferencias y similitudes entre los métodos tradicionales y modernos de seguridad aeroportuaria, centrándose en la implementación de IA y reconocimiento facial. Se analizarán las ventajas y desventajas de cada enfoque, incluyendo la precisión, tiempo de respuesta y otros indicadores clave.

Tabla 2: Comparación de métodos tradicionales vs. modernos.

Comparación Métodos Tradicionales vs. Modernos		
Aspecto	**Métodos tradicionales**	**Métodos modernos (IA y Reconocimiento Facial)**
Precisión	- Depende de la habilidad del personal.	- Alta precisión en la identificación si los sistemas están bien calibrados.
	- Posibilidad de errores humanos.	- Puede presentar problemas de sesgo y precisión variable en ciertos grupos demográficos.
Tiempo de respuesta	- Tiempo de espera puede ser largo debido a procesos manuales.	- Respuesta rápida y eficiente mediante automatización.
	- Proceso de verificación más lento.	- Reducción significativa en el tiempo de espera.
Escalabilidad	- Limitada en la capacidad de manejar grandes volúmenes de pasajeros.	- Alta escalabilidad, capaz de gestionar grandes volúmenes de manera efectiva.
	- Aumento en tiempos de espera durante picos de tráfico.	- Manejo eficiente de grandes flujos de pasajeros.
Adaptabilidad	- Flexibilidad para adaptar respuestas a situaciones imprevistas.	- Adaptación a nuevas amenazas mediante actualizaciones de software.

JESUITAS ECUADOR

	- Evaluación contextual de comportamientos sospechosos.	- Adaptación automática a patrones de comportamiento mediante IA.
Costos iniciales	- Menor costo inicial, principalmente para capacitación y manejo del personal.	- Alto costo inicial de implementación y mantenimiento.
	- Costos asociados con la formación continua.	- Inversión significativa en tecnología avanzada.
Costos de mantenimiento	- Costos de mantenimiento generalmente más bajos.	- Costos continuos de mantenimiento y actualización de software.
	- - Requiere formación periódica del personal.	- Requiere actualizaciones regulares y supervisión del sistema.
Privacidad	- - Menos preocupaciones de privacidad directamente relacionadas con datos biométricos.	- Preocupaciones significativas sobre la privacidad y la protección de datos biométricos.
	- Protección de datos basada en métodos de seguridad física.	- Necesidad de políticas estrictas de protección de datos y consentimiento.
Transparencia	- Proceso manual puede ser menos transparente.	- Mayor transparencia en el proceso, pero requiere divulgación clara sobre el uso de datos.
	- Decisiones tomadas por personal con interacción directa.	- Decisiones automatizadas pueden ser difíciles de interpretar.
Riesgo de sesgo	- Menor riesgo de sesgo sistemático, pero posible sesgo humano.	- Riesgo de sesgo en el algoritmo, afectando la precisión en ciertos grupos.
	- Evaluación subjetiva de comportamientos.	- Evaluación basada en datos que pueden ser sesgados.
Interacción humana	- Interacción directa con el personal, permitiendo evaluación contextual.	- Menos interacción humana directa durante el proceso de verificación.
	- Evaluación subjetiva y contextual por parte del personal.	- Mayor dependencia en la tecnología para la evaluación.

Análisis de Resultados:

- **Métodos tradicionales**: Ofrecen la ventaja de la flexibilidad, interacción humana y adaptación contextual, pero son más lentos y menos escalables. Al principio, pueden ser más económicos, pero el tiempo de respuesta y la capacidad de manejar grandes volúmenes de pasajeros son problemas.

JESUITAS ECUADOR

- **Métodos Modernos (IA y Reconocimiento Facial)**: Proporcionan una alta precisión, rapidez y escalabilidad, pero enfrentan problemas relacionados con la privacidad, sesgo y costos iniciales. Aunque requieren una inversión significativa y políticas estrictas de protección de datos, son efectivos en la gestión de grandes volúmenes y en la reducción de tiempos de espera.

- **Aspectos éticos**: Se abordarán las preocupaciones éticas relacionadas con la privacidad, vigilancia y sesgos algorítmicos en la utilización de tecnologías de IA, destacando estudios relevantes en este ámbito.

La aplicación de la IA en la seguridad aeroportuaria presenta un panorama complejo con implicaciones éticas profundas. Aunque la IA ofrece herramientas innovadoras para mejorar la seguridad, también genera preocupaciones sobre la privacidad, la vigilancia y la posibilidad de sesgos algorítmicos. A continuación, se profundiza en estos aspectos y se exploran casos específicos en los que las preocupaciones éticas han impulsado cambios en las políticas o la implementación de las tecnologías:

1. Privacidad:

Escáneres corporales: Los escáneres corporales, basados en tecnología de IA, han generado debates sobre la privacidad de los viajeros.

Ejemplos:

- En Estados Unidos, la TSA (Transportation Security Administration) fue criticada por el uso de escáneres corporales sin opción de rechazo.
- En Europa, la Agencia Europea de Seguridad Aérea (EASA) emitió regulaciones para minimizar la exposición de los pasajeros a las imágenes escaneadas.

Reconocimiento facial: La utilización de reconocimiento facial para identificar viajeros plantea preocupaciones sobre la recopilación masiva de datos biométricos y su potencial uso para vigilancia no autorizada.

Ejemplos:

- En el Reino Unido, el uso del reconocimiento facial en los aeropuertos fue cuestionado por grupos de derechos civiles, quienes argumentaron que la tecnología podría utilizarse para rastrear a individuos sin su consentimiento.
- En China, la implementación del reconocimiento facial en aeropuertos ha sido criticada por su potencial uso para la vigilancia masiva y la persecución política.

2. Vigilancia:

Análisis predictivo: La IA puede utilizarse para analizar patrones de comportamiento y predecir posibles amenazas a la seguridad. Sin embargo, esto puede llevar a la creación de perfiles de pasajeros basados en criterios subjetivos, lo que genera preocupaciones sobre la discriminación y la vigilancia excesiva.

Ejemplos:

- El programa "Pre-Crime" desarrollado por la policía de Los Ángeles fue criticado por su uso de algoritmos de predicción para identificar posibles delitos, lo que resultó en la vigilancia de grupos minoritarios sin evidencia sólida.
- Algunos aeropuertos están utilizando análisis predictivo para identificar a los viajeros con mayor riesgo de presentar amenazas, pero no siempre es claro cómo se eligen estos criterios.

3. Sesgos algorítmicos:

Imparcialidad: Los algoritmos de IA están entrenados con datos existentes, lo que puede generar sesgos si los datos son sesgados. Esto puede conducir a decisiones injustas en materia de seguridad.

Ejemplos:

- Se ha demostrado que los algoritmos de reconocimiento facial son menos precisos para identificar a personas con tonos de piel oscura, lo que genera preocupaciones sobre la discriminación racial.
- Algunos sistemas de detección de armas en aeropuertos han mostrado sesgos hacia ciertos grupos étnicos, lo que puede llevar a un trato injusto.

Abordando los desafíos éticos:

Para mitigar los riesgos éticos de la IA en la seguridad aeroportuaria, se requieren regulaciones y ajustes en las tecnologías:

Transparencia: Las agencias gubernamentales deben ser transparentes en la manera en que utilizan la IA y los criterios que utilizan para el análisis de datos.

Privacidad: Las regulaciones deben garantizar la protección de los datos personales y la minimización de la recopilación de datos biométricos.

Imparcialidad: Los algoritmos de IA deben ser diseñados y probados para garantizar que no discriminen a grupos específicos.

Participación pública: Se necesita la participación pública en la formulación de las políticas para la implementación de la IA en la seguridad aeroportuaria, con el fin de garantizar que las decisiones se tomen de manera ética y responsable.

- **Casos prácticos**: a través del análisis de casos de estudio, se evaluará cómo las implementaciones de IA han funcionado en diferentes contextos aeroportuarios, identificando los factores de éxito y los desafíos encontrados.

- **Recomendaciones y conclusiones**: Finalmente, se extraerán conclusiones sobre las mejores prácticas y se propondrán recomendaciones para futuras investigaciones y desarrollos en este campo.

4.4. Fase 2: Investigación empírica

4.4.1. Parte cualitativa

- **Resultados de la entrevista a la señora Jefe de Operaciones experto en seguridad de aeropuertos**

  A continuación, se detalla los resultados a la entrevista realizada a la señora Jefe de Operaciones del aeropuerto:

1. Métodos tradicionales de reconocimiento facial

1.1. ¿Cuáles son los métodos tradicionales de reconocimiento facial que se utilizan actualmente en los aeropuertos?

Detección de rostro: Los sistemas primero localizan la cara en una imagen o video. Este proceso implica identificar la región de la cara y separar los rostros del fondo.

Alineación de rostro: Una vez detectado, el rostro se alinea para que las características faciales clave (ojos, nariz, boca) estén en posiciones consistentes.

1.2. ¿Cuáles son las principales ventajas y limitaciones de estos métodos en términos de precisión y eficiencia?

Ventajas:

- Alta precisión en condiciones controladas
- Capacidad de identificación en tiempo real
- Reducción de errores humanos

- Rápido procesamiento
- Menor necesidad de intervención humana
- Integración con otros sistemas

Limitaciones:

- Sensibilidad a condiciones variables.
- Problemas con diversidad de rostros.
- Falsos positivos y negativos.
- Requerimientos de hardware y software.
- Dependencia de la calidad de la base de datos.
- Privacidad y preocupaciones legales.

1.3. ¿Qué tipo de tecnología y personal es necesario para operar estos sistemas tradicionales?

