



UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE INGENIERÍA Y ARQUITECTURA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

Sistema de Reconocimiento facial con aprendizaje profundo para el control de acceso del almacén, en la Clínica Multident Buenos Aires,
2022

TESIS PARA OBTENER EL TÍTULO PROFESIONAL DE:

Ingeniero de Sistemas

AUTORES:

Chavez Vasquez, Nicolas (orcid.org/0000-0002-3705-8324)

Valentin Arana, Armando Jean Pierre (orcid.org/0000-0002-2016-6302)

ASESOR:

Mgr. Cohello Aguirre, Rogelio Gonzalo (orcid.org/0000-0001-5526-5231)

LÍNEA DE INVESTIGACIÓN:

Sistema de información y comunicaciones

LÍNEA DE RESPONSABILIDAD SOCIAL UNIVERSITARIA:

Desarrollo Económico, empleo y emprendimiento

LIMA - PERÚ

2022

DEDICATORIA:

Queremos dedicar esta tesis a Dios que es la fuerza que nos empuja día a día a ser mejores personas y poder culminar nuestras metas trazadas.

A nuestros Padres por su dedicación y amor hacia nosotros, que nos inspiran a poder alcanzar nuestros sueños y metas. Por su sacrificio diario que nos permitieron llegar hasta aquí y poder convertirnos en Ingenieros. Nos sentimos muy orgullosos de tener unos padres luchadores y sobre todo buenas personas.

AGRADECIMIENTO:

Queremos agradecer a Dios por sus bendiciones diarias que derrama sobre nosotros y nos brinda esa paz que nos permite concentrarnos en nuestros deberes.

Darle las Gracias a nuestros Padres por sus consejos y apoyo desinteresado. Gracias por confiar en nosotros al enseñarnos valores y principios que nos hacen buenas personas.

También queremos agradecer a nuestro asesor Mgtr. Rogelio Cohello Aguirre por su tiempo y apoyo en la elaboración de nuestro Proyecto de Tesis.

ÍNDICE DE CONTENIDOS

DEDICATORIA	ii
AGRADECIMIENTO	iii
ÍNDICE DE CONTENIDOS	iv
ÍNDICE DE TABLAS	v
ÍNDICE DE GRÁFICOS Y FIGURAS	vi
RESUMEN	vii
ABSTRACT	viii
I. INTRODUCCIÓN	1
II.MARCO TEÓRICO	4
III. METODOLOGÍA	18
3.1. Tipo y diseño de Investigación	18
3.2. Variables y operacionalización	18
3.3. Población, muestra, muestreo	19
3.4. Técnicas e instrumentos de recolección de datos	21
3.5. Procedimientos	23
3.6. Método de análisis de datos	23
3.7. Aspectos éticos	25
IV.RESULTADOS	27
V. DISCUSIÓN	37
VI. CONCLUSIONES	38
VII. RECOMENDACIONES	39
REFERENCIAS	40
ANEXOS	46

ÍNDICE DE TABLAS

Tabla 1. Criterios Básicos	12
Tabla 2. Matriz de Confusión	15
Tabla 3. Criterios Básicos	16
Tabla 4. Matriz de Operacionalización	19
Tabla 5. Población	20
Tabla 6. Juicio de expertos	21
Tabla 7. Técnica e instrumentos utilizados	22
Tabla 8. Medidas para test y retest	22
Tabla 9. Estadística descriptiva de control de Acceso	27
Tabla 10. Estadística descriptiva de precisión de Acceso	28
Tabla 11. Prueba de Normalidad de Control de Acceso Autorizado	29
Tabla 12. Prueba de Normalidad de Precisión de Acceso	31
Tabla 13. Prueba de rangos Wilcoxon para el Control de Acceso Autorizado	33
Tabla 14. Prueba de Wilcoxon para el Control de Acceso Autorizado	34
Tabla 15. Prueba T para la Precisión de Acceso	35

