



UNIVERSIDAD CÉSAR VALLEJO

**FACULTAD DE INGENIERÍA Y ARQUITECTURA
ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS**

**Reconocimiento facial para la gestión de control de acceso de la
empresa Spirella**

**TESIS PARA OBTENER EL TÍTULO PROFESIONAL DE:
Ingeniero de Sistemas**

AUTOR:

Flores Reyes, Nehemias David (orcid.org/0000-0003-4441-3774)

ASESOR:

Mg. Alarcon Cajas, Yohan Roy (orcid.org/0000-0001-5382-3754)

LÍNEA DE INVESTIGACIÓN:

Sistema de Información y Comunicación

LÍNEA DE RESPONSABILIDAD SOCIAL UNIVERSITARIA:

Desarrollo económico, empleo y emprendimiento

LIMA – PERÚ

2022

Dedicatoria

Este trabajo de investigación se lo dedico a mi madre Gloria por apoyarme en todo momento, a mi enamorada Yovanna por su apoyo incondicional, la motivación y todo el amor que me da. Muchas gracias por estar presente en esta etapa importante de mi vida y carrera profesional, este logro es de todos nosotros.

Agradecimiento

A mis docentes Manuel Mondragón, Johnny Valverde y en especial a mi asesor por su ayuda, paciencia y dedicación. Agradecimiento también a mi familia por motivarme y darme animo durante este proceso.

Índice de contenidos

Dedicatoria	ii
Agradecimiento	iii
Índice de contenidos	iv
Índice de tablas	v
Índice de figuras	vi
RESUMEN	vii
ABSTRACT	viii
I. INTRODUCCIÓN	1
II. MARCO TEÓRICO	7
III. METODOLOGÍA	23
3.1. Tipo y diseño de investigación	24
3.2. Variables y operacionalización	25
3.3. Población, muestras y muestreo	26
3.4. Técnicas e instrumentos de recolección de datos	27
3.5. Procedimientos	29
3.6. Método de análisis de datos	30
3.7. Aspectos éticos	31
IV. RESULTADOS	32
V. DISCUSIÓN	38
VI. CONCLUSIONES	40
VII. RECOMENDACIONES	42
REFERENCIAS	44
ANEXOS	50

Índice de tablas

Tabla 1 Tabla de confiabilidad.....	28
Tabla 2 Correlación de Acceso no autorizado.....	28
Tabla 3 Correlación de Precisión.....	29
Tabla 4 Comparación estadístico descriptiva del control de acceso no autorizado.....	33
Tabla 5 Prueba de normalidad pre y post acceso no autorizado.....	34
Tabla 6 Prueba de muestra emparejada.....	35
Tabla 7 Comparación estadístico descriptivo variable precisión.....	35
Tabla 8 Prueba de normalidad de pre y post de variable precisión.....	36
Tabla 9 Prueba de hipótesis variable precisión.....	37

Índice de figuras

Figura 1 Metodología Comonkads	18
Figura 2 Media de acceso no autorizado pre-test y post-test	20
Figura 3 Media de la precisión en el pre-test y post-test.....	23
Figura 4 Diagrama de base de datos	63
Figura 5 Aquitectura del tecnologica	22
Figura 6 Arquitectura del algoritmo Viola-Jones	22
Figura 7 Arquitectura del sistema	21
Figura 8 Login de usuario	65
Figura 9 Código de entrenamiento del algoritmo	66
Figura 10 Marcar la asistencia ingreso y salida	67
Figura 11 Registrar personal	68
Figura 12 Agregar fotos	69
Figura 13 Reporte de asistencia por empleado	70
Figura 14 Reporte de asistencia por día.....	70
Figura 15 Menú principal del sistema	71
Figura 16 Login del sistema de asistencia	71
Figura 17 Panel de administración del sistema.....	72
Figura 18 Reconociendo facial para asistencia ingreso.....	72
Figura 19 Menú de reportes de asistencia	73

RESUMEN

Las tecnologías de reconocimiento facial a lo largo de los años han ido experimentando mejoras a gran escala y están siendo muy populares en los sectores de la seguridad, vigilancia pública y el comercio. Este trabajo de investigación describe el desarrollo de un sistema de asistencia automatizado en tiempo real basado en reconocimiento facial, marcara la asistencia de los empleados de la empresa Spirella.

El sistema Reconocimiento facial para la gestión de control de acceso en la empresa Spirella tiene como objetivo reducir los accesos no autorizados de las personas y la precisión así mismo reducir los tiempos en la toma de asistencia al momento de ingreso y salida. Para el despliegue de este sistema se utilizó la metodología ComonKads, en cuanto al desarrollo se utilizó Python, librerías de OpenCV, algoritmo viola-jones y una base de datos SQLite. Esta investigación es de tipo aplicada de diseño pre-experimental, se usó como muestra la cantidad de 306 registros de asistencias además la técnica para recolectar estos datos fue el fichaje usando el instrumento ficha de registro.

Como resultado se obtuvo un sistema de asistencia basado en reconocimiento facial muy robusto que tiene una alta precisión logrando reducir los accesos no autorizados en un 24 % y incrementado la precisión en un 11%, En conclusión, podemos decir que usar el algoritmo Viola-Jones es muy beneficioso ya que tiene una alta tasa de precisión y requiere pocos recursos computacionales para ser implementado.

Palabras clave: reconocimiento facial, python, control de acceso, precisión, seguridad.

ABSTRACT

Facial recognition technologies have undergone large-scale improvements over the years and are becoming very popular in the security, public surveillance and commerce sectors. This research work describes the development of a real-time automated attendance system based on facial recognition, to mark the attendance of the employees of the Spirella company.

The facial recognition system for the management of access control in the Spirella company aims to reduce unauthorized access by people and precision, as well as reduce the times in taking assistance at the time of entry and exit. For the deployment of this system, the ComonKads methodology was used, in terms of development, Python, OpenCV libraries, viola-jones algorithm and an SQLite database were used. This research is of the applied type of pre-experimental design, the number of 306 attendance records was used as a sample, in addition the technique to collect these data was the signing using the record card instrument.

As a result, a very robust facial recognition-based assistance system was obtained, which has high precision, reducing unauthorized access by 24% and increasing precision by 11%. In conclusion, we can say that using the Viola-Jones algorithm it is very beneficial since it has a high accuracy rate and requires few computational resources to be implemented.

Keywords: facial recognition, python, access control, accuracy, security.

I. INTRODUCCIÓN

El presente capítulo busca dar a entender las circunstancias que conllevan la siguiente investigación, mencionamos las circunstancias globales como nacionales, siendo la problemática presentada en líneas posteriores. Daremos a conocer los objetivos y definiremos el problema general.

Universal Security Solutions (2018), indicaron que muchas pequeñas empresas aseguran sus puertas con un simple candado al finalizar sus operaciones diarias, hasta el inicio del siguiente día hábil. Además, durante el día suelen dejar la puerta abierta sin ninguna medida de seguridad, por lo que pueden estar expuestos a diversas amenazas. Debido a tales situaciones, los ladrones pueden entrar fácilmente y llevarse equipos informáticos, máquinas y otros objetos de valor. Por lo tanto, es importante que su empresa comience a eliminar vulnerabilidades y han manifestado que esta es una medida necesaria a tomar en cuenta, incluye la instalación de controles de acceso, incorporando cerraduras magnéticas, asegurar que quienes ingresan y egresan del negocio tengan la autorización correspondiente para hacerlo.

Por consiguiente, según indico Rosas (2019), es la necesidad de un esquema de seguridad de una empresa comprende múltiples elementos integrados en pro de ofrecer la mejor protección y llevar los riesgos al mínimo, para ello se ha determinado que existe seguridad en el perímetro, dentro de las instalaciones y sectores de mayor vulnerabilidad; no obstante se debe considerar que la fortaleza de la protección de la empresa debe ser en el control de accesos, teniendo en consideración que por allí diariamente entran y salen múltiples personas, elementos, automóviles, paquetes, correspondencia. Por otra parte, una de las necesidades de los controles de acceso son ante todo protocolos previamente establecidos que articulados con dispositivos adecuados permiten el ingreso de personas a una entidad o a lugares particulares de la misma, los primeros equipos que se emplearon en Colombia fueron en las entidades bancarias a través de claves alfanuméricas, posteriormente han evolucionado a tarjetas lectoras, lectores biométricos y tarjetas de proximidad, que en la actualidad son comunes en todo tipo de entidades; es decir se ha evolucionado de lo manual a lo técnico, de ahí a lo mecánico, luego a lo electromecánico y en la actualidad los sistemas inteligentes

mediante la utilización de tecnologías de comunicación e información además de avanzados sistemas biométricos.

Sin embargo, el empleo de biométricos basados en huellas digitales, en Perú, bajo la pandemia, se vieron afectados, dado al empleo de material inadecuado, con el fin de prevenir el contagio, Kilmadi (2019) indicó, que la forma adecuada es atravesar el apagado terminal, se puede humedecer flotando circularmente con movimientos suaves y echando alcohol sobre la superficie, esto se debe realizar también sobre el sensor de huella dactilar. Es indispensable que no se esparza de manera directa el líquido. Según la recomendación sanitaria, refirió que este procedimiento de limpieza debe realizarse en cada momento que el equipo sea utilizado en caso se observa un contacto directo sobre el terminal y la huella dactilar. De igual forma, en los casos de que la identificación sea por medio de reconocimiento facial o radiofrecuencia, la desinfección debe situarse en cada ocasión.

Por su parte, Huillca (2019), en su investigación acerca de la seguridad con el fin de mejorar el control de acceso mediante un sistema de reconocimiento facial, concluyo que la mejora del control de acceso dejo que se mejore el grado de seguridad y decrecer el peligro de vulnerabilidad de la entidad en un en un 16%. Además, que hubo mejoras significativas en los tiempos de ingresos.

En la empresa Spirella, ubicada en el centro de San Juan de Lurigancho, dedicada al sector textil presenta muchos factores de riesgo, con respecto a la maquinaria; se cuenta con hiladoras profesionales que trabajan 24x7, y que son monitoreadas constantemente. La empresa cuenta con diversas áreas que manejan información confidencial como lo es el área de diseño, que cuenta no solo los modelos de todas las colecciones generadas, sino también los patrones, como todos los modelos de las futuras colecciones. Por lo que el factor seguridad, es requerido, para no vulnerar los activos de la organización.

Cabe mencionar, que uno de los problemas que cuenta la empresa, es el poder asegurar, la asistencia en su momento, ya que la transcripción manual, genera un cuello de botella en el ingreso. Llevando a que se tenga que registrar esta información en los aplicativos de la empresa, con el fin de conocer la presencia del

personal, como también sus horarios de ingreso, por lo que el tiempo de gestión en conocer dicha información es llevada en un gran tiempo.

También, como se puede ver, la aglomeración de personas, en el ingreso, conlleva ciertos riesgos, así que agilizar estos tiempos, es una forma práctica, así mismo, el poder tener la certeza de reconocer al individuo que está ingresando a la empresa de una manera más acertada. Mensualmente se identificó un promedio de acceso no autorizados del 34% y la precisión al momento de identificar a una persona es de 88%.

En adición, también existe personal que no asiste a laborar y la persona encargada de registrar manualmente la asistencia no registra la falta, esta persona recibe el pago de sus haberes sin el descuento respectivo por el día no laborado. En consecuencia, genera pérdidas económicas a la empresa.

El empleo de la tecnologías de reconocimiento facial han brindado apoyo en diferentes aspectos, como en el área de la policía, como lo menciona Villalobos (2020), en la que ha demostrado, una gran ayuda, en la identificación de personas. El sistema que se desarrolló e implemento usando inteligencia artificial y reconocimiento facial en esta empresa permitió llevar una correcta gestión de control de acceso de personal en el ingreso a las instalaciones así mismo llevar la asistencia. Además, el sistema de reconocimiento facial satisface la nueva necesidad emergente de limitar la exposición física a gérmenes y virus al ofrecer una solución de control de acceso de alta precisión sin necesidad de contacto.

En base al problema expuesto se planteó la problemática general y los problemas específicos para esta investigación. El problema general del estudio fue:

¿Cuál es el efecto de utilizar una aplicación con reconocimiento facial para gestión del control de acceso en la empresa Spirella?

Los problemas específicos para la presente investigación son los siguientes.

PE1: ¿Cuál es el efecto de utilizar una aplicación con reconocimiento facial para mejorar el control de acceso no autorizado en la gestión del control de acceso en la empresa Spirella?

PE2: ¿Cuál es el efecto de utilizar de una aplicación con reconocimiento facial para mejorar la precisión en la gestión del control de acceso de la empresa Spirella?

A través de esta investigación se plantea obtener conocimiento, el cual justificamos en base a estos puntos; teórico, práctica y metodológica. Consideramos que esta investigación puede brindar pertinencia, e impacto ya sea en un mediano o corto plazo. Especificaremos, estos tres puntos a continuación:

Desde el punto de la justificación teórica, Bernal (2010), mencionó que esta se basa en un conocimiento ya adquirido, en fin, de confrontar no solo la parte teórica, sino también validar los resultados obtenidos. Asimismo, la justificación teórica pretende generar debate académico en base al conocimiento existente y reflexión. Almonacid (2020) indicó que, bajo la pandemia, el empleo de mascarillas, disminuye el área de reconocimiento, lo que dificultó en gran medida la captura de datos. Estos errores se explican por el hecho de que la capacidad de reconocer rostros se ha reducido a la mitad. Esta situación ha llevado a las empresas desarrolladoras de software crear nuevos algoritmos que incluyen las mascarillas, reduciendo el área de reconocimiento facial. Por lo cual podemos afirmar, que a través de esta investigación brindaremos mayor información del empleo del reconocimiento facial, aplicado para la toma de asistencia en la empresa Spirella. El reconocimiento facial es una parte esencial de la biometría consta de tres pasos: procesamiento, extracción y clasificación, este permite identificar a una persona mediante el uso de tecnología y algoritmos de IA. Tiene diversas aplicaciones como la seguridad pública, gestión de la asistencia y el control de acceso

Por otro lado, otro punto es la justificación práctica, según Bernal (2010), como la práctica en búsqueda de obtener resultados a los problemas planteados, generar medios para resolverlos, que puedan aplicarse dependiendo de la situación problemática. En esta investigación para dar solución a la problemática encontrada se implementó un modelo de reconocimiento para la gestión en el control de accesos usando algoritmos de inteligencia artificial, ya que el sistema reduce los accesos no autorizados y mejora la precisión asimismo es muy seguro.

Finalmente, la justificación metodológica, definida por Bernal (2010), nos indica que la aplicación de esta investigación genera nuevos métodos o estrategias con el fin de generar nuevo conocimiento que sea efectivo y sobre todo veraz. Hemos visto a través de las investigaciones que el empleo de reconocimiento facial, mediante el empleo de nuevas tecnologías, pueden ser beneficiosas y generar nuevas estrategias. Para llevar a cabo el estudio se empleó la metodología de ComonKads empleando tecnologías de clasificación de imágenes usando librería de Python como Numpy y OpenCV.

El objetivo general que se planteo fue: Determinar el efecto de utilizar de un sistema aplicación con reconocimiento facial para la gestión del control de acceso de la empresa Spirella

Los objetivos específicos para esta investigación son las siguientes.

OE1: Determinar el efecto del uso de una aplicación con reconocimiento facial para mejorar el acceso no autorizado en la gestión del control de acceso en la empresa Spirella.

OE2: Determinar el efecto del uso de una aplicación con reconocimiento facial para mejorar la precisión en la gestión en el control de acceso de la empresa Spirella

La hipótesis general fue: El uso de una aplicación con reconocimiento facial para mejorar la gestión del control de acceso de la empresa Spirella.

Las hipótesis específicas son las siguientes:

HE1: El uso de una aplicación con reconocimiento facial para mejorar el control de acceso no autorizado en la gestión del control de acceso de la empresa Spirella.

HE2: El uso de una aplicación con reconocimiento facial mejora la precisión en la gestión del control de acceso de la empresa Spirella

II. MARCO TEÓRICO

El presente capítulo muestra un resumen de estudios relacionados al tema de investigación, se obtienen antecedentes de tipo nacional e internacional como tesis e investigaciones de revistas. Además, conceptualizamos teorías relacionadas al tema. Para obtener dicha información se llevó a cabo una búsqueda en diversas fuentes como base de datos científicas: IOPScience, ScienDirect y Scopus.