Tecnología necesaria:

- Cámaras de alta calidad
- Sistemas de iluminación
- Servidores y almacenamiento
- Software de reconocimiento facial
- Redes y comunicaciones
- Bases de datos

Personal necesario:

- Ingenieros de software y hardware
- Especialistas en seguridad informática
- Operadores de sistemas
- Analistas de datos
- Personal de mantenimiento
- Formadores y capacitación

Integración y coordinación:

- Colaboración con autoridades de seguridad
- Equipos multidisciplinarios

1.4. ¿Qué desafíos enfrentan los aeropuertos al utilizar estos métodos tradicionales?

Desafíos técnicos:

- Variabilidad en condiciones de iluminación
- Problemas con ángulos y posiciones de captura
- Reconocimiento de rostros parcialmente ocultos

JESUITAS ECUADOR

- Dificultades con la diversidad de rostros
- Actualización y mantenimiento de bases de datos
- Requisitos de hardware y software de alto rendimiento

Desafíos operativos:

- Integración con sistemas existentes
- Capacitación y gestión de personal
- Mantenimiento y soporte continuo
- Gestión de fallos y respuesta a incidentes

Desafíos de seguridad y privacidad:

- Protección de datos personales
- Cumplimiento de normativas y regulaciones
- Riesgos de ciberseguridad

Desafíos éticos y sociales:

- Preocupaciones sobre la privacidad
- Aceptación pública
- Posibles sesgos en el reconocimiento facial
- Impacto en la experiencia del pasajero

2. Técnicas de inteligencia artificial en reconocimiento facial

2.1. ¿Qué técnicas de inteligencia artificial se están utilizando actualmente para el reconocimiento facial en los aeropuertos?

- Redes neuronales convolucionales (CNN)
- Aprendizaje profundo (Deep Learning)
- Reconocimiento facial en 3D

2.2. ¿Qué algoritmos o modelos de IA son los más comúnmente utilizados para el reconocimiento facial en aeropuertos?

- Convolutional neural networks (CNN)
- Deep neural networks (DNN)
- FaceNet
- VGG-Face
- ResNet

2.3 ¿Cuáles son las principales ventajas y limitaciones de las técnicas de IA en comparación con los métodos tradicionales?

Ventajas de las Técnicas de IA:

- Mayor precisión y capacidad de adaptación a variaciones en iluminación, ángulos y expresiones faciales.
- Capacidad de procesamiento en tiempo real con grandes volúmenes de datos.
- Autoaprendizaje y mejora continua a medida que se procesan más datos.

Limitaciones de las Técnicas de IA:

- Requerimientos elevados de hardware y recursos computacionales.
- Necesidad de grandes volúmenes de datos etiquetados para el entrenamiento.
- Posibles sesgos y problemas éticos relacionados con la privacidad y el uso de datos.

2.4 ¿Qué avances recientes se han dado en el campo del reconocimiento facial basado en IA?

- Mejora en la Precisión con Modelos de Última Generación
- Reconocimiento Facial en Condiciones Adversas
- Reducción de Sesgos y Mejoras en Inclusividad

3. Análisis comparativo de precisión

3.1. ¿Cómo se mide y compara la precisión de los métodos tradicionales versus las técnicas de IA para reconocimiento facial en aeropuertos?

Tasa de Verdaderos Positivos

- Métodos Tradicionales: Evaluación de cuántas veces el sistema identifica correctamente un rostro conocido.
- Técnicas de IA: Medición de la tasa de coincidencias correctas en comparación con una base de datos de rostros.

Tasa de Falsos Positivos y Negativos

- Métodos Tradicionales: Frecuencia con la que el sistema identifica incorrectamente a alguien como un individuo conocido (falsos positivos) o no lo identifica cuando debería (falsos negativos).
- Técnicas de IA: Evaluación de la tasa de errores en la identificación y verificación facial, incluyendo falsos positivos y negativos.

Precisión y Recall

- Métodos Tradicionales: Precisión de las identificaciones correctas frente al total de identificaciones realizadas.
- Técnicas de IA: Medición de la precisión (proporción de identificaciones correctas) y recall (proporción de verdaderos positivos detectados) utilizando métricas avanzadas de evaluación.

3.2. ¿Cuáles son las métricas clave que se utilizan para evaluar el desempeño y la precisión de estas tecnologías?

- Tasa de verdaderos positivos
- Tasa de falsos positivos
- Tasa de falsos negativos
- Precisión
- Recall

3.3 ¿Qué desafíos técnicos se enfrentan al implementar sistemas de IA en comparación con los sistemas tradicionales?

- Requerimientos elevados de hardware y recursos computacionales
- Necesidad de grandes volúmenes de datos etiquetados para el entrenamiento
- Complejidad en la integración con sistemas existentes

3.4 ¿Ha habido casos específicos en los que los sistemas de IA hayan demostrado ser significativamente más efectivos que los métodos tradicionales?

Sí, ha habido casos específicos en los que los sistemas de IA han demostrado ser significativamente más efectivos que los métodos tradicionales:

Caso: Sistemas de IA como los basados en reconocimiento facial en 3D han mostrado una mayor efectividad en identificar rostros en condiciones de baja iluminación o con ángulos difíciles, superando a los métodos tradicionales que luchan con estas variaciones.

4. Implicaciones éticas del reconocimiento facial

4.1. ¿Cuáles son las principales preocupaciones éticas asociadas con el uso del reconocimiento facial en los aeropuertos?

- Privacidad y protección de datos personales
- Potencial para vigilancia masiva
- Sesgo y discriminación

4.2 ¿Cómo se manejan los problemas de privacidad y protección de datos en los sistemas de reconocimiento facial basados en IA?

- Implementación de encriptación robusta para proteger los datos faciales almacenados y transmitidos, asegurando que solo las partes autorizadas puedan acceder a ellos.

- Adopción de regulaciones de protección de datos como el Reglamento General de Protección de Datos (GDPR) en Europa o Ley de Privacidad del Consumidor de California (CCPA) en EE.UU. para garantizar el cumplimiento de estándares legales de privacidad.

- Obtención de consentimiento explícito de los individuos antes de la recopilación de datos faciales y transparencia en cómo se utilizan y almacenan estos datos, incluyendo la implementación de políticas claras sobre el uso y manejo de la información personal.

4.3 ¿Qué políticas o regulaciones están en vigor para garantizar el uso ético y responsable de las tecnologías de reconocimiento facial?

- Ley Orgánica de Protección de Datos Personales: Regula la recolección, tratamiento y protección de datos personales, exigiendo el consentimiento explícito de los individuos y estableciendo medidas para la protección y seguridad de los datos.

- Reglamento General a la Ley Orgánica de Protección de Datos Personales: Detalla los procedimientos y obligaciones para el manejo de datos personales, incluyendo el reconocimiento facial, y establece derechos para los titulares de datos.

- Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos: Regula el uso de firmas electrónicas y el comercio electrónico, que puede incluir la recopilación y el tratamiento de datos personales en línea, asegurando la integridad y confidencialidad de los datos.

4.4 ¿Qué buenas prácticas se pueden implementar para mitigar los riesgos éticos del reconocimiento facial en aeropuertos?

- Obtener el consentimiento explícito de los individuos antes de la recopilación y uso de sus datos faciales, proporcionando información clara sobre cómo se utilizarán y almacenarán los datos.

- Implementar políticas transparentes sobre el uso de tecnologías de reconocimiento facial y permitir a los individuos acceder a sus datos y solicitar correcciones o eliminaciones si es necesario.

- Realizar auditorías periódicas para asegurar que el uso del reconocimiento facial cumple con las normativas y estándares éticos, y establecer mecanismos de supervisión para detectar y abordar posibles abusos o violaciones.

5. Impacto en la seguridad y eficiencia

5.1. ¿Cómo ha impactado la implementación de IA en la seguridad y eficiencia de los controles de seguridad en aeropuertos?

- La IA, especialmente mediante el uso de redes neuronales avanzadas y aprendizaje profundo, ha incrementado la precisión en la identificación de pasajeros, reduciendo errores y falsos positivos/negativos.

- Los sistemas de IA permiten una verificación más rápida de identidades y la automatización de procesos, lo que reduce significativamente los tiempos de espera y mejora el flujo de pasajeros.

- La IA mejora la detección de comportamientos sospechosos y la identificación de patrones de riesgo en tiempo real, aumentando la capacidad para prevenir incidentes de seguridad antes de que ocurran.

5.2. ¿Qué cambios operativos se han observado con la adopción de sistemas de IA en comparación con los métodos tradicionales?

- Procesos automatizados y análisis en tiempo real han reducido significativamente los tiempos de espera para los pasajeros en los controles de seguridad.

- La automatización y la IA permiten al personal de seguridad enfocarse en tareas más complejas y críticas, redistribuyendo recursos humanos de manera más efectiva.

- Los sistemas de IA ayudan a predecir y gestionar flujos de pasajeros, facilitando una planificación más eficiente y mejorando la capacidad de respuesta en períodos de alta demanda.

5.3. ¿Existen estudios de caso que demuestren la efectividad de los sistemas de IA en la seguridad aeroportuaria?

- **Aeropuerto de Singapur (Changi):** Implementación de sistemas de IA para reconocimiento facial en el proceso de inmigración y seguridad. Mejora en la precisión de la identificación de pasajeros y reducción en los tiempos de espera en los controles de seguridad.

- **Aeropuerto de Atlanta (Hartsfield-Jackson)**: Uso de IA y análisis de video para monitorear y gestionar flujos de pasajeros y detectar comportamientos sospechosos. Aumento en la eficiencia operativa y detección más temprana de potenciales amenazas de seguridad.

6. Percepción del usuario

6.1. ¿Cuál es la percepción de los pasajeros sobre la seguridad y la eficiencia de los sistemas de reconocimiento facial basados en IA en los aeropuertos?

