UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE INGENIERÍA Y ARQUITECTURA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

Implementación de un sistema con reconocimiento facial para generar alertas de intrusión basados en IA en un centro educativo, Lima 2024

TESIS PARA OBTENER EL TÍTULO PROFESIONAL DE:

Ingeniero de Sistemas

AUTOR:

Cordova Quispe, Roman Jesus (orcid.org/0000-0002-1085-569X)

ASESOR:

Dr. Iparraguirre Villanueva, Orlando Clemente (orcid.org/0000-0001-8185-2034)

LÍNEA DE INVESTIGACIÓN:

Sistemas de Información y Comunicaciones

LÍNEA DE RESPONSABILIDAD SOCIAL UNIVERSITARIA:

Desarrollo económico, empleo y emprendimiento.

LIMA – PERÚ

2024

UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE INGENIERÍA Y ARQUITECTURA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

Declaratoria de Autenticidad del Asesor

Yo, IPARRAGUIRRE VILLANUEVA ORLANDO CLEMENTE, docente de la FACULTAD DE INGENIERÍA Y ARQUITECTURA de la escuela profesional de INGENIERÍA DE SISTEMAS de la UNIVERSIDAD CÉSAR VALLEJO SAC - LIMA ESTE, asesor de Tesis titulada: "Implementación de un sistema con reconocimiento facial para generar alertas de intrusión basados en IA en un Centro Educativo, Lima 2024", cuyo autor es CORDOVA QUISPE ROMAN JESUS, constato que la investigación tiene un índice de similitud de 17%, verificable en el reporte de originalidad del programa Turnitin, el cual ha sido realizado sin filtros, ni exclusiones.

He revisado dicho reporte y concluyo que cada una de las coincidencias detectadas no constituyen plagio. A mi leal saber y entender la Tesis cumple con todas las normas para el uso de citas y referencias establecidas por la Universidad César Vallejo.

En tal sentido, asumo la responsabilidad que corresponda ante cualquier falsedad, ocultamiento u omisión tanto de los documentos como de información aportada, por lo cual me someto a lo dispuesto en las normas académicas vigentes de la Universidad César Vallejo.

LIMA, 06 de Julio del 2024

Apellidos y Nombres del Asesor:	**Firma**
IPARRAGUIRRE VILLANUEVA ORLANDO CLEMENTE **DNI:** 40604944 **ORCID:** 0000-0001-8185-2034	Firmado electrónicamente por: OCIPARRAGUIRREI el 30-07-2024 15:30:48

Código documento Trilce: TRI - 0798985

INVESTIGA UCV

UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE INGENIERÍA Y ARQUITECTURA
ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

Declaratoria de Originalidad del Autor

Yo, CORDOVA QUISPE ROMAN JESUS estudiante de la FACULTAD DE INGENIERÍA Y ARQUITECTURA de la escuela profesional de INGENIERÍA DE SISTEMAS de la UNIVERSIDAD CÉSAR VALLEJO SAC - LIMA ESTE, declaro bajo juramento que todos los datos e información que acompañan la Tesis titulada: "Implementación de un sistema con reconocimiento facial para generar alertas de intrusión basados en IA en un Centro Educativo, Lima 2024", es de mi autoría, por lo tanto, declaro que la Tesis:

1. No ha sido plagiada ni total, ni parcialmente.
2. He mencionado todas las fuentes empleadas, identificando correctamente toda cita textual o de paráfrasis proveniente de otras fuentes.
3. No ha sido publicada, ni presentada anteriormente para la obtención de otro grado académico o título profesional.
4. Los datos presentados en los resultados no han sido falseados, ni duplicados, ni copiados.

En tal sentido asumo la responsabilidad que corresponda ante cualquier falsedad, ocultamiento u omisión tanto de los documentos como de la información aportada, por lo cual me someto a lo dispuesto en las normas académicas vigentes de la Universidad César Vallejo.

Nombres y Apellidos	Firma
ROMAN JESUS CORDOVA QUISPE **DNI:** 46580040 **ORCID:** 0000-0002-1085-569X	Firmado electrónicamente por: RCORDOVAQ el 06-07-2024 20:49:42

Código documento Trilce: TRI - 0798986

INVESTIGA UCV

Dedicatoria

Para mi inspiración constante, mi familia y amigos, quienes me han sostenido en cada paso de este viaje académico. A mis profesores, mentores y colegas, gracias por desafiarme a crecer y por compartir su sabiduría. A mi tesis, un testimonio de perseverancia y pasión, que representa el fruto de incontables horas de trabajo y reflexión. Que estas palabras escritas no solo sean un tributo a mi esfuerzo, sino también un recordatorio de que el conocimiento es un viaje interminable. ¡Por los desafíos superados y los logros alcanzados, esta tesis es para todos nosotros!

Agradecimiento

Quiero expresar mi más profundo agradecimiento a todas las personas que han contribuido de alguna manera a la realización de este trabajo. A mi familia, por su apoyo incondicional, paciencia y amor infinito a lo largo de este viaje. A mis amigos, por las risas compartidas que han aliviado las tensiones y por ser mi refugio en los momentos difíciles. A mis profesores y asesores, por su guía experta, sus consejos sabios y su constante estímulo para alcanzar nuevas metas. A mis compañeros de estudio, por compartir ideas, debates enriquecedores y por ser una fuente inagotable de inspiración. A todas las personas que de alguna manera han contribuido, ¡gracias por ser parte de este logro que celebramos juntos!

Índice de contenidos

Índice de tablas

Resumen

El reconocimiento facial basado en IA es una herramienta para detectar rostros dentro de un área monitoreada tomando relevancia dentro de las alertas de intrusión. El objetivo de la investigación fue establecer la implementación de un sistema con reconocimiento facial para generar alertas de intrusión basados en IA, que mejore la seguridad en un Centro Educativo. Asimismo, se usó la metodología de tipo aplicada, de nivel explicativo, contando con un diseño pre experimental; en suma, la muestra fue de 30 docentes, evaluados en un pretest y postest, empleándose como instrumento dos fichas de registros previamente validados. Como resultado, se tuvo un p valor de 0,003 que indica que el sistema de reconocimiento facial basado en IA para generar alertas de intrusión si mejora la seguridad de un centro educativo. Se concluye que, la tecnología ofrece una solución efectiva para detectar intrusiones y prevenir incidentes de seguridad en el entorno escolar.

Palabras clave: Reconocimiento facial, IA, Alertas de intrusión, Educativo

Abstract

Facial recognition based on AI is a tool to detect faces within a monitored area, gaining relevance within intrusion alerts. The aim of the research was to establish the implementation of a facial recognition system to generate intrusion alerts based on AI, enhancing security in an Educational Center. Moreover, an applied methodology, of explanatory level, with a pre-experimental design was used; in summary, the sample consisted of 30 teachers, evaluated in a pretest and posttest, using two previously validated registration forms as instruments. As a result, a p-value of 0.003 was obtained, indicating that the facial recognition system based on AI for generating intrusion alerts does improve the security of an educational center. It is concluded that the technology offers an effective solution for detecting intrusions and preventing security incidents in the school environment.

Keywords: Facial recognition, AI, Intrusion alerts, Educational

I. INTRODUCCIÓN

Las instituciones educativas a menudo carecen de protocolos internos y tecnologías de seguridad para supervisar la entrada y salida de los estudiantes, lo que las hace vulnerables, han surgido situaciones donde los alumnos son víctimas de intimidación, robo o acoso tanto dentro como fuera de las instalaciones educativas (Martinez et al., 2023). El avance del reconocimiento facial, aunque aplicado en diversos campos como la educación, enfrenta desafíos técnicos, legales, éticos y económicos (Tovar et al., 2020). Asimismo, mediante algoritmos de inteligencia artificial, se puede detectar intrusiones no autorizadas y generar alertas para el personal de seguridad (Rekha et al., 2020). Esta investigación contribuiría al ODS 4 al mejorar la seguridad en los centros educativos, lo que a su vez crea un entorno más propicio para el aprendizaje. Al proteger a los estudiantes, profesores y personal administrativo de posibles amenazas, se promueve un ambiente educativo seguro y favorable.

A nivel internacional, el reconocimiento facial se ha extendido internacionalmente en sistemas de vigilancia públicos y privados, en Europa como en Reino Unido es utilizado para identificar criminales (Domingo, 2021). Tanto en China y Estados Unidos se implementa en escuelas para gestionar la asistencia y mejorar la seguridad, debido a preocupaciones por la inseguridad (Rubio, 2019). Un caso extremo de falta de seguridad es Nigeria, porque el incremento de la violencia y el vandalismo en las escuelas se atribuye a la ausencia de medidas de seguridad adecuadas(Onuorah & Eziamaka, 2020).

A nivel Latinoamérica, el caso de México los eventos estudiantiles frecuentes dificultan el control de acceso al público generando inseguridad entre los estudiantes; asimismo, el aumento de establecimientos no seguros para menores de edad pone en riesgo su bienestar. Algunos centros educativos han optado por integrar tecnología, como el uso de tarjetas RFID (Acevedo et al., 2023). En Colombia se reporta un alto porcentaje de agresiones en colegios públicos, lo que revela una falta de estrategias de seguridad (Camargo, 2023). Por otro lado, el Ministerio de Educación del Ecuador reportó 200 emergencias relacionadas con robos, actos vandálicos y extorsión en

instituciones educativas en 2022, lo que ha llevado al desarrollo del plan Escuelas Seguras debido al incremento de la violencia hacia menores de edad (El Comercio Ecuador, 2023).

En el Perú, se destaca por su implementación de biometría digital en empresas, ocupando el tercer lugar a nivel regional, sin embargo, el reconocimiento facial enfrenta desafíos de conectividad y cobertura (El Peruano, 2023). En Huancayo en 2023 se registraron dos casos de intrusión de falsos escolares a instituciones educativas, debido a la deficiencia de protocolos de seguridad para el ingreso, así como deficiencia en la tecnología biométrica (Vivanco, 2023). Asimismo, el Ministerio de Educación, aunque se promueve la instalación de cámaras de vigilancia en áreas comunes, muchas escuelas aún no adoptan esta medida(Gestión, 2023).

Los centros educativos locales enfrentan riesgos como intimidación, actos violentos y robos como resultado de la presencia de personas no autorizadas y la falta de medidas de seguridad adecuadas, por ende, la falta de este sistema biométrico se genera por la falta de comprensión de la importancia de la seguridad escolar y las limitaciones presupuestarias, que podría afectar negativamente el bienestar y la reputación de la comunidad educativa. Siendo crucial implementar sistemas de reconocimiento facial con inteligencia artificial (IA) en puntos de acceso clave y promover la conciencia sobre la seguridad escolar.

Por lo tanto, se planteó el problema general de investigación ¿En qué medida la implementación de un sistema con reconocimiento facial para generar alertas de intrusión basados en IA mejora la seguridad en un Centro Educativo?; asimismo, los problemas específicos son: ¿En qué medida la implementación de un sistema con reconocimiento facial basado en IA mejora la seguridad física en un Centro Educativo?; ¿En qué medida la implementación de un sistema con reconocimiento facial basado en IA mejora la precisión de similitud en un Centro Educativo?.

Se justificó teóricamente la generación de conocimientos sobre la aplicación de un sistema de reconocimiento facial que estará baso en el funcionamiento de la IA para alertas de intrusión, con el objetivo de crear entornos seguros en instituciones

educativas y promover el desarrollo académico de los estudiantes, lo cual servirá como prototipo para investigaciones futuras. Además, se respaldó prácticamente mediante la evidencia de la creciente incidencia de intrusión y violencia en centros educativos, lo que destaca la urgencia de adoptar medidas preventivas. La justificación metodológica se basó en investigación aplicada para evaluar la efectividad del sistema, con participación activa de todas las partes interesadas y un enfoque iterativo de desarrollo y pruebas para adaptarlo a las necesidades específicas del contexto educativo en Lima.

En base a lo antes mencionado, se consideró como objetivo general: Establecer la implementación de un sistema con reconocimiento facial para generar alertas de intrusión basados en IA, que mejore la seguridad en un Centro Educativo. Asimismo, los objetivos específicos son: Establecer la implementación de un sistema con reconocimiento facial basado en IA que mejore la seguridad física en un Centro Educativo. Establecer la implementación de un sistema con reconocimiento facial basado en IA que mejore la precisión de similitud en un Centro Educativo.

Asimismo, el presente estudio posee un conjunto de antecedentes previos, contando en el ámbito internacional el estudio de Oyebode y Ukaoha (2022) desarrollaron un sistema de reconocimiento facial mejorado para escuelas en Nigeria en 2022, sin necesidad de formación de datos. La metodología fue aplicada, explicativa y pre-experimental, con una muestra de 223 personas. Los resultados mostraron que los sistemas de reconocimiento facial son cruciales para la identificación y el acceso a las instalaciones escolares, aunque es preferible en entornos donde las caras a reconocer son conocidas. Concluye que el sistema ofrece seguridad relevante para las escuelas, aunque los costos de instalación pueden ser elevados.