A nivel internacional:

Morales & et. al (2022), en su investigación se ha propuesto que se caracteriza el reconocimiento de las emociones faciales en poblaciones pediátricas y adolescentes. Se realizó una adaptación digital de “Test de pictures of fácil affects” para 147 contribuyentes de 9 y 18 años. El resulta mostro una asociación negativa sobre la edad y las tasas de éxito para la felicidad y positivo para el miedo y asco. De igual forma, se visualizó una significancia en las edades sobre el tiempo de reacción de todas las emociones, salvo de las del miedo. El resultado mostro que conforme se va madurando y creciendo, la capacidad de percibir emociones se vuelve más rápida, sin embargo, esto significa que la capacidad de percibir emociones mejora solo en el asco y el miedo. Se discute la importancia de estas emociones para la adolescencia.

Asi mismo, Ortiz y Camargo (2022) en su investigación plantearon el diseño de un sistema de reconocimiento de lengua de señas en el contexto colombiano. El nivel de reconocimiento se encargó de que extraiga la característica de imagen en la entrada y de la base de datos, las cuales son fundamentales en el proceso de comparación para identificar la señal correspondiente a la lengua de señas colombiana. También se encargó de tomar la imagen de las señales de lengua de colombiana entregadas por los usuarios y encontrarla, con el mejor nivel de certeza, en merito a la información recaba. Para el reconocimiento confiable y preciso, toda característica extraída de la imagen de entrada debe ser detectable incluido con cambios en la relación al ruido, iluminación o imagen. Se encontró una mejora en la respuesta del sistema, con el uso de un normalizador de mano para elementos de color, el uso de guantes tipo quirúrgico. La condición de iluminación debe ser suficiente para obtener resultados precisos.

Además, Rodríguez (2022), en su investigación de identificación de armas en imágenes de rayos x. Según los expertos, la revisión de equipaje con esta técnica tiene una eficacia limitada para identificar objetos peligrosos y otros factores. Esto está influenciado en cierta medida por las propiedades de las imágenes de rayos X, que son muy diferentes de las imágenes espectrales algoritmos visibles, lo que afecta su interpretación. Es por esto que tanto el método de adquisición como los para mejorar, procesar o reconocer los objetos en estas imágenes se caracterizan por operaciones computacionales costosas que requieren un tiempo de ejecución elevado. Reducir el tiempo de ejecución en aplicaciones seguras puede ser un objetivo de alta prioridad, en sistemas que soportan una rápida toma de decisiones, entre otros. Además, las técnicas de programación paralela han demostrado ser una alternativa viable para resolver rápidamente problemas de visión artificial. Este artículo hace una presentación del desarrollo de un componente de software escrito en C/C que describe un proceso basado en el algoritmo BoVW para la detección de pequeñas ramas. La implementación utiliza técnicas de programación paralela a través de OpenMP, lo que logra reducir el tiempo de ejecución de una implementación anterior en MATLAB hasta en un 93,36%. El método de clasificación también se probó con una nueva base de datos de imágenes de radiación del probador de energía dual.

También, Cáceres, Amaya y Ramos (2022), en el proceso de imágenes para identificar las plagas utilizando la visión artificial por computadora, dio como resultado una herramienta de diagnóstico. La fotografía es realizada por un agente robótico aéreo (dron) equipado con una cámara, que puede registrar el estado de las hojas de un área conocida como el árbol de la 'flor de azúcar'. (*Begonia semperflorens*). Estas imágenes se procesan mediante técnicas de visión artificial para determinar la probabilidad de ataques de plagas en los cultivos. Las técnicas utilizadas son filtrado morfológico, desenfoque gaussiano y filtrado HSL, respectivamente. El principal resultado de este trabajo fue el descubrimiento de pinchazos en las hojas debido al ataque de plagas, en particular babosas, caracoles, arañas rojas.

Así mismo, Villa, Valencia y Berrio (2018), en su investigación analizaron el lenguaje de señas, el cual incluye expresiones y movimientos realizados con

diversas partes del cuerpo principalmente con la mano. Actualmente en Colombia existe muy poca tecnología para aprenderla e interpretarla; es por tanto un compromiso social de que se emprenda una iniciativa promoviendo la optimización en la calidad de vida de la sociedad que padece del problema de sordera. Esta investigación busca presentar el procedimiento de implementación y diseño de un sistema de reconocimiento en el gesto no portátil utilizando el entorno Matlab como herramienta principal de desarrollo, donde se ha implementado el algoritmo SIFT. Este sistema deja que se visualicen las imágenes como el resultante y su traducción a la lengua de señas colombiana correspondiente. Por medio de la identificación de puntos centrales en la imagen, posterior a las comparaciones con el modelo de SIFT SIFT en la base de datos del sistema, se pueden obtener traducciones. Este medio lleva a cabo el reconocimiento de veinte letras inmóviles, generando una interfaz gráfica en Matlab, facilitando su visualización, volviéndose de fácil uso y acceso por el lado de los usuarios. Se verifica una mejora en las respuestas por medio del uso de un normalizador de imagen, lo que genera un % de confianza del 77% y la demanda amplia del propio. Para que se continúe con la otra parte del proyecto, se propone optimizar el sistema empleado métodos de redes neuronales en un tiempo determinado, logrando de tal manera un impacto mayor en la necesidad actual de los colombianos.

Por último, Poveda y Merchán (2015) realizaron el despliegue de un sistema de control de accesos que se basa en el reconocimiento facial. Esto busca que se verifique en tiempo real quienes ingresan a la instalación y forman parte de una base de información de empleados que trabajan allí. La condición de función sobre los sistemas no son cooperativas. Es decir, el usuario no se posicionará en ubicaciones determinadas para que adquiera imágenes. Para solucionar las dificultades que esto puede ocasionar, se diseñaron varios bloques de pre procesamiento y ajuste de imágenes antes de aplicar el grado de algoritmo del reconocimiento facial. Esto bajo una condición operativa esperada, el sistema debe ser robusto sobre diversas condiciones de iluminación y el número de rostros en la imagen que se obtiene. El sistema que se propuso tiene como objetivo proporcionar un mecanismo de solución a un bajo precio adecuada para los requisitos de entornos que no se controlan.

A nivel nacional:

Inicialmente, Alejo (2021), en su investigación busco determinar la influencia de los algoritmos de reconocimiento facial en la gestión del control de acceso de Altoque PS S.A. Así mismo, tiene como primer objetivo específico determinar el impacto de algoritmos de IA en el control de acceso no autorizados y segundo objetivo específico determinar el impacto de algoritmos de IA en el tiempo medio de verificación de acceso. Se consideró 338 acceso como la muestra. La investigación concluyo con el desarrollo de un algoritmo de reconocimiento facial para que permitió disminuir los accesos no autorizado y el tiempo promedio en la verificación en la empresa Altoque PS S.A, logrando concretar los objetivos de la investigación.

Asimismo, Huilca (2019), en su investigación acerca de la seguridad con el fin de mejorar el control de acceso, tuvo como objetivo adecuar los niveles de seguridad de la empresa San Miguel Industrias Pet a las nuevas exigencias, planteo distinguir tres vulnerabilidades en el ingreso, perímetro de la instalaciones y áreas críticas. Huilca (2019) concluyo que a mejoro los controles de accesos permitió mejorar los niveles de seguridad y decrecer el peligro de vulnerabilidad en la empresa en un 16%. Además, que hubo mejoras significativas en los tiempos de ingresos.

También, Noriega (2018), presento como objetivos el mejorar la detección de autos robados, con un aplicativo que permita el reconocimiento de las placas. Para tal tarea, empleo el muestreo aleatorio simple, asumiendo como población, el personal administrativo de la municipalidad de Trujillo. Para cual se asumieron dos muestras, 103 referidas al tiempo de identificación un auto robado y 67 para el tiempo de identificación de las placas de autos robados. Empleándose para esta labor, la creación de un aplicativo, que disminuyo el tiempo de identificación de autos robados en comparación a los métodos empleados por el personal del municipio.

Por otra parte, Villalobos señalo la importancia de la tecnología y el uso de un sistema de reconocimiento facial puede ayudar a identificar a las personas con órdenes de arresto, gracias a un sistema biométrico que cuenta con una cámara, realizando reconocimiento facial y alertando de inmediato a los policías que se encuentran en las entradas y salidas de estos lugares para realizar la detención. El comisario Molina recordó que, hasta el momento todas las dudas que suscitan los

avisos que plantea esta herramienta, cerca del 95 % han dado como resultado una captura efectiva. El sistema opera los 365 días 24/7.

También, Aquijes y Ampuero (2021) en su investigación, implemento un sistema de reconocimiento facial para el control de acceso del personal para mejorar la precisión y el nivel de acceso, es decir el nivel de seguridad protegiendo los activos que tiene la empresa y no se hurtada por una persona ajena a la organización. Esta investigación es de tipo aplicada, y tiene una población de 20 personas. En el aspecto de desarrollo uso diferentes técnicas de extracción de característica del rostro para identificar al individuo.

A partir de este punto, definiremos teorías relacionadas a la presente investigación, centrándonos en la conceptualización de las variables. Definiremos que el reconocimiento facial, Burbano, Navia y Díaz (2021), el proceso de reconocimiento Balmaceda, Schleider y Pedace (2021), así como el apoyo del lenguaje Python (Cisco Networking) y el empleo de librerías como NumPy, (IArtificial, 2022) y OpenCv (INESEM, 2022).

Según, Burbano, Navia y Díaz (2021), señalo que la biometría se enfoca en el estudio, control y análisis de datos biométricos, las características únicas de un organismo se pueden utilizar para identificarlos. Estos datos se pueden recopilar mediante diferentes técnicas: sistemas de reconocimiento de iris, que sintetizan información de los ojos del sujeto; reconocimiento de huellas dactilares, recopilación de datos de huellas dactilares; reconocimiento vascular, extrayendo patrones únicos de venas en la mano o el dedo; y el reconocimiento facial, que analiza las características faciales únicas de una persona.

Además, mencionaron que las características que usa la biometría con el objetivo de identificar a las personas son perfectas y únicas para la singularidad y el control de estos. Sin embargo, según el método se aplique en una u otra característica, la identificación será precisa en mayor o menor grado.

Asimismo, mencionaron que un sistema de reconocimiento facial. Su singularidad radica en el hecho que ofrecen la mayor ventaja para identificar a un individuo, ya

que no requiere un sujeto interactúe con el dispositivo. Este sistema cuenta con tres partes fundamentales. 1) Sistema de vigilancia, que consta de cámaras de vigilancia o seguridad. 2) software de reconocimiento, el cual es el core del mecanismo porque se encarga de identificar y analizar las imágenes recogidas, y 3) base de datos, el cual almacena la información recogida por el sistema. Si falta uno de estos componentes el reconocimiento facial no es posible.

También, dijeron que el proceso de reconocimiento facial consta de tres etapas: 1) detección: se identifica el rostro, 2) extracción de características faciales: el algoritmo extrae las características del rostro mediante una imagen, 3) comparación: los rasgos faciales obtenidas se comparan con los de la base de datos 4) reconocimiento y confirmación: el software mediante un porcentaje define positivamente o negativamente si el rostro detectado es el que está en la base de datos. Sin embargo, aunque todos los componentes estén en funcionamiento, no se garantiza el desarrollo completo de las etapas. Para que el sistema de reconocimiento facial funcione de manera efectiva, se debe considerar las condiciones ambientales como las condiciones de luz, ángulo, etc.

Por ello, es importante aclarar que cuando se habla de tipos de reconocimiento facial, se está refiriendo a las técnicas de reconocimiento. Este sistema tiene varias formas de distinguir un rostro; difieren en su efectividad, precisión y en como recopilan datos faciales.

Es decir, mencionaron que las técnicas de reconocimiento se distribuyen en grupos. En primer lugar, el tradicional que consiste en reconocer y extraer los datos de imágenes estáticas; se mapea el rostro humano para clasificar sus rasgos. Este tiene un gran inconveniente ya que influye mucho de las condiciones de luz y ángulo de visión del rostro. En segundo lugar, el reconocimiento 3D que necesita un dispositivo adicional usualmente un sensor laser que captura la forma del rostro en 3D. Este método tiene una desventaja ya que necesita que la persona este de manera estática frente al sensor. En tercer y último lugar, el método de análisis de textura de piel caracterizado por analizar las líneas, formas y tono de piel de la persona por identificar. Funciona, como los métodos tradicionales, por lo que tiene los mismo pro y contras.

Por otro lado, Balmaceda, Schleider y Pedace (2021), mencionaron que el reconocimiento facial funciona a través de un software alimentado por imágenes y su procesamiento se realiza a través de un algoritmo entrenado para el reconocimiento de rostros y personalizar sus rasgos. Después de mapear las características faciales, el software crea un modelo con una representación matemática de esa cara única. Este patrón coincide con los datos biométricos de la tecnología de reconocimiento facial. Con las plantillas biométricas, los rostros ahora pueden ser leídas por una computadora y comparadas con una base de datos que previamente almacenaba todos los rostros.

NEC (2020), indico que el reconocimiento facial examina los rostros humanos, estos juegan un rol indispensable en nuestras interacciones sociales, logrando transmitir la identidad. Empleando el rostro como un punto de seguridad, la tecnología de biométrica de reconocimiento, recibió una atención importante en los últimos tiempos esto a causa del potencial de aplicación tanto en agencias de seguridad y otras industrias; en comparación con sistemas biométricos que usa huella e iris, el reconocimiento facial tiene ventajas por su proceso sin necesidad de contacto físico. Las imágenes de la cara se pueden capturar de forma remota sin tocar a la persona identificada, y el reconocimiento no requiere interacción con esa persona. Además, el reconocimiento facial sirve para la prevención de delitos, ya que las imágenes faciales que se han grabado y almacenado pueden ayudar a identificar a una persona.

A continuación, presentaremos las diversas tecnologías usadas en el desarrollo este proyecto, Logroño & et. al (2022), mencionó que Python es un lenguaje de programación más utilizado para el desarrollo de software. Su construcción de lenguaje como el enfoque está orientado a objetos, están destinados a que se apoye a todo programador a que se prescriba códigos lógicos y claros para todo proyecto de gran y pequeña escala. En este sentido, Python es un lenguaje que se puede utilizar para desarrollar software para aplicaciones científicas, estadísticas, redes, aplicaciones de escritorio, juegos, aplicaciones web, entre otros. Python emplea diversas librerías, que lo apoyan a dar mayor flexibilidad y más potencia al momento de aplicar la inteligencia artificial.

La verificación manual tradicional de identidad en la sala de examen tiene desventajas como baja eficiencia y grandes factores humanos. Se diseña e implementa un sistema de reconocimiento facial en la sala de examen. El sistema está basado en el algoritmo PCA e implementado en OpenCV. La prueba logra el efecto esperado y proporciona un poderoso soporte. Con las crecientes necesidades de control de acceso de seguridad y seguridad financiera y comercial, la tecnología de identificación biométrica tiene un amplio desarrollo y necesidades de aplicación. Como una de las direcciones de investigación más populares, el reconocimiento facial requiere una alta tasa de detección y precisión de reconocimiento. En este documento, Haar El clasificador en cascada se usa para caracterizar la cara capturada, y el algoritmo LBPH se usa para extraer las características del histograma, a fin de realizar el reconocimiento facial dinámico. Los resultados experimentales muestran que este algoritmo puede reconocer caras dinámicas de manera efectiva en condiciones de oclusión parcial y sonrisa. (Tej Chinimilli et al. 2020)

IArtificial (2022), definió a NumPy como una estructura universal de datos que facilita el análisis de datos e intercambio de información sobre los distintos algoritmos. La estructura de información que se implementa son vectores matrices y multidimensionales con la capacidad para brindar una alta cantidad de información En la definición la biblioteca de Python que brinda un objetivo como matriz multi-dimensional, varios objetos que se derivan, como matrices ocultas o matrices y varios procedimientos para operaciones rápidas con matrices, lógica, incluidas matemáticas, clasificación, manipulación de formas, transformadas discretas de Fourier, E/S, selección, operaciones básicas, operaciones estadísticas básicas, algebra lineal, simulaciones random y más.

Otra de las librerías usadas, Marín (2020), definió OpenCV (Open Source Computer Vision) que empezó como un proyecto de estudio de Intel. Actualmente es la biblioteca de visión más completa por computadora, ya que tiene diversas funciones y cuenta con más de 2500 algoritmos, además está disponible de forma gratuita. Esta gran biblioteca cuenta con múltiples lenguajes como Python, Java y C++.

A continuación, se define las variables, dimensiones e indicadores usadas en esta investigación. Villa, Valencia y Berrio (2018), definieron que el reconocimiento debe

ser preciso y confiable, ya que toda característica extraída de la imagen de entrada debe ser detectable incluso sobre el cambio en la escala, ruido e iluminancia de la imagen.