- Muchos pasajeros valoran la reducción en los tiempos de espera y la agilización de los procesos de seguridad proporcionados por los sistemas de reconocimiento facial.

- Algunos pasajeros están preocupados por la recopilación y almacenamiento de sus datos faciales, y temen sobre el manejo y la protección de su privacidad.

- Mientras que algunos pasajeros confían en que los sistemas de IA mejoran la seguridad al proporcionar una identificación más precisa, otros pueden ser escépticos sobre la precisión y la capacidad de estos sistemas para manejar situaciones excepcionales.

6.2 ¿Qué niveles de confianza y aceptación tienen los pasajeros hacia los sistemas de reconocimiento facial basados en IA?

- Muchos pasajeros aceptan y confían en los sistemas de reconocimiento facial por su capacidad para reducir los tiempos de espera y agilizar el proceso de seguridad.

- Hay una aceptación general, pero algunos pasajeros mantienen reservas sobre la precisión y la fiabilidad de los sistemas, especialmente en situaciones complejas o excepcionales.

- Existen preocupaciones significativas sobre la privacidad y la protección de datos, que pueden afectar negativamente la aceptación general de estos sistemas, especialmente entre aquellos que valoran la confidencialidad de sus datos personales.

6.3 ¿Qué recomendaciones haría para mejorar la aceptación y efectividad de estos sistemas?

- Proporcionar información detallada sobre cómo se recopilan, usan y protegen los datos faciales. Educar a los pasajeros sobre los beneficios y medidas de seguridad para aumentar la confianza.

- Asegurar que los pasajeros puedan dar consentimiento explícito para el uso de sus datos faciales y ofrecer opciones de exclusión para quienes prefieran no utilizar estos sistemas.

- Implementar medidas de seguridad robustas para proteger los datos personales y cumplir con las normas de privacidad.

- Realizar auditorías regulares y auditar el manejo de datos para asegurar el cumplimiento de las regulaciones.

- Invertir en tecnología avanzada y actualizar los sistemas regularmente para mejorar la precisión y adaptabilidad.

- Capacitar al personal para manejar situaciones excepcionales y procesos de emergencia relacionados con el reconocimiento facial. Asegurar que el personal esté bien informado y preparado para resolver problemas rápidamente.

4.4.1. Parte Cuantitativa

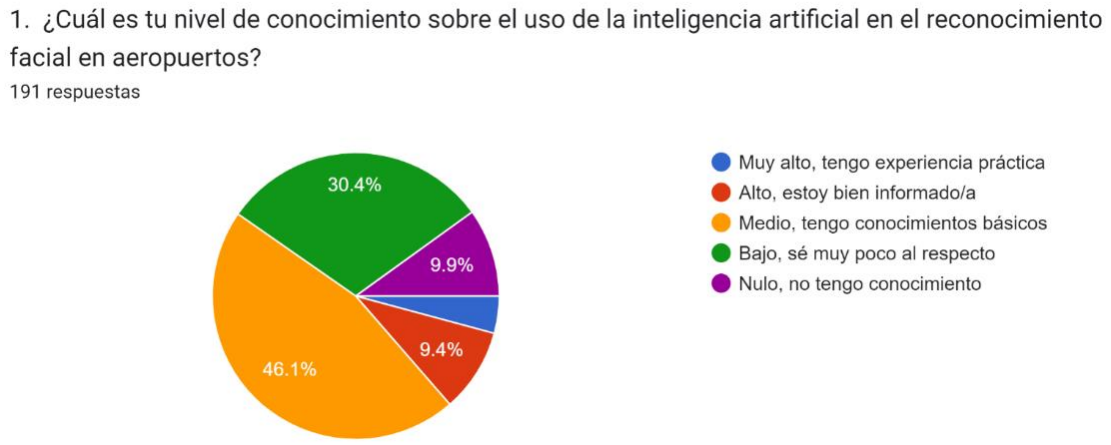
En el aeropuerto trabajan 300 personas en la seguridad del aeropuerto, distribuidos en 4 grupos de trabajo. La muestra ideal con un nivel de confianza del 95%, con un margen de error de + - 5%, es 169 encuestados. Cabe mencionar que, la encuesta fue contestada por 191 personas del personal del aeropuerto. A continuación, se detalla el análisis de los resultados de las encuestas aplicadas al personal de seguridad:

1. **¿Cuál es tu nivel de conocimiento sobre el uso de la inteligencia artificial en la seguridad ciudadana en aeropuertos?**

Tabla 3: Resultados pregunta 1 de la encuesta.

Ítem	Frecuencia	Porcentaje
Muy alto, tengo experiencia práctica	18	9.4%
Alto, estoy bien informado/a	8	4.2%
Medio, tengo conocimientos básicos	88	46.1%
Bajo, sé muy poco al respecto	58	30.4%
Nulo, no tengo conocimiento	19	9.9%
Total	**191**	**100%**

Figura 1: Resultados pregunta 1 de la encuesta.



Análisis

La mayoría de los encuestados (46.1%) indica que su conocimiento es medio, lo que sugiere un entendimiento básico pero no profundo. Un 30.4% afirma tener un conocimiento bajo, lo que puede indicar una falta de formación o información en el uso de inteligencia artificial. Un 9.4% presenta un conocimiento muy alto, mientras que el 9.9% no tiene conocimiento alguno. Estos datos reflejan la necesidad de capacitación continua en el área de inteligencia artificial para mejorar la seguridad.

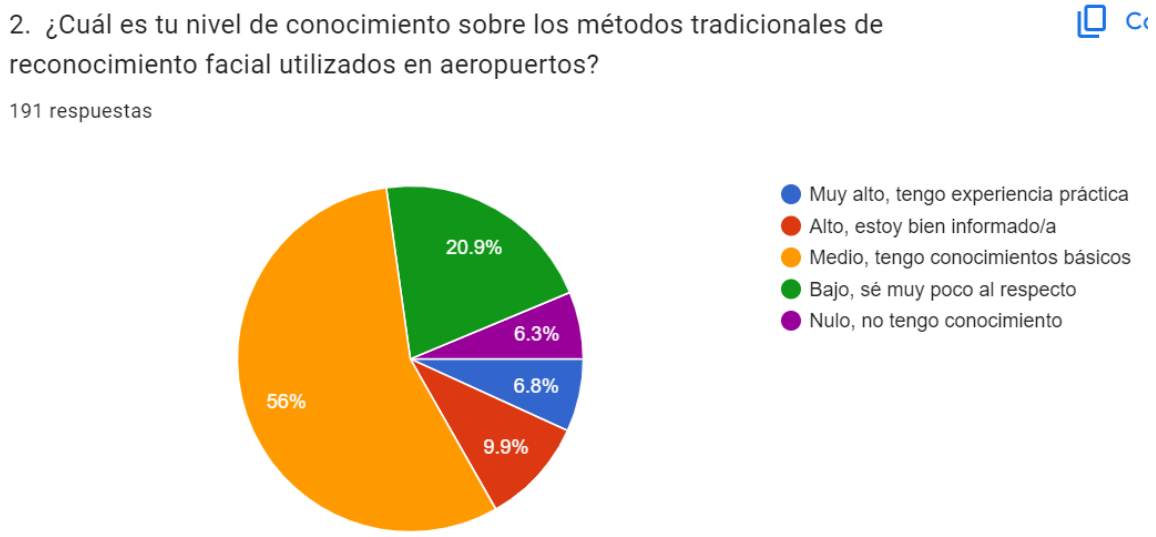
JESUITAS ECUADOR

¿Cuál es tu nivel de conocimientos sobre los métodos tradicionales de reconocimiento facial utilizados en aeropuertos?

Tabla 4: Resultados pregunta 2 de la encuesta.

Ítem	Frecuencia	Porcentaje
Muy alto, tengo experiencia práctica	13	6.8%
Alto, estoy bien informado/a	19	9.9%
Medio, tengo conocimientos básicos	107	56%
Bajo, sé muy poco al respecto	40	20.9%
Nulo, no tengo conocimiento	12	6.3%
Total	**191**	**100%**

Figura 2: Resultados pregunta 2 de la encuesta.



Análisis:

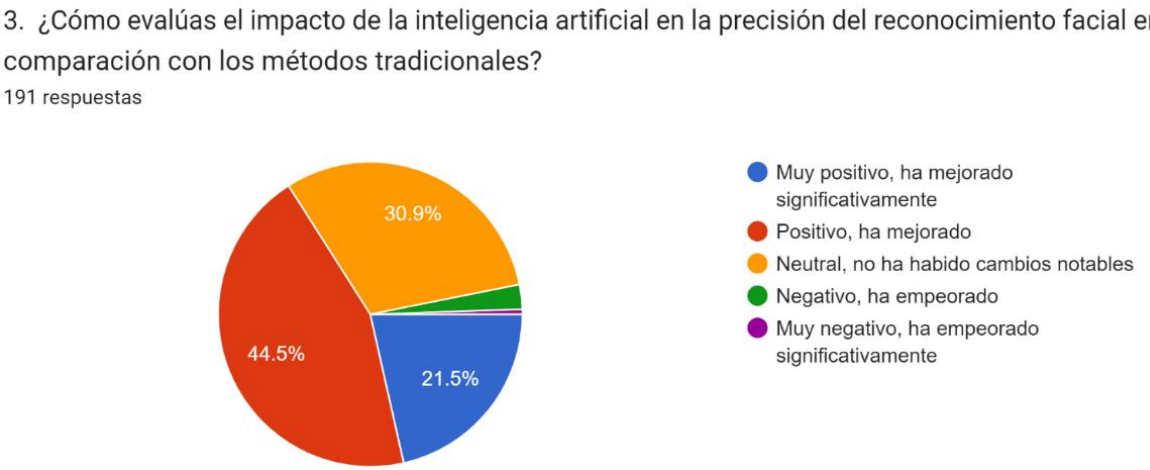
La mayoría (56%) tiene conocimientos básicos, seguido de un 20.9% con conocimiento bajo. Un 6.8% indica tener experiencia práctica y 9.9% está bien informado. Este resultado revela una brecha de conocimiento en métodos tradicionales, lo que podría limitar la capacidad de los empleados para juzgar la efectividad frente a sistemas más avanzados.