Kamil et al. (2023), desarrollaron un sistema de asistencia basado en reconocimiento facial y detección de mascarillas, accesible online a través de un navegador. El estudio fue aplicativo, explicativo y pre-experimental. Los resultados demostraron el éxito del sistema de reconocimiento facial, el cual puede ser utilizado por los usuarios a través de una aplicación web en cualquier navegador. En conclusión, el proyecto produjo un sistema que facilita el control de asistencia y monitoreo de

seguridad pública al detectar mascarillas para prevenir la propagación del virus.

Correa et al. (2023), implementaron un sistema de reconocimiento facial basado en IA, utilizando el algoritmo K-means para el control de acceso. Se empleó el desarrollo ágil Scrum, generando alertas en tiempo real por correo electrónico. Los resultados mostraron una detección temprana de intrusiones en instalaciones universitarias, permitiendo decisiones informadas del personal de seguridad para prevenir intrusiones no autorizadas. Se redujeron los tiempos de espera para usuarios autorizados, mejorando su satisfacción y aumentando la productividad. La conclusión fue que este sistema aumentaría la seguridad del acceso a las instalaciones universitarias mediante la detección temprana de intrusos y alertas en tiempo real.

Syed et al. (2020), elaboraron un sistema bajo IA para ayudar al propietario/administrador del establecimiento a mejorar su seguridad, se empleó el método Viola-Jones o Haar Cascade para la detección de rostros, junto con la detección de puntos de referencia faciales de 68 puntos de dlib en Python. Además, se incorporó el sensor PIR para identificar movimientos, activando la captura de fotogramas durante 10 segundos con OpenCV. Los resultados demostraron una implementación exitosa en aplicaciones del mundo real, con *datasets* precisos. Este sistema compacto y ligero puede ser implementado fácilmente en hogares o institutos. La precisión del reconocimiento puede mejorarse con hardware de vanguardia para aumentar la eficiencia y reducir el consumo de tiempo.

Echavez (2020), desarrollaron un sistema de control automático de acceso basado en biometría facial, utilizando Tecnologías de la Información y la comunicación (Tics), como estrategia para mejorar la seguridad del campus de la Universidad de Cartagena. Aplicó la metodología RUP y se desarrolló el software utilizando Python junto con las librerías OpenCV y Face-Recognition. Los resultados evidenciaron una exitosa detección y reconocimiento facial a una distancia de hasta 3 metros. Se concluyó que el sistema puede reconocer múltiples personas, incluso en movimiento y con diversos accesorios, con un tiempo de respuesta rápido.

De la misma manera se tiene como antecedentes nacionales Reyes et al. (2023) , crearon un sistema de reconocimiento facial con IA para el control de accesos.

Utilizando un dataset de 450 imágenes por individuo, se logró un acierto aproximado del 88% en la predicción por persona. Se concluyó que el sistema es eficiente y su eficacia mejora con el aumento del tamaño de los datasets por individuo.

Rojas et al. (2022) en este artículo plantearon el reconocimiento de expresiones faciales y características personales como herramienta para identificar personas en un sistema de transporte público. Se empleó IA con machine learning en Python, junto con las librerías OpenCV2 y CV2, con la aplicación del algoritmo de Viola-Jones para enviar alertas de texto SMS a la supervisión. Los resultados mostraron que el algoritmo de Viola-Jones traduce las características faciales y Jetson Nano detecta coincidencias. Se concluyó que la IA puede ser útil en varias situaciones, siendo el algoritmo mencionado adecuado para el reconocimiento facial.

López et al. (2022) en su artículo tuvieron como objetivo detectar personas con antecedentes legales mediante un sistema de monitoreo de reconocimiento facial. Se utilizó una metodología experimental con una base de datos SQL Server y los lenguajes de programación PyCharm y Python. Los resultados mostraron que el sistema puede capturar y buscar imágenes, emitiendo alertas en tiempo real al detectar señales positivas, y rastrear el movimiento de la persona identificada. Se concluyó que el desarrollo del software de reconocimiento facial mejora la comprensión de estos sistemas y su integración en temas de seguridad es esencial para mejorar la calidad de vida en diversas ciudades.

Alejo (2021) presentó un estudio cuyo objetivo fue determinar la influencia de un algoritmo de reconocimiento facial en la gestión del control de acceso de la empresa Altoque PS S.A.. Se llevó a cabo un estudio de tipo aplicado bajo la metodología XP, utilizando programación en Python con las librerías OpenCV y MySQL. Los resultados mostraron una reducción del indicador de accesos no autorizados en un 47% y una disminución significativa en el tiempo de verificación de accesos de 1.84 minutos a 0.32 minutos, lo que genero un aumento de 1.52 m. Se concluyó una capacidad de adaptación y rápida respuesta del sistema, mejorando la gestión del control de accesos no autorizados en la empresa estudiada.

Aguirre (2021) presentó un estudio con la finalidad de desarrollar un modelo de identificación de personas basado en Deep Learning y visión computacional para mejorar el control de acceso a una empresa privada. Se aplicó algoritmos de Deep Learning bajo la metodología Design-Thinking, utilizando XAMPP para configuraciones y pruebas, y MySQL para la base de datos. Se emplearon los algoritmos Haar Cascades y LBPH con OpenCV. Los resultados mostraron un reconocimiento superior al 99% y la capacidad de integración con servicios de AWS como KINESIS, E3 y LAMBDA. El prototipo logró automatizar el registro de acceso y puede escalar con la cantidad de usuarios, restringiendo el acceso al personal autorizado.

A continuación, se detallan teorías relacionadas al tema en estudio y los enfoques conceptuales orientados con las variables de la investigación:

Woodrow Bledsoe considerado como el pionero en la implementacion del reconocimiento facial, realizando trabajos en la década de 1960 con un sistema manual de clasificación de rasgos faciales utilizando una tabla RAND y un lápiz óptico. Durante los años 70, Goldstein, Lesk y Harmon elevaron la exactitud del reconocimiento facial incorporando rasgos subjetivos particulares, como la textura de los labios y la tonalidad del cabello, basados en 22 indicadores faciales calculados manualmente para la identificación automática de individuos (López et al., 2022).

Asimismo, con el objetivo de obtener representaciones de imágenes faciales de dimensiones reducidas, Sirovich y Kirby presentaron en 1988 el uso del álgebra lineal en el reconocimiento facial mediante el método *Eigenfaces*, por ende, que es viable generar un conjunto fundamental de características al analizar diversas imágenes faciales (López et al., 2022). Además, el procesamiento de múltiples imágenes y la identificación de patrones han mejorado con la técnica de análisis de componentes principales (PCA), que es una estrategia común para reducir la complejidad dimensional y busca encontrar representaciones más simples de los datos manteniendo su variabilidad (Canazas et al., 2022).

En 1991, Turk y Pentland aplicaron el método *Eigenfaces*, el cual se encargó de reducir la complejidad dimensional para identificar rostros (Canazas et al., 2022).

Además, utilizaron esta representación para evaluar la distancia entre caras y permite el reconocimiento facial al determinar la correspondencia con una base de datos registrada previamente (Monteiro, 2020).

Los algoritmos Eigenfaces (EF), Fisherface (FF) y el histograma de patrón binario local (LBPH), proporcionado por OpenCV, tienen varias ventajas a diferencia de otras técnicas de reconocimiento facial; puesto que, son fáciles de implementar y es más utilizado, posee un rendimiento estable en conjuntos de datos pequeño, se ejecuta sin problemas en una computadora, Chrome Book, Tab y dispositivo móvil con CPU promedio y requiera menos tiempo de cálculo (Ahsan et al., 2021). *Fisherfaces* representa una evolución de los *Eigenfaces* y emplea tanto el análisis de componentes principales como el discriminante para perfeccionar el reconocimiento facial. Sin embargo, su desarrollo enfrentó desafíos como el alto procesamiento necesario debido a su complejidad y las variaciones en iluminación, expresiones y posiciones en las imágenes utilizadas para probar el algoritmo. (Monteiro, 2020).

Respecto al algoritmo LBPH (*Local Binary Pattern Histogram*) se define como un método de reconocimiento facial que se basa en el patrón binario local (LBP) para identificar la textura de la imagen en el reconocimiento facial, por ende, en su entrenamiento utilizan conjuntos de datos de imágenes faciales etiquetadas, a las cuales se les aplica la operación LBP para crear una representación intermedia mejorada de la imagen original, considerando características como el radio y los píxeles adyacentes, los histogramas generados a partir de la representación intermedia se emplean en el proceso de reconocimiento facial (Daood et al., 2023).

El algoritmo de Viola-Jones, propone algoritmos para detectar objetos en imágenes, como rostros, con un bajo coste computacional para aplicaciones en tiempo real; se basa en características *Haar-Like* calculadas utilizando una imagen integral para la comparación de intensidades luminosas en regiones rectangulares (González & Velásquez, 2019). Por otro lado, el algoritmo *K-means* agrupa grandes conjuntos de datos asignando puntos a grupos basados en la cercanía a centroides iterativamente (Carvalho & Valente, 2021).

Por su parte, la variable independiente reconocimiento facial es definido como una tecnología biométrica ampliamente utilizada en seguridad ciudadana para verificar la identidad a través del rostro y prevenir delitos, siendo características faciales únicas son clave en esta identificación, aunque la precisión puede variar según el método utilizado para analizarlas (Montero, 2022).

Los sistemas de reconocimiento facial pertenecientes a la IA y visión artificial, analizan imágenes para capturar características faciales únicas, donde este procedimiento abarca la captura de una imagen, el análisis de la estructura facial para generar un patrón único, la confrontación con una base de conformado por rostros y la identificación de similitudes (Danesi, 2022). Los sistemas de reconocimiento facial automatizan procesos organizacionales al identificar a personas mediante imágenes de cámaras, facilitando su acceso (Arrieta et al., 2022).

También, es considerada como el proceso automático implica comparar dos imágenes para verificar si representan a la misma persona. El algoritmo primero normaliza las caras en las fotos, facilitando la comparación mediante la alineación y extracción de características como la posición de los ojos. Luego, genera un resultado numérico que refleja la similitud entre las caras. (Trench, 2022).

En cuanto a la dimensión de reconocimiento facial se presenta a la capacidad de procesamiento de imagen y/o vídeo basada en la recopilación de datos biométricos como imágenes faciales o datos dactiloscópicos para identificar a una persona de manera única y rápida; debido a la sensibilidad de estos datos, el proceso, desde la recolección hasta el almacenamiento, es delicado (Danesi, 2022). Cabe mencionar, que la verificación facial determina si dos imágenes pertenecen a la misma persona, mientras que la identificación facial busca entre varias imágenes para determinar quién es la persona en una imagen específica (Álvarez et al., 2022).

Por ende, posee dos elementos el tiempo de procesamiento y las identificaciones correctas, la cual se refiere al tiempo que lleva al sistema analizar y procesar una imagen o video para identificar rostros y realizar comparaciones con las bases de datos existentes; ya que, una rápida capacidad de procesamiento es

fundamental para aplicaciones en tiempo real, como la seguridad dentro de instituciones que están propensos al ingreso de personas no autorizadas (Danesi, 2022).

De la misma manera, la variable dependiente alertas de intrusión constituyen un pilar esencial para gestionar amenazas cibernéticas, activadas por la detección de eventos potencialmente peligrosos, una vez registrados, estos eventos se examinan y analizan para su seguimiento, con supervisión de gestión de eventos en ciberseguridad, esta gestión es crucial para la administración y resolución de auditorías de riesgos e impactos (Postigo, 2020).

Los sistemas de detección de intrusión (IDS) vigilan el tráfico en redes para encontrar actividades sospechosas, utilizando bases de datos de firmas para identificar patrones de ataques conocidos; lo cual permite diferenciar entre tráfico normal y potencialmente malicioso, así como entre usos legítimos y fraudulentos del sistema, cabe mencionar que incluyen la detección de patrones y la detección de anomalías en los protocolos, las cuales se orientan a buscar la seguridad física y la precisión de similitud que se puede determinar por persona autorizada (Kasar et al., 2020).

En cuanto a la dimensión de alertas de intrusión se presenta: seguridad física, la cual protege los activos tangibles de una organización contra accesos no autorizados, daños, robos o destrucciones, incluyendo maquinaria, equipos e infraestructura; asimismo, implica la protección de la integridad, sistemas, disponibilidad y confidencialidad de la información (Klonoff et al., 2022). Para actividades detectadas por el sistema de monitoreo, este podría estar configurado para enviar una alerta al personal, por ende, está diseñado también para identificar situaciones que puedan comprometer la seguridad física de las instalaciones (Vega, 2021). Asimismo, es medible mediante la cantidad de accesos no autorizados, que aseguran el uso eficiente del software y supervisan el flujo de información (Oyebode & Ukaoha, 2022).