Castaño y Alonso (2019), afirmaron que el reconocimiento consiste en clasificar la característica extraída de los sujetos, indicando a que sujeto pertenece cada patrón, para el diseño de clasificación pudiendo distinguirse sobre la aproximación probabilística, optimización del criterio de error.

La seguridad física son aquellos mecanismos físicos utilizados para que se prevenga y disminuya todo desastre en el entorno natural, cámara de seguridad y medios físicos para portátiles en la sala de servidores (Peres,2018, p13).

Ramírez y Hernández (2017), indicaron que el servicio de control de entrada, es importante para que se evite el empleo no autorizado de algún recurso vale decir, permite que solo personas autorizadas pueden tener el acceso a aquellos recursos que necesiten y de los cuales tenga permiso y autorización. Se espera que el control tenga la mejor precisión posible y que sea eficaz.

En otras palabras, manifestaron el control de acceso es el proceso de otorgar permisos a usuarios o grupos y determinar quién puede acceder a los sistemas y recursos de información. Su concepto se puede resumir en tres pasos: identificación, autenticación y autorización. En el caso de comunicaciones móviles existentes, redes inalámbricas, portátiles, etc. También es necesario establecer una política de control de acceso basada en las necesidades de seguridad de la organización.

También, definieron el control de acceso es la acción que el sistema realiza para identificar el usuario. El ID de usuario se usa comúnmente, todas las acciones realizadas en el sistema son responsabilidad del usuario, por lo que hablamos de la necesidad de auditorías que permitan guardar las acciones realizadas en el sistema e identificar al usuario autenticado.

Por otra parte, Restrepo (2018), indico que el control de acceso es un elemento de seguridad que buscar verificar los permisos que tiene un dispositivo o persona para acceder a un área. Esta función se encuentra dentro de la gestión de acceso e identidad de una organización. El primer indicador, en esta investigación de acceso

no autorizado buscara que se mida el % de entrada visitante no autorizada en la organización.

$$ANA = \frac{ANA}{TA} * 100$$

Dónde:

- **ANA:** Accesos no autorizados
- **TNA:** Total de acceso no autorizados
- **TA:** Total de accesos

El segundo indicador, Precisión es una métrica que mide la calidad de modelo de inteligencia artificial en tareas de clasificación, donde se medirá el porcentaje de exactitud del reconocimiento facial en la gestión del control de acceso. Es necesario mencionar que le valor de 0.00 quiere decir que no tiene precisión y 1.00 precisión perfecta.

$$P = \frac{VP}{(VP + FP)}$$

Donde:

- **P:** Precisión
- **VP:** Verdadero positivo
- **FP:** Falso positivo

La metodología para el desarrollo del Sistema de gestión de control de acceso será ComonKads. Esta es una metodología para desarrollar y construir sistemas inteligentes establecidos en la gestión del conocimiento, ha sido desarrollado por varias universidades y empresas, basado en múltiples modelos que reúnen todos los aspectos importantes y criterios a tener en cuenta, la metodología propone seis modelos que están relacionados entre sí.

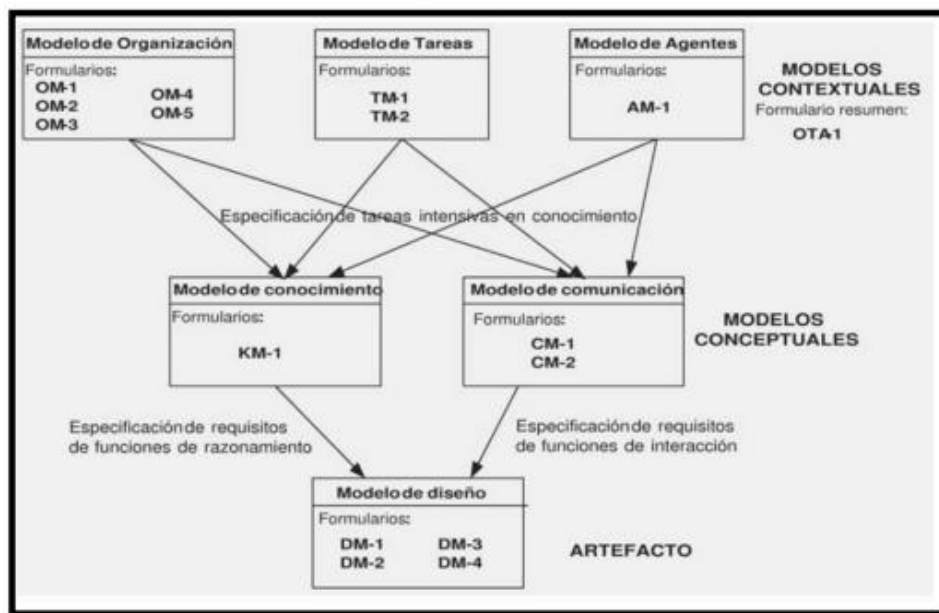


Figura 1 Metodología Comonkads

A continuación, presentaremos cada uno de los modelos propuestos por esta metodología.

- a) **Modo de organización(OM):** En esta etapa se determina el alcance del proyecto, permite identificar las áreas de la problemática y evaluar el impacto que tendrá en la organización
- b) **Modelo de tarea(TM):** Se describe de manera detallada las tareas y los elementos en incluye el desarrollo del SBC
- c) **Modelo de agente (AM):** En esta etapa se define los actores que se encargan de desarrollar el sistema puede ser una persona o un sistema
- d) **Modelo de Conocimiento(EM)**Se describe de manera conceptual los elementos que participan en la resolución del problema y el rol que juegan
- e) **Modelo de Comunicaciones (CM):** Describe interlocución entre los agentes pertenecientes en una tarea.
- f) **Modelo de Diseño (DM):** Describe el procedimiento para implementar el conocimiento en un sistema informático, en función de una arquitectura de software.

También, Miao, Janchai y Panyanuwat (2020) mencionaron que CommonKADS es una de las metodologías que abarcan el conocimiento, captura y uso de la experiencia de expertos activos, entonces, en consecuencia, se diseñan herramientas apropiadas para compartir conocimientos referidos a proceso de gestión.

Además, CommonKADS es el método central para que se apoye la ingeniería de conocimiento estructurado. Siendo llevado a cabo de manera gradual y esto sea validado por diversas universidades y empresas en el programa ESPRIT IT. Actualmente es el estándar europeo de factor para analizar el conocimiento y el desarrollo de sistemas intensivos en conocimiento, y este se adoptó en su totalidad o parcialmente incorporado en la metodología existente por diversas organizaciones relevantes en Europa, así como en Japón y EE.UU.

Es decir, CommonKADS permite que se detecte toda oportunidad y los cuellos de botella en la forma en que las organizaciones desarrollan, distribuyen y apliquen su recurso de conocimiento, por lo que otorga herramientas de gestión de conocimientos corporativos, CommonKADS brinda métodos para el análisis detallado del proceso y tarea intensiva en los conocimientos. Finalmente, CommonKADS respalda el desarrollo de sistema de conocimiento que respaldan partes seleccionadas del proceso comercial.

Para la gestión del trabajo se usó la metodología Scrum. Es una metodología ágil que brinda flexibilidad para controlar y gestionar los requerimientos, así mismo también el desarrollo del software, este fue diseñado para aumentar la productividad en el proceso de desarrollo.

Esta metodología ágil se adapta a los cambios de los requisitos en un futuro y tiene mucha flexibilidad para majear costo alcance y la calidad del software según los requerimientos del cliente. Scrum se centra en la gestión del proyecto por días.

Los procesos de Scrum envuelven al Scrum Master, al equipo de trabajo y interesado. Este se divide en Sprint que contiene todos los requisitos, el objetivo de cada sprint es entregar un producto organizado y sin errores. (Hayat et al. 2019)

Scrum es uno de los marcos de referencia más utilizados ampliamente en la industria que están plasmados según Scrum Alliance. Esta consta de tres componentes principales que son el Scrum Master, Product Owner y el equipo de desarrollo. En Scrum se realizan pequeñas reuniones para establecer estrategias para el desarrollo del producto y definición de tiempo de entrega del sprint. Por otra parte, también es importante mencionar que Scrum permite utilizar diversos procedimientos y técnicas. (Saleh, Huq y Rahman 2019)

La metodología ágil se desarrolló en el año 1990 cuando un grupo de ingenieros de software llegó a la conclusión de que las metodologías de la época no podían entregar el producto a tiempo y tampoco lograba la satisfacción del cliente. Esta metodología fue incluida en marzo de 2018 en la PMBOK donde indica la importancia de esta metodología para la gestión de proyecto y la importancia del Scrum Master que tiene muchas responsabilidades. Scrum es una de las metodologías más aceptadas y utilizadas a nivel mundial. (Ereiz y Music 2019)

El proceso de reconocimiento facial, inicia en el registro de personas y adquisición de imágenes mediante una cámara web, donde el sistema captura imágenes que serán usadas como entrada para el reconocimiento facial.

Luego, se realiza el procesamiento de imágenes, donde las imágenes se estandarizan y corrigen para mejorar el reconocimiento facial, además se cambia la dimensión de las imágenes

La imagen de cara estandarizada sirve como entrada para la extracción de características donde se utilizan técnicas de clasificación cada imagen se transformó en una matriz. Una vez registrada la imagen se procede con el módulo de entrenamiento donde se entrena al algoritmo; después de realizar este paso el algoritmo ya se puede iniciar los módulos de Registrar Ingreso y Registrar Salida.

Cuando se inicia el módulo de registro de asistencia, la imagen capturada se compara con los datos registrados en la base de datos SQLite y si esta registrara marca su asistencia y si no está lo detecta como un desconocido.

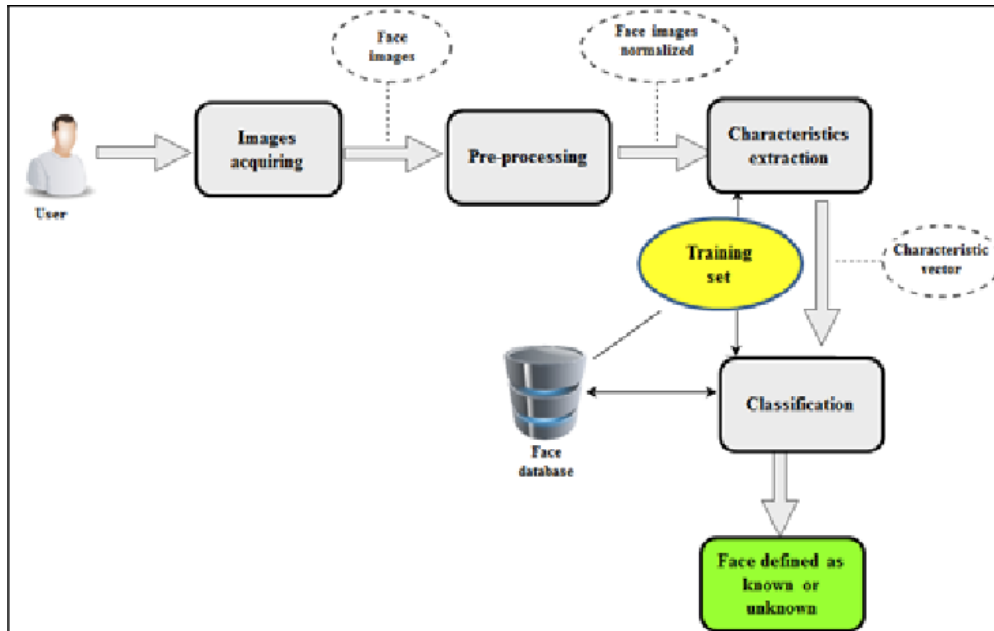


Figura 2 Etapas del reconocimiento facial (Diniz et al. 2017)

Para realizar el conocimiento facial se usó un método tradicional basado en las características geométricas de rostro. Este se utiliza en combinación con Haar Cascade para la detección del rostro. Los datos capturados se guardan en un arreglo donde cada pixel tiene un número. El algoritmo viola-jones divide el rostro de la imagen en pixeles y los asocia con los 8 pixeles para posteriormente comparar los valores con pixeles vecinos. Luego se obtiene características únicas del rostro mediante el análisis de 68 puntos del rostro. Tal como se muestra en la figura 3.

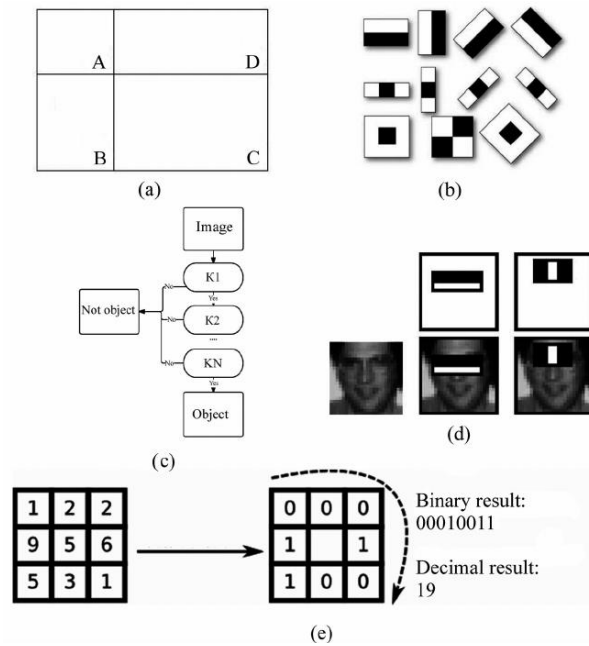


Figura 3 Arquitectura del algoritmo Viola-Jones (Egorov, Shtanko y Minin 2017)

En la figura 7, se describe las partes del algoritmo Viola-Jones: (a) Combinación de regiones, (b) Funciones Haar, (c) Clasificador en cascada, (d) Aplicación de las funciones Haar a la imagen y (e) función LBP

Para el desarrollo y la implementación del sistema de reconocimiento facial para la empresa Spirella se usó el algoritmo Viola-Jones usando una base de datos SQLite, el lenguaje de programación usado es Python con sus librerías OpenCV. Para el modelo vista del usuario se usó Django, html5 CSS, bootstrap, jquery que se presente en la arquitectura tecnológica del sistema en la figura 4.

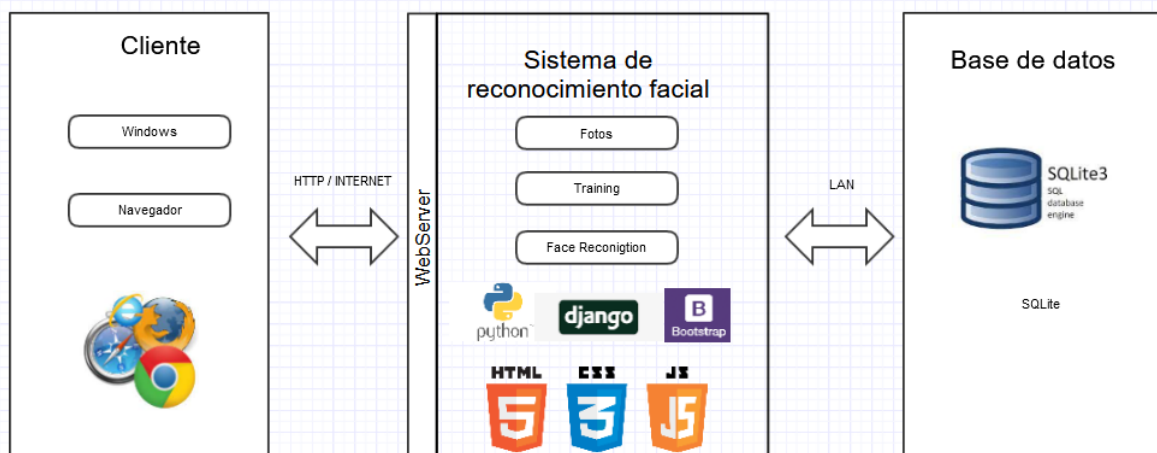


Figura 4 Aquitectura del tecnologica

III. METODOLOGÍA

El presente capítulo explica el diseño de la investigación como el tipo, analizamos las variables, así como la operacionalización de las mismas, la población, muestra y técnica de muestreo empleado. Analizaremos el instrumento y la recolección de datos, y aquellos referidos a los aspectos éticos.

3.1. Tipo y diseño de investigación

Este estudio es de tipo aplicada, de diseño pre experimental, tiene como objetivo que se determine la influencia de reconocimiento facial en la gestión de control de acceso. Así como también buscar que se pruebe la hipótesis dentro de un entorno determinado.