2. ¿Cómo evalúas el impacto de la implementación de la inteligencia artificial en la mejora de la seguridad en los aeropuertos?

Tabla 5: Resultados pregunta 3 de la encuesta.

Ítem	Frecuencia	Porcentaje
Muy positivo, ha mejorado significativamente	41	21,50%
Positivo, ha mejorado	58	44,50%
Neutral, no ha habido cambios notables	59	30,90%
Negativo, ha empeorado	21	2%
Muy negativo, ha empeorado significativamente	12	1%
Total	**191**	**100%**

Figura 3: Resultados pregunta 3 de la encuesta.



Analisis:

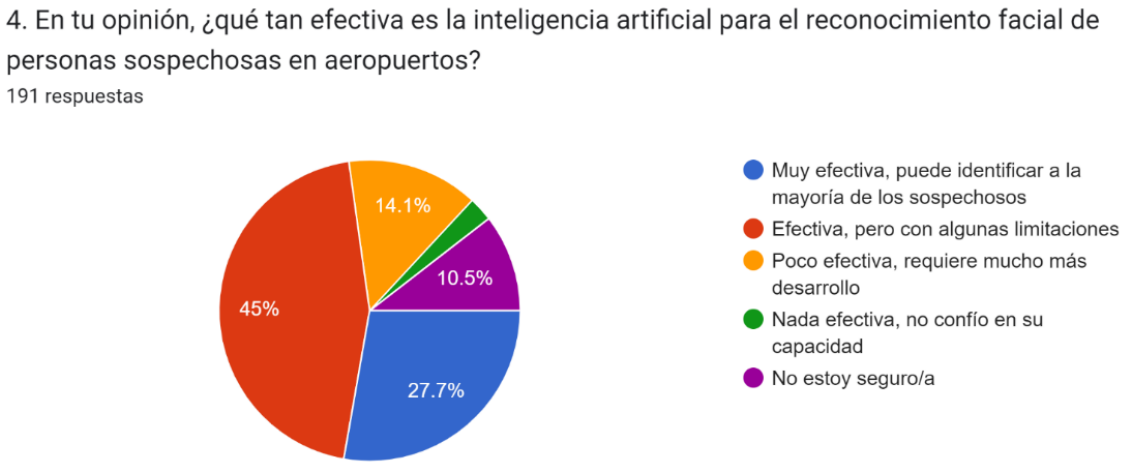
Casi la mitad de los encuestados (44.5%) considera que el impacto ha sido positivo, y un 21.5% señala que ha mejorado significativamente. Sin embargo, un 30.9% es neutral, lo que puede señalar opiniones mixtas o la falta de impactos notables en su trabajo diario. Los resultados muestran una tendencia mayoritariamente optimista sobre la IA, aunque un segmento importante se muestra escéptico.

3. **En tu opinión, ¿qué tan efectiva es la inteligencia artificial para el reconocimiento facial de personas sospechosas en aeropuertos?**

Tabla 6: Resultados pregunta 4 de la encuesta.

Ítem	Frecuencia	Porcentaje
Muy efectiva, puede identificar a la mayoría de los sospechosos	53	27,70%
Efectiva, pero con algunas limitaciones	86	45,00%
Poco efectiva, requiere mucho más desarrollo	27	14,10%
Nada efectiva, no confió en su capacidad	3	2,00%
No estoy seguro/a	21	11%
Total	**191**	**100%**

Figura 4: Resultados pregunta 4 de la encuesta.



Análisis:

La percepción de efectividad es alta entre los encuestados, con un 27.7% considerando que es muy efectiva y un 45% que la encuentra efectiva a pesar de algunas limitaciones. Sin embargo, un 14.1% la califica como poco efectiva, reflejando una cierta preocupación sobre su desarrollo. Esto sugiere que hay confianza en la tecnología, pero también una conciencia de sus limitaciones.

JESUITAS ECUADOR

4. **¿Como comparas la efectividad de los métodos tradicionales de reconocimiento facial con la inteligencia artificial en la identificación de personas sospechosas?**

Tabla 7: Resultados pregunta 5 de la encuesta.

Ítem	Frecuencia	Porcentaje
Los métodos tradicionales son más efectivos	27	14,10%
La inteligencia artificial es más efectiva	56	29,30%
Ambos son igual de efectivos	70	36,60%
No estoy seguro/a	38	19,90%
Total	**191**	**100%**

Figura 5: Resultados pregunta 5 de la encuesta.



Análisis:

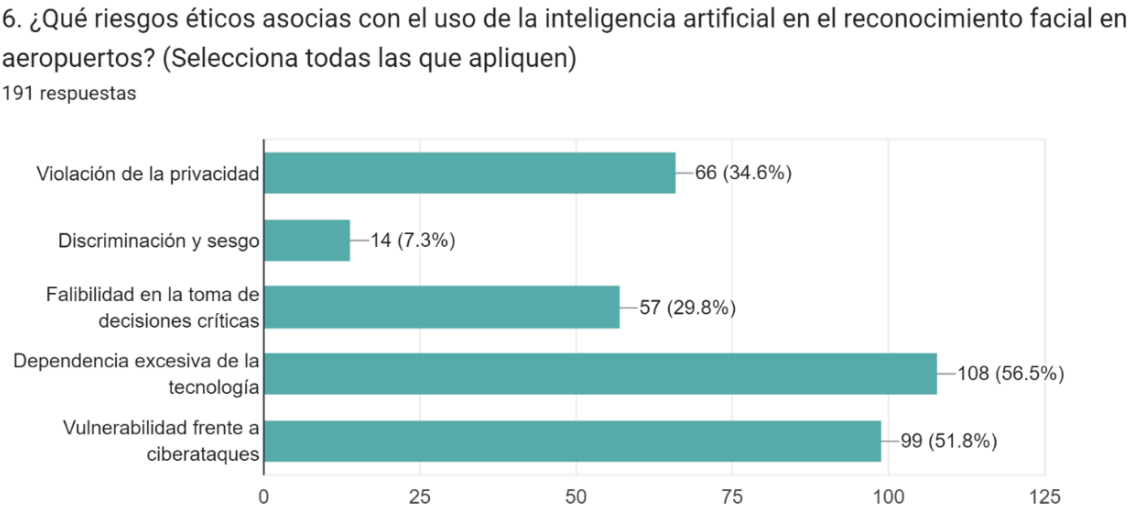
La inclinación hacia la inteligencia artificial es notable, con un 29.3% considerándola más efectiva y un 36.6% opinando que ambos métodos son igualmente efectivos. Sin embargo, un 14.1% cree que los métodos tradicionales son más efectivos. Esto sugiere que, aunque la IA es vista como una mejora, aún hay defensores de los métodos tradicionales que podrían influir en la toma de decisiones.

5. ¿Qué riesgos éticos asocias con el uso de inteligencia artificial en el reconocimiento facial en aeropuertos? (Selecciona todas las que apliquen)

Tabla 8: Resultados pregunta 6 de la encuesta.

Ítem	Frecuencia	Porcentaje
Violación de la privacidad	66	34.6%
Discriminación y sesgo	14	7.3%
Falibilidad en la toma de decisiones criticas	57	29.8%
Dependencia excesiva de tecnología	108	56.5%
Vulnerabilidad frente a ciberataques	99	51.8%
Total	**191**	**100%**

Figura 6: Resultados pregunta 6 de la encuesta.



Análisis:

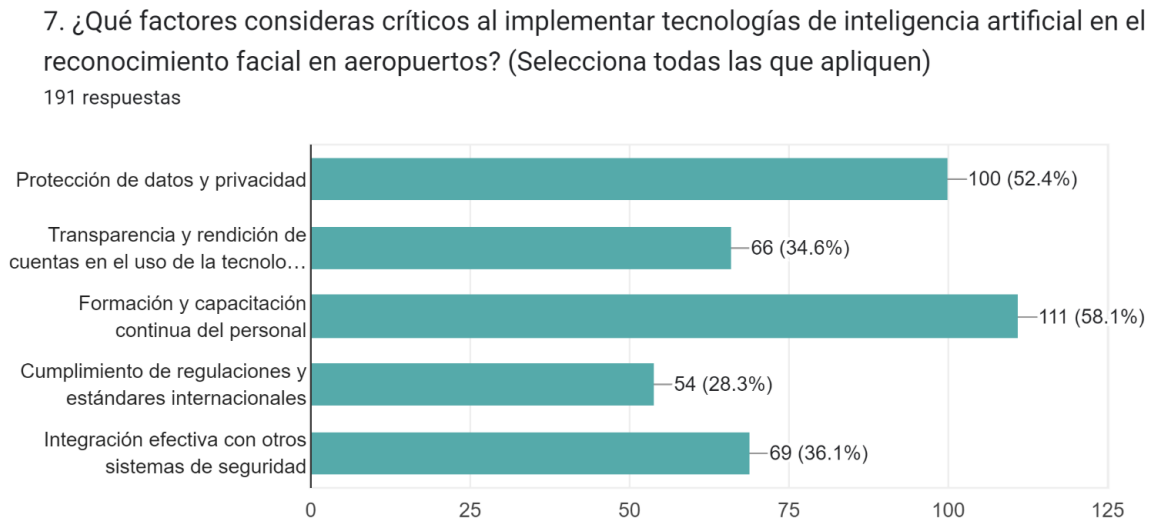
La preocupación por la dependencia excesiva de la tecnología (56.5%) y la vulnerabilidad a ciberataques (51.8%) es significativa. Además, la violación de la privacidad también genera una fuerte preocupación (34.6%). Estas respuestas indican una conciencia crítica de los posibles efectos adversos de la IA, lo que señala la necesidad de un marco ético robusto en su implementación.