Respecto a la dimensión precisión de similitud del sistema de inteligencia de amenazas se evalúa mediante el número de detecciones correctas y falsos positivos,

se pueden usar tasas de confianza o indicadores de certeza, ya que identificar eventos maliciosos reales es crucial para la efectividad de la inteligencia de amenazas (Chaudhary & Singh, 2024). Asimismo, para verificar si el rostro se puede identificar se extraen características faciales para verificar la identificación y se informa al propietario si hay similitud, pero puede ser desventajoso si las condiciones de captura no son uniformes, por ende, la extracción de características específicas de partes faciales puede ser más eficaz en condiciones variables (Álvarez et al., 2022).

Por ende, se planteó como hipótesis general: El sistema con reconocimiento facial para generar alertas de intrusión basados en IA, mejora la seguridad en un Centro Educativo. Además, los específicos: El sistema con reconocimiento facial basado en IA mejora la seguridad física en un Centro Educativo; El sistema con reconocimiento facial basado en IA mejora la precisión de similitud en un Centro Educativo.

II. METODOLOGÍA

2.1. Tipo, enfoque y diseño de investigación

El tipo fue aplicada, siendo distinguido por su objetivo inmediato y práctico, que busca inducir cambios o transformaciones en un campo específico de la realidad; asimismo, busca implementar cambios en las variables de estudio para mejorar el fenómeno en cuestión y luego evaluar cómo se comporta antes y después de la intervención, con el propósito de validar una hipótesis en un contexto determinado (Hadi et al., 2023). Por ende, fue aplicada, porque buscará poner en práctica una actividad para conocer los efectos de la variable sobre una población.

Por lo tanto, el enfoque fue cuantitativo, el cual se distingue por la recolección de datos en forma numérica que luego pueden ser analizados a través de métodos estadísticos inferenciales o descriptivos, lo cual posibilita la obtención de resultados que pueden ser expresados en términos cuantificables, proporcionando así una clarificación de la hipótesis que se ha planteado (Hadi et al., 2023). En base a ello, el estudio fue cuantitativo, porque detallará mediante datos cuantificables los efectos estudiados.

El diseño fue pre experimental se introduce la intervención o tratamiento en un grupo de sujetos y se comparan los resultados con otro grupo que no recibe la intervención; pueden proporcionar información preliminar sobre el efecto de una intervención, su validez interna puede ser cuestionada debido a la falta de control sobre variables potencialmente influyentes (Hadi et al., 2023). Por tanto, se determina de la siguiente forma:

$$G \quad O_1 \quad X \quad O_2$$

Siendo: G: Grupo experimental; X: Tratamiento; O_1: Medición pretest; O_2: Medición pretest.

2.2. Variables y operacionalización

Variable 1. Reconocimiento facial

Definición conceptual. Según Montero (2022) es definido como una tecnología biométrica que se puede aplicar en varios ámbitos, siendo la seguridad ciudadana el más destacable.

Definición operacional. Cuenta con una dimensión; que posee dos indicadores; fue evaluada mediante una ficha de recolección de datos.

Variable 2: Alerta de intrusión

Definición conceptual. Según Postigo (2020) constituyen un pilar esencial para gestionar amenazas cibernéticas, activadas por la detección de eventos potencialmente peligrosos.

Definición operacional. Posee dos dimensiones: Seguridad física y precisión de similitudes, cada una de ellas tiene un indicador, por ende, fue medida en base a una ficha de recolección de datos.

2.3. Población, muestra y muestreo

La población, se refiere al conjunto completo con características específicas que conforman el objeto de estudio, los cuales pueden ser individuos, unidades o elementos; asimismo, la comprensión completa de la población es fundamental para diseñar y llevar a cabo investigaciones representativas y significativas (Barbosa et al., 2020). Por ende, la población estuvo conformado por los 30 trabajadores que conforman el personal educativo de una I.E. de Lima.

La muestra, constituye un conjunto más reducido pero representativo de la población objeto de estudio; por otro lado, la muestra censal involucra a toda la población para la recopilación de datos, es decir, cada individuo o elemento es considerado en el análisis, haciendo que la muestra total sea una réplica exacta de la población en su totalidad, por ende, este tipo se utiliza cuando es viable y beneficioso para el estudio (Villanueva, 2022). Por ende, la muestra fue censal ya que contó con

la participación de los 30 trabajadores que conforman el personal educativo de una I.E. de Lima, asimismo, se usó el registro de los trabajadores en un lapso de 11 días, para verificar el proceso del reconocimiento facial.

El muestreo fue no probabilístico, dado que se eligen los elementos más fáciles o convenientes de acceder, también conocido como un muestreo por juicio, en el cual el investigador utiliza su criterio para seleccionar los elementos que percibe como representativos de la población (Pereyra, 2022). Por ello, la investigación tuvo un muestreo no probabilístico, ya que los participantes fueron elegidos por beneficio de la investigación sin requerir un cálculo muestral.

2.4. Técnicas e instrumentos de recolección de datos

La técnica fue la observación; el cual es utilizado para llevar a cabo una tarea específica o alcanzar un objetivo determinado, abarca la observación de fenómenos o el análisis detallado de documentos y registros de datos (Pereyra, 2022). Entonces, en este análisis se empleó esta técnica, que posibilitará una percepción directa del objeto de estudio con el fin de detallar y examinar situaciones vinculadas a la realidad investigada.

El instrumento será la ficha de registro, el cual es el medio de recolección de datos durante la investigación, utilizados para analizar la información requerida durante el proceso investigativo (Barbosa et al., 2020). Por lo tanto, en este estudio se construyó dos fichas de registro, las cuales sirvieron como herramientas para identificar y registrar las fuentes de información, así como para recopilar y almacenar los datos o evidencias obtenidos.

Para la primera variable se elaboró una Ficha de Registro para reconocimiento facial, el cual, contiene los datos de: Fecha, Total de identificaciones, Identificaciones correctas, Tiempo de procesamiento e Identificaciones correctas; siendo estos ítems los que permitirán arrojar el resultado del grado de reconocimiento y porcentaje de precisión. Respecto a la segunda variable, se elaboró una Ficha de Registro para alertas de intrusión, el cual fue evaluado con los ítems de Total de accesos no

autorizados, Total de accesos, Verdadero Positivo y Falso Positivo, las cuales dieron respuesta a los indicadores accesos no autorizados y precisión, para evaluar la dimensión seguridad física.

2.5. Procedimientos

Respecto a la validez, es un método utilizado en investigación para evaluar la validez de un instrumento, se basó en la consulta y valoración de profesionales con una sólida trayectoria y conocimientos especializados en el ámbito de investigación. Los expertos revisan el contenido y la estructura del instrumento, así como su adecuación para medir el fenómeno o constructo de interés (Barbosa et al., 2020). Por ende, la validez fue mediante tres jueces de expertos quienes garantizaron que el instrumento es válido y adecuado para su uso en la investigación.

2.6. Método de análisis de datos

En cuanto a las técnicas de análisis de datos en la investigación sobre la Implementación de un sistema con reconocimiento facial para generar alertas de intrusión basados en IA en un Centro Educativo en Lima para el año 2024, se dio inicio con la recopilación minuciosa de información proveniente de diversas fuentes, este proceso comprendió la recolección de datos detallados sobre el funcionamiento del sistema de reconocimiento facial, así como sobre los incidentes de intrusión previamente registrados en el centro educativo. Se utilizaron cuadros o tablas para presentar información específica sobre los resultados, mientras que los gráficos de barra, mostraron las tendencias. Además, se emplearon imágenes para ilustrar conceptos y reforzar los hechos del sistema.

Por otro lado, se empleó la estadística inferencial para evaluar las hipótesis planteadas en el estudio. En primer lugar, se realizó la prueba de normalidad, por ende, por el tamaño de la muestra se tomó los resultados de Shapiro-Wilk (inferior a 30); T de Student; sin embargo, si los datos resultan obtener una distribución no normal, asimismo, si los datos exhiben una distribución normal, se procederá con la prueba de fue usada la prueba de Wilcoxon; fue este procedimiento crucial para analizar los datos recopilados y validó las hipótesis propuestas en el centro educativo.

2.7. Aspectos éticos

Finalmente, se ha puesto especial énfasis en salvaguardar la confidencialidad, integridad y veracidad de los datos proporcionados por la institución, debido a que es fundamental resaltar que estos datos han sido empleados únicamente con propósitos educativos, en estricto cumplimiento de los principios éticos establecidos por la Universidad Cesar Vallejo y el Colegio de Ingenieros del Perú. También se obtuvo las autorizaciones pertinentes de la Institución Educativa de Lima para realizar este estudio, aplicando medidas para preservar la confidencialidad de los datos obtenidos del cuerpo docente. Además, el sistema creado contó con procedimientos de seguridad que aseguran que únicamente personas autorizadas puedan acceder a él, lo que refuerza la salvaguarda de la información.

III. RESULTADOS

En esta etapa se presentan los resultados obtenidos del estudio. Se tienen en cuenta indicadores como tiempo de procesamiento, identificaciones correctas, acceso no autorizado y precisión. Los datos se procesarán como parte de las pruebas previas y posteriores, incluido el uso del software IBM SPSS Statistics 26.

3.1 Resultados Análisis Descriptivo

3.1.1 Variable 1: Dimensión capacidad de procesamiento de imagen y/o video

Indicador: Identificaciones correctas

Al evaluar los datos del pre y pos test del indicador Tiempo de procesamiento obtenemos los siguientes datos:

Tabla 1

Estadísticos descriptivos indicador Identificaciones correctas

	N	Mínimo	Máximo	Media	Desv. Desviación
D1V1PRE	11	63,33	80,00	74,5445	5,00640
D1V1POS	11	93,33	100,00	97,2727	2,91402
N válido (por lista)	11				

Nota: Se muestra la distribución según mínimo, máximo, media y desviación. Fuente: SPSS v.26

En la tabla 1, se puede observar que Identificaciones correctas en la prueba anterior promedió porcentual de 74,54 y luego obtuvo 97, 27 lo que indica que la tasa ha mejorado por la función respecto a las identificaciones correctas. Mientras que, en la prueba preliminar el mínimo obtuvo 63, 33 y el máximo 80,00 y para la prueba final el mínimo 93,33 y el máximo 100, 00 lo que demuestra una mejora en las identificaciones correctas de imagen y video para el reconocimiento facial.

Indicador: Tiempo de procesamiento

Al evaluar los datos del pre y pos test del indicador Identificaciones correctas, obtenemos los siguientes datos:

Tabla 2

Estadísticos descriptivos indicador Tiempo de procesamiento

	N	Mínimo	Máximo	Media	Desv. Desviación
D2V1PRE	11	110,00	168,00	134,0000	21,17073
D2V1POS	11	56,00	725,00	130,7273	197,49688
N válido (por lista)	11				

Nota: Se muestra la distribución según mínimo, máximo, media y desviación. Fuente: SPSS v.26

En la tabla 2, se puede observar que el tiempo de procesamiento de reconocimiento en la prueba anterior promedió en segundos 134,00, luego obtuvo 130,72; lo que indica que la tasa ha mejorado identificando de forma correcta. Mientras que, en la prueba preliminar el mínimo obtuvo 110,00 y el máximo 168,00 y para la prueba final el mínimo 56,00 y el máximo 725, 00 lo que demuestra una mejora en el tiempo de procesamiento para el reconocimiento facial.

3.1.1 Variable 2: Dimensión seguridad física y precisión de similitud

Indicador: Acceso no autorizado

Al evaluar los datos del pre y pos test del indicador control de acceso no autorizado obtenemos los siguientes datos:

Tabla 3

Estadísticos descriptivos indicador acceso no autorizado

	N	Mínimo	Máximo	Media	Desv. Desviación
D1V2PRE	11	20,00	36,67	25,4555	5,00640
D1V2POS	11	,00	6,67	2,7273	2,91402
N válido (por lista)	11				

Nota: Se muestra la distribución según mínimo, máximo, media y desviación. Fuente: SPSS v.26

En la tabla 3, se puede apreciar que el control de acceso no autorizado antes de la prueba (pre test) promedio de forma porcentual 25.46 y luego de la prueba (post test) promedio 2.73, lo que indica que la tasa ha mejorado de forma adecuada. Mientras que, en la prueba preliminar el mínimo es 20 y el máximo es 36.67, y en la prueba final el mínimo es 0.00 y 6.67, lo que muestra una mejora en el control de acceso no autorizado para la alerta de intrusión.