Según Ortega (2017), la investigación práctica o aplicada se diferencia por la búsqueda del uso o aplicación del conocimiento adquirido. Es decir, su aplicación busca resolver problemas en el desarrollo de un proyecto a partir de la investigación continua y recopilación de información para adquirir nuevos conocimientos científicos del investigador. Por su parte Hernández (2014), es aquel conjunto de tareas desarrolladas una después de otra con el fin de probar algo. Generalmente, están divididas en fases, y las tareas que conlleva no pueden sufrir retrasos o adelantos. La investigación es aplicada por que permite recolectar información y aplicarla en el desarrollo de una solución tecnológica para resolver un problema específico; cabe mencionar que este enfoque debe ser detallado y delimitado, bajo la generación de objetivos como de preguntas que apoyen a la investigación, siendo necesario la revisión de literatura propias u orientadas a proveer más conocimiento.

Esta investigación es de tipo pre-experimental porque se trata de aproximar a la variable, genera una hipótesis y se mide una o más variables.

Hernández y Mendoza (2018), los cuales indican que los pre experimentos a diferencia de los experimentos puros, se caracterizan por el bajo control que tiene. Cabe mencionar que esta clase de experimentos pueden tener una sola medida, pero esta no afecta a la variable dependiente. Por otro lado, los de diseño preprueba/ posprueba aplicada a un grupo de control, este diseño ofrece dos ventajas, la primera ayudan a los fines del experimento ya que cuenta con valores que al compararse con los de preprueba, se evalúan de forma aleatoria. La segunda, es que podemos analizar, o comparar tanto el pre como la pos prueba.

El tipo de investigación que se plantea es un diseño pre-experimental. Para esta investigación se eligió el segundo básico, ya que se realizarán pruebas antes y después del uso de la aplicación con un solo grupo.

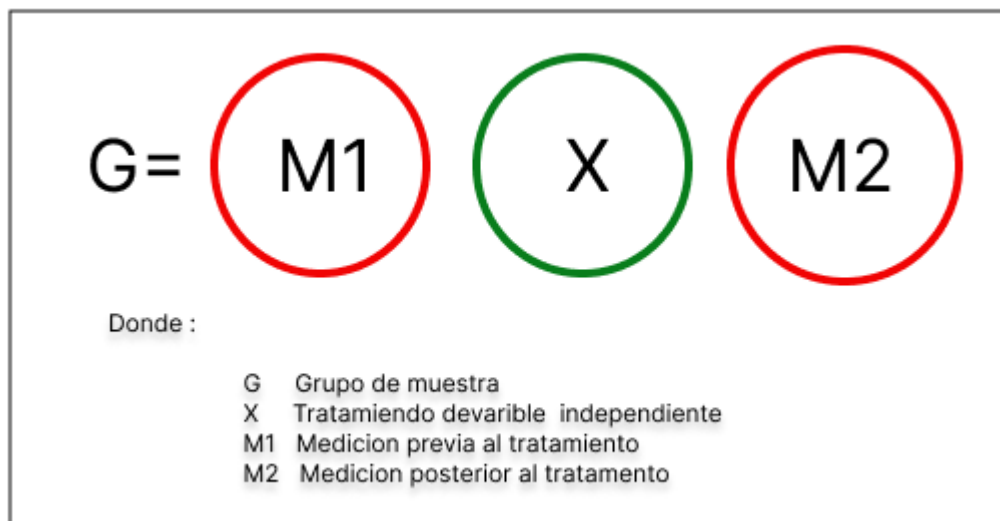


Figura 5. Diseño Pre - Experimental

3.2. Variables y operacionalización

Variable

La variable estudiada es el efecto de reconocimiento facial para ver la mejora en la gestión de control de acceso. Adicionalmente, se presenta la matriz de operacionalización de variables en los anexos. A continuación, se define cada aspecto:

- A. Definición conceptual: indicaron que el control de acceso es una técnica que administra el ingreso y la salida, determina quien está autorizado, los horarios, entre otros (Restrepo, 2018).
- B. Definición operacional: indicaron que el servicio de control de acceso se utiliza para evitar el uso no autorizado de los recursos, es decir, solo las personas autorizadas pueden tener acceso a aquellos recursos que necesiten y de los cuales tenga permiso y autorización. Se espera que el control tenga la mejor precisión posible y que sea eficaz (Ramírez y Hernández, 2017).
- C. Dimensiones:
 - Seguridad física

D. Indicadores:

- Precisión (Brownlee,2020; Aquijes y Ampuero, 2021)
- Control de acceso no autorizado (Huillca, 2019; Alejo, 2021)

E. Instrumento:

- Ficha de registro
- Ficha de registro

F. Escala de medición:

- Escala razón
- Escala razón

3.3. Población, muestras y muestreo

Población: Es el conjunto de datos que son obtenidos de un determinado espacio o ambiente de estudio, escogiéndose un número específico para determinar el valor global (Hernández, Fernández y Baptista, 2014).

Según Hernández, Fernández y Baptista (2014), la población es definida como un conjunto de elementos relacionados del que se busca tener conocimiento. Este conocimiento, puede manifestarse de diferentes formas estadísticas. Para este proyecto de investigación se utilizó como población los registros de la base de datos de la empresa Spirella, empleando la data histórica. Es decir, se usará 1500 registros de asistencia en un lapso de 26 días.

Muestra: Es una parte de la población o universo, donde se llevará a cabo el estudio, Existe procedimientos para que se obtenga la cantidad de componentes de la muestra como lógica, formulas y otros que se podrá ver en el proyecto, la muestra es una porción que representa a la población. Las muestras pueden obtenerse de dos formas, como probabilística y no probabilísticas (López, 2010). Para esta investigación se considera un total de 306 registros como muestra, con un nivel de confianza del 95%.

Muestreo: La técnica de muestreo probabilístico simple, permite que se conozca la probabilidad de que cada sujeto sea incluido en la muestra por medio de una selección al azar. (Guillot,2022).

Unidad de análisis: Son los elementos de la comunicación en el que se centrara el análisis. Conviene que se establezca una precisión mayor, y para ello se distinguirá entre las unidades de registro, muestra y unidades de contexto (García, Ibáñez y Alvira, 1996).

La unidad de análisis en la presente investigación son los registros de los trabajadores de la empresa Spirella, referentes a su ingreso.

3.4. Técnicas e instrumentos de recolección de datos

En esta sección, se dará una descripción de herramientas de recolección de datos incorporando las herramientas y conceptos clave seleccionados en el trabajo. Además, también se describe la validez y confiabilidad de estas herramientas aplicadas.

Según Carrasco, las técnicas definen grupos y procedimientos que dirigen las actividades de las personas involucradas en la etapa de la investigación científica, además menciona que para el trabajo de una investigación se recolecta información mediante análisis de documentos. (p.274)

Esta investigación el instrumento que se usó para la recolección de datos es la ficha de registro ya que se adecua más a nuestra investigación. El instrumento que se empleará será la ficha de registro por cada indicador de una dimensión, en las fichas se registrará los datos obtenidos que será usada posteriormente para realizar pruebas. La ficha de registro recolectará los datos de los investigadores obtengan antes y después de la implementación del sistema. (Gallo y Nunura, 2021).

Además, la validez es uno de los requisitos indispensables que debe cumplir el instrumento, por lo que Hernández et al. (2014) establecieron que la validez como el nivel en que un instrumento mide con precisión la variable que está tratando de calcular (p. 200). Esto significa para que la investigación tenga información real debe contar con un instrumento confiable y que valide todos los aspectos desarrollados durante su construcción (Pereira et al, 2018).

Así mismo, la confiabilidad requiere que los resultados obtenidos en la prueba piloto y en la prueba final sean mayores a 0.70 (Kline, 2016, p. 92).

Hernández et al. (2014) explicó que es un instrumento, en el que su aplicación produce resultados uniformes y consistentes, tiene una alta confiabilidad. (p. 200).

También, para Hernandez la correlación de Pearson es una prueba que evalúa en el análisis de una la relación de datos donde se miden las variables en intervalos de tiempo o de razón.

Tabla 1 Tabla de confiabilidad

Escala	Nivel
-0.20	Correlacion debil
-0.10	Correlacion muy debil
0.00	No existe correlacion
+0.25	Correlacion debil
+0.50	Correlacion media
+0.70	Correlacion considerable
+0.90	Correlacion fuerte

Fuente: Elaboración propia

En esta investigación se utilizó el método test y retest, donde se repite la aplicación del mismo instrumento en dos o más veces. De acuerdo a los resultados de correlación se determina si el instrumento es confiable o no.

Tabla 2. Correlación de Acceso no autorizado

Correlaciones		TEST-ANA	RETES-ANA
TEST-ANA	Correlación de Pearson	1	,877**
	Sig. (bilateral)		0.000
	N	26	26
RETES-ANA	Correlación de Pearson	,877**	1
	Sig. (bilateral)	0.000	
	N	26	26
** . La correlación es significativa en el nivel 0,01 (bilateral).			

Fuente: Elaboración propia

Según la tabla 2, se llega a obtener que el resultado de 0.877, esto quiere decir que está en la escala mayor a 0.70, de esta forma se pude concluir que

el instrumento tiene un nivel aceptable para el indicador Control de acceso no autorizado.

Tabla 3. Correlación de Precisión

Correlaciones			
		TEST-Precision	RETES-Precision
TEST-Precision	Correlación de Pearson	1	,904**
	Sig. (bilateral)		0.000
	N	26	26
RETES-Precision	Correlación de Pearson	,904**	1
	Sig. (bilateral)	0.000	
	N	26	26
**. La correlación es significativa en el nivel 0,01 (bilateral).			

Fuente: Elaboración propia

Según la tabla 3, se llega a obtener que el resultado de 0.904, esto quiere decir que está en la escala mayor a 0.90, de esta forma se puede concluir que el instrumento tiene un nivel aceptable para el indicador Precisión.

Según Hernández, afirmó que es el nivel que posee un instrumento de poder evaluar, si han existido cambios en la realidad. Para esta investigación experimento emplearemos el juicio de expertos.

Asimismo, afirmó que la confiabilidad es una de las características de un instrumento de medición, donde se asume que tiene un alto grado de reproducibilidad en los resultados de los datos, es decir, si se presenta un nuevo experimento en las mismas condiciones, entonces el instrumento puede ser reutilizado y producir los mismos resultados, ya que deben presentar autenticidad y consistencia.

3.5. Procedimientos

En esta investigación se enfoca en la problemática en la empresa Spirella que es la gestión del control de acceso. Teniendo en cuenta esta realidad se realizó una investigación a nivel nacional e internacional donde se recabó información de técnicas y procedimiento aplicado en anteriores proyectos, llegando a la conclusión de implementar un sistema de reconocimiento facial

para la gestión del control de acceso. También se analizó las variables recopilando información de diversos autores que sirven como antecedentes y sirven como una fundamentación teórica que respalda el presente trabajo. La investigación que se planteo es de tipo aplicada, de diseño pre-experimental, posteriormente se implementara este proyecto y se realizara un contraste entre el pre prueba y post prueba de los indicadores. Se recolecto información mediante técnica de fichaje, usando el instrumento ficha de registro; luego se determinó el método de análisis de datos y el software que se usó es el SPSS 26 utilizando análisis descriptivo e inferencia. Finalmente se determina la parte administrativa del proyecto, donde se define los recursos, presupuesto, financiamiento y el cronograma de la ejecución del proyecto.

3.6. Método de análisis de datos

Para el estudio se usó un análisis descriptivo, puesto que es un método determinante para que se recopile información y posteriormente proceder a que se describa la relación existente sobre los datos.

La estadística descriptiva según lo definieron Rendón et al., (2016), es aquella rama de la estadística que formula la recomendación de como sintetizar de forma sencilla y clara, los datos de una investigación en tablas, graficas, cuadros o figuras. Antes de que se lleve a cabo un análisis descriptivo es importante que se retome cada objetivo de investigación, así como que se identifique la escala de medición de las diversas variables que se registraron en la investigación. El objetivo de las cuadros o tablas es que se proporcione datos puntuales sobre el resultado. Las gráficas muestran toda tendencia y pueden ser histogramas, representaciones en “cajas con bigotes”, “pastel” puntos de dispersión o gráficos de líneas. La imagen sirve para dar ejemplo de conceptos, buscando reforzar los hechos. La selección de un gráfico, imagen o cuadro debe basarse en el objetivo de investigación.

Ramírez y Polack (2020) definieron la estadística inferencial, como aquella que busca que se identifique la prueba no paramétrica no sujeta a la

distribución de probabilidad normalizada para el análisis inferencial adecuado sobre la información proveniente de muestras pequeñas. Por medio de la teoría que se fundamenta en 1 muestra (Chi-cuadrado, Binomial, Kolmogorov - Smirnov, de rachas), 2 muestras independientes (Kolmogorov – Smirnov, Moses, U-Mann Whitney, rachas de Wald-Holfowitz), 2 muestras pareadas (McNemar, De signo y Wilcoxon), m muestras no pareadas (Kruskal – Wallis, Mediana, Jonckheere – Terpstra) y m muestras pareadas (Q-Cochran, Fridman, W-Kendall) Se llegó a concluir que esta prueba es robusta y valiosa, la elección está sujeta al número, diseño y escala de medición sobre cada variable de estudio.

En esta investigación para el análisis inferencial de la variable acceso no autorizado se aplicó la prueba de normalidad Shapiro-Wilk por que el tamaño de nuestra muestra es menor a 30, el resultado obtenido demuestra que los datos tienen distribución normal por ende se aplicó la prueba de t-student. Asimismo, en la variable precisión se aplicó la misma prueba de normalidad, que dio como resultado que los datos no tienen distribución normal por ello se aplicó la prueba de Wilcoxon.

3.7. Aspectos éticos

Para la elaboración de esta investigación se tuvo en cuenta mantener la confidencialidad, seguridad y veracidad de la información proporcionada por la empresa, además esta información solo se utilizó con fines educativos, respetando los códigos de ética de la Universidad Cesar Vallejo y del colegio de ingenieros del Perú.

Así mismo, se cuenta con los permisos respectivos por parte de la empresa Spirella para el desarrollo de esta investigación. Para garantizar la confidencialidad de la información se recodificaron los datos obtenidos de Spirella, además el sistema desarrollado tiene medidas de seguridad que garantiza que solo las personas autenticadas puedan ingresar al sistema.

IV. RESULTADOS

En la presente investigación se emplea el reconocimiento facial para el control acceso de los empleados de Spirella, bajo las dos variables: precisión, control de acceso no autorizado. Para lo cual, se realizará el análisis descriptivo, del conjunto de datos recolectados tanto en el pre test como pos test. Finalmente pasaremos los datos para evaluación mediante el empleo de la estadística inferencial. Con el fin de ver la aceptación o rechazo de las hipótesis planteadas.

Indicador: Control de acceso no autorizado

Análisis Descriptivo

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

Tabla 4. Comparación estadístico descriptiva del control de acceso no autorizado

Estadísticos descriptivos						
	N	Mínimo	Máximo	Media	Desv. Desviación	Varianza
TEST-ANA	26	22	50	34.15	8.601	73.975
POST-ANA	26	7	20	10.42	4.216	17.774
N válido (por lista)	26					

Fuente: Elaboración Propia

De acuerdo, a los datos obtenidos, se observa que antes del aplicativo (pre test) el dato mínimo era 22% de control de acceso no autorizado, y después del aplicativo fue de un 7%. Mientras la media obtenida en el pre test resultó un 34.15% para el control de acceso no autorizado y después de la prueba se obtuvo un 10.42%.

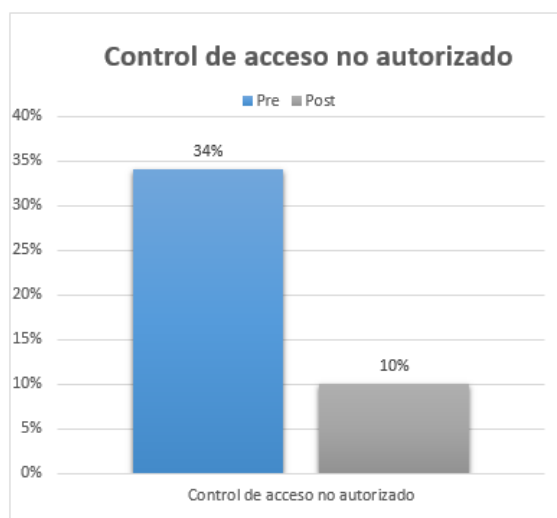


Figura 6 Media de accesos no autorizados

Análisis Inferencial

Analizaremos la normalidad de los datos, para analizar el tipo de prueba a seguir con el fin de someterlas a la estadística inferencial. Dado que nuestra muestra es menor a 30, veremos los valores obtenidos por Shapiro Wilk.