6. ¿Qué factores consideras críticos al implementar tecnologías de inteligencia artificial en la seguridad de los aeropuertos? (Selecciona todas las que apliquen)

Tabla 9: Resultados pregunta 7 de la encuesta.

Ítem	Frecuencia	Porcentaje
Protección de datos y privacidad	100	52.4%
Transparencia y rendición de cuentas en el uso de la tecnología	66	34.6%
Formación y capacitación continua del personal	111	58.1%
Cumplimiento de regulaciones y estándares internacionales	54	28.3%
Integración efectiva con otros sistemas de seguridad	69	36.1%
Total	**191**	**100%**

Figura 7: Resultados pregunta 7 de la encuesta.



Análisis:

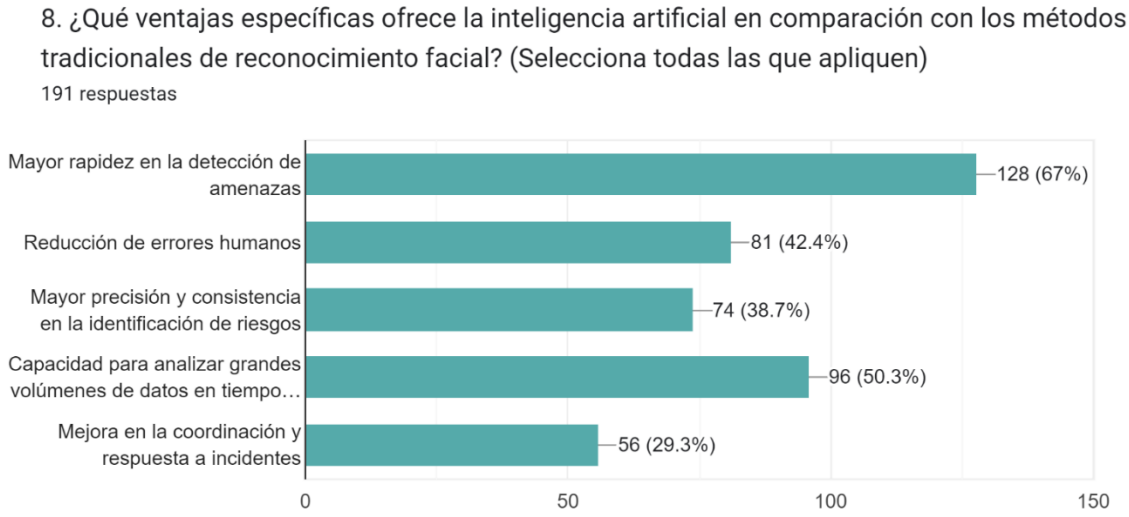
La necesidad de formación continua del personal es vista como un factor crítico (58.1%), lo que subraya la importancia de que los operadores estén capacitados en nuevas tecnologías. La protección de datos y la privacidad también son considerados importantes (52.4%). Esto sugiere que cualquier implementación debe priorizar la capacitación y el respeto por la privacidad.

7. ¿Qué ventajas específicas crees que ofrece la inteligencia artificial en comparación con los métodos tradicionales de reconocimiento facial? (Selecciona todas las que apliquen)

Tabla 10: Resultados pregunta 8 de la encuesta.

Ítem	Frecuencia	Porcentaje
Mayor rapidez en la detección de amenazas	128	67%
Reducción de errores humanos	81	42.4%
Mayor precisión y consistencia en la identificación de riesgos	74	38.7%
Capacidad para analizar grandes volúmenes de datos en tiempo	96	50.3%
Mejora en la coordinación respuesta a incidentes	56	29.3%
Total	**191**	**100%**

Figura 8: Resultados pregunta 8 de la encuesta.



Análisis:

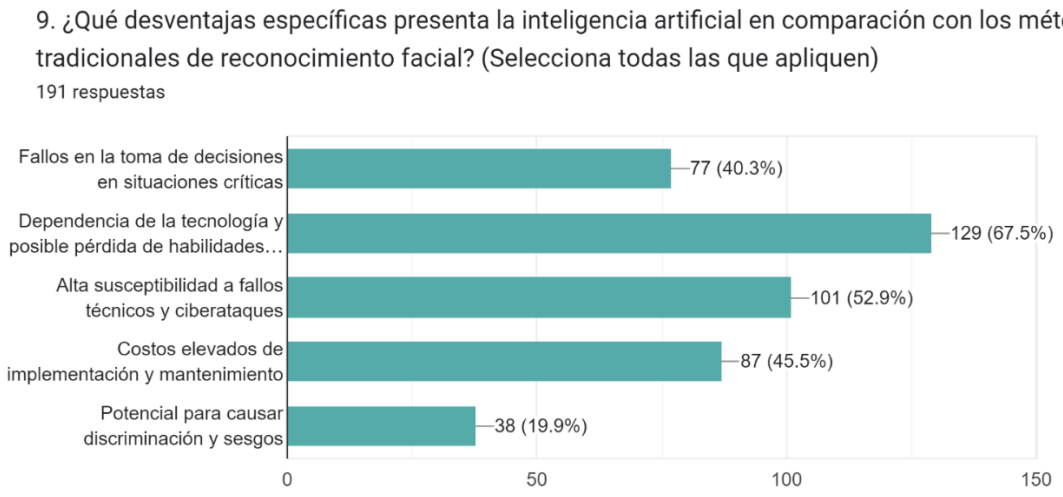
Las ventajas más citadas son la rapidez en la detección de amenazas (67%) y la capacidad para analizar grandes volúmenes de datos (50.3%). Esto demuestra una apreciación clara por la agilidad y la eficiencia que la IA puede brindar en escenarios de manejo de seguridad, lo que probablemente influye en su aceptación.

8. ¿Qué desventajas específicas crees que presenta la inteligencia artificial en la seguridad de los aeropuertos? (Selecciona todas las que apliquen)

Tabla 11: Resultados pregunta 9 de la encuesta.

Ítem	Frecuencia	Porcentaje
Fallos en la toma de decisiones en situaciones críticas	77	40.3%
Dependencia de la tecnología y posible pérdida de habilidades humanas	129	67.5%
Alta susceptibilidad a fallos técnicos y ciberataques	101	52.9%
Costos elevados de implementación y mantenimiento	87	45.5%
Potencial para causar discriminación y sesgos	38	19.9%
Total	**191**	**100%**

Figura 9: Resultados pregunta 9 de la encuesta.



Análisis

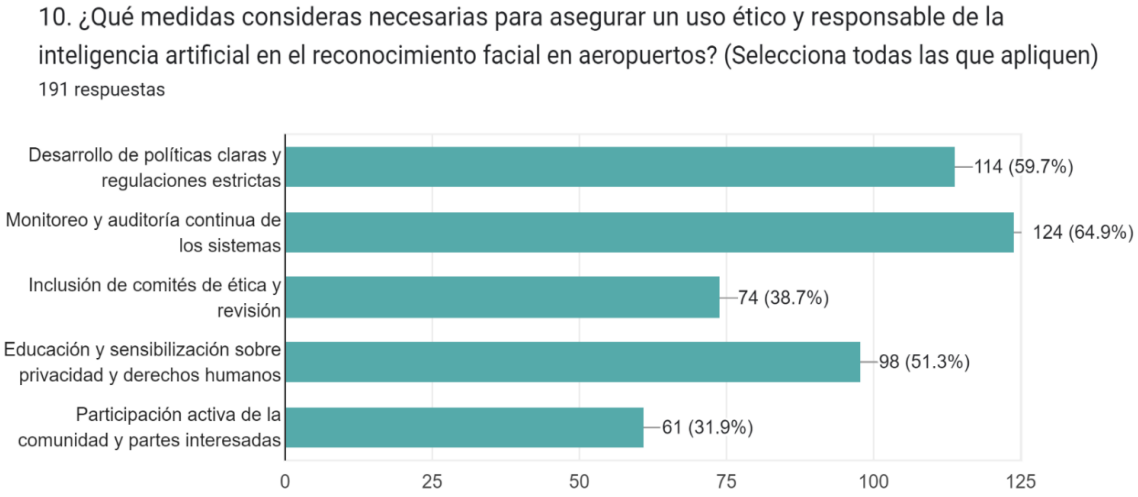
La dependencia de la tecnología y la posible pérdida de habilidades humanas (67.5%) es la preocupación más elevada, seguida de la alta susceptibilidad a fallos técnicos (52.9%). Esto podría reflejar temores sobre la capacidad humana para manejar situaciones críticas sin apoyo tecnológico, sugiriendo que debe haber un equilibrio entre tecnología y competencias humanas.

9. ¿Qué medidas consideras necesarias para asegurar un uso ético y responsable de la inteligencia artificial en la seguridad aeroportuaria? (Selecciona todas las que apliquen)

Tabla 12: Resultados pregunta 10 de la encuesta.

Ítem	Frecuencia	Porcentaje
Desarrollo de políticas claras y regulaciones estrictas	114	59.7%
Monitoreo y auditoría continua de los sistemas	124	64.9%
Inclusión de comités de ética y revisión	74	38.7%
Educación y sensibilización sobre privacidad y derechos humanos	98	51.3%
Participación activa de la comunidad y partes interesadas	61	31.9%
Total	**191**	**100%**

Figura 10: Resultados pregunta 10 de la encuesta.