ÍNDICE DE FIGURAS

Figura 1. Componentes de los sistemas biométricos	12
Figura 2. Formula de acceso autorizado	14
Figura 3. Formula de precisión	15
Figura 4. Diseño de investigación.....	18
Figura 5. Gráficos de control de acceso autorizado pre y post Test	27
Figura 6. Gráficos de precisión de acceso pre y post Test	28
Figura 7. Histograma de Control de Acceso Autorizado Pre Test	30
Figura 8. Histograma de Control de Acceso Autorizado Post Test	30
Figura 9. Histograma de Precisión de Acceso Pre Test	31
Figura 10. Histograma de Precisión de Acceso Post Test	32
Figura 11. Zona de Rechazo	35
Figura 12. Tabla T Student 2	36

RESUMEN

El uso de Sistemas de Reconocimiento Facial con aprendizaje profundo ha cobrado mucha fuerza en los últimos años, esto es debido a la seguridad y accesibilidad que nos brinda para los diferentes procesos que pueden existir en una empresa, institución educativa, etc. A pesar de haber aumentado su uso estos últimos años, todavía hay un cierto grado de desconocimiento o incertidumbre en su aplicación puesto que los avances tecnológicos son cada vez más rápidos y muchas veces los códigos y aplicaciones experimentan cambios o modificaciones en tiempos cada vez más cortos. Es por ello que en el presente trabajo desarrollamos un Sistema de Reconocimiento Facial con aprendizaje profundo de control de acceso para el almacén de la Clínica Multident Buenos Aires, en la cual nos permitirá poder llevar un mejor control de las personas que tienen acceso y las que no están autorizadas de ingresar al almacén y poder evitar pérdidas de materiales odontológicos. Este proyecto ha sido implementado bajo la metodología XP ya que nos permite poder tener una respuesta rápida a los cambios que puedan ocurrir durante el proceso, de igual manera se utilizó para el reconocimiento facial el aprendizaje profundo puesto que nos permite tener una mejor precisión para los rostros a identificar. Finalmente se obtiene que el aplicativo redujo significativamente la pérdida de materiales, también se redujo significativamente el ingreso de personas no autorizadas al almacén que muchas veces generaban molestia a los dueños de la Clínica.

Palabras Clave: Aprendizaje Profundo, Reconocimiento facial, Metodología XP.

ABSTRACT

The use of Facial Recognition Systems with deep learning has gained a lot of strength in recent years, this is due to the security and accessibility that it offers us for the different processes that may exist in a company, educational institution, etc. Despite having increased its use in recent years, there is still a certain degree of ignorance or uncertainty in its application since technological advances are faster and faster and many times codes and applications undergo changes or modifications in shorter and shorter times. That is why in the present work we develop a Facial Recognition System with deep learning of access control for the warehouse of the Clinica Multident Buenos Aires, in which it will allow us to be able to better control the people who have access and those who do not. they are not authorized to enter the warehouse and be able to avoid loss of dental materials. This work has been implemented under the Xp methodology since it allows us to have a quick response to the changes that may occur during the process, in the same way deep learning was used for facial recognition since it allows us to have a better precision for the faces to identify. Finally, it is obtained that the application significantly reduced the loss of materials, also the entry of unauthorized persons to the warehouse was significantly reduced, which often caused annoyance to the owners of the Clinic.

Keywords: Deep Learning, Facial Recognition, Xp Methodology.

I. Introducción

El sistema de reconocimiento facial ha ido evolucionando desde hace 50 años, cuando un grupo de estudiantes comenzó a trabajar con el objetivo de probar que las computadoras podían reconocer rostros humanos. Las mejoras tecnológicas en las cámaras de video han hecho posible que se puedan realizar reconocimientos faciales. El uso que se le ha dado a esta tecnología es diverso, pero principalmente se usan para el proceso de seguridad como el control de acceso, etc. En cuanto al control de acceso con el transcurrir del tiempo, se ha ido perfeccionando y no solo abarca el acceso físico sino también el lógico. Esta tecnología está siendo usada para tener un mejor control en la seguridad de las empresas, de la misma manera se usa para el control de asistencia facilitando en gran medida a los trabajadores de recursos humanos para realizar un mejor reporte en relación a las horas extras, tardanza etc. Por otro lado, de manera lógica se usa en el acceso para programas web o de escritorio permitiendo así que únicamente la persona asignada pueda acceder, protegiendo mucho más nuestros activos de información.