Tabla 5. Prueba de normalidad pre y post acceso no autorizado

Pruebas de normalidad						
	Kolmogorov-Smirnov ^a			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
TEST-ANA	0.146	26	0.163	0.927	26	0.065
POST-ANA	0.248	26	0.000	0.771	26	0.000

a. Corrección de significación de Lilliefors

Fuente: Elaboración propia

Los criterios de normalidad para este indicador son:

P-valor $\Rightarrow \alpha$, Aceptamos H_0 = Los datos provienen de una distribución normal.

P-valor $< \alpha$, Aceptamos H_1 = Los datos no provienen de una distribución normal.

P-valor (accesos no autorizados antes) = 0.065 $>$ $\alpha=0.05$

P-valor (accesos no autorizados después) = 0.00 $<$ $\alpha=0.05$

Por lo que concluimos que los datos provienen de una distribución normal. Lo que nos indica, que debemos pasar por la prueba de t-student para muestras relacionadas. Recordaremos también que las hipótesis planteadas para este indicador son:

H1: El uso de una aplicación con reconocimiento facial mejorará el control de acceso no autorizado en la gestión del control de acceso de la empresa Spirella

H0: El uso de una aplicación con reconocimiento facial no mejorará el control de acceso no autorizado en la gestión del control de acceso de la empresa Spirella

Tabla 6. Prueba de muestra emparejada

Prueba de muestras emparejadas									
Diferencias emparejadas									
		Media	Desviación estandar	Media de error estandar	95% de intervalo de confianza de la diferencia		t	gl	Sig. (bilateral)
					Inferior	Superior			
Par 1	TEST-ANA POST-ANA	23.731	9.067	1.778	20.069	27.393	13.346	25	0.000

Fuente: Elaboración propia.

Analizando los datos obtenidos tenemos, donde el p-valor es igual a la sig. Bilateral obtenida:

$$p\text{-valor} = 0.00 < \alpha$$

Donde $\alpha=0.05$, el criterio a decidir es:

Si la probabilidad obtenida p-valor $\leq \alpha$, rechazamos H0

Si la probabilidad obtenida p-valor $> \alpha$, no rechazamos H0

Es así que rechazamos la hipótesis nula. Dado que hay una diferencia significativa en los datos referentes al control de acceso antes y después de la aplicación de reconocimiento facial. Por lo cual se concluye que el uso de una aplicación con reconocimiento facial mejora el control de acceso no autorizado en la gestión del control de acceso de la empresa Spirella

Indicador: Precisión

Análisis Descriptivo

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

Tabla 7. Comparación estadístico descriptivo variable precisión

Estadísticos descriptivos					
	N	Mínimo	Máximo	Media	Desv. Desviación
TEST-Precision	26	0.79	0.94	0.8812	0.04676
POST-Precision	26	0.90	1.00	0.9931	0.02462
N válido (por lista)	26				

Fuente: Elaboración propia

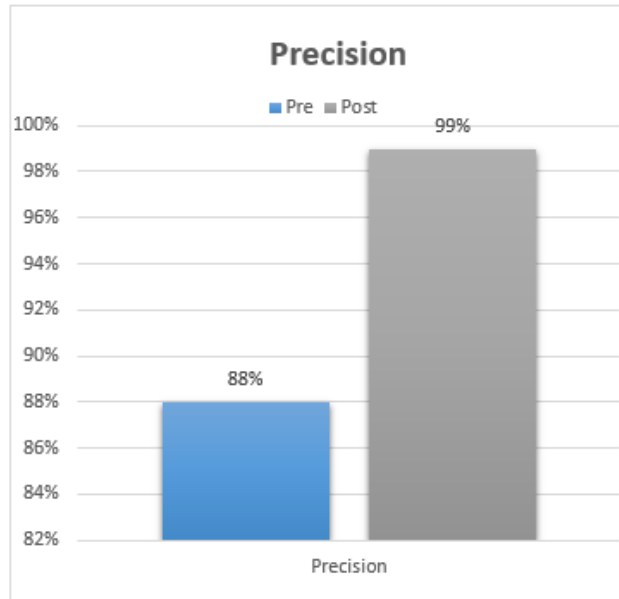


Figura 7 Media de Precisión pre-test y post-test

En la figura 3, observamos que la media obtenida para el indicador precisión en el pre-test es 88%, mientras que el pos-test un 99; que representa una mejora de la precisión de un 11%.

Análisis Inferencial

Analizaremos la normalidad de los datos, para analizar el tipo de prueba a seguir con el fin de someterlas a la estadística inferencial. Dado que nuestra muestra es menor a 30, veremos los valores obtenidos por Shapiro Wilk.

Tabla 8. Prueba de normalidad de pre y post de variable precisión

Pruebas de normalidad						
	Kolmogorov-Smirnov ^a			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
TEST-Precision	0.220	26	0.002	0.892	26	0.010
POST-Precision	0.534	26	0.000	0.308	26	0.000

a. Corrección de significación de Lilliefors

Fuente: Elaboración propia

Los criterios de normalidad para este indicador son:

P-valor $\Rightarrow \alpha$, Aceptamos H_0 = Los datos provienen de una distribución normal.

P-valor $< \alpha$, Aceptamos H_1 = Los datos no provienen de una distribución normal.

P-valor (precisión antes) = 0.010 > $\alpha=0.05$

P-valor (precisión después) = 0.00 < $\alpha=0.05$

Por lo que concluimos que los datos no provienen de una distribución normal. Lo que nos indica, que debemos pasar por la prueba de Wilcoxon. Recordaremos también que las hipótesis planteadas para este indicador son:

H1: El uso de una aplicación con reconocimiento facial para mejorar la precisión en la gestión del control de acceso de la empresa Spirella.

H0: El uso de una aplicación con reconocimiento facial no da mejoras la precisión en la gestión del control de acceso de la empresa Spirella.

Tabla 9. Prueba de hipótesis variable precisión.

	Hipótesis nula	Prueba	Sig.	Decisión
1	La mediana de las diferencias entre TEST-Precision y POST-Precision es igual a 0.	Prueba de rangos con signo de Wilcoxon para muestras relacionadas	,000	Rechazar la hipótesis nula.

Se muestran significaciones asintóticas. El nivel de significación es de ,05.

Fuente: Elaboración propia

Finalmente, en el SPSS obtenemos que los resultados por la prueba de Wilcoxon, nos indica que rechazamos la hipótesis nula. Siendo la alterna la aceptada. Por lo que el uso de una aplicación con reconocimiento facial mejora la precisión en la gestión del control de acceso de la empresa Spirella.

V. DISCUSIÓN

En esta investigación Reconocimiento facial para la gestión de control de acceso en la empresa Spirella se obtuvo que ANA control de acceso no autorizados redujo el control de acceso de los trabajadores de un 34 % a un 10%, por lo que se deduce que se redujo los accesos no autorizados en un 24%.

Del mismo modo, Alejo Paul; en su tesis “Algoritmo de reconocimiento facial para la gestión de control de acceso de la empresa Altoque PS S.A redujo el control de accesos de un 63 % a un 16% por lo que hubo una reducción del 47%, en comparación con la presente investigación que redujo un 24 %; esta diferencia se debe a que el dato recolectado para la investigación de Alejo solo fue 24 días y su muestra fue de 320 registros. Además, se usó un algoritmo diferente al empleado en esta investigación.

Además, como resultado en el Reconocimiento facial para la gestión de control de acceso en la empresa Spirella se incrementó la precisión de 88% a un 99%, por lo que se deduce en un incremento de la precisión en un 11%.

De la misma manera, Aquijes y Ampuero en su tesis “Implementación de un sistema de reconocimiento facial para el control de acceso del personal en la empresa GUIMARTBOT S.A.C” se obtuvo una mejora de la precisión en 8%, en comparación con la presente investigación que obtuvo una mejora en la precisión de 11%; esta diferencia se debe a que los datos recolectados en la investigación de Aquijes y Ampuero se realizaron en 25 días y su muestra fue mayor cantidad. También, se usó una base de datos diferente el Mysql, en comparación con el SQLite que se usó en esta investigación.

Por ello se afirma que el Reconocimiento facial para la gestión de control de acceso mejoro el control de acceso y la precisión en la empresa Spirella.

VI. CONCLUSIONES

1. En la investigación realizada en la empresa Textil Spirella, se concluye que el Sistema de reconocimiento facial influye de manera positiva en el proceso de toma de asistencia del personal, donde se puede evidenciar la mejoría de los indicadores, ya que redujo los accesos no autorizados y mejoro la precisión en la toma de asistencia del personal, demostrando una mejora significativa después de la implementación del Sistema de Reconocimiento facial.
2. Con respecto al primer indicador, control de acceso no autorizado, se demostró que el sistema de reconocimiento facial redujo el índice de accesos no autorizados de un 34% a un 10%, lo que representa una reducción significativa de accesos no autorizados del 24%, determinando una reducción y mejora en los procesos de toma de asistencia del personal. Además, en la prueba de hipótesis dio como resultado una significancia de 0.00 por lo tanto se rechaza la hipótesis nula.
3. Con respecto al segundo indicador, precisión, se evidencio que la precisión en el proceso de registro de asistencia mejoro en un 11%. Puesto que inicialmente tenía un 88% y después de la implementación un 99%, por ello se concluye que el Sistema de reconocimiento facial mejoro la precisión en la gestión de control de acceso en la empresa Textil Spirella. Además, en la prueba de hipótesis dios como resultado una significancia de 0.00 por lo tanto se rechaza la hipótesis nula.

VII. RECOMENDACIONES

Basado en el despliegue del Sistema de reconocimiento facial para la empresa Spirella y evidenciado la mejoras después de la implementación del Sistema, se dan las siguientes recomendaciones para posteriores investigaciones:

1. Se recomienda para mejorar el impacto de la aplicación de reconocimiento facial en la organización elaborar un manual de usuario y capacitar al personal que opera el sistema para un uso correcto.
2. Para mejorar y reducir los índices de accesos no autorizados se recomienda integrar el sistema de reconociendo facial con dispositivos electrónicos que integran inteligencia artificial para que puedes servir de apoyo y futuras mejoras al sistema.
3. Agregar modelos entrenados de reconocimiento facial para que se puede reconocer rostros en diversos ángulos y niveles de luz, de esta manera así mejorar aún más la precisión y robustez del sistema.

Además, utilizar una cámara web de muy buena resolución y enfoque panorámico para que posteriormente al momento de capturar la imagen se pueda extraer características del rostro con más detalle. Así mismo, implementar algoritmos y sistemas de seguridad que no permitan burlar el sistema.

También, que el sistema genere un reporte mensual de asistencia, precisión y los accesos no autorizados para que sirva de apoyo al área administrativa.

REFERENCIAS

UNIVERSAL SOLUTIONS SECURITY, 2018. Problemas de seguridad en las pequeñas empresas. [En línea] <https://uss.com.ar/corporativo/problemas-de-seguridad-de-las-pequenas-empresas/>.

CARRASCO, Sergio. Metodología de la investigación científica. 19 ed. Perú. San Marcos. 2019. 476 pp. ISBN: 978-9972-38-344-1.

ROSAS, Zulli. Análisis de la seguridad física en una empresa del sector de la construcción en su edificio central. Bogota.2019.

KIMALDI, 2019.Expertos en seguridad. [En línea]. <https://www.kimaldi.com/blog/como-desinfectar-los-terminales-de-huella-y-lectores-rfid/>

HUILLCA, Pedro. Innovación en seguridad para mejorar los controles de acceso en la empresa San Miguel Industrial PET.Peru.2019.

VILLALOBOS, Fonseca. El desarrollo tecnológico en materia policial: una receta de éxito para la prevención del delito. Revista Relaciones Internacionales,2019 Estrategia Y Seguridad, 15(1). pp. 79-97. DOI: <https://doi.org/10.18359/ries.4243>

RODRÍGUEZ, Alejandra. Facial recognition: A two-sided story. Peru.2019.

MIGUEL, Noriega. Aplicativo de Reconocimiento de Placas vehiculares para mejorar la Detección de vehículos robados en la Municipalidad Provincial de Trujillo 2018. [consultado el 5 de junio de 2022]. Disponible en: <https://repositorio.ucv.edu.pe/handle/20.500.12692/35656>

ALEJO, Paul. Algoritmo de reconocimiento facial para la gestión del control de acceso de la empresa Altoque PS S.A. 2021. Disponible en: <https://repositorio.ucv.edu.pe/handle/20.500.12692/84197>

AQUIJES, Ronny y AMPUERO, Lizardo. Implementación de un Sistema de Reconocimiento Facial para el control de acceso del personal en la empresa GUIMARTBOT S.A.C, 2021. Disponible en:

<https://repositorio.ucv.edu.pe/handle/20.500.12692/83111>

CASTAÑO, David y ALONSO, Juan. Sistema de reconocimiento facial para control de acceso a viviendas. Trabajo de titulación. Colombia. Universidad Católica de Colombia, Facultad de Ingeniería.2019.153 pp.

HERNÁNDEZ, Benjamín. Técnicas estadísticas de investigación social. Madrid: Ediciones Díaz de Santos, 2001.ISBN: 978847978505.

HERNÁNDEZ, Roberto et al. Metodología de la investigación [En línea]. 6 ed. México. McGRAW-HILL / Interamericana Editores, S.A. DE C.V. 2014. [Fecha de consulta: 20 de mayo de 2021] Disponible en:
https://www.ucv.edu.pe/datafiles/FONDO%20EDITORIAL/Manual_ISO.pdf
ISBN: 978-1-4562-2396-0.

PÉREZ, Hugo y ALTAMIRANO, Santiago. Sistema de control de acceso por reconocimiento de iris para el ingreso de personal a la empresa electro servicios querubín de la ciudad de puyo. Trabajo de Titulación. Ecuador. Universidad técnica de Ambato, Facultad de ingeniería en sistemas. 2018. 118 pp.

ALMONACID, Cristian. Consideraciones teóricas y éticas del reconocimiento facial de las emociones en contexto de pandemia. Veritas [online]. 2020, n.46 [citado 2022-05-13], pp.55-75. Disponible en: ISSN 0718-9273.

Bernal, C. (2010). Metodología de la Investigación. (3a ed.). Bogotá, Colombia: Pearson Educación.

BAI, X., JIANG, F., SHI, T. y WU, Y., 2020. Design of attendance system based on face recognition and android platform. *Proceedings - 2020 International Conference on Computer Network, Electronic and Automation, ICCNEA 2020*, pp. 117-121. DOI 10.1109/ICCNEA50255.2020.00033.

BHARADWAJ, R.S., RAO, T.S. y VINAY, T.R., 2019. Attendance management using facial recognition. *International Journal of Innovative Technology and Exploring Engineering*, vol. 8, no. 6, pp. 1619-1623. ISSN 22783075.

CAHYONO, F., WIRAWAN, W. y FUAD RACHMADI, R., 2020. Face recognition

- system using facenet algorithm for employee presence. *4th International Conference on Vocational Education and Training, ICOVET 2020*, pp. 57-62. DOI 10.1109/ICOVET50258.2020.9229888.
- CHEN, E., WU, X., WANG, C. y DU, Y., 2019. Application of improved convolutional neural network in image classification. *Proceedings - 2019 International Conference on Machine Learning, Big Data and Business Intelligence, MLBDBI 2019*, pp. 109-113. DOI 10.1109/MLBDBI48998.2019.00027.
- COSTA MARI, D., CÁRAVE, J., ALEJANDRO BAUTISTA GÓMEZ, FELIPE, J., FONSECA, C., SISTEMA, D.E.U.N., EN, D.E.A. y BUESTÁN VERA, J.C., 2020. Análisis De Un Sistema De Reconocimiento Facial a Partir De Una Base De Datos Realizado Mediante Python. *Dpto. Organización Industrial y Gestión de Empresas Escuela Técnica Superior de Ingeniería Universidad de Sevilla* [en línea], pp. 80. Disponible en: <http://hdl.handle.net/2117/331277>.
- DEL TORO, E., SARMIENTO, C. y SOLANO, S., 2012. Implementación Híbrida Hardware Software Del Algoritmo De Detección De Rostros De Viola-Jones Sobre Fpga Hybrid Hardware Software Implementation of Viola-Jones Face Detection Algorithm Using an Fpga. [en línea], vol. 16, no. 63, pp. 114-124. Disponible en: <http://www.scielo.org.ve/pdf/uct/v16n63/art05.pdf>.
- DINIZ, F.A., MILTON, F., NETO, M., LIMA, C., MABEL, L. y FONTES, D.O., 2017. A Facial Recognition System Based on Techniques of Principal Component Analysis and Autofaces with K-NN , K-Star and Random. , vol. 12, no. April, pp. 7-14. DOI 10.4156/rnis.vol12.2.
- EGOROV, A.D., SHTANKO, A.N. y MININ, P.E., 2015. Selection of Viola–Jones algorithm parameters for specific conditions. *Bulletin of the Lebedev Physics Institute*, vol. 42, no. 8, pp. 244-248. ISSN 1934838X. DOI 10.3103/S1068335615080060.
- EGOROV, A.D., SHTANKO, A.N. y MININ, P.E., 2017. Selection of Viola–Jones algorithm parameters for specific conditions. *Bulletin of the Lebedev Physics Institute*, vol. 42, no. 8, pp. 244-248. ISSN 1934838X. DOI 10.3103/S1068335615080060.