Análisis:

Las propuestas más apoyadas incluyen el desarrollo de políticas claras y regulaciones estrictas (59.7%) y el monitoreo continuo de los sistemas (64.9%), lo que indica un fuerte deseo de transparencia y responsabilidad en el uso de IA. Además, la sensibilización sobre privacidad y derechos humanos (51.3%) sugiere un compromiso hacia el respeto de estos principios en la implementación de nuevas tecnologías.

JESUITAS ECUADOR

CAPÍTULO V: ANÁLISIS DE RESULTADOS

5. ANÁLISIS DE RESULTADOS

En este capítulo se realizará el análisis de los resultados obtenidos a partir de datos cuantitativos y cualitativos sobre la implementación de tecnologías de IA en aeropuertos. Se examinarán las percepciones de efectividad para entender mejor cómo esta tecnología impacta la seguridad ciudadana. Además, se evaluarán las ventajas y desventajas de las tecnologías modernas en comparación con los enfoques tradicionales

5.1. Análisis de la entrevista aplicada al experto de seguridad

A continuación, se realiza un análisis a la entrevista realizada a la Jefe de Operaciones del aeropuerto:

1. Métodos tradicionales de reconocimiento facial

Los métodos tradicionales se basan en prácticas que han sido perfeccionadas a lo largo del tiempo, como la detección y alineación de rostros, con ventajas notables en condiciones controladas. Sin embargo, las limitaciones destacan problemas de precisión en diversas condiciones y potenciales sesgos hacia ciertos grupos demográficos.

- **Ventajas:**
    - Alta precisión en entornos óptimos.
    - Mayor eficiencia en el procesamiento en situaciones controladas.
- **Limitaciones:**
    - Sensibilidad a cambios en el entorno (iluminación, cobertura facial).
    - Problemas asociados con el sesgo en la calidad del reconocimiento.

2. Técnicas de inteligencia artificial en reconocimiento facial

Las técnicas de IA representan un avance significativo, con la implementación de redes neuronales convolucionales y aprendizaje profundo mejorando la capacidad de adaptación a variaciones en las condiciones. Este análisis subraya que, a pesar de sus ventajas, también existe una dependencia de data etiquetada y altas necesidades computacionales.

- **Ventajas:**

    - Mayor adaptabilidad a diferentes condiciones y variedades de datos.
    - Eficiencia en el procesamiento de altas cantidades de información.

JESUITAS ECUADOR

- **Limitaciones:**

    - Altos requerimientos de hardware.
    - Desafíos éticos relacionados con la privacidad de los datos.

3. Análisis comparativo de precisión

El análisis de precisión entre métodos tradicionales y técnicas de IA se basa en métricas objetivas como la tasa de verdaderos positivos y la tasa de falsos, proporcionando un marco para evaluar la efectividad de cada aproximación.

- **Desafíos Técnicos:**

    - Necesidad de infraestructura avanzada para IA.
    - Dificultades en la integración con sistemas tradicionales.

4. Implicaciones éticas del reconocimiento facial

Las preocupaciones éticas son un tema clave. La privacidad, la vigilancia masiva y el sesgo en los algoritmos son cuestiones que deben ser abordadas para mejorar la aceptación pública de estos sistemas. La implementación de regulaciones como el GDPR es crucial para ofrecer un marco legal que proteja los derechos de los individuos.

5. Impacto en la seguridad y eficiencia

La implementación de la inteligencia artificial ha mostrado un impacto positivo en términos de seguridad, eficiencia y optimización de los recursos en aeropuertos. La detección proactiva de amenazas y la reducción de tiempos de espera son beneficios clave.

- **Cambios Operativos:**

    - Procesos más rápidos y una mejor gestión de los flujos de pasajeros.
    - Redistribución de los recursos humanos hacia tareas más críticas.

6. Percepción del usuario

La percepción del usuario se encuentra dividida entre el reconocimiento de la eficiencia mejorada y las preocupaciones sobre la privacidad. La confianza se ve afectada por la capacidad de estos sistemas para manejar situaciones complejas y garantizar la protección de los datos personales.

- **Recomendaciones para Mejorar la Aceptación:**

    - Fomentar la transparencia sobre el uso de datos.
    - Implementar sistemas que permitan el consentimiento informado.
    - Capacitación del personal para manejar emergencias y garantizar el correcto uso de la tecnología.

El análisis reveló que la transición hacia el reconocimiento facial basado en inteligencia artificial en aeropuertos presenta tanto oportunidades como desafíos. La mejora en la precisión y eficiencia resalta la capacidad de la IA para revolucionar los procesos de seguridad; sin embargo, las preocupaciones éticas y la necesidad de protecciones robustas para la privacidad deben ser abordadas. La implementación de buenas prácticas y la comunicación clara con los pasajeros son fundamentales para garantizar que estas tecnologías se utilicen de manera ética y que cuenten con la aceptación pública necesaria. La participación de los usuarios en la retroalimentación y el diseño de los sistemas puede también contribuir a mejorar tanto la efectividad como la confianza en estas tecnologías.

5.2. Análisis de los resultados de la encuesta aplicada al personal de seguridad del aeropuerto

La encuesta sobre el uso de inteligencia artificial en la seguridad ciudadana en aeropuertos revela un panorama mixto en cuanto al nivel de conocimiento de los encuestados. Un 46.1% se considera con un conocimiento medio sobre IA, lo cual indica que la mayoría tiene una comprensión básica pero limitada. Un 30.4% señala tener un conocimiento bajo, lo que destaca la necesidad de mayor capacitación en esta área. En el ámbito de los métodos tradicionales de reconocimiento facial, la tendencia es similar, donde un 56% tiene conocimientos básicos y un 20.9% se siente poco informado. Esto pone de manifiesto una brecha que podría limitar la percepción crítica y evaluación de la efectividad de estos métodos en comparación con la IA.

Respecto al impacto de la implementación de la inteligencia artificial en la seguridad aeroportuaria, un 44.5% de los encuestados considera que ha sido positivo, y un 21.5% señala que ha mejorado significativamente. Sin embargo, la opinión neutral de un 30.9% puede indicar la percepción de que los cambios no son lo suficientemente visibles en su trabajo diario, lo que sugiere que se necesita más información o experiencias directas sobre los beneficios de la tecnología. En cuanto a la efectividad de la IA en el reconocimiento facial, un 27.7% la califica como muy efectiva, mientras que un 45% la ve como efectiva a pesar de limitaciones, aunque un 14.1% expresa preocupaciones sobre su desarrollo.

JESUITAS ECUADOR

La comparación de efectividad entre los métodos tradicionales y la IA muestra que el 29.3% considera que la IA es más efectiva, mientras que un 36.6% opina que ambos son igualmente efectivos, lo que sugiere que, a pesar de la inclinación hacia la IA, aún hay defensores de los métodos tradicionales. En términos de riesgos éticos, los encuestados destacan la dependencia excesiva de la tecnología (56.5%), la vulnerabilidad ante ciberataques (51.8%) y la violación de la privacidad (34.6%) como sus principales preocupaciones, lo que refleja una toma de conciencia crítica sobre las adversidades que podrían derivarse del uso de la IA.

Al analizar los factores críticos para la implementación de IA en la seguridad aeroportuaria, la formación continua del personal se considera crucial (58.1%), junto con la protección de datos y privacidad (52.4%). Esto indica que un buen manejo de la tecnología debe ir de la mano con la capacitación y el respeto por la privacidad de las personas. Además, los encuestados identifican ventajas significativas de la IA, como una mayor rapidez en la detección de amenazas (67%) y la capacidad para analizar grandes volúmenes de datos (50.3%), lo que demuestra la apreciación por la efectividad y agilidad que la IA puede ofrecer en situaciones de seguridad.

Sin embargo, también se manifiestan desventajas, siendo la dependencia de la tecnología y la posible pérdida de habilidades humanas la preocupación predominante (67.5%), seguida de la alta susceptibilidad a fallos técnicos y ciberataques (52.9%). Esto sugiere que, si bien hay confianza en la tecnología, hay un deseo de mantener un equilibrio entre la IA y las competencias humanas. Finalmente, se resaltan medidas necesarias para un uso ético de la IA, como el desarrollo de políticas claras (59.7%) y la auditoría continua de sistemas (64.9%), lo que indica una demanda por un marco ético robusto en la implementación de la IA en el contexto de la seguridad aeroportuaria.

JESUITAS ECUADOR

CAPÍTULO VI: CONCLUSIONES Y RECOMENDACIONES

6. CONCLUSIONES Y RECOMENDACIONES

En el presente capítulo se describen las conclusiones y recomendaciones obtenidas del análisis realizado referente al impacto de la inteligencia artificial en la seguridad ciudadana en aeropuertos.

6.1. Conclusiones

- **Mejora en la seguridad**: La implementación de inteligencia artificial (IA) en el reconocimiento facial en aeropuertos ha demostrado mejorar la eficacia en la detección de amenazas, así como agilidad en los procesos de control de pasajeros. Los sistemas basados en IA superan en muchos casos a los métodos tradicionales en términos de precisión y velocidad.

- **La brecha del conocimiento**: Existe una notable brecha en el conocimiento del personal de seguridad respecto a la IA y los métodos tradicionales de reconocimiento facial. Aunque una parte significativa del personal considera que la IA es efectiva, muchos también reportan un nivel de conocimiento medio o bajo sobre su aplicación.