Indicador: Precisión

Al evaluar los datos del pre y pos test del indicador precisión, obtenemos los siguientes datos:

Tabla 4

Estadísticos descriptivos indicador precisión

	N	Mínimo	Máximo	Media	Desv. Desviación
D2V2PRE	11	63,00	80,00	74,4545	5,14517
D2V2POS	11	93,00	100,00	97,2727	3,03615
N válido (por lista)	11				

Nota: Se muestra la distribución según mínimo, máximo, media y desviación. Fuente: SPSS v.26

En la tabla 4, se puede aprecia que el indicador precisión antes de la prueba (pre test) promedio porcentual de 74.45 y luego de la prueba (post test) promedio 97.27. lo que indica que la tasa tuvo una mejora significativa. En cambio, en la prueba preliminar el mínimo es 63 y el máximo es 80, y en la prueba final el mínimo es 93.00 y 100.00, lo que muestra una mejora en el nivel de precisión para la alerta de intrusión.

3.2 Resultado Análisis Inferencial

3.2.1 Prueba de normalidad

La prueba estándar permite analizar la distribución de los resultados en una investigación o estudio. Para muestras menores de 50 casos, se recomienda utilizar la prueba de normalidad de Shapiro-Wilk para determinar si los datos siguen una distribución normal en caso la significancia sea mayor a 0,05. Por ende, la mayoría de muestras no siguen una distribución normal, tal como se muestra en la tabla 5, por ello se decidió optar por la prueba no paramétrica de Wilcoxon para comparar dos muestras relacionadas, evaluando las diferencias en sus medianas, asegurando resultados fiables y válidos para este estudio.

Tabla 5

Prueba de normalidad

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
PRE_RECONOCIMIENTO	,243	11	,068	,786	11	,006
POST_RECONOCIMIENTO	,304	11	,005	,714	11	,001
PRE_ ALERTAS DE INT.	,182	11	,200*	,918	11	,303
POST_ALERTAS DE INT.	,282	11	,015	,785	11	,006
PRE_ Seguridad física	,222	11	,135	,882	11	,111
POST_ Seguridad física	,280	11	,016	,785	11	,006
PRE_ Precisión de similitud	,207	11	,200*	,881	11	,106
POS_ Precisión de similitud	,270	11	,024	,777	11	,005

*. Esto es un límite inferior de la significación verdadera.

a. Corrección de significación de Lilliefors

Nota. Se detalla la prueba de normalidad para las variables y las dimensiones involucradas en las hipótesis de estudio. Fuente: SPSS v.26

3.2.2 Prueba de Hipótesis

Las pruebas para determinar las hipótesis de estudio, tendrá la siguiente regla de decisión, para conocer el valor significativo que rechazará o aprobará la hipótesis de estudio:

Regla de decisión: Si sig. valor < 0,05 se rechaza el Ho

Si sig. valor > 0,05 en este caso se acepta el Ho

Por ende, para la hipótesis general se plantea:

Ha: El sistema con reconocimiento facial para generar alertas de intrusión basados en IA, mejora la seguridad en un Centro Educativo.

Ho: El sistema con reconocimiento facial para generar alertas de intrusión basados en IA, no mejora la seguridad en un Centro Educativo.

Tabla 6

Prueba de hipótesis general

		N	Rango promedio	Suma de rangos
POST_RECONOCIMIENTO - PRE_RECONOCIMIENTO	Rangos negativos	11[a]	6,00	66,00
	Rangos positivos	0[b]	,00	,00
	Empates	0[c]		
	Total	11		
POST_SEGURIDAD - PRE_SEGURIDAD	Rangos negativos	0[d]	,00	,00
	Rangos positivos	11[e]	6,00	66,00
	Empates	0[f]		
	Total	11		

Tabla 7

Prueba de hipótesis general acorde a Wilcoxon

	POST_RECONOCIMIENTO - PRE_RECONOCIMIENTO	POST_SEGURIDAD - PRE_SEGURIDAD
Z	-2,952[b]	-2,940[c]
Sig. asintótica(bilateral)	,003	,003

a. Prueba de rangos con signo de Wilcoxon
b. Se basa en rangos positivos.
c. Se basa en rangos negativos.

De la tabla 7 se puede observar que el valor de significancia es 0.003, lo cual, de acuerdo con los criterios establecidos, permite aceptar la hipótesis del estudio. Esta hipótesis sostiene que un sistema de reconocimiento facial basado en IA para generar

alertas de intrusión mejora la seguridad en un centro educativo.

Por lo tanto, se plantea para las hipótesis especificas:

Ha: El sistema con reconocimiento facial basado en IA mejora la seguridad física en un Centro Educativo.

Ho: El sistema con reconocimiento facial basado en IA no mejora la seguridad física en un Centro Educativo.

Tabla 8

Prueba de hipótesis específica 1

		N	Rango promedio	Suma de rangos
PRE Y POS TEST DE LA SEGURIDAD FISICA	Rangos negativos	0[a]	,00	,00
	Rangos positivos	11[b]	6,00	66,00
	Empates	0[c]		
	Total	11		

Tabla 9

Prueba de hipótesis específica 1 acorde a Wilcoxon

	PRE_SEGURIDAD FÍSICA POST_SEGURIDAD FÍSICA
Z	-2,943[b]
Sig. asintótica(bilateral)	,003
a. Prueba de rangos con signo de Wilcoxon	
b. Se basa en rangos negativos.	

A partir de los datos presentados en la tabla 9, se evidencia que el valor de significancia es 0.003. Conforme a los criterios establecidos, esto permite aceptar la hipótesis del estudio, la cual propone que la implementación de un sistema de reconocimiento facial basado en IA, diseñado para generar alertas de intrusión, mejora la seguridad física en un centro educativo.

Ha: El sistema con reconocimiento facial basado en IA mejora la precisión de similitud en un Centro Educativo.

Ho: El sistema con reconocimiento facial basado en IA no mejora la precisión de similitud en un Centro Educativo.

Tabla 10

Prueba de hipótesis específica 2

		N	Rango promedio	Suma de rangos
PRE Y POST PRECISIÓN DE SIMILITUD	Rangos negativos	0[a]	,00	,00
	Rangos positivos	11[b]	6,00	66,00
	Empates	0[c]		
	Total	11		

Tabla 11

Prueba de hipótesis específica 2 acorde a Wilcoxon

	PRE_ PRECISIÓN DE SIMILITUD POST_ PRECISIÓN DE SIMILITUD
Z	-2,943[b]
Sig. asintótica(bilateral)	,003
a. Prueba de rangos con signo de Wilcoxon	
b. Se basa en rangos negativos.	

Los datos presentados en la tabla 11 muestra un valor de significancia de 0.003, según los criterios establecidos, esto permite aceptar la hipótesis del estudio, la cual indica que la implementación de un sistema de reconocimiento facial basado en IA, diseñado para generar alertas de intrusión, mejora la precisión de similitud en un centro educativo.

IV. DISCUSIÓN

Respecto al objetivo general, que buscó establecer la implementación de un sistema con reconocimiento facial para generar alertas de intrusión basados en IA, que mejore la seguridad en un Centro Educativo. Acorde a la prueba de hipótesis los resultados mostraron un valor de significancia es 0.003, aceptando esta mejora. Este hallazgo coincide con lo propuesto por López et al. (2022), quienes destacaron la importancia de incorporar rasgos subjetivos específicos fáciales que destaca en la persona, para aumentar la precisión del reconocimiento facial, por ende, sugiere que el software puede reconocer aproximadamente 22 indicadores faciales calculados manualmente para la identificación automática de individuos.

Además, los resultados del estudio coinciden con la investigación de Oyebode y Ukaoha (2022), quienes también abogaron por la utilidad de los sistemas de reconocimiento facial en entornos escolares para la identificación y el control de acceso. Sin embargo, señalaron que estos sistemas son más efectivos en entornos donde las personas a reconocer son conocidas previamente. Por otro lado, se alinean con la investigación de Kamil et al. (2023), que propuso un sistema de reconocimiento facial no solo para el control de asistencia, sino también para el monitoreo de la seguridad pública mediante la detección de mascarillas para prevenir la propagación del virus, por ello resalta la versatilidad de los sistemas de reconocimiento facial y su capacidad para adaptarse a diferentes necesidades de seguridad en diversos entornos.

Por último, los resultados coinciden con el estudio de Syed et al. (2020), que destacó la importancia de utilizar conjuntos de datos precisos para mejorar la eficiencia del reconocimiento facial. En suma, con López et al. (2022) demostraron la efectividad de capturar imágenes, realizando verdaderos positivos que genera alertas en tiempo real y mantener un rastreo en el movimiento de la persona no autorizada.

Por ende, esta contrastación sugiere que la implementación de hardware de vanguardia puede aumentar la precisión del reconocimiento y reducir el tiempo requerido para el proceso, a su vez, los sistemas son más efectivos cuando las personas a reconocer son conocidas previamente; asimismo, esta limitación debe tenerse en cuenta al diseñar y aplicar soluciones de reconocimiento facial en contextos

educativos.

En relación con el primer objetivo específico, la implementación de un sistema de reconocimiento facial basado en IA para mejorar la seguridad física en un Centro Educativo ha mostrado resultados significativos. El valor de significancia de 0.003 obtenido en los análisis valida la mejora en la seguridad, y la prueba preliminar de accesos autorizados arrojó valores mínimos de 20 y máximos de 36.67. En contraste, la prueba final mostró valores mínimos de 0.00 y máximos de 6.67, lo que indica una notable mejora en el control de acceso no autorizado y la alerta de intrusión. Estos hallazgos son consistentes con el estudio de Correa et al. (2023), que también reportó una mejora significativa en el control de acceso no autorizado, reduciendo notablemente el tiempo de espera para los usuarios autorizados.

Además, la investigación de Rojas et al. (2022) refuerza estos resultados al destacar la utilidad del algoritmo de Viola-Jones y el Jetson Nano en la detección y traducción de características faciales para el reconocimiento facial, siendo estos avances tecnológicos que no solo mejoran la precisión del reconocimiento, sino aumentan la velocidad y eficiencia del sistema, permitiendo una respuesta más rápida ante posibles intrusiones, por ende, el algoritmo de Viola-Jones en particular ha sido ampliamente reconocida por su capacidad para identificar y procesar características faciales en tiempo real, lo que lo convierte en una herramienta valiosa para la seguridad en entornos educativos, los cuales pueden ser aplicados en diversos contextos.

Asimismo, los hallazgos se alinean con la investigación de Klonoff et al. (2022), que afirmó que la implementación de sistemas de reconocimiento facial basados en IA fortalece la seguridad física al proteger los activos tangibles e infraestructura y garantizar la integridad, disponibilidad y confidencialidad de la información, por ende, coincide con su perspectiva que destaca la multifuncionalidad del reconocimiento facial, no solo como una medida de seguridad, sino también como un mecanismo integral para la protección de recursos y datos en el ámbito educativo. En conjunto, estos estudios respaldan la eficacia del reconocimiento facial basado en IA en mejorar la seguridad física en entornos educativos, promoviendo una respuesta temprana ante intrusos y proporcionando alertas en tiempo real que son cruciales para la seguridad y

el bienestar de la comunidad educativa.

El análisis del segundo objetivo específico revela que la implementación del sistema de reconocimiento facial basado en IA para mejorar la precisión de similitud en un Centro Educativo ha arrojado resultados significativos. Con un valor de significancia de 0.003, según los criterios establecidos, se confirma la validez de la hipótesis del estudio, respaldando la efectividad de este sistema. Además, se observa una mejora sustancial en la precisión de similitud, evidenciada por los promedios de precisión antes y después de la prueba, que pasaron de 74.45 a 97.27, respectivamente, por ende, hubo mejoras en este aspecto.

En base a los resultados mencionados coinciden con lo propuesto por Echavez (2020), quien afirmó, la capacidad del sistema para detectar y reconocer rostros a distancia y en movimiento es porque la tecnología de reconocimiento facial ha avanzado notablemente, permitiendo la identificación precisa incluso en condiciones dinámicas, siendo capaz de programarlas para detectar rostros en movimiento es particularmente útil en un entorno educativo donde el flujo constante de estudiantes y personal puede presentar un desafío para los sistemas de seguridad tradicionales, por ende, respalda la idea de que los sistemas basados en IA pueden superar estas limitaciones y ofrecer una seguridad robusta y precisa.

Además, los hallazgos de Reyes et al. (2023) respaldan la eficacia del sistema, demostrando una alta precisión en la predicción por persona, especialmente cuando se utilizan datasets más grandes, ya que, indica que la precisión de similitud se ve notablemente mejorada con la disponibilidad de más datos, lo que permite al sistema aprender y adaptarse mejor a las variaciones faciales individuales, por ende con lo demostrado, es crucial resaltar para la implementación efectiva de sistemas de seguridad en centros educativos, donde la diversidad y el número de individuos a reconocer pueden ser significativos, por ende, esta contrastación respalda la importancia de utilizar grandes volúmenes de datos para entrenar los sistemas de IA, lo que resulta en una mejora continua de la precisión y la efectividad del reconocimiento facial.