- EREIZ, Z. y MUSIC, D., 2019. Scrum Without a Scrum Master. *2019 IEEE International Conference on Computer Science and Educational Informatization, CSEI 2019*, pp. 325-328. DOI 10.1109/CSEI47661.2019.8938877.
- EIAMSAARD, K., BAMRUNGTHAI, P. y JITPAKDEEBODIN, S., 2021. Smart Inventory Access Monitoring System (SIAMS) using Embedded System with Face Recognition. *JCSSE 2021 - 18th International Joint Conference on Computer Science and Software Engineering: Cybernetics for Human Beings*, pp. 9-12. DOI 10.1109/JCSSE53117.2021.9493815.
- HAYAT, F., REHMAN, A.U., ARIF, K.S., WAHAB, K. y ABBAS, M., 2019. The Influence of Agile Methodology (Scrum) on Software Project Management. *Proceedings - 20th IEEE/ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing, SNPD 2019*, pp. 145-149. DOI 10.1109/SNPD.2019.8935813.
- HENAO CÁLAD MÓNICA, 2017. CommonKADS-RT: Una Metodología para el Desarrollo de Sistemas Basados en el Conocimiento de Tiempo Real. [en línea], pp. 28-30. Disponible en: <http://users.dsic.upv.es/grupos/ia/sma/thesis/pdf/TesisMonicaH.pdf>.
- J.*, B.K. y B.*, M.M., 2020. Feature Based Face Recognition using Machine Learning Techniques'. *International Journal of Recent Technology and Engineering (IJRTE)*, vol. 8, no. 6, pp. 1313-1317. DOI 10.35940/ijrte.f7497.038620.
- K, V. y DR.S.PADMAVATHI, 2017. Facial Parts Detection Using Viola. *International Conference on Advanced Computing and Communication Systems (ICACCS -2015)*, pp. 1-4.
- LI, S.Z., 2019. Machine Translated by Google AutenMetric F1 : Un sistema de reconocimiento facial rápido y de alta precisión Resumen Machine Translated by Google. ,
- LIU, L., LUAN, X., TANG, S., GENG, H. y ZHANG, Y., 2018. A face recognition method based on residual image representation and feature extraction. *2017*

- International Conference on Security, Pattern Analysis, and Cybernetics, SPAC 2017*, vol. 2018-Janua, pp. 636-641. DOI 10.1109/SPAC.2017.8304354.
- LU, W.Y. y YANG, M., 2019. Face detection based on viola-jones algorithm applying composite features. *Proceedings - 2019 International Conference on Robots and Intelligent System, ICRIS 2019*, no. 4, pp. 82-85. DOI 10.1109/ICRIS.2019.00029.
- MANTORO, T. y AYU, M.A., 2018. Proceso de reconocimiento de múltiples caras
Uso de cascadas de Haar y métodos de caras propias. ,
- MOHAMMED, S.I., 2019. Face Recognition Based on Viola-Jones Face Detection Method and Local Binary Pattern (LBP). *Iraqi Journal of Computer, Communication, Control and System Engineering*, vol. 19, no. 3, pp. 50-55. ISSN 1811-9212. DOI 10.33103/uot.ijccce.19.3.5.
- NYEIN, T. y OO, A.N., 2019. University Classroom Attendance System Using FaceNet and Support Vector Machine. *2019 International Conference on Advanced Information Technologies, ICAIT 2019*, pp. 171-176. DOI 10.1109/AITC.2019.8921316.
- OLALERE, M. y UGWU, J.N., 2015. Organization Attendance Record System :
Frauds and A Proposed Facial Recognition Technique. , vol. 5, no. 2, pp. 1-7.
- SALEH, S.M., HUQ, S.M. y RAHMAN, M.A., 2019. Comparative Study within Scrum, Kanban, XP Focused on Their Practices. *2nd International Conference on Electrical, Computer and Communication Engineering, ECCE 2019*, pp. 1-6. DOI 10.1109/ECACE.2019.8679334.
- SAMEEM, M.S.I., QASIM, T. y BAKHAT, K., 2017. Real time recognition of human faces. *ICOSST 2016 - 2016 International Conference on Open Source Systems and Technologies, Proceedings*, pp. 62-65. DOI 10.1109/ICOSST.2016.7838578.
- SUN, Y., REN, Z. y ZHENG, W., 2022. Research on Face Recognition Algorithm Based on Image Processing. *Computational Intelligence and Neuroscience*, vol. 2022. ISSN 16875273. DOI 10.1155/2022/9224203.

- SURAKRATANASAKUL, B., 2017. Lightweight CommonKADS in knowledge intensive organization. *2017 9th International Conference on Information Technology and Electrical Engineering, ICITEE 2017*, vol. 2018-Janua, pp. 1-5. DOI 10.1109/ICITEED.2017.8250504.
- TEJ CHINIMILLI, B., ANJALI, A., KOTTURI, A., REDDY KAIPU, V. y VARMA MANDAPATI, J., 2020. Face Recognition based Attendance System using Haar Cascade and Local Binary Pattern Histogram Algorithm. *Proceedings of the 4th International Conference on Trends in Electronics and Informatics, ICOEI 2020*, no. Icoei, pp. 701-704. DOI 10.1109/ICOEI48184.2020.9143046.
- ULLAH, R., HAYAT, H., SIDDIQUI, A.A., SIDDIQUI, U.A., KHAN, J., ULLAH, F., HASSAN, S., HASAN, L., ALBATTAH, W., ISLAM, M. y KARAMI, G.M., 2022. A Real-Time Framework for Human Face Detection and Recognition in CCTV Images. *Mathematical Problems in Engineering*, vol. 2022. ISSN 15635147. DOI 10.1155/2022/3276704.
- YANG, Z., GE, W. y ZHANG, Z., 2020. Face recognition based on MTCNN and integrated application of FaceNet and LBP method. *Proceedings - 2020 2nd International Conference on Artificial Intelligence and Advanced Manufacture, AIAM 2020*, pp. 95-98. DOI 10.1109/AIAM50918.2020.00024.
- ZHOU, Y., NI, H., REN, F. y KANG, X., 2019. Face and gender recognition system based on convolutional neural networks. *Proceedings of 2019 IEEE International Conference on Mechatronics and Automation, ICMA 2019*, pp. 1091-1095. DOI 10.1109/ICMA.2019.8816192.

ANEXOS

Anexo 1 Matriz de operacionalización

Variables	Definición Conceptual	Definición Operacional	Dimensiones	Indicadores	Escala de medición
Independiente					
Reconocimiento facial	Castaño y Alonso (2019), afirmaron que el reconocimiento consiste en la clasificación de características extraídas del de la cara del sujeto se está indicando a que sujeto pertenecen esos patrones, para el diseño de clasificadores se pueden distinguir en la aproximación probabilística, optimización del criterio de error	Villa, Valencia y Berrio (2018), definieron que el reconocimiento debe ser preciso y fiable, dado que las características extraídas de la imagen de entrada deben ser detectables incluso en los cambios en la escala de la imagen, el ruido y la iluminación.	Errores de medición		
Dependiente					
Gestión de control de acceso	TIC portal (2019), indicaron que el control de acceso es una técnica de seguridad que verifica el permiso que tiene una persona o dispositivo para entrar en un área y hasta qué punto. Esta función se encuentra dentro de la gestión de identidad y acceso de una empresa.	Ramírez y Hernández (2017), indicaron que el servicio de control de acceso sirve para evitar el uso no autorizado de los recursos, es decir, permite que solo personas autorizadas pueden tener el acceso a aquellos recursos que necesiten y de los cuales tenga permiso y autorización. Se espera que el control tenga la mejor precisión posible y que sea eficaz.	Seguridad Física	Accesos no autorizados $ANA = \frac{TNA}{TA} * 100$	Razón
				Precisión $P = \frac{VP}{(VP + FP)}$	Razón

Anexo 2 Matriz de consistencia

Problemas	Objetivos	Hipótesis	Variables	Dimensión	Indicador	Metodología
General	General	General	Independiente			<p>Tipo de Estudio: Aplicada</p> <p>Diseño de estudio: Experimental</p> <p>Diseño de Estudio: Pre-Experimental</p> <p>Población: I1: Todos los registros de acceso registrados en 26 días (Mes mayo=1500) I2: Todos los registros de acceso registrados en 26 días (Mes mayo=1500)</p> <p>Muestra: I1:306 registros I2: 306 registros</p> <p>Muestreo: Aleatoria simple</p> <p>Instrumento: Ficha de registro</p>
<p>OG: ¿Cuál es el efecto del uso de una aplicación con reconocimiento facial para la gestión del control de acceso de la empresa Spirella?</p>	<p>OG: Determinar el efecto del uso de una aplicación con reconocimiento facial para la gestión del control de acceso de la empresa Spirella</p>	<p>HG: El uso de una aplicación con reconocimiento facial mejorar la gestión del control de acceso de la empresa Spirella.</p>	<p>X1: Reconocimiento facial</p>			
Específico	Específico	Específico	Dependiente			
<p>P1: ¿Cuál es el efecto del uso de una aplicación con reconocimiento facial para mejorar el control de acceso no autorizado en la gestión del control de acceso de la empresa Spirella?</p> <p>P2: ¿Cuál es el efecto de utilizar de una aplicación con reconocimiento facial para mejorar la precisión en la gestión del control de acceso de la empresa Spirella?</p>	<p>O1: Determinar el efecto del uso de una aplicación con reconocimiento facial para mejorar el control de acceso no autorizado en la gestión del control de acceso de la empresa Spirella.</p> <p>O2: Determinar el efecto del uso de una aplicación con reconocimiento facial para mejorar la precisión en la gestión en el control de acceso de la empresa Spirella</p>	<p>H1: El uso de una aplicación con reconocimiento facial mejorar el control de acceso no autorizado en la gestión del control de acceso de la empresa Spirella.</p> <p>H2: El uso de una aplicación con reconocimiento facial mejora la precisión en la gestión del control de acceso de la empresa Spirella.</p>	<p>Y1:Gestión de control de acceso</p>	Seguridad Física	<p>I1: Accesos no autorizados</p> <p>I2: Precisión</p>	

Anexo 3 Carta de aceptación



NAZARIO CRUZ TAPIA

RUC : 10096625303

La empresa Textil Spirella a cargo del gerente general Sr. Nazario Cruz Tapia, debidamente certificado con el RUC N° 10096625303.

Certifica:

Que el Sr. **NEHEMIAS DAVID FLORES REYES**, con el DNI N° 48086858, estudiante de la escuela profesional de Ingeniería de sistemas de la Universidad Cesar Vallejo, se encuentra llevando a cabo de manera satisfactoria su proyecto de investigación y desarrollo de tesis titulada "Reconocimiento facial para la gestión de control de acceso de la empresa Spirella", en nuestra entidad.

Dicha investigación está siendo desarrollada durante los semestres 2022-I de los ciclos académicos correspondientes a la carrera de Ingeniería de Sistemas.

Se expide el presente documento a solicitud del interesado, para los fines que crea conveniente.

San Juan de Lurigancho, 11 de abril de 2022


Nazario Cruz Tapia
D.N.I. 09662530
Jr. Las Rimarinas N° 125 S.J.L.
Telf.: 458-7701

Nazario Cruz Tapia
GERENTE GENERAL

Jr. Las Rimarinas N° 125 – Urb. San Hilarión S.J.L. Telf. : 017149151
Correo: spirella2@hotmail.com

Anexo 4 Validación de Metodología



TABLA DE EVALUACIÓN DE EXPERTOS METODOLOGÍA DE DESARROLLO

Apellidos y Nombres del Experto:	Alarcón Cajas, Yohan Roy
Título y/o Grado Académico:	Ingeniero de Sistemas
Doctor () Magister (X) Ingeniero (X)	Licenciado () Otro ()
Fecha:	01/04/2022

TESIS: Reconocimiento facial para la gestión de control de acceso de la empresa Spirella

Autores: Flores Reyes Nehemías David

MUY MAL (1) MALO (2) REGULAR (3) BUENO (4) EXCELENTE (5)

Mediante la tabla de evaluación de expertos usted tiene la facultad de evaluar la metodología de desarrollo de software involucradas mediante una serie de preguntas con puntuaciones especificadas al final de la tabla. Asimismo, se exhorta a las sugerencias de cambio de items que crea pertinente, con la finalidad de mejorar la coherencia de las preguntas.

ÍTEM	PREGUNTAS	METODOLOGÍA		
		GROVER	BUCHANAN	COMMON KADS
1	¿Qué metodología brinda un mejor modelo de conocimiento para el trabajo de investigación?	4	4	5
2	¿Qué metodología propone un ciclo de vida en donde se indican las fases, las actividades y los productos más relevantes en el trabajo de investigación?	3	3	5
3	¿Qué metodología está enfocado a proyectos y es más fácil de entender y más autoorganizado del equipo?	4	4	5
4	¿Qué metodología define claramente las reglas que se utilizaran en el sistema experto del trabajo de investigación?	3	3	5
5	¿Qué metodología tiene una estructura más jerárquica?	4	4	4
6	¿Qué metodología es más flexible?	3	3	5
7	¿Qué metodología cuenta con un énfasis una documentación de los procesos para el desarrollo del proyecto?	4	4	5
PUNTUACIÓN		25	25	34

SUGERENCIAS

FIRMA DEL EXPERTO

Anexo 5 Validación de Instrumentos



TABLA DE VALIDACIÓN DEL INSTRUMENTO DE EXPERTOS: Accesos no autorizados

I. DATOS GENERALES

Apellidos y Nombres del Experto: Alarcón Cajas, Yohan Roy
 Título y/o Grado Académico: Ingeniero de Sistemas

Doctor () Magister (X) Ingeniero (X) Licenciado () Otro ().....

Universidad que labora: Universidad César Vallejo
 Fecha: 01/04/2022

TESIS: Reconocimiento facial para la gestión de control de acceso de la empresa Spirella

Autores: Flores Reyes, Nehemias David

Deficiente (0-20%) Regular(21-50%) Bueno(51-70%) Muy Bueno(71-80%) Excelente(81-100%)

Mediante la evaluación de expertos usted tiene la facultad de calificar la tabla de validación del instrumento involucradas mediante una serie de indicadores con puntuaciones especificadas en la tabla, con la valoración de 0% - 100%. Asimismo, se exhorta a las sugerencias de cambio de ítems que crea pertinente, con la finalidad de mejorar la coherencia de los indicadores para su valoración.

II. ASPECTOS DE VALIDACIÓN

INDICADOR	CRITERIO	VALORACIÓN				
		0-20%	21-50%	51-70%	71-80%	81-100%
CLARIDAD	Es formulado con lenguaje apropiado.				80%	
OBJETIVIDAD	Está expresado en conducta observable.				80%	
ACTUALIDAD	Es adecuado el avance, la ciencia y tecnología.				80%	
ORGANIZACIÓN	Existe una organización lógica.				80%	
SUFICIENCIA	Comprende los aspectos de cantidad y calidad.				80%	
INTENCIONALIDAD	Adecuado para valorar los aspectos del sistema metodológico y científico.				80%	
CONSISTENCIA	Está basado en aspectos teóricos y científicos.				80%	
COHERENCIA	En los datos respecto al indicador.				80%	
METODOLOGÍA	Responde al propósito de investigación.				80%	
PERTENENCIA	El instrumento es adecuado al tipo de investigación.				80%	
TOTAL					80%	

III. PROMEDIO DE VALIDACIÓN

80

IV. OPCIÓN DE APLICABILIDAD

(X) El instrumento puede ser aplicado, tal como está elaborado

El instrumento debe ser mejorado antes de ser
 () aplicado

FIRMA DEL EXPERTO



TABLA DE VALIDACIÓN DEL INSTRUMENTO DE EXPERTOS: Precisión

I. DATOS GENERALES

Apellidos y Nombres del Experto: Alarcón Cajas, Yohan Roy
 Título y/o Grado Académico: Ingeniería de Sistemas

Doctor () Magister (X) Ingeniero (X) Licenciado () Otro ().....