Clínica Multident Buenos Aires es una empresa independiente, cuya actividad principalmente es la salud y estética bucal. Además, ha sido creada el 03 de mayo de 2018, con RUC 20603153104, razón social ODONTO.BK E.I.R.L., su actividad comercial actividades de médicos y odontólogos. Su sede principal está ubicada en la av. Wiese mza. D1 lote. 27 Asc. de comerciantes industriales y artesanos (a dos cuadras de la estación santa rosa) lima - lima - San Juan de Lurigancho.

La Clínica Multident Buenos Aires no tenía un control de acceso adecuado en las distintas áreas de la empresa, en este caso específico en el área de almacén, además, por el área de almacén se llega al archivero contable, el personal que tiene a cargo la supervisión muchas veces no se da abasto para estar pendiente en el área en mención. Además, hubo incidencias de personas no autorizadas en el área laboral generando inseguridad de los bienes y ralentización del trabajo del personal, ya que muchas veces el personal de diferentes áreas se pone a conversar o hacer otras cosas que no deben según su rol de trabajo, por lo cual indicó el autor Ferro (2020), define que un sistema biométrico permite controlar el acceso del personal o usuario a una cierta área o lugar específico por medio de la

identificación basada en características únicas de la persona (p.134). Por lo tanto, la empresa busca consolidarse, adaptándose a nuevas tecnologías con la finalidad de cumplir sus objetivos propuestos en todos los ámbitos. Por ello, se precisó la urgencia de implementar un sistema de reconocimiento facial para mejorar la el control de acceso de en el área de almacén, permitiendo alcanzar y fijar los objetivos empresariales propuestos, para que pudiera llegar a mantenerse la empresa siempre a la vanguardia.

A través de la situación que tenía la Clínica Multident Buenos Aires se presentó la formulación del planteamiento del problema general: ¿De qué manera influye el Sistema de Reconocimiento Facial para mejorar el control de acceso en el área de almacén de la Clínica Multident Buenos Aires? además de unos problemas específicos, los cuales son: ¿Cuál será el efecto del Sistema de Reconocimiento Facial para el control de acceso autorizado en el área de almacén de la Clínica Multident Buenos Aires? y ¿Cuál será la precisión de un Sistema de Reconocimiento Facial en el control de acceso de la Clínica Multident Buenos Aires?

Esta investigación se justificó tecnológicamente, en base a la necesidad de una solución para la problemática, a través del software que identifica al personal autorizado en el área de almacén, enviando alertas al sistema con sus respectivos datos, dando una innovación tecnológica del sistema de reconocimiento facial que ayudara a resolver algunos inconvenientes como la precisión y control de acceso del personal, por ello indica Carrasco (2019), las investigaciones en base a los resultados enfoca que incrementa el desarrollo de las actividades por medio de diseños e instalaciones tecnológicas de software y equipos. (p. 120). La investigación se justifica económicamente, por el desarrollo de la programación del software es open source y la empresa cuenta con una parte de dispositivos para la implementación, esta justificación indicó Carrasco (2019), punto de inicio para la implementación de proyectos se primeriza los beneficios y acuerdos de los resultados económicamente mediante censos. (p. 120). La investigación se justificó operativamente, porque se tiene identificado al personal en el sistema con su respectiva foto y área laboral, permitiendo la identificación del personal en el ingreso al almacén, además el sistema emite una alerta al WhatsApp de seguridad