Finalmente, los hallazgos tienen similitudes con lo mencionado por Chaudhary y Singh (2024), quienes indican que la precisión de similitud es fundamental para

evaluar la efectividad de la inteligencia de amenazas, además resalta que identificar eventos maliciosos reales es importante para cualquier sistema de seguridad, y la alta precisión de similitud permite una respuesta rápida y precisa ante amenazas potenciales, por ende, acorde a los hallazgos, el reconocimiento facial mejora la seguridad física del entorno educativo y en suma contribuye a una gestión más eficaz de las amenazas, permitiendo a las autoridades responder de manera adecuada y oportuna. Por ende, estos estudios respaldan la utilidad del reconocimiento facial basado en IA para mejorar la precisión de similitud en entornos educativos, proporcionando una solución avanzada y confiable para la seguridad y protección dentro del contexto educativo.

En consecuencia, estas comparaciones con los resultados de la investigación permiten corroborar las afirmaciones de Ahsan et al. (2021), quienes indican que existen algoritmos de fácil implementación, siendo OpenCV uno de los más utilizados, por su rendimiento estable en conjuntos de datos pequeños y su capacidad para ejecutarse sin problemas en una variedad de dispositivos, como computadoras y dispositivos móviles con CPUs de rendimiento promedio; por ende, aporta mejoras para convertirlo en una opción ideal para integrar el reconocimiento facial en entornos educativos donde la eficiencia y la accesibilidad son cruciales para mantener la seguridad.

Además, los hallazgos respaldan lo mencionado por Danesi (2022) respecto a cómo la inteligencia artificial y la visión artificial analizan imágenes para capturar características faciales únicas, lo cual este enfoque proporciona una precisión del reconocimiento facial garantizando una respuesta rápida siendo esencial para mantener la seguridad en centros educativos y otros entornos sensibles.

Para actividades detectadas por el sistema de monitoreo, este podría configurarse para enviar alertas al personal, respaldando lo propuesto por Vega (2021), donde el sistema no solo identifica rostros y verifica su identidad, sino que también es capaz de detectar situaciones que puedan comprometer la seguridad física de las instalaciones, el sistema proporciona una capa adicional de seguridad, permitiendo una respuesta inmediata ante posibles amenazas, siendo fundamental para la protección proactiva de cualquier instalación.

Finalmente, podemos afirmar de la propuesta aplicada en este estudio, sobre reconocimiento facial basada en inteligencia artificial para alertas de intrusión, destacó por su enfoque integral; siguiendo una metodología Scrum y aplicando técnicas complementarias, por ende, se complementó el uso de Fisherfaces para la reducción de tiempos y reconocimiento preciso, con OpenCV para una implementación flexible en diversos dispositivos, en suma, el método lbpcascades garantizó un entrenamiento rápido y eficiente, por ello, se sugiere que el sistema posee una cuidadosa configuración del entorno de desarrollo y la captura de imágenes de alta calidad, junto con el entrenamiento del modelo y su integración para el reconocimiento en tiempo real, aseguran alta precisión y rapidez; por ello, el sistema estuvo diseñado para enviar alertas en tiempo real ante posibles amenazas, mejorando significativamente la seguridad de las instalaciones educativas, pudiéndose replicar en este sector según las necesidades de las instituciones educativas.

V. CONCLUSIONES

1. Se concluye que el sistema con reconocimiento facial para generar alertas de intrusión basados en IA, mejora la seguridad en un Centro Educativo, respaldado con un p valor de 0,003. Por ende, la tecnología ofrece una solución efectiva para detectar intrusiones y prevenir incidentes de seguridad en el entorno escolar, lo que puede contribuir a crear un ambiente más seguro y protegido para estudiantes, profesores y personal administrativo.
2. El sistema con reconocimiento facial basado en IA mejora la seguridad física en un Centro Educativo, demostrado con un p valor de 0,003. Por lo tanto, la implementación de esta tecnología ha contribuido a fortalecer los controles de acceso y a prevenir el ingreso de personas no autorizadas a la instalación escolar.
3. El sistema con reconocimiento facial basado en IA mejora la precisión de similitud en un Centro Educativo, consolidado con un p valor de 0,003. Por lo tanto, la mejora en la precisión de similitud puede contribuir a una identificación más confiable de individuos y a una respuesta más rápida ante posibles amenazas o situaciones de riesgo.

VI. RECOMENDACIONES

1. Se recomienda a los directivos de la institución que continúen invirtiendo en tecnologías similares y que sigan actualizándolas para mantener un ambiente escolar seguro; además se sugiere la implementación de programas de capacitación para el personal encargado de utilizar y mantener esta tecnología, con el fin de maximizar su eficacia y garantizar su correcto funcionamiento en todo momento.
2. Se recomienda a los directivos de la institución que continúen utilizando y mejorando esta tecnología; asimismo, fomentar que se establezcan políticas claras y protocolos de seguridad para el uso adecuado del sistema, así como medidas para proteger la privacidad de los estudiantes y el personal.
3. Se recomienda a los directivos de la institución que aprovechen esta tecnología para fortalecer aún más la seguridad en el campus; además de complementarlas con otras medidas de seguridad existentes, como sistemas de videovigilancia y alarmas, para crear un enfoque integral de seguridad.
4. Se recomienda explorar posibles extensiones del sistema de reconocimiento facial basado en inteligencia artificial, como su aplicación en otros contextos educativos o su integración con sistemas de gestión escolar para optimizar la administración de recursos y mejorar la experiencia educativa. Estas extensiones podrían ampliar el alcance y la utilidad de la tecnología, beneficiando a un mayor número de instituciones educativas y usuarios.
5. Se recomienda identificar áreas no abordadas en el ámbito del reconocimiento facial y la seguridad en entornos educativos, como la integración de tecnologías complementarias o la evaluación de su impacto en la privacidad y la ética. Esto podría brindar una visión más completa de los desafíos y oportunidades en este campo en constante evolución.

REFERENCIAS

Acevedo, G., Gómez, A., & Perez, J. (2023). Aprovechamiento e integración de la tecnología RFID en la administración de la educación. *Revista IPSUMTEC*, *6*(5), 149–159. https://revistas.milpaalta.tecnm.mx/index.php/IPSUMTEC/article/view/234

Aguirre, J. (2021). *Desarrollo de un sistema basado en deep learning y visión computacional de reconocimiento facial para mejorar el control de acceso a una empresa privada*. https://renati.sunedu.gob.pe/handle/sunedu/3133222

Ahsan, M., Li, Y., Zhang, J., Ahad, T., & Gupta, K. (2021). Evaluating the Performance of Eigenface, Fisherface, and Local Binary Pattern Histogram-Based Facial Recognition Methods under Various Weather Conditions. *Technologies*, *9*(2), 31. https://doi.org/10.3390/technologies9020031

Alejo, P. (2021). *Algoritmo de reconocimiento facial para la gestión del control de acceso de la empresa Altoque PS S.A.* https://renati.sunedu.gob.pe/handle/sunedu/3097857

Alvarez, A., Maranon, E., & Orozco, R. (2022). Revisión de los métodos de reconocimiento facial en imágenes RGB-D adquiridas mediante un sensor Kinect. *Revista Cubana de Ciencias Informáticas*, *16*(2), 157–187. http://scielo.sld.cu/scielo.php?script=sci_abstract&pid=S2227-18992022000200157&lng=es&nrm=iso&tlng=es

Ardila, A., López, A., & Losada, S. (2022). Sistemas de vigilancia y su efecto en el derecho a la intimidad desde el discurso de la seguridadEn la actualidad, existen sistemas de vigilancia, como las herramientas de reconocimiento facial, que justifican su existencia en la noción de seguridad perso. *RLDH*, *33*(1), 33–51. https://doi.org/10.15359/rldh.33-1.2

Barbosa, M., Mar, C., & Molar, J. (2020). *Metodología de la investigación. Métodos y técnicas*. Patria Educación.

Canazas, A., Blaz, J., Martínez, P., & Mamani, X. (2022). Sistema de identificación de emociones a través de reconocimiento facial utilizando inteligencia artificial. *Innovación y Software*, *3*(2), 140–150. https://doi.org/10.48168/innosoft.s9.a74

Carvalho, D. A. de, & Valente, G. de F. S. (2021). Algoritmo K-Means para avaliação

de aceitação sensorial de iogurtes light elaborados com Xilitol e Estévia / K-Means algorithm for assessing sensory acceptance of light yogurts made with Xylitol and Stevia. *Braz. J. Develop.*, *7*(7), 74154–74163. https://doi.org/10.34117/bjdv7n7-546

Chaudhary, S., & Singh, K. (2024). Application of Transfer Learning & Independent Estimation on Transformed Facial Recognition. *International Journal of Intelligent Systems and Applications in Engineering*, *12*(3), 151–160.

Correa, S., Méndez, A., & Varón, O. (2023). *Modelo de reconocimiento facial basado en IA, Generador de alertas de intrusión*. https://repositoriocrai.ucompensar.edu.co/handle/compensar/5173

Danesi, C. (2022). *El imperio de los algoritmos: IA inclusiva, ética y al servicio de la humanidad*. Editorial Galerna.

Daood, A., Al-Saegh, A., & Mahmood, A. (2023). Handwriting Detection And Recognition Of Arabic Numbers And Characters Using Deep Learning Methods. *Journal of Engineering Science and Technology*, *18*(3), 1581–1598.

Echavez, M. (2020). *Diseño e implementación de un sistema de biometría facial para el control de acceso en la Universidad de Cartagena*. https://hdl.handle.net/11227/14852

González, H., & Velásquez, S. (2019). Facial recognition using viola_jones and binary patterns. *Control de Procesos*, *23*(92), 7. https://uctunexpo.autanabooks.com/index.php/uct/article/view/126

Hadi, M., Martel, C., Huayta, F., Rojas, C., & Arias, J. (2023). *Metodología de la investigación: Guía para el proyecto de tesis*. Instituto Universitario de Innovación Ciencia y Tecnología Inudi Perú S.A.C.

Hamandi, H. R., & Sarhan, N. J. (2020). Novel Analytical Models of Face Recognition Accuracy in Terms of Video Capturing and Encoding Parameters. *2020 IEEE International Conference on Multimedia and Expo (ICME)*, 1–6. https://doi.org/10.1109/ICME46284.2020.9102791

Infantia, H., Subhashini, G., Karthi, M., Pandi, A., Gomathi, S., & Sivapriya, J. (2023). *Security System to Analyze, Recognize and Alert in Real Time using AI-Models*. 754–760. https://doi.org/10.1109/ICEARS56392.2023.10085421

Jaramillo, C. D. (2021). Utilización del sistema de reconocimiento facial para preservar la seguridad ciudadana. *El Criminalista Digital. Papeles de Criminología*, *9*, 20–37. https://dialnet.unirioja.es/servlet/articulo?codigo=7988280

Kadhim, O., Abdulameer, M., & Al-Mayali, Y. (2024). *A Multimodal Biometric System for Iris and Face Traits Based on Hybrid Approaches and Score Level Fusion*. *97*. https://doi.org/10.1051/bioconf/20249700016

Kamil, M. H. M., Zaini, N., Mazalan, L., & Ahamad, A. H. (2023a). Online attendance system based on facial recognition with face mask detection. *Multimedia Tools and Applications*, *82*(22), 34437–34457. https://doi.org/10.1007/S11042-023-14842-Y/TABLES/6

Kasar, S., Kshirsagar, V., Bokan, S., & Rathod, N. (2020). Smart Physical Intruder Detection System for Highly Sensitive Area. *Smart Innovation, Systems and Technologies*, *165*, 221–229. https://doi.org/10.1007/978-981-15-0077-0_23

Klonoff, D. C., Shang, T., Zhang, J. Y., Cengiz, E., Mehta, C., & Kerr, D. (2022). Digital Connectivity: The Sixth Vital Sign. *Journal of Diabetes Science and Technology*, *16*(5), 1303–1308. https://doi.org/10.1177/19322968211015241

López, A. F. G., Ortega, N. R., Arango, D. A. G., & Ibarra, C. H. O. (2022). Desarrollo de un sistema de monitoreo basado en reconocimiento facial para identificar personas con antecedentes legales. *ICTI*, *9*(2), 218–225. https://doi.org/10.26495/icti.v9i2.2273

Martínez, S., Alarcón, J., Porras, J., & Sosa, A. (2023). Aplicativo Web que optimiza el control de asistencia del personal. *Revista IPSUMTEC*, *6*(4). https://revistas.milpaalta.tecnm.mx/index.php/IPSUMTEC/article/view/275