- **Preocupaciones éticas**: Se identificaron preocupaciones sustanciales relacionadas con la privacidad y la posible discriminación que proviene del uso de sistemas de reconocimiento facial basados en IA. La dependencia excesiva de la tecnología y la vulnerabilidad a ciberataques son cuestiones que requieren atención y regulación rigurosa.

- **Percepción mixta de la tecnología**: Aunque muchos encuestados ven la IA como un avance positivo, existe un segmento blanco que se muestra escéptico. Este es un indicador de que todavía hay trabajo por hacer para consolidar la confianza del público en la tecnología.

- **Recomendaciones de implementación**: Los encuestados sugieren que la capacitación del personal, la transparencia y el cumplimiento de regulaciones son factores críticos para garantizar la eficacia y la aceptación de los sistemas de IA en la seguridad aeroportuaria

6.2. Recomendaciones

- **Capacitación continua**: Se recomienda elaborar programas de capacitación que permitan al personal de seguridad familiarizarse con el uso de IA en sistemas de reconocimiento facial. Esto no solo aumentaría el nivel de competencia del personal, sino que también le daría confianza a la hora de operar dichas tecnologías.

JESUITAS ECUADOR

- **Establecimiento de marcos regulatorios**: Es fundamental que las autoridades competentes desarrollen y apliquen regulaciones estrictas para el uso de IA en el reconocimiento facial, garantizando la protección de la privacidad y regulando la recopilación, almacenamiento y uso de datos personales.

- **Fomento de la transparencia**: Las organizaciones deben ser transparentes sobre cómo se utilizan los datos biométricos y el funcionamiento de sus sistemas de reconocimiento facial, además de recopilar el consentimiento informado de los usuarios.

- **Implementación de comités de ética**: Se sugiere establecer comités de ética para supervisar la implementación de IA en aeropuertos, asegurando que las decisiones relacionadas con su uso se realicen de manera ética y responsable.

- **Auditorías y monitoreo**: Es esencial implementar auditorías regulares y sistemas de monitoreo continuo de los sistemas de reconocimiento facial para garantizar su eficacia y minimizar posibles sesgos o errores.

- **Participación comunitaria**: Fomentar la participación activa de la comunidad y de las partes interesadas en la discusión sobre los sistemas de reconocimiento facial. Esto asegurará que diversas perspectivas sean consideradas y ayudará a construir confianza pública en el uso de estas tecnologías.

- **Investigación continua**: Se recomienda la realización de estudios adicionales para evaluar la efectividad de la inteligencia artificial en la seguridad aeroportuaria en diversos contextos, lo que ayudará a mejorar las prácticas y procedimientos ya establecidos.

CAPÍTULO VII: REFERENCIAS

7. REFERENCIAS BIBLIOGRÁFICAS

Vista de La utilización policial de los sistemas de reconocimiento facial automático. (s/f). Edu.pe. Recuperado el 25 de enero de 2024, de https://revistas.pucp.edu.pe/index.php/iusetveritas/article/view/22715/21843

Vista de Utilización del sistema de reconocimiento facial para preservar la seguridad ciudadana. (s/f). Ugr.es. Recuperado el 25 de enero de 2024, de https://revistaseug.ugr.es/index.php/cridi/article/view/20899/20280

Balmaceda, T., Schleider, T., & Pedace, K. (2021). Bajo observación: inteligencia artificial, reconocimiento facial y sesgos. *ArtefaCToS Revista de estudios sobre la ciencia y la tecnología*, *10*(2), 21–43. https://doi.org/10.14201/art20211022143

de Zárate Alcarazo, L. O. (s/f). *Sesgos de género en la inteligencia artificial*. Ortegaygasset.edu. Recuperado el 26 de enero de 2024, de https://ortegaygasset.edu/wp-content/uploads/2023/03/RevistadeOccidente_Marzo2023_L.Ortiz_de_Zarate.pdf

Cuenca, S. (s/f). *UNIVERSIDAD POLITÉCNICA SALESIANA*. Edu.ec. Recuperado el 25 de enero de 2024, de https://dspace.ups.edu.ec/bitstream/123456789/22341/1/UPS-CT009675.pdf

(S/f). Edu.pe. Recuperado el 26 de enero de 2024, de https://repositorio.continental.edu.pe/bitstream/20.500.12394/11570/1/IV_FIN_103_TE_Galindo_Huaringa_Samaniego_2021.pd

Sistemas, Y., & De Investicagión, L. (s/f). PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR SEDE ESMERALAS. Edu.ec. Recuperado el 26 de enero de 2024, de https://repositorio.pucese.edu.ec/bitstream/123456789/2603/1/S%c3%a1nchez%20Maila%20%20Menghy%20Ra%c3%bal.pdf

VELARDE, Ingrid y YABARRENA, Josue. Sistema de reconocimiento facial para el control de la trata de personas en Perú. Tesis (Título de Ingeniero de Sistemas). Cusco : Universidad Andina del Cusco, 2018.

(S/f). Edu.pe. Recuperado el 26 de enero de 2024, de https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/35964/meza_va.pdf?sequence=1&isAllowed=y

Almache Barreiro, J. C., & Márquez., J. A. (2023). Implicaciones éticas de la IA y su potencial impacto en el derecho internacional. Revista San Gregorio, 1(54), 209–231. https://doi.org/10.36097/rsan.v0i54.2203

ICAO. (2020). Global Aviation Security Plan. International Civil Aviation Organization.

JESUITAS ECUADOR

Zhang, Z., & Zhuang, J. (2020). "Artificial intelligence in airport operations and management: a review of research and applications." Transport Reviews, 40(4), 529-550.

Hu, M., & Luo, J. (2018). "A comprehensive study of airport security checkpoint performance objectives." Journal of Air Transport Management, 67, 92-104.

Gates, K. (2011). Our Biometric Future: Facial Recognition Technology and the Culture of Surveillance. NYU Press.

Smith, M. E. (2018). "The Role of Artificial Intelligence in Airport Security." *Journal of Transportation Security*, 11(3-4), 149-163.

European Union Agency for Cybersecurity (ENISA). (2020). *Artificial Intelligence Cybersecurity Challenges*. ENISA.

Roymo, D. (2023, marzo 29). *Tipos de inteligencia artificial: Capacidad y Funcionalidad*. GAMCO, SL. https://gamco.es/tipos-de-inteligencia-artificial-capacidad-funcionalidad/

Inteligencia artificial: usos y aplicaciones más populares. (2023, abril 21). Escala. https://escala.com/blog/inteligencia-artificial-usos-aplicaciones

¿Qué es la inteligencia artificial y cómo se usa? (s/f). Temas | Parlamento Europeo. Recuperado el 26 de mayo de 2024, de https://www.europarl.europa.eu/topics/es/article/20200827STO85804/que-es-la-inteligencia-artificial-y-como-se-usa

¿Qué es el Reconocimiento Facial y para qué sirve? (2023, enero 11). Veridas. https://veridas.com/es/reconocimiento-facial/

Seguridad aeroportuaria. (s/f). Ferrovial. Recuperado el 26 de mayo de 2024, de https://www.ferrovial.com/es/recursos/seguridad-aeroportuaria/

Tridia. (2018, septiembre 25). *Reconocimiento facial en aeropuertos*. ingenieria y eficiencia. https://ingenieriayeficiencia.com/reconocimiento-facial-en-aeropuertos/

¿Qué son las redes neuronales convolucionales? (2023, julio 5). Ibm.com. https://www.ibm.com/es-es/topics/convolutional-neural-networks

El Fascinante Mundo de las Redes Neuronales Profundas. (s/f). Victormolla.com. Recuperado el 26 de mayo de 2024, de https://www.victormolla.com/redes-neuronales-profundas

(S/f). Fastercapital.com. Recuperado el 26 de mayo de 2024, de https://fastercapital.com/es/tema/las-implicaciones-%C3%A9ticas-del-reconocimiento-facial.html

Carrasco, M. I. (2020). La utilización policial de los sistemas de reconocimiento facial automático. *La utilización policial de los sistemas de reconocimiento facial automático*. Revistas PUCP . Obtenido de http://revistas.pucp.edu.pe/index.php/iusetveritas/article/view/22715/21843

Jaramillo, C. D. (2020). UTILIZACIÓN DEL SISTEMA DE RECONOCIMIENTO FACIAL PARA PRESERVAR LA SEGURIDAD CIUDADANA. doi:ISSN 2340-6046

Ortiz, L. (2021). Sesgos de género en la inteligencia artificial. Obtenido de https://ortegaygasset.edu/wp-content/uploads/2023/03/RevistadeOccidente_Marzo2023_L.Ortiz_de_Zarate.pdf

Tomás Balmaceda, Tobías Schleider, & Karina Pedace. (2021). Bajo observación: inteligencia artificial, reconocimiento facial y sesgos. doi:https://doi.org/10.14201/art20211022143

8. ANEXOS

8.1. Encuesta sobre el impacto de la inteligencia artificial en la seguridad ciudadana en aeropuertos

ENCUESTA SOBRE EL IMPACTO DE LA INTELIGENCIA ARTIFICIAL EN LA SEGURIDAD CIUDADANA EN AEROPUERTOS

Estimado/a profesional de seguridad:

Agradecemos tu participación en esta encuesta diseñada para comprender el uso y el impacto de la inteligencia artificial en el reconocimiento facial de personas sospechosas o buscadas por la justicia en aeropuertos. Tus respuestas son fundamentales para realizar un estudio comparativo con los métodos tradicionales de reconocimiento facial. Por favor, responde con sinceridad a las siguientes preguntas:

* Indica que la pregunta es obligatoria

Nivel de Conocimiento y Experiencia

1. 1. ¿Cuál es tu nivel de conocimiento sobre el uso de la inteligencia artificial en el reconocimiento facial en aeropuertos? *

Marca solo un óvalo.