de personas no autorizadas en el área, con la respectiva foto y datos si fuera del personal, todo a tiempo real, esta justificación mencionó Gómez y Mayumi (2017), a través que pasa el tiempo los científicos expertos en el desarrollo de reconocimiento facial siguen entrenando máquinas para identificar a las personas u objetos por medio de redes para obtener cada vez respuestas más bajas. (p. 20). Por último, esta investigación se justificó institucionalmente, porque la empresa en base a sus objetivos permite asimilarse al uso de tecnologías para mejorar el apoyo de los procesos de la organización y crecer de forma eficiente y competitiva en el mercado competitivo, esta justificación mencionó Bravo, Ramírez y Arena (2018), A inicios de la década 1960 ya se tenía estudiando e investigando el reconocimiento facial con la finalidad de poder implementarlos en las instituciones y lograr ver el impacto. (p. 115).

El objetivo general fue: Desarrollar un Sistema de Reconocimiento Facial para mejorar el control de acceso en el almacén de la Clínica Multident Buenos Aires. Los objetivos específicos son: Determinar la influencia de un Sistema de Reconocimiento Facial en el control de acceso autorizado del personal en el área de almacén en la Clínica Multident Buenos Aires. El siguiente objetivo específico es: Calcular la precisión de acceso del Sistema de Reconocimiento Facial del personal en el área de almacén en la Clínica Multident Buenos Aires.

La hipótesis general fue: El Sistema de Reconocimiento Facial mejora el control de acceso del personal en el almacén de la Clínica Multident Buenos Aires. Además, de las hipótesis específicas que fueron: El Sistema de Reconocimiento Facial mejora el control de acceso autorizado del personal en el área de almacén en la Clínica Multident Buenos Aires, el Sistema de Reconocimiento Facial mejora la precisión de acceso del reconocimiento del personal en el área de almacén en la Clínica Multident Buenos Aires.

II. Marco teórico

Los siguientes antecedentes hechos por otros autores nos ayudaron en la investigación y tuvieron relación con las variables de estudio:

En los antecedentes internacionales el autor Lai (2020), en su tesis titulada “Multi-Spectral Facial Biometrics in Access Control” Universidad of Drive NW Calgary-Canadá, tuvo como objetivo demostrar que los datos de la biometría facial que se adquiere mediante los sensores multiespectrales como RGB e infrarrojos puedan ayudar en el proceso de reconocimiento facial para el control de acceso por medio de los datos biométricos, de la misma manera propusieron realizar un algoritmo que pueda filtrar los movimientos no deseados de cabeza que genera el individuo y que muchas veces dificulta el reconocimiento facial, se obtuvo como resultado un 9% más de precisión para el reconocimiento facial, también se redujo el tiempo de procesamiento en un 32% y como conclusión se tuvo que el algoritmo si redujo el tiempo de reconocimiento facial y se propuso poder utilizarlo para poder detectar incluso si un paciente presenta fiebre, de la misma manera nos indica que se podría utilizar en el futuro una combinación de modelo 3D y 2D para mejorar aún más el reconocimiento biométrico para el control de acceso.

El autor Norvik (2022) en su tesis titulada: “Facial recognition techniques comparison for in-field applications: Database setup and environmental influence of the access control” Uppsala-Suecia, tuvo como objetivo desarrollar un sistema de reconocimiento facial que ayude a prevenir los robos de autos en los aparcamientos con un control de acceso como si fuese una llave, en cuanto a su problemática nos dice que fue el alto índice de robo de autos en la ciudad para fines terroristas, para ser más específicos en los aparcamientos, se tuvo como resultados de la prueba que el algoritmo de red neuronal convolucional funcionó bien y las pruebas concluyen que el rendimiento es adecuado para las aplicaciones de control de acceso. Los otros tres algoritmos, Eigenfaces, Fisherfaces y LBHP, estaban funcionando mal, tenían dificultades con las imágenes donde las caras tenían una fuerte iluminación o sombras presentes, por tanto, se concluye que estos algoritmos no son adecuados para aplicaciones de control de acceso.