Mohammad, S. M. (2020). Facial Recognition Technology. *SSRN Electronic Journal*. https://doi.org/10.2139/SSRN.3622882

Monteiro, L. A. F. (2020). Inteligencia Artificial: A importancia do reconhecimiento facial na educacao. *RPGeo*, *7*(1), 111. https://doi.org/https://doi.org/10.36026/rpgeo.v7i1.5317

Montero, A. (2022). El reconocimiento facial como instrumento de investigación y prevención del delito. *Anu Fac Der UDC*, *26*, 64–88. https://doi.org/10.17979/afdudc.2022.26.0.9145

Mousavi, A., Sadeghi, A. H., Ghahfarokhi, A. M., Beheshtinejad, F., & Masouleh, M. M. (2023). Improving the Recognition Percentage of the Identity Check System by Applying the SVM Method on the Face Image Using Special Faces. *International Journal of Robotics and Control Systems*, *3*(2), 221–232. https://doi.org/10.31763/ijrcs.v3i2.939

Niño, O. J. A., Henríquez, A. M. R., Quintero, J. J. S., Herrera, C. J. R., & Granados, G. de J. A. (2022). *Diseño de un prototipo para el control de acceso de seguridad mediante reconocimiento facial*. https://hdl.handle.net/20.500.12442/11781

Nosrati, L., Bidgoli, A. M., & Javadi, H. H. S. (2024). Identifying People's Faces in Smart Banking Systems Using Artificial Neural Networks. *International Journal of Computational Intelligence Systems*, *17*(1). https://doi.org/10.1007/s44196-023-00383-7

Onuorah, H., & Eziamaka, C. (2020). Assessment of physical security management practices applied by principals for ensuring safety in secondary schools in anambra state. *National Journal Of Educational Leadership*, *5*(2). https://journals.ezenwaohaetorc.org/index.php/NJOEL/article/view/1399

Oyebode, K., & Ukaoha, K. (2022a). A fast and non-trainable facial recognition system for schools. *Indonesian Journal of Electrical Engineering and Computer Science*, *25*(2), 989–994. https://ijeecs.iaescore.com/index.php/IJEECS/article/view/26092

Paucar, E. (2023). *El 2022 cerró con 200 alertas de inseguridad en escuelas*. https://www.elcomercio.com/tendencias/sociedad/escuelas-inseguridad-balance-2022-extorsion.html

Pereyra, L. (2022). *Metodologia de la investigación*. Klik.

El Peruano (2023). *Cómo ha avanzado la biometría digital en la prevención de fraudes en el Perú*. https://elperuano.pe/noticia/226630-como-ha-avanzado-la-biometria-digital-en-la-prevencion-de-fraudes-en-el-peru

Rekha, G., Malik, S., Tyagi, A. K., & Nair, M. M. (2020). Intrusion Detection in Cyber Security: Role of Machine Learning and Data Mining in Cyber Security. *ASTES*, *5*(3), 72–81. https://doi.org/http://dx.doi.org/10.25046/aj050310

Reyes, J., Castañeda, C., Alva, L., & Mendoza, A. (2023). Sistema de reconocimiento

facial para el control de accesos mediante Inteligencia Artificial. *Revista Innovación y Software*, *4*(1), 24–36. https://doi.org/https://doi.org/10.48168/innosoft.s11.a78

Rojas, U., Goñi, J., & Paredes, F. (2022). Reconocimiento de expresiones faciales y características personales como herramienta para identificar personas en un sistema de transporte público. *Ing. Ind. (Lima)*, 261–277. https://doi.org/10.26439/ing.ind2022.n.5811

Rubio, I. (2019). La escuela que usa reconocimiento facial para controlar la asistencia. *El País*. https://elpais.com/tecnologia/2019/08/30/actualidad/1567157371_609647.html

Sidhom, O., Ghazouani, H., & Barhoumi, W. (2024). Three-phases hybrid feature selection for facial expression recognition. *Journal of Supercomputing*, *80*(6), 8094–8128. https://doi.org/10.1007/s11227-023-05758-3

Syed, I. (2020). Design of Intelligent Facial Recognition System using AI for Surveillance Application. *IJSRCSEIT*, *6*(3), 346–356. https://doi.org/https://doi.org/10.32628/CSEIT206383

Tovar, L., Echavez, M., & Martelo, R. (2020). Diseño e implementación de un sistema de biometría facial para el control de acceso en instituciones de educación superior. *Revista Espacios*, *41*(44). https://revistaespacios.com/a20v41n44/a20v41n44p26.pdf

Trench, S. N. P. (2022). Los sistemas de reconocimiento facial: una mirada a la luz del examen de proporcionalidad. *Revista Internacional de Derechos Humanos*, *12*(1), 55–88. https://doi.org/10.26422/RIDH.2022.1201.per

Vega, E. (2021). Seguridad de la información. In *3Ciencias*. https://books.google.com.pe/books?id=nx4uEAAAQBAJ&newbks=1&newbks_redir=0&dq=seguridad+fisica+%2B+alerta&source=gbs_navlinks_s

Villanueva, F. (2022). *Metodología de la investigación*. Klik soluciones educativas. S. A.

Vivanco, T. (2023). *Luego de intrusión de falsa escolar en colegio, identificarán a escolares con sistema biométrico y carnets EDICION*. https://diariocorreo.pe/edicion/huancayo/luego-de-intrusion-de-falsa-escolar-

en-colegio-identificaran-a-escolares-con-sistema-biometrico-y-carnets-noticia/

Wolsing, K., Kus, D., Wagner, E., Pennekamp, J., Wehrle, K., & Henze, M. (2024). One IDS Is Not Enough! Exploring Ensemble Learning for Industrial Intrusion Detection. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *14345 LNCS*, 102–122. https://doi.org/10.1007/978-3-031-51476-0_6

ANEXOS

Anexo 1. Tabla de operacionalización de variables.

Variables de estudio	Definición Conceptual	Definición Operacional	Dimensiones	Indicadores	Escala De Medición
Reconocimiento facial	Es la capacidad de procesamiento de imagen y/o vídeo, la cual implica recopilar datos biométricos como imágenes faciales o datos dactiloscópicos para identificar a una persona de manera única y rápida; debido a la sensibilidad de estos datos, el proceso, desde la recolección hasta el almacenamiento, es delicado (Danesi, 2022).	Esta variable fue medida con la ficha de registro para reconocimiento facial	La capacidad de procesamiento de imagen y/o vídeo.	Tiempo de procesamiento Identificaciones correctas	Razón
Alertas de intrusión	Las alertas de intrusión constituyen un pilar esencial para gestionar amenazas cibernéticas, activadas por la detección de eventos potencialmente peligrosos (Postigo, 2020).	Esta variable fue medida con la ficha de registro para alerta de intrusión, cabe mencionar que el instrumento fue adaptado en base a los aportes de Chávez et al. (2022)	Seguridad Física.	Accesos no autorizados. $ANA = \frac{TNA}{TA} * 100$	Razón
			Precisión de similitud	Precisión. $P = \frac{VP}{(VP + FP)}$	

Anexo 2. Matriz de consistencia

Titulo: Implementación de un sistema con reconocimiento facial para generar alertas de intrusión basados en IA en un Centro Educativo, Lima 2024.

PROBLEMA	OBJETIVOS	HIPÓTESIS	VARIABLES	METODOLOGÍA
GENERAL: ¿En qué medida la implementación de un sistema con reconocimiento facial genera alertas de intrusión basados en IA mejora la seguridad en un Centro Educativo? **ESPECÍFICOS:** ¿En qué medida la implementación de un sistema con reconocimiento facial basado en IA mejora la seguridad física en un Centro Educativo? ¿En qué medida la implementación de un sistema con reconocimiento facial basado en IA mejora la precisión de similitud en un Centro Educativo?.	**GENERAL:** Establecer la implementación de un sistema con reconocimiento facial para generar alertas de intrusión basados en IA, que mejore la seguridad en un Centro Educativo. **ESPECÍFICOS:** Establecer la implementación de un sistema con reconocimiento facial basado en IA que mejore la seguridad física en un Centro Educativo. Establecer la implementación de un sistema con reconocimiento facial basado en IA que mejore la precisión de similitud en un Centro Educativo.	**GENERAL:** El sistema con reconocimiento facial para generar alertas de intrusión basados en IA, mejora la seguridad en un Centro Educativo. **ESPECÍFICOS:** El sistema con reconocimiento facial basado en IA mejora la seguridad física en un Centro Educativo. El sistema con reconocimiento facial basado en IA mejora la precisión de similitud en un Centro Educativo.	**VARIABLE INDEPENDIENTE:** Reconocimiento facial. **Dimensiones:** - Capacidad de procesamiento de imagen. **VARIABLE DEPENDIENTE:** Alertas de intrusión **Dimensiones:** - Seguridad Física. - Precisión de similitud.	**Tipo:** Aplicada **Nivel:** Explicativa **Diseño de investigación:** -Pre experimental **Población:** 30 trabajadores que conforman el personal educativo de una I.E. de Lima. **Muestra:** 30 trabajadores que conforman el personal educativo de una I.E. de Lima. **Instrumento:** Ficha de registro

Anexo 3. Instrumentos de recolección de datos

Ficha de registro para reconocimiento facial					
Fecha	**Capacidad de procesamiento de imagen**				
	Identificaciones			Tiempo	
	Total de identificaciones (TI)	Identificaciones correctas (IC)	TOTAL % (TC/IC)* 100	Tiempo de procesamiento (TP)	TOTAL (IC/TI) * TP

Ficha de registro para alerta de intrusión						
Fecha	SEGURIDAD FISICA					
	Accesos no autorizados (TNA/TA)*100			Precisión de similitud VP / (VP+FP)		
	Total de accesos no autorizados (TNA)	Total de accesos (TA)	TOTAL	Verdadero Positivo (VP)	Falso Positivo (FP)	TOTAL

Anexo 3. Evaluación por juicio de expertos

CARTA DE PRESENTACIÓN

Señor(a)(ita): Dr.(a)/Mg.

Presente

Asunto: VALIDACIÓN DE INSTRUMENTOS A TRAVÉS DE JUICIO DE EXPERTOS

Me es muy grato comunicarme con usted para expresarle mis saludos; asimismo, hacer de su conocimiento que, siendo estudiante de la Universidad César Vallejo, de la Facultad de Ingeniería en Sistemas requiero validar los instrumentos con los cuales recogeré la información necesaria para poder desarrollar mi investigación y con la cual optaré al título profesional de Ingeniero de Sistemas.

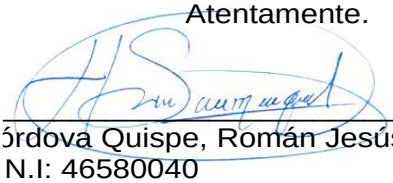
El título de mi proyecto de investigación es: “Implementación de un sistema con reconocimiento facial para generar alertas de intrusión basados en IA en un Centro Educativo, Lima 2024” y siendo imprescindible contar con la aprobación de especialistas para poder aplicar los instrumentos en mención, he considerado conveniente recurrir a usted, ante su connotada experiencia en temas de sistemas de información y comunicaciones y/o investigación tecnológica.

El expediente de validación, que le hago llegar contiene:

- Carta de presentación.
- Validación de contenido del instrumento
- Matriz de validación de instrumento
- Instrumentos
- Ficha de validación de juicio de expertos
- Matriz de consistencia

Expresándole mis sentimientos de respeto y consideración me despido de usted, no sin antes agradecerle por la atención que dispense a la presente.

Atentamente.



órdova Quispe, Román Jesús	Asesor: Dr. Iparraguirre Villanueva Orlar
N.I: 46580040	ORCID: (orcid.org/0000-0001-8185-203

VALIDACIÓN DE CONTENIDO DE FICHA DE REGISTRO SOBRE RECONOCIMIENTO FACIAL

INSTRUCCIÓN: A continuación, se le hace llegar la presente ficha de registro que permitirá recoger los datos para la investigación: **Implementación de un sistema con reconocimiento facial para generar alertas de intrusión basados en IA en un Centro Educativo, Lima 2024.** Por lo que se le solicita que tenga a bien evaluar este instrumento, haciendo, de ser caso, las sugerencias para realizar las correcciones pertinentes. Los criterios de validación de contenido son:

Criterios	Detalle	Calificación
Suficiencia	El ítem pertenece a la dimensión y basta para obtener la medición de esta	1: de acuerdo 0: en desacuerdo
Claridad	El ítem se comprende fácilmente, es decir, su sintáctica y semántica son adecuadas	1: de acuerdo 0: en desacuerdo
Coherencia	El ítem tiene relación lógica con el indicador que está midiendo	1: de acuerdo 0: en desacuerdo
Relevancia	El ítem es esencial o importante, es decir, debe ser incluido	1: de acuerdo 0: en desacuerdo

Nota. Criterios adaptados de la propuesta de Escobar y Cuervo (2008).