- ◯ Muy alto, tengo experiencia práctica
- ◯ Alto, estoy bien informado/a
- ◯ Medio, tengo conocimientos básicos
- ◯ Bajo, sé muy poco al respecto
- ◯ Nulo, no tengo conocimiento

2. 2. ¿Cuál es tu nivel de conocimiento sobre los métodos tradicionales de reconocimiento facial utilizados en aeropuertos? *

Marca solo un óvalo.

- Muy alto, tengo experiencia práctica
- Alto, estoy bien informado/a
- Medio, tengo conocimientos básicos
- Bajo, sé muy poco al respecto
- Nulo, no tengo conocimiento

Evaluación del Impacto y Eficacia

3. 3. ¿Cómo evalúas el impacto de la inteligencia artificial en la precisión del reconocimiento facial en comparación con los métodos tradicionales? *

Marca solo un óvalo.

- Muy positivo, ha mejorado significativamente
- Positivo, ha mejorado
- Neutral, no ha habido cambios notables
- Negativo, ha empeorado
- Muy negativo, ha empeorado significativamente

4. 4. En tu opinión, ¿qué tan efectiva es la inteligencia artificial para el reconocimiento facial de personas sospechosas en aeropuertos? *

Marca solo un óvalo.

- Muy efectiva, puede identificar a la mayoría de los sospechosos
- Efectiva, pero con algunas limitaciones
- Poco efectiva, requiere mucho más desarrollo
- Nada efectiva, no confío en su capacidad
- No estoy seguro/a

JESUITAS ECUADOR

5. 5. ¿Cómo comparas la efectividad de los métodos tradicionales de reconocimiento facial con la inteligencia artificial en la identificación de personas sospechosas? *

Marca solo un óvalo.

- ◯ Los métodos tradicionales son más efectivos
- ◯ La inteligencia artificial es más efectiva
- ◯ Ambos son igual de efectivos
- ◯ No estoy seguro/a

Aspectos Éticos y de Seguridad

6. 6. ¿Qué riesgos éticos asocias con el uso de la inteligencia artificial en el reconocimiento facial en aeropuertos? (Selecciona todas las que apliquen) *

Selecciona todas las opciones que correspondan.

- ☐ Violación de la privacidad
- ☐ Discriminación y sesgo
- ☐ Falibilidad en la toma de decisiones críticas
- ☐ Dependencia excesiva de la tecnología
- ☐ Vulnerabilidad frente a ciberataques

7. 7. ¿Qué factores consideras críticos al implementar tecnologías de inteligencia artificial en el reconocimiento facial en aeropuertos? (Selecciona todas las que apliquen) *

Selecciona todas las opciones que correspondan.

- ☐ Protección de datos y privacidad
- ☐ Transparencia y rendición de cuentas en el uso de la tecnología
- ☐ Formación y capacitación continua del personal
- ☐ Cumplimiento de regulaciones y estándares internacionales
- ☐ Integración efectiva con otros sistemas de seguridad

Comparación de Ventajas y Desventajas

8. 8. ¿Qué ventajas específicas ofrece la inteligencia artificial en comparación con los métodos tradicionales de reconocimiento facial? (Selecciona todas las que apliquen) *

Selecciona todas las opciones que correspondan.

- [ ] Mayor rapidez en la detección de amenazas
- [ ] Reducción de errores humanos
- [ ] Mayor precisión y consistencia en la identificación de riesgos
- [ ] Capacidad para analizar grandes volúmenes de datos en tiempo real
- [ ] Mejora en la coordinación y respuesta a incidentes

9. 9. ¿Qué desventajas específicas presenta la inteligencia artificial en comparación con los métodos tradicionales de reconocimiento facial? (Selecciona todas las que apliquen) *

Selecciona todas las opciones que correspondan.

- [ ] Fallos en la toma de decisiones en situaciones críticas
- [ ] Dependencia de la tecnología y posible pérdida de habilidades humanas
- [ ] Alta susceptibilidad a fallos técnicos y ciberataques
- [ ] Costos elevados de implementación y mantenimiento
- [ ] Potencial para causar discriminación y sesgos

Medidas para un Uso Ético y Responsable

10. 10. ¿Qué medidas consideras necesarias para asegurar un uso ético y responsable de la inteligencia artificial en el reconocimiento facial en aeropuertos? (Selecciona todas las que apliquen) *

Selecciona todas las opciones que correspondan.

- [ ] Desarrollo de políticas claras y regulaciones estrictas
- [ ] Monitoreo y auditoría continua de los sistemas
- [ ] Inclusión de comités de ética y revisión
- [ ] Educación y sensibilización sobre privacidad y derechos humanos
- [ ] Participación activa de la comunidad y partes interesadas

JESUITAS ECUADOR

Agradecimiento

Agradecemos profundamente tu colaboración en esta investigación. Tu participación es clave para mejorar los métodos de seguridad en los aeropuertos y garantizar un enfoque ético y eficaz en el uso de la inteligencia artificial.

11. ⏩ (DO NOT MODIFY THIS ANSWER-for official purposes only) FORM_TIMER_UNIQUE_IDENTIFIER *

This is your unique identifier. Please do not modify this.

Google no creó ni aprobó este contenido.

Google Formularios

8.2. Entrevista sobre el impacto de la inteligencia artificial en la seguridad ciudadana en aeropuertos

ENTREVISTA SOBRE EL IMPACTO DE LA INTELIGENCIA ARTIFICIAL EN LA SEGURIDAD CIUDADANA EN AEROPUERTOS

Estimado/a participante:

Agradecemos su colaboración en esta encuesta diseñada para comprender el uso y el impacto de la inteligencia artificial en el reconocimiento facial en aeropuertos. Sus respuestas nos ayudarán a realizar un estudio comparativo con los métodos tradicionales de reconocimiento facial, en términos de precisión y ética.

1. Métodos Tradicionales de Reconocimiento Facial

1.1. ¿Cuáles son los métodos tradicionales de reconocimiento facial que se utilizan actualmente en los aeropuertos?

_____
_____
_____
_____

1.2. ¿Cuáles son las principales ventajas y limitaciones de estos métodos en términos de precisión y eficiencia?

_____
_____
_____
_____

1.3. ¿Qué tipo de tecnología y personal es necesario para operar estos sistemas tradicionales?

_____
_____
_____
_____

1.4. ¿Qué desafíos enfrentan los aeropuertos al utilizar estos métodos tradicionales?

_____
_____

1

2. Técnicas de Inteligencia Artificial en Reconocimiento Facial

2.1. ¿Qué técnicas de inteligencia artificial se están utilizando actualmente para el reconocimiento facial en los aeropuertos?

2.2. ¿Qué algoritmos o modelos de IA son los más comúnmente utilizados para el reconocimiento facial en aeropuertos?

2.3 ¿Cuáles son las principales ventajas y limitaciones de las técnicas de IA en comparación con los métodos tradicionales?

2.4 ¿Qué avances recientes se han dado en el campo del reconocimiento facial basado en IA?

3. Análisis Comparativo de Precisión

3.1. ¿Cómo se mide y compara la precisión de los métodos tradicionales versus las técnicas de IA para reconocimiento facial en aeropuertos?

_____
_____
_____
_____

3.2. ¿Cuáles son las métricas clave que se utilizan para evaluar el desempeño y la precisión de estas tecnologías?

_____
_____
_____
_____

3.3 ¿Qué desafíos técnicos se enfrentan al implementar sistemas de IA en comparación con los sistemas tradicionales?

_____
_____
_____
_____

3.4 ¿Ha habido casos específicos en los que los sistemas de IA hayan demostrado ser significativamente más efectivos que los métodos tradicionales?

_____
_____
_____
_____

4. Implicaciones Éticas del Reconocimiento Facial

4.1. ¿Cuáles son las principales preocupaciones éticas asociadas con el uso del reconocimiento facial en los aeropuertos?

_____
_____
_____
_____

4.2 ¿Cómo se manejan los problemas de privacidad y protección de datos en los sistemas de reconocimiento facial basados en IA?

_____
_____
_____
_____

4.3 ¿Qué políticas o regulaciones están en vigor para garantizar el uso ético y responsable de las tecnologías de reconocimiento facial?

_____
_____
_____
_____

4.4 ¿Qué buenas prácticas se pueden implementar para mitigar los riesgos éticos del reconocimiento facial en aeropuertos?

_____
_____
_____
_____

5. Impacto en la Seguridad y Eficiencia

5.1. ¿Cómo ha impactado la implementación de IA en la seguridad y eficiencia de los controles de seguridad en aeropuertos?

_____
_____
_____
_____

5.2. ¿Qué cambios operativos se han observado con la adopción de sistemas de IA en comparación con los métodos tradicionales?

_____
_____
_____
_____

5.3. ¿Existen estudios de caso que demuestren la efectividad de los sistemas de IA en la seguridad aeroportuaria?

_____
_____
_____
_____

6. Percepción del Usuario

6.1. ¿Cuál es la percepción de los pasajeros sobre la seguridad y la eficiencia de los sistemas de reconocimiento facial basados en IA en los aeropuertos?

_____
_____
_____
_____

6.2 ¿Qué niveles de confianza y aceptación tienen los pasajeros hacia los sistemas de reconocimiento facial basados en IA?

_____
_____
_____
_____

6.3 ¿Qué recomendaciones haría para mejorar la aceptación y efectividad de estos sistemas?

_____
_____
_____
_____

Agradecemos profundamente su colaboración en esta investigación. Su participación es clave para mejorar los métodos de seguridad en los aeropuertos y garantizar un enfoque ético y eficaz en el uso de la inteligencia artificial.