El autor Calles (2019), en su tesis que lleva por nombre: "Sistema informático de reconocimiento facial para el registro y control de asistencia de los socios de la cooperativa de taxis y camionetas Puyo", Universidad Regional Autónoma de los Andes, Puyo Ecuador, como objetivo principal propuso implementar una aplicación de reconocimiento facial de los trabajadores y el nivel de acceso a los diversos eventos que se llevan a cabo. El método que se usó en la investigación fue el analítico- sistémico, histórico- lógico, inductivo deductivo, la problemática fue la inadecuada gestión que se tiene en la cooperativa de taxis cada vez que registran su asistencia en los muchos acontecimientos que se llevan a cabo, el nivel de acceso hace perder tiempo valioso puesto que dificulta cuando se realiza el reporte de asistencia. Por otra parte, se llevó a cabo la muestra de una población de 79 trabajadores de la cooperativa que usan el control de accesos, en el pre test logramos 70% y luego de la implementación de la aplicación, el post test llegó a 90% en base al nivel de acceso de los trabajadores de la cooperativa, el presente trabajo tuvo como conclusión que el aplicativo satisface con las metas trazadas de manera positiva para el correcto registro de la asistencia y de la misma manera para el control de acceso de los socios.

Según Estremadoro (2016) en su tesis con nombre, "Modelo propuesto para la toma de asistencia con reconocimiento facial en imágenes capturadas con múltiples rostros en la escena", El objetivo principal fue el diseño e implementación de un sistema que nos permita llevar un adecuado control de asistencia de los estudiantes a los distintos laboratorios que se encuentran en la facultad de ingeniería de sistemas, el tipo de investigación que usaron fue aplicada y de nivel explicativo, se tuvo una población de 24 personas, en cuanto a la realidad problemática es la escasez o falta que presentan algunos aplicativos de reconocimiento facial, en este caso se refiere al ángulo de la captura, cambios en el rostro, maquillaje y uso de objetos que hagan difícil poder identificar. Los resultados obtenidos nos dieron a conocer que el aplicativo nos permite registrar a varios alumnos a la vez mediante el reconocimiento facial, realizando un trabajo más rápido y fácil para el registro de asistencia del alumnado. Se concluye que después de implementar el sistema que se propuso para el control de asistencia y haber buscado, comparado y elegido los algoritmos idóneos para el reconocimiento facial, podemos decir que EigenFaces es una de las técnicas que existen para reconocimiento facial que es muy completa

ya que no usa elementos adicionales para poder realizar el reconocimiento, también el algoritmo de Vila & Jones tiene una buena precisión, así mismo una buena elasticidad para el reconocimiento facial. Se pudo demostrar que el modelo propuesto puede reconocer rostros incluso en ausencia de una buena iluminación, y también puede realizar el reconocimiento facial con objetos como anteojos u otros accesorios que puedan dificultar un buen reconocimiento.

Según Taylor (2020) en su tesis de nombre, "Did research called Setting intentions: considering racial justice implications of facial recognition technology", nos dice que: Tuvo como objetivo el concientizar a la población sobre el uso del reconocimiento facial para temas de seguridad mediante uso de la videovigilancia, mezclando la seguridad pública con la tecnología, tuvo como problemática la injusticia racial que existe en los Estados Unidos de Norteamérica. Se analizaron a una parte de la población mediante encuestas relacionadas al reconocimiento facial dando como resultado que el 79% de africanos estadounidense se sienten discriminados y desconfían del uso de un sistema de reconocimiento facial. Además, el 51% de los encuestados se sienten incómodos de la implementación del sistema de reconocimiento facial en el sistema de seguridad. Por ello, el resultado brindado es que hay una diferencia significativa de no aceptación para la implementación del sistema de reconocimiento facial para la seguridad pública puesto que genera más división racial.

En los antecedentes nacionales se