MATRIZ DE VALIDACIÓN DE LA FICHA DE REGISTRO DE LA VARIABLE RECONOCIMIENTO FACIAL

Definición de la variable: la capacidad de procesamiento de imagen y/o vídeo, la cual implica recopilar datos biométricos como imágenes faciales o datos dactiloscópicos para identificar a una persona de manera única y rápida; debido a la sensibilidad de estos datos, el proceso, desde la recolección hasta el almacenamiento, es delicado (Danesi, 2022). https://www.google.com.br/books/edition/El_imperio_de_los_algoritmos/Kb6UEAAAQBAJ?hl=es-419&gbpv=0

Instrumento elaborado en base a los aportes de Danesi (2022).

Dimensión	Indicador	Ítem o enunciado	Suficiencia	Claridad	Coherencia	Relevancia	Observación
Capacidad de procesamiento de imagen	Identificaciones correctas		x	x	x	x	
			x	x	x	x	
	Tiempo de procesamiento		x	x	x	x	

Ficha de registro para medir la variable Reconocimiento facial

Estimado/a participante:

Esta es una investigación llevada a cabo por estudiantes de la Universidad César Vallejo; los datos recopilados serán anónimos, serán tratados de forma confidencial y tienen finalidad netamente académica. Por tanto, en forma voluntaria; SÍ (_) NO( ) doy mi consentimiento para participar en la investigación que tiene como título **Implementación de un sistema con reconocimiento facial para generar alertas de intrusión basados en IA en un Centro Educativo, Lima 2024**. Asimismo, autorizo para que los resultados de la presente investigación se publiquen manteniendo mi anonimato.

Ficha de registro para reconocimiento facial					
Fecha	Capacidad de procesamiento de imagen				
	Identificaciones			Tiempo	
	Total de identificaciones (TI)	Identificaciones correctas (IC)	TOTAL % (TC/IC)* 100	Tiempo de procesamiento (TP)	TOTAL (IC/TI) * TP

¡Muchas gracias por su participación!

FICHA DE VALIDACIÓN DE JUICIO DE EXPERTO

Nombre del instrumento	Ficha de registro de Alertas de Intrusión
Nombres y apellidos del experto	JOSE LUIS HERRERA SALAZAR
Documento de identidad	41922075
Años de experiencia laboral	20
Máximo grado académico	DOCTOR EN ING. DE SISTEMAS
Nacionalidad	PERUANA
Institución laboral	UNTELS
Labor que desempeña	DOCENTE PRINCIPAL
Número telefónico	988827979
Correo electrónico	Jose210281@hotmail.com
Firma	
Fecha	22 /05 / 2024

VALIDACIÓN DE CONTENIDO DE FICHA DE REGISTRO SOBRE ALERTAS DE INTRUSIÓN

INSTRUCCIÓN: A continuación, se le hace llegar la presente ficha de registro que permitirá recoger los datos para la investigación: **Implementación de un sistema con reconocimiento facial para generar alertas de intrusión basados en IA en un Centro Educativo, Lima 2024.** Por lo que se le solicita que tenga a bien evaluar este instrumento, haciendo, de ser caso, las sugerencias para realizar las correcciones pertinentes. Los criterios de validación de contenido son:

Criterios	Detalle	Calificación
Suficiencia	El ítem pertenece a la dimensión y basta para obtener la medición de esta	1: de acuerdo 0: en desacuerdo
Claridad	El ítem se comprende fácilmente, es decir, su sintáctica y semántica son adecuadas	1: de acuerdo 0: en desacuerdo
Coherencia	El ítem tiene relación lógica con el indicador que está midiendo	1: de acuerdo 0: en desacuerdo
Relevancia	El ítem es esencial o importante, es decir, debe ser incluido	1: de acuerdo 0: en desacuerdo

Nota. Criterios adaptados de la propuesta de Escobar y Cuervo (2008).

MATRIZ DE VALIDACIÓN DE LA FICHA DE REGISTRO DE LA VARIABLE ALERTAS DE INTRUSIÓN

Definición de la variable: Las alertas de intrusión son un pilar esencial para gestionar amenazas cibernéticas activadas para la detección de eventos potencialmente peligrosos, que una vez registradas las alertas se examinan y analizan para su seguimiento con supervisión de gestión de eventos en la seguridad (Postigo, 2020).
https://www.google.com.pe/books/edition/Seguridad_inform%C3%A1tica_Edici%C3%B3n_2020/UCjnDwAAQBAJ?hl=es&gbpv=0

Instrumento adaptado en base a los aportes de Chávez, Nicolas y Valentín, Armando (2022), instrumento ficha de registro de control de acceso no autorizado y de precisión de acceso. https://hdl.handle.net/20.500.12692/111492

Dimensión	Indicador	Ítem o enunciado	Suficiencia	Claridad	Coherencia	Relevancia	Observación
Seguridad Física	. Accesos no autorizados.	$ANA = \frac{TNA}{TA} * 100$	x	x	x	x	
Precisión de similitud	Precisión.	$P = \frac{VP}{(VP + FP)}$	x	x	x	x	

Ficha de registro para medir la variable Alertas de intrusión

Estimado/a participante:

Esta es una investigación llevada a cabo por estudiantes de la Universidad César Vallejo; los datos recopilados serán anónimos, serán tratados de forma confidencial y tienen finalidad netamente académica. Por tanto, en forma voluntaria; SÍ ( ) NO( ) doy mi consentimiento para participar en la investigación que tiene como título **Implementación de un sistema con reconocimiento facial para generar alertas de intrusión basados en IA en un Centro Educativo, Lima 2024**. Asimismo, autorizo para que los resultados de la presente investigación se publiquen manteniendo mi anonimato.

Ficha de registro para alerta de intrusión						
Fecha	SEGURIDAD FISICA					
	Accesos no autorizados (TNA/TA)*100			Precisión de similitud VP / (VP+FP)		
	Total de accesos no autorizados (TNA)	Total de accesos (TA)	TOTAL	Verdadero Positivo (VP)	Falso Positivo (FP)	TOTAL

¡Muchas gracias por su participación!

FICHA DE VALIDACIÓN DE JUICIO DE EXPERTO

Nombre del instrumento	Ficha de registro de Alertas de Intrusión
Nombres y apellidos del experto	JOSE LUIS HERRERA SALAZAR
Documento de identidad	41922075
Años de experiencia laboral	20
Máximo grado académico	DOCTOR EN ING. DE SISTEMAS
Nacionalidad	PERUANA
Institución laboral	UNTELS
Labor que desempeña	DOCENTE PRINCIPAL
Número telefónico	988827979
Correo electrónico	Jose210281@hotmail.com
Firma	
Fecha	22 /05 / 2024

CARTA DE PRESENTACIÓN

Señor(a)(ita): Dr.(a)/Mg.

Presente

Asunto: VALIDACIÓN DE INSTRUMENTOS A TRAVÉS DE JUICIO DE EXPERTOS

Me es muy grato comunicarme con usted para expresarle mis saludos; asimismo, hacer de su conocimiento que, siendo estudiante de la Universidad César Vallejo, de la Facultad de Ingeniería en Sistemas requiero validar los instrumentos con los cuales recogeré la información necesaria para poder desarrollar mi investigación y con la cual optaré al título profesional de Ingeniero de Sistemas.

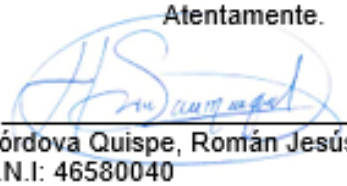
El título de mi proyecto de investigación es: "Implementación de un sistema con reconocimiento facial para generar alertas de intrusión basados en IA en un Centro Educativo, Lima 2024" y siendo imprescindible contar con la aprobación de especialistas para poder aplicar los instrumentos en mención, he considerado conveniente recurrir a usted, ante su connotada experiencia en temas de sistemas de información y comunicaciones y/o investigación tecnológica.

El expediente de validación, que le hago llegar contiene:

- Carta de presentación.
- Validación de contenido del instrumento
- Matriz de validación de instrumento
- Instrumentos
- Ficha de validación de juicio de expertos
- Matriz de consistencia

Expresándole mis sentimientos de respeto y consideración me despido de usted, no sin antes agradecerle por la atención que dispense a la presente.

Atentamente.



Córdova Quispe, Román Jesús	Asesor: Dr. Iparraguirre Villanueva Orlando
D.N.I: 46580040	ORCID: (orcid.org/0000-0001-8185-2034)

VALIDACIÓN DE CONTENIDO DE FICHA DE REGISTRO SOBRE RECONOCIMIENTO FACIAL

INSTRUCCIÓN: A continuación, se le hace llegar la presente ficha de registro que permitirá recoger los datos para la investigación: **Implementación de un sistema con reconocimiento facial para generar alertas de intrusión basados en IA en un Centro Educativo, Lima 2024.** Por lo que se le solicita que tenga a bien evaluar este instrumento, haciendo, de ser caso, las sugerencias para realizar las correcciones pertinentes. Los criterios de validación de contenido son:

Criterios	Detalle	Calificación
Suficiencia	El ítem pertenece a la dimensión y basta para obtener la medición de esta	1: de acuerdo 0: en desacuerdo
Claridad	El ítem se comprende fácilmente, es decir, su sintáctica y semántica son adecuadas	1: de acuerdo 0: en desacuerdo
Coherencia	El ítem tiene relación lógica con el indicador que está midiendo	1: de acuerdo 0: en desacuerdo
Relevancia	El ítem es esencial o importante, es decir, debe ser incluido	1: de acuerdo 0: en desacuerdo

Nota. Criterios adaptados de la propuesta de Escobar y Cuervo (2008).

MATRIZ DE VALIDACIÓN DE LA FICHA DE REGISTRO DE LA VARIABLE RECONOCIMIENTO FACIAL

Definición de la variable: la capacidad de procesamiento de imagen y/o vídeo, la cual implica recopilar datos biométricos como imágenes faciales o datos dactiloscópicos para identificar a una persona de manera única y rápida; debido a la sensibilidad de estos datos, el proceso, desde la recolección hasta el almacenamiento, es delicado (Danesi, 2022). https://www.google.com.br/books/edition/El_imperio_de_los_algoritmos/Kb6UEAAAQBAJ?hl=es-419&gbpv=0

Instrumento elaborado en base a los aportes de Danesi (2022).

Dimensión	Indicador	Ítem o enunciado	Suficiencia	Claridad	Coherencia	Relevancia	Observación
Capacidad de procesamiento de imagen	Identificaciones correctas		x	x	x	x	
			x	x	x	x	
	Tiempo de procesamiento		x	x	x	x	

Ficha de registro para medir la variable Reconocimiento facial

Estimado/a participante:

Esta es una investigación llevada a cabo por estudiantes de la Universidad César Vallejo; los datos recopilados serán anónimos, serán tratados de forma confidencial y tienen finalidad netamente académica. Por tanto, en forma voluntaria; SÍ (_) NO( ) doy mi consentimiento para participar en la investigación que tiene como título **Implementación de un sistema con reconocimiento facial para generar alertas de intrusión basados en IA en un Centro Educativo, Lima 2024**. Asimismo, autorizo para que los resultados de la presente investigación se publiquen manteniendo mi anonimato.

Ficha de registro para reconocimiento facial					
Fecha	Capacidad de procesamiento de imagen				
	Identificaciones			Tiempo	
	Total de identificaciones (TI)	Identificaciones correctas (IC)	TOTAL % (TC/IC)* 100	Tiempo de procesamiento (TP)	TOTAL (IC/TI) * TP

¡Muchas gracias por su participación!

FICHA DE VALIDACIÓN DE JUICIO DE EXPERTO

Nombre del instrumento	Ficha de registro de Alertas de Intrusión
Nombres y apellidos del experto	JOSE LUIS HERRERA SALAZAR
Documento de identidad	41922075
Años de experiencia laboral	20
Máximo grado académico	DOCTOR EN ING. DE SISTEMAS
Nacionalidad	PERUANA
Institución laboral	UNTELS
Labor que desempeña	DOCENTE PRINCIPAL
Número telefónico	988827979
Correo electrónico	Jose210281@hotmail.com
Firma	
Fecha	22 /05 / 2024

VALIDACIÓN DE CONTENIDO DE FICHA DE REGISTRO SOBRE ALERTAS DE INTRUSIÓN

INSTRUCCIÓN: A continuación, se le hace llegar la presente ficha de registro que permitirá recoger los datos para la investigación: **Implementación de un sistema con reconocimiento facial para generar alertas de intrusión basados en IA en un Centro Educativo, Lima 2024.** Por lo que se le solicita que tenga a bien evaluar este instrumento, haciendo, de ser caso, las sugerencias para realizar las correcciones pertinentes. Los criterios de validación de contenido son:

Criterios	Detalle	Calificación
Suficiencia	El ítem pertenece a la dimensión y basta para obtener la medición de esta	1: de acuerdo 0: en desacuerdo
Claridad	El ítem se comprende fácilmente, es decir, su sintáctica y semántica son adecuadas	1: de acuerdo 0: en desacuerdo
Coherencia	El ítem tiene relación lógica con el indicador que está midiendo	1: de acuerdo 0: en desacuerdo
Relevancia	El ítem es esencial o importante, es decir, debe ser incluido	1: de acuerdo 0: en desacuerdo

Nota. Criterios adaptados de la propuesta de Escobar y Cuervo (2008).

MATRIZ DE VALIDACIÓN DE LA FICHA DE REGISTRO DE LA VARIABLE ALERTAS DE INTRUSIÓN

Definición de la variable: Las alertas de intrusión son un pilar esencial para gestionar amenazas cibernéticas activadas para la detección de eventos potencialmente peligrosos, que una vez registradas las alertas se examinan y analizan para su seguimiento con supervisión de gestión de eventos en la seguridad (Postigo, 2020).
https://www.google.com.pe/books/edition/Seguridad_inform%C3%A1tica_Edici%C3%B3n_2020/UCjnDwAAQBAJ?hl=es&gbpv=0

Instrumento adaptado en base a los aportes de Chávez, Nicolas y Valentín, Armando (2022), instrumento ficha de registro de control de acceso no autorizado y de precisión de acceso. https://hdl.handle.net/20.500.12692/111492

Dimensión	Indicador	Ítem o enunciado	Suficiencia	Claridad	Coherencia	Relevancia	Observación
Seguridad Física	. Accesos no autorizados.	$ANA = \frac{TNA}{TA} * 100$	x	x	x	x	
Precisión de similitud	Precisión.	$P = \frac{VP}{(VP + FP)}$	x	x	x	x	

Ficha de registro para medir la variable Alertas de intrusión

Estimado/a participante:

Esta es una investigación llevada a cabo por estudiantes de la Universidad César Vallejo; los datos recopilados serán anónimos, serán tratados de forma confidencial y tienen finalidad netamente académica. Por tanto, en forma voluntaria; SÍ (_) NO( ) doy mi consentimiento para participar en la investigación que tiene como título **Implementación de un sistema con reconocimiento facial para generar alertas de intrusión basados en IA en un Centro Educativo, Lima 2024**. Asimismo, autorizo para que los resultados de la presente investigación se publiquen manteniendo mi anonimato.

Ficha de registro para alerta de intrusión						
Fecha	SEGURIDAD FISICA					
	Accesos no autorizados (TNA/TA)*100			Precisión de similitud VP / (VP+FP)		
	Total de accesos no autorizados (TNA)	Total de accesos (TA)	TOTAL	Verdadero Positivo (VP)	Falso Positivo (FP)	TOTAL

¡Muchas gracias por su participación!

FICHA DE VALIDACIÓN DE JUICIO DE EXPERTO

Nombre del instrumento	Ficha de registro de Reconocimiento Facial
Nombres y apellidos del experto	Rogelio Gonzalo Cohello Aguirre
Documento de identidad	07634626
Años de experiencia laboral	12
Máximo grado académico	Magister
Nacionalidad	Peruano
Institución laboral	UNFV
Labor que desempeña	DOCENTE
Número telefónico	947507335
Correo electrónico	RCOHELLO@UNFV.EDU.PE
Firma	
Fecha	27/05/2024

CARTA DE PRESENTACIÓN

Señor(a)(ita): Dr.(a)/Mg. Rosalynn O. Flores Castañeda

Presente

Asunto: VALIDACIÓN DE INSTRUMENTOS A TRAVÉS DE JUICIO DE EXPERTOS

Me es muy grato comunicarme con usted para expresarle mis saludos; asimismo, hacer de su conocimiento que, siendo estudiante de la Universidad César Vallejo, de la Facultad de Ingeniería en Sistemas requiero validar los instrumentos con los cuales recogeré la información necesaria para poder desarrollar mi investigación y con la cual optaré al título profesional de Ingeniero de Sistemas.

El título de mi proyecto de investigación es: "Implementación de un sistema con reconocimiento facial para generar alertas de intrusión basados en IA en un Centro Educativo, Lima 2024" y siendo imprescindible contar con la aprobación de especialistas para poder aplicar los instrumentos en mención, he considerado conveniente recurrir a usted, ante su connotada experiencia en temas de sistemas de información y comunicaciones y/o investigación tecnológica.

El expediente de validación, que le hago llegar contiene:

- Carta de presentación.
- Validación de contenido del instrumento
- Matriz de validación de instrumento
- Instrumentos
- Ficha de validación de juicio de expertos
- Matriz de consistencia

Expresándole mis sentimientos de respeto y consideración me despido de usted, no sin antes agradecerle por la atención que dispense a la presente.

Atentamente.

Córdova Quispe, Román Jesús	Asesor: Dr. Iparraguirre Villanueva Orlando
D.N.I: 46580040	ORCID: (orcid.org/0000-0001-8185-2034)

VALIDACIÓN DE CONTENIDO DE FICHA DE REGISTRO SOBRE RECONOCIMIENTO FACIAL

INSTRUCCIÓN: A continuación, se le hace llegar la presente ficha de registro que permitirá recoger los datos para la investigación: **Implementación de un sistema con reconocimiento facial para generar alertas de intrusión basados en IA en un Centro Educativo, Lima 2024.** Por lo que se le solicita que tenga a bien evaluar este instrumento, haciendo, de ser caso, las sugerencias para realizar las correcciones pertinentes. Los criterios de validación de contenido son:

Criterios	Detalle	Calificación
Suficiencia	El ítem pertenece a la dimensión y basta para obtener la medición de esta	1: de acuerdo 0: en desacuerdo
Claridad	El ítem se comprende fácilmente, es decir, su sintáctica y semántica son adecuadas	1: de acuerdo 0: en desacuerdo
Coherencia	El ítem tiene relación lógica con el indicador que está midiendo	1: de acuerdo 0: en desacuerdo
Relevancia	El ítem es esencial o importante, es decir, debe ser incluido	1: de acuerdo 0: en desacuerdo

Nota. Criterios adaptados de la propuesta de Escobar y Cuervo (2008).

MATRIZ DE VALIDACIÓN DE LA FICHA DE REGISTRO DE LA VARIABLE RECONOCIMIENTO FACIAL

Definición de la variable: la capacidad de procesamiento de imagen y/o vídeo, la cual implica recopilar datos biométricos como imágenes faciales o datos dactiloscópicos para identificar a una persona de manera única y rápida; debido a la sensibilidad de estos datos, el proceso, desde la recolección hasta el almacenamiento, es delicado (Danesi, 2022). https://www.google.com.br/books/edition/El_imperio_de_los_algoritmos/Kb6UEAAAQBAJ?hl=es-419&gbpv=0

Instrumento elaborado en base a los aportes de Danesi (2022).

Dimensión	Indicador	Ítem o enunciado	Suficiencia	Claridad	Coherencia	Relevancia	Observación
Capacidad de procesamiento de imagen	Identificaciones correctas		x	x	x	x	
			x	x	x	x	
	Tiempo de procesamiento		x	x	x	x	

Ficha de registro para medir la variable Reconocimiento facial

Estimado/a participante:

Esta es una investigación llevada a cabo por estudiantes de la Universidad César Vallejo; los datos recopilados serán anónimos, serán tratados de forma confidencial y tienen finalidad netamente académica. Por tanto, en forma voluntaria; SÍ (_) NO( ) doy mi consentimiento para participar en la investigación que tiene como título **Implementación de un sistema con reconocimiento facial para generar alertas de intrusión basados en IA en un Centro Educativo, Lima 2024**. Asimismo, autorizo para que los resultados de la presente investigación se publiquen manteniendo mi anonimato.

Ficha de registro para reconocimiento facial					
Fecha	Capacidad de procesamiento de imagen				
	Identificaciones			Tiempo	
	Total de identificaciones (TI)	Identificaciones correctas (IC)	TOTAL % (TC/IC)* 100	Tiempo de procesamiento (TP)	TOTAL (IC/TI) * TP

¡Muchas gracias por su participación!

FICHA DE VALIDACIÓN DE JUICIO DE EXPERTO

Nombre del instrumento	Ficha de registro de Reconocimiento Facial
Nombres y apellidos del experto	Rogelio Gonzalo Cohello Aguirre
Documento de identidad	07634626
Años de experiencia laboral	12
Máximo grado académico	Magister
Nacionalidad	Peruano
Institución laboral	UNFV
Labor que desempeña	DOCENTE
Número telefónico	947507335
Correo electrónico	RCOHELLO@UNFV.EDU.PE
Firma	
Fecha	27 / 05 / 2024

VALIDACIÓN DE CONTENIDO DE FICHA DE REGISTRO SOBRE ALERTAS DE INTRUSIÓN

INSTRUCCIÓN: A continuación, se le hace llegar la presente ficha de registro que permitirá recoger los datos para la investigación: **Implementación de un sistema con reconocimiento facial para generar alertas de intrusión basados en IA en un Centro Educativo, Lima 2024.** Por lo que se le solicita que tenga a bien evaluar este instrumento, haciendo, de ser caso, las sugerencias para realizar las correcciones pertinentes. Los criterios de validación de contenido son:

Criterios	Detalle	Calificación
Suficiencia	El ítem pertenece a la dimensión y basta para obtener la medición de esta	1: de acuerdo 0: en desacuerdo
Claridad	El ítem se comprende fácilmente, es decir, su sintáctica y semántica son adecuadas	1: de acuerdo 0: en desacuerdo
Coherencia	El ítem tiene relación lógica con el indicador que está midiendo	1: de acuerdo 0: en desacuerdo
Relevancia	El ítem es esencial o importante, es decir, debe ser incluido	1: de acuerdo 0: en desacuerdo

Nota. Criterios adaptados de la propuesta de Escobar y Cuervo (2008).

MATRIZ DE VALIDACIÓN DE LA FICHA DE REGISTRO DE LA VARIABLE ALERTAS DE INTRUSIÓN

Definición de la variable: Las alertas de intrusión son un pilar esencial para gestionar amenazas cibernéticas activadas para la detección de eventos potencialmente peligrosos, que una vez registradas las alertas se examinan y analizan para su seguimiento con supervisión de gestión de eventos en la seguridad (Postigo, 2020).
https://www.google.com.pe/books/edition/Seguridad_inform%C3%A1tica_Edici%C3%B3n_2020/UCjnDwAAQBAJ?hl=es&gbpv=0

Instrumento adaptado en base a los aportes de Chávez, Nicolas y Valentín, Armando (2022), instrumento ficha de registro de control de acceso no autorizado y de precisión de acceso. https://hdl.handle.net/20.500.12692/111492

Dimensión	Indicador	Ítem o enunciado	Suficiencia	Claridad	Coherencia	Relevancia	Observación
Seguridad Física	. Accesos no autorizados.	$ANA = \frac{TNA}{TA} * 100$	x	x	x	x	
Precisión de similitud	Precisión.	$P = \frac{VP}{(VP + FP)}$	x	x	x	x	

Ficha de registro para medir la variable Alertas de intrusión

Estimado/a participante:

Esta es una investigación llevada a cabo por estudiantes de la Universidad César Vallejo; los datos recopilados serán anónimos, serán tratados de forma confidencial y tienen finalidad netamente académica. Por tanto, en forma voluntaria; SÍ ( ) NO( ) doy mi consentimiento para participar en la investigación que tiene como título **Implementación de un sistema con reconocimiento facial para generar alertas de intrusión basados en IA en un Centro Educativo, Lima 2024**. Asimismo, autorizo para que los resultados de la presente investigación se publiquen manteniendo mi anonimato.

Ficha de registro para alerta de intrusión						
Fecha	SEGURIDAD FISICA					
	Accesos no autorizados (TNA/TA)*100			Precisión de similitud VP / (VP+FP)		
	Total de accesos no autorizados (TNA)	Total de accesos (TA)	TOTAL	Verdadero Positivo (VP)	Falso Positivo (FP)	TOTAL

¡Muchas gracias por su participación!

FICHA DE VALIDACIÓN DE JUICIO DE EXPERTO

Nombre del instrumento	Ficha de registro de Reconocimiento Facial
Nombres y apellidos del experto	Rosalynn O. Flores Castañeda
Documento de identidad	40650095
Años de experiencia laboral	20
Máximo grado académico	Doctora
Nacionalidad	Peruana
Institución laboral	Universidad Cesar Vallejo
Labor que desempeña	Docente
Número telefónico	956609163
Correo electrónico	rfloresc@ucv.edu.pe
Firma	
Fecha	22 /05 / 2024