Universidad que labora: Universidad César Vallejo
 Fecha: 01/04/2022

TESIS: Reconocimiento facial para la gestión de control de acceso de la empresa Spirella

Autores: Flores Reyes, Nehemias David

Deficiente (0-20%) Regular(21-50%) Bueno(51-70%) Muy Bueno(71-80%) Excelente(81-100%)

Mediante la evaluación de expertos usted tiene la facultad de calificar la tabla de validación del instrumento involucradas mediante una serie de indicadores con puntuaciones especificadas en la tabla, con la valoración de 0% - 100%. Asimismo, se exhorta a las sugerencias de cambio de ítems que crea pertinente, con la finalidad de mejorar la coherencia de los indicadores para su valoración.

II. ASPECTOS DE VALIDACIÓN

INDICADOR	CRITERIO	VALORACIÓN				
		0-20%	21-50%	51-70%	71-80%	81-100%
CLARIDAD	Es formulado con lenguaje apropiado.				80%	
OBJETIVIDAD	Esta expresado en conducta observable.				80%	
ACTUALIDAD	Es adecuado el avance, la ciencia y tecnología.				80%	
ORGANIZACIÓN	Existe una organización lógica.				80%	
SUFICIENCIA	Comprende los aspectos de cantidad y calidad.				80%	
INTENCIONALIDAD	Adecuado para valorar los aspectos del sistema metodológico y científico.				80%	
CONSISTENCIA	Está basado en aspectos teóricos y científicos.				80%	
COHERENCIA	En los datos respecto al indicador.				80%	
METODOLOGÍA	Responde al propósito de investigación.				80%	
PERTENENCIA	El instrumento es adecuado al tipo de investigación.				80%	
TOTAL					80%	

III. PROMEDIO DE VALIDACIÓN

80

IV. OPCIÓN DE APLICABILIDAD

(X) El instrumento puede ser aplicado, tal como está elaborado

El instrumento debe ser mejorado antes de ser
 () aplicado

FIRMA DEL EXPERTO

Ficha de registro de Accesos no autorizados

<u>Autores</u>	Flores Reyes Nehemias David
<u>Objetivo</u>	Recolectar datos de acceso no autorizados
<u>Periodo</u>	En un periodo de 26 días
<u>Fecha de aprobación</u>	01-04-2022
<u>Tipo de Prueba</u>	PRE-TEST

N° Ficha de registro		1		
Variable Dependiente		Dimensión	Indicador	Formula
Gestión del control de acceso		Seguridad Física	Accesos no autorizados	$ANA = \frac{TNA}{TA} * 100$
Fecha	Día	Abril 2022		Acceso no autorizados
		TNA	TA	
2/04/2022	1	3	11	27%
3/04/2022	2	4	12	33%
4/04/2022	3	4	8	50%
5/04/2022	4	6	14	43%
6/04/2022	5	5	12	42%
7/04/2022	6	7	15	47%
8/04/2022	7	5	14	36%
9/04/2022	8	4	11	36%
10/04/2022	9	2	9	22%
11/04/2022	10	4	12	33%
12/04/2022	11	3	10	30%
13/04/2022	12	4	14	29%
14/04/2022	13	3	12	25%
15/04/2022	14	4	14	29%
16/04/2022	15	3	10	30%
17/04/2022	16	3	12	25%
18/04/2022	17	4	14	29%
19/04/2022	18	5	10	50%
20/04/2022	19	4	12	33%
21/04/2022	20	3	13	23%
22/04/2022	21	3	6	50%
23/04/2022	22	4	13	31%
24/04/2022	23	4	11	36%
25/04/2022	24	5	14	36%
26/04/2022	25	4	10	40%
27/04/2022	26	3	13	23%

Ficha de registro de Accesos no autorizados

Autores	Flores Reyes Nehemias David
Objetivo	Recolectar datos de acceso no autorizados
Periodo	En un periodo de 26 días
Fecha de aprobación	01-04-2022
Tipo de Prueba	RETEST-TEST

N° Ficha de registro		1		
Variable Dependiente		Dimensión	Indicador	Formula
Gestión del control de acceso		Seguridad Física	Accesos no autorizados	$ANA = \frac{TNA}{TA} * 100$
Fecha	Día	Mayo 2022		Acceso no autorizados
		TNA	TA	
2/05/2022	1	7	11	64%
3/05/2022	2	5	12	42%
4/05/2022	3	4	8	50%
5/05/2022	4	2	14	14%
6/05/2022	5	4	11	36%
7/05/2022	6	3	15	20%
8/05/2022	7	4	14	29%
9/05/2022	8	3	12	25%
10/05/2022	9	4	9	44%
11/05/2022	10	5	12	42%
12/05/2022	11	3	13	23%
13/05/2022	12	3	12	25%
14/05/2022	13	4	12	33%
15/05/2022	14	4	14	29%
16/05/2022	15	5	10	50%
17/05/2022	16	4	12	33%
18/05/2022	17	3	14	21%
19/05/2022	18	3	11	27%
20/05/2022	19	4	12	33%
21/05/2022	20	5	8	63%
22/05/2022	21	4	10	40%
23/05/2022	22	3	13	23%
24/05/2022	23	4	11	36%
25/05/2022	24	4	12	33%
26/05/2022	25	6	10	60%
27/05/2022	26	5	14	36%

Ficha de registro de Accesos no autorizados

<u>Autores</u>	Flores Reyes Nehemias David
<u>Objetivo</u>	Recolectar datos de acceso no autorizados
<u>Periodo</u>	En un periodo de 26 días
<u>Fecha de aprobación</u>	01-04-2022
<u>Tipo de Prueba</u>	POST-TEST

N° Ficha de registro		1		
Variable Dependiente		Dimensión	Indicador	Formula
Gestión del control de acceso		Seguridad Física	Accesos no autorizados	$ANA = \frac{TNA}{TA} * 100$
Fecha	Día	Junio 2022		Acceso no autorizados
		TNA	TA	
2/06/2022	1	2	12	17%
3/06/2022	2	1	12	8%
4/06/2022	3	1	14	7%
5/06/2022	4	2	10	20%
6/06/2022	5	1	12	8%
7/06/2022	6	1	9	11%
8/06/2022	7	1	12	8%
9/06/2022	8	1	10	10%
10/06/2022	9	1	14	7%
11/06/2022	10	1	14	7%
12/06/2022	11	2	12	17%
13/06/2022	12	1	15	7%
14/06/2022	13	1	14	7%
15/06/2022	14	1	11	9%
16/06/2022	15	2	10	20%
17/06/2022	16	1	12	8%
18/06/2022	17	1	13	8%
19/06/2022	18	1	9	11%
20/06/2022	19	1	11	9%
21/06/2022	20	1	12	8%
22/06/2022	21	1	8	13%
23/06/2022	22	1	14	7%
24/06/2022	23	2	12	17%
25/06/2022	24	1	14	7%
26/06/2022	25	1	11	9%
27/06/2022	26	1	9	11%

Ficha de registro de Precisión

Autores	Flores Reyes Nehemias David
Objetivo	Recolectar datos sobre la precisión
Periodo	En un periodo de 26 días
Fecha de aprobación	01-04-2022
Tipo de Prueba	PRE- TEST

N° Ficha de registro		2		
Variable Dependiente		Dimensión	Indicador	Formula
Gestión del control de acceso		Seguridad Física	Precisión	$P = \frac{VP}{(VP + FP)}$
Fecha	Día	Abril 2022		Precisión
		VP	FP	
2/04/2022	1	11	2	0.85
3/04/2022	2	12	1	0.92
4/04/2022	3	8	2	0.80
5/04/2022	4	14	1	0.93
6/04/2022	5	12	2	0.86
7/04/2022	6	15	1	0.94
8/04/2022	7	14	1	0.93
9/04/2022	8	11	2	0.85
10/04/2022	9	9	2	0.82
11/04/2022	10	12	1	0.92
12/04/2022	11	10	1	0.91
13/04/2022	12	14	2	0.88
14/04/2022	13	12	1	0.92
15/04/2022	14	14	1	0.93
16/04/2022	15	10	2	0.83
17/04/2022	16	12	2	0.86
18/04/2022	17	14	1	0.93
19/04/2022	18	10	2	0.83
20/04/2022	19	12	1	0.92
21/04/2022	20	13	2	0.87
22/04/2022	21	6	1	0.86
23/04/2022	22	13	2	0.87
24/04/2022	23	11	3	0.79
25/04/2022	24	14	1	0.93
26/04/2022	25	10	2	0.83
27/04/2022	26	13	1	0.93

Ficha de registro de Precisión de control de acceso

Autores	Flores Reyes Nehemias David
Objetivo	Recolectar datos sobre la precisión
Periodo	En un periodo de 26 días
Fecha de aprobación	01-04-2022
Tipo de Prueba	RETEST- TEST

N° Ficha de registro		2		
Variable Dependiente		Dimensión	Indicador	Formula
Gestión del control de acceso		Seguridad Física	Precisión	$P = \frac{VP}{(VP + FP)}$
Fecha	Día	Mayo 2022		Precisión
		VP	FP	
2/05/2022	1	12	3	0.80
3/05/2022	2	12	1	0.92
4/05/2022	3	8	2	0.80
5/05/2022	4	15	2	0.88
6/05/2022	5	12	2	0.86
7/05/2022	6	15	1	0.94
8/05/2022	7	14	1	0.93
9/05/2022	8	11	2	0.85
10/05/2022	9	10	2	0.83
11/05/2022	10	12	1	0.92
12/05/2022	11	10	1	0.91
13/05/2022	12	13	2	0.87
14/05/2022	13	12	1	0.92
15/05/2022	14	15	1	0.94
16/05/2022	15	10	2	0.83
17/05/2022	16	13	1	0.93
18/05/2022	17	14	1	0.93
19/05/2022	18	10	2	0.83
20/05/2022	19	12	1	0.92
21/05/2022	20	12	2	0.86
22/05/2022	21	6	1	0.86
23/05/2022	22	13	2	0.87
24/05/2022	23	11	4	0.73
25/05/2022	24	14	1	0.93
26/05/2022	25	10	2	0.83
27/05/2022	26	12	1	0.92

Ficha de registro de Precisión de control de acceso

Autores	Flores Reyes Nehemias David
Objetivo	Recolectar datos sobre la precisión
Periodo	En un periodo de 26 días
Fecha de aprobación	01-04-2022
Tipo de Prueba	POST- TEST

N° Ficha de registro		2		
Variable Dependiente		Dimensión	Indicador	Formula
Gestión del control de acceso		Seguridad Física	Precisión	$P = \frac{VP}{(VP + FP)}$
Fecha	Día	Junio 2022		Precisión
		VP	FP	
2/06/2022	1	11	0	1.00
3/06/2022	2	12	0	1.00
4/06/2022	3	8	0	1.00
5/06/2022	4	14	0	1.00
6/06/2022	5	12	0	1.00
7/06/2022	6	15	0	1.00
8/06/2022	7	14	0	1.00
9/06/2022	8	11	0	1.00
10/06/2022	9	9	1	0.90
11/06/2022	10	12	0	1.00
12/06/2022	11	10	0	1.00
13/06/2022	12	14	0	1.00
14/06/2022	13	12	0	1.00
15/06/2022	14	14	0	1.00
16/06/2022	15	10	0	1.00
17/06/2022	16	12	0	1.00
18/06/2022	17	14	0	1.00
19/06/2022	18	10	0	1.00
20/06/2022	19	12	0	1.00
21/06/2022	20	13	0	1.00
22/06/2022	21	6	0	1.00
23/06/2022	22	13	0	1.00
24/06/2022	23	11	1	0.92
25/06/2022	24	14	0	1.00
26/06/2022	25	10	0	1.00
27/06/2022	26	13	0	1.00

Diagrama de base de datos

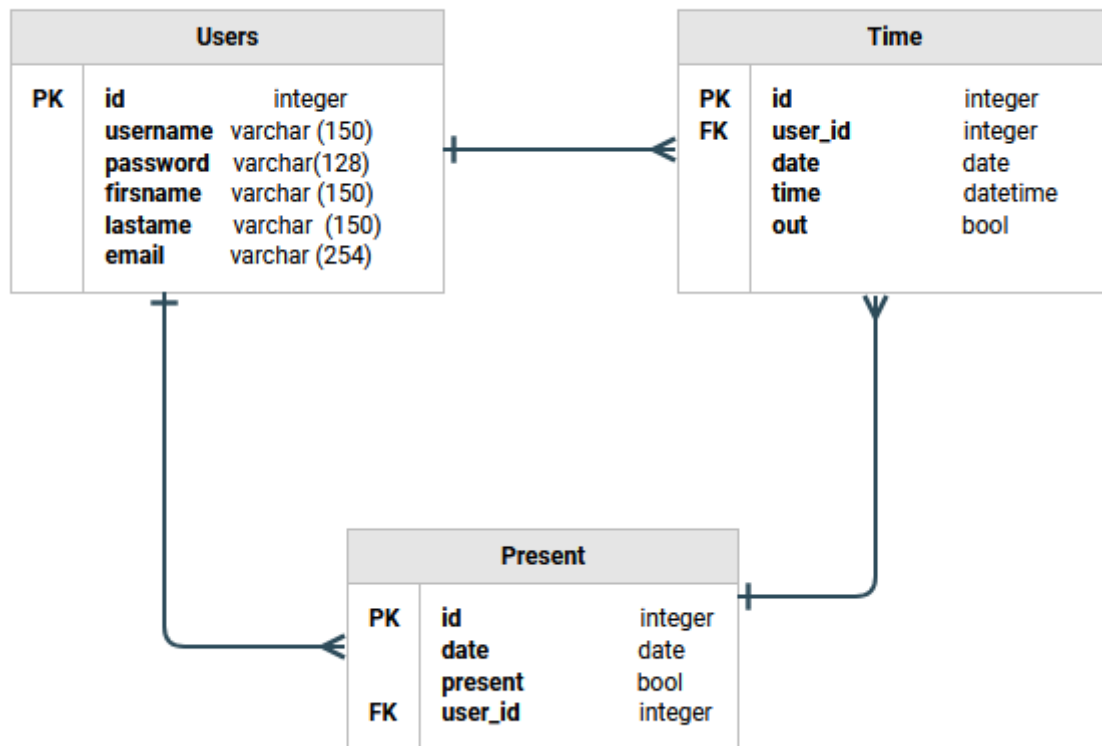


Figura 8 Diagrama de base de datos

Definición de módulos del sistema

Se definen los módulos: Registro de asistencia, Acceso y sesión, Registros de personal, Entrenamiento, Reportes de asistencia, Panel de control.

En el módulo de Registro de Asistencia, el personal de la empresa puede marcar su asistencia, se queda registrada de forma automática la hora de ingreso y salida.

En el módulo de Acceso y Sesión, el usuario del sistema puede logearse para ingresar al panel de administración del sistema y usar las diversas opciones.

En el módulo de Registro de Personal el usuario del sistema puede agregar usuarios al sistema y registrar trabajadores nuevos.

En el módulo de Entrenamiento, se ejecutará el algoritmo de reconocimiento para analizar los rostros e identificar a la persona.

En el módulo de Reporte de asistencia, se permite emitir un reporte de asistencia y horas trabajadas ya sea por día o por empleado.

Cuadro comparativo de metodologías

Tabla 10 Tabla comparativa de metodologías

METODOLOGÍA		
GROVER	BUCHANAN	COMMON KADS
Permite definir claramente las reglas que se utilizaron en el sistema experto y las estructuras que permitieron representarlo.	Este método define una serie de etapas de la documentación de los procesos	Principal cualidad es el planteamiento del desarrollo de modelos que reflejan diferentes vistas del proyecto
Representa la descripción del problema.	Propone con énfasis una documentación de los procesos	Ofrece un marco para la especificación del conocimiento
Consiste en la creación de escenarios nuevos de conocimiento	Se basa en el ciclo de vida en cascada utilizado en los inicios de la ingeniería de software	Propone un ciclo de vida en donde se indican las fases, las actividades y los productos más relevantes para un proyecto
Para obtener el conocimiento fundamental usa una técnica de simulación de proceso construyendo verbalmente las reglas de razonamiento que utiliza.	Se identifica los participantes y roles, los recursos, fuentes de conocimiento	Combinando un conjunto de modelos de conocimiento reutilizable para unas tareas que se realizan frecuentemente
Cada fase está acompañada de una documentación detallada que reemplazan parcialmente al experto.	La característica más importante constante relación ente el Ingeniero de conocimiento y el experto del área	Le permiten al sistema coordinar las actividades con otros agentes y ser más que un sistema basado en el conocimiento para ser un sistema que coopera con otros.

Código

Login

```
# Create your views here.
def home(request):

    return render(request, 'recognition/home.html')

@login_required
def dashboard(request):
    if(request.user.username=='admin'):
        print("admin")
        return render(request, 'recognition/admin_dashboard.html')
    else:
        print("not admin")

        return render(request, 'recognition/employee_dashboard.html')
```

Figura 2 Login de usuario

Entrenamiento

```
@login_required
def train(request):
    if request.user.username != 'admin':
        return redirect('not-authorized')
    training_dir = 'face_recognition_data/training_dataset'

    count = 0
    for person_name in os.listdir(training_dir):
        curr_directory = os.path.join(training_dir, person_name)
        if not os.path.isdir(curr_directory):
            continue
        for imagefile in image_files_in_folder(curr_directory):
            count += 1

    X = []
    y = []
    i = 0
    for person_name in os.listdir(training_dir):
        print(str(person_name))
        curr_directory = os.path.join(training_dir, person_name)
        if not os.path.isdir(curr_directory):
            continue
        for imagefile in image_files_in_folder(curr_directory):
            print(str(imagefile))
            image = cv2.imread(imagefile)
            try:
                X.append((face_recognition.face_encodings(image)[0]).tolist())

                y.append(person_name)
                i += 1
            except:
                print("removed")
                os.remove(imagefile)

    targets = np.array(y)
    encoder = LabelEncoder()
    encoder.fit(y)
    y = encoder.transform(y)
    X1 = np.array(X)
    print("shape: " + str(X1.shape))
    np.save('face_recognition_data/classes.npy', encoder.classes_)
    svc = SVC(kernel='linear', probability=True)
    svc.fit(X1, y)
    svc_save_path = "face_recognition_data/svc.sav"
    with open(svc_save_path, 'wb') as f:
        pickle.dump(svc, f)

    visualize_Data(X1, targets)
    messages.success(request, f'Training Complete.')
    return render(request, "recognition/train.html")
```

Figura 3 Código de entrenamiento del algoritmo

Registrar Asistencia Ingreso y Salida

```
detector = dlib.get_frontal_face_detector()

predictor = dlib.shape_predictor('face_recognition_data/shape_predictor_68_face_landmarks.dat')
svc_save_path="face_recognition_data/svc.sav"

with open(svc_save_path, 'rb') as f:
    svc = pickle.load(f)
fa = FaceAligner(predictor , desiredFaceWidth = 96)
encoder=LabelEncoder()
encoder.classes_ = np.load('face_recognition_data/classes.npy')

faces_encodings = np.zeros((1,128))
no_of_faces = len(svc.predict_proba(faces_encodings)[0])
count = dict()
present = dict()
log_time = dict()
start = dict()
for i in range(no_of_faces):
    count[encoder.inverse_transform([i])[0]] = 0
    present[encoder.inverse_transform([i])[0]] = False

vs = VideoStream(src=0).start()

sampleNum = 0

while(True):

    frame = vs.read()

    frame = imutils.resize(frame ,width = 800)

    gray_frame = cv2.cvtColor(frame, cv2.COLOR_BGR2GRAY)

    faces = detector(gray_frame,0)

    for face in faces:
        print("INFO : inside for loop")
        (x,y,w,h) = face_utils.rect_to_bb(face)
```

Figura 4 Marcar la asistencia ingreso y salida

Agregar Personal y registrar Fotos

```
@login_required
def add_photos(request):
    if request.user.username != 'admin':
        return redirect('not-authorised')
    if request.method == 'POST':
        form = usernameForm(request.POST)
        data = request.POST.copy()
        username = data.get('username')
        if username_present(username):
            create_dataset(username)
            messages.success(request, f'Dataset Created')
            return redirect('add-photos')
        else:
            messages.warning(request, f'No such username found. Please register employee first.')
            return redirect('dashboard')
    else:
        form = usernameForm()
        return render(request, 'recognition/add_photos.html', {'form': form})
```

Figura 5 Registrar personal

```

def create_dataset(username):
    id = username
    if(os.path.exists('face_recognition_data/training_dataset/{}/'.format(id))==False):
        os.makedirs('face_recognition_data/training_dataset/{}/'.format(id))
    directory='face_recognition_data/training_dataset/{}/'.format(id)

    print("[INFO] Loading the facial detector")
    detector = dlib.get_frontal_face_detector()
    predictor = dlib.shape_predictor('face_recognition_data/shape_predictor_68_face_landmarks.dat')
    fa = FaceAligner(predictor , desiredFaceWidth = 96)

    print("[INFO] Initializing Video stream")
    vs = VideoStream(src=0).start()

    while(True):

        frame = vs.read()

        frame = imutils.resize(frame ,width = 800)

        gray_frame = cv2.cvtColor(frame, cv2.COLOR_BGR2GRAY)

        for face in faces:
            print("inside for loop")
            (x,y,w,h) = face_utils.rect_to_bb(face)

            face_aligned = fa.align(frame,gray_frame,face)

            sampleNum = sampleNum+1

            if face is None:
                print("face is none")
                continue

            cv2.imwrite(directory+'/' +str(sampleNum)+'.jpg' , face_aligned)
            face_aligned = imutils.resize(face_aligned ,width = 400)

            cv2.rectangle(frame,(x,y),(x+w,y+h),(0,255,0),1)

```

Figura 6 Agregar fotos

Reporte de asistencia por empleado

```
@login_required
def view_attendance_employee(request):
    if request.user.username != 'admin':
        return redirect('not-authorized')
    time_qs=None
    present_qs=None
    qs=None

    if request.method == 'POST':
        form=UsernameAndDateForm(request.POST)
        if form.is_valid():
            username=form.cleaned_data.get('username')
            if username_present(username):

                u=User.objects.get(username=username)

                time_qs=Time.objects.filter(user=u)
                present_qs=Present.objects.filter(user=u)
                date_from=form.cleaned_data.get('date_from')
                date_to=form.cleaned_data.get('date_to')

                if date_to < date_from:
                    messages.warning(request, f'Invalid date selection.')
                    return redirect('view-attendance-employee')
                else:

                    time_qs=time_qs.filter(date__gte=date_from).filter(date__lte=date_to).order_by
                    present_qs=present_qs.filter(date__gte=date_from).filter(date__lte=date_to).or

                if (len(time_qs)>0 or len(present_qs)>0):
                    qs=hours_vs_date_given_employee(present_qs,time_qs,admin=True)
                    return render(request,'recognition/view_attendance_employee.html', {'form':
                else:
                    #print("inside qs is None")
                    messages.warning(request, f'No records for selected duration.')
                    return redirect('view-attendance-employee')
```

Figura 7 Reporte de asistencia por empleado

Reporte de asistencia por día

```
login_required
def view_attendance_date(request):
    if request.user.username != 'admin':
        return redirect('not-authorized')
    qs=None
    time_qs=None
    present_qs=None

    if request.method == 'POST':
        form=DateForm(request.POST)
        if form.is_valid():
            date=form.cleaned_data.get('date')
            print("date:"+ str(date))
            time_qs=Time.objects.filter(date=date)
            present_qs=Present.objects.filter(date=date)
            if (len(time_qs)>0 or len(present_qs)>0):
                qs=hours_vs_employee_given_date(present_qs,time_qs)

            return render(request,'recognition/view_attendance_date.html',
        else:
            messages.warning(request, f'No records for selected date.')
            return redirect('view-attendance-date')
```

Figura 8 Reporte de asistencia por día

Sistema en funcionamiento



Figura 9 Menú principal del sistema

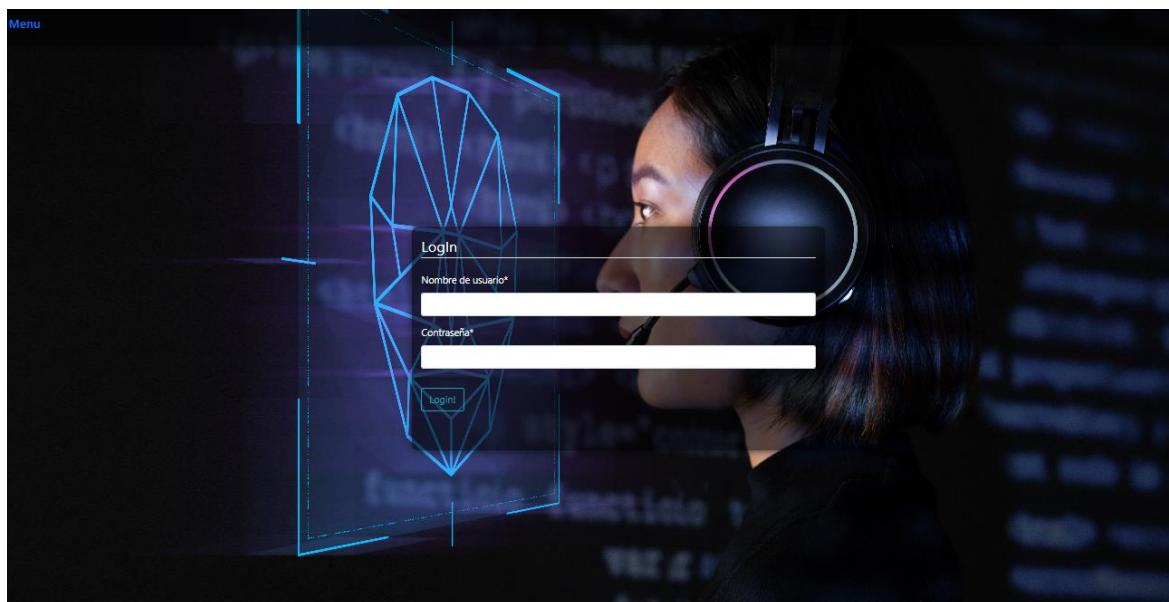


Figura 10 Login del sistema de asistencia

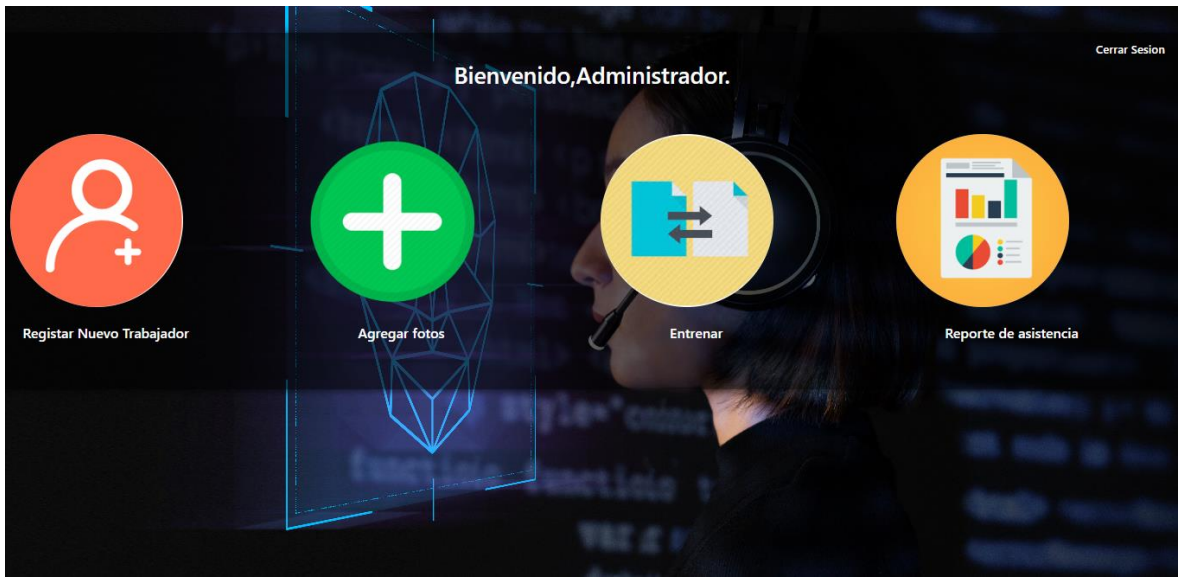


Figura 11 Panel de administración del sistema

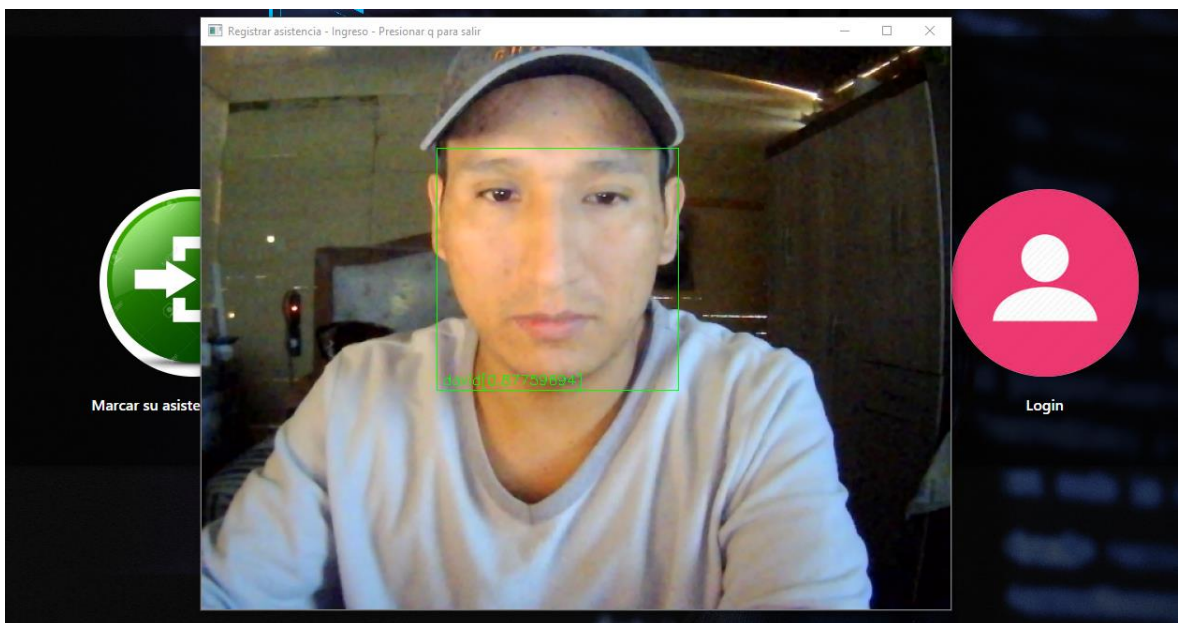
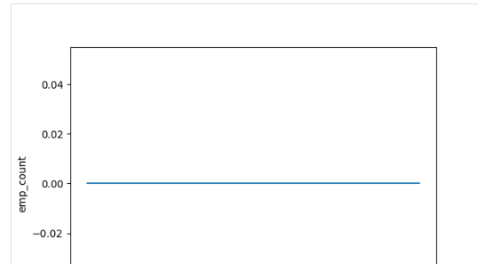


Figura 12 Reconocimiento facial para asistencia ingreso

Estadísticas de hoy



Semana Pasada



Esta semana

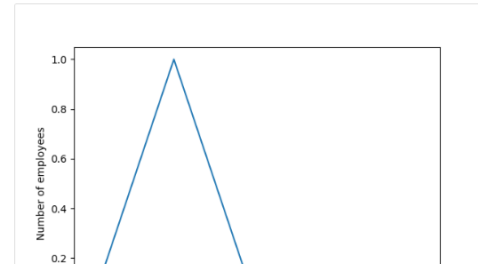


Figura 13 Menú de reportes de asistencia



UNIVERSIDAD CÉSAR VALLEJO

**FACULTAD DE INGENIERÍA Y ARQUITECTURA
ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS**

Declaratoria de Autenticidad del Asesor

Yo, ALARCON CAJAS YOHAN ROY, docente de la FACULTAD DE INGENIERÍA Y ARQUITECTURA de la escuela profesional de INGENIERÍA DE SISTEMAS de la UNIVERSIDAD CÉSAR VALLEJO SAC - LIMA NORTE, asesor de Tesis titulada: "Reconocimiento facial para la gestión de control de acceso de la empresa Spirella", cuyo autor es FLORES REYES NEHEMIAS DAVID, constato que la investigación cumple con el índice de similitud establecido, y 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, 16 de Julio del 2022

Apellidos y Nombres del Asesor:	Firma
ALARCON CAJAS YOHAN ROY DNI: 46189705 ORCID 0000-0001-5382-3754	Firmado digitalmente por: YALARCONCA el 23-07- 2022 16:26:08

Código documento Trilce: TRI - 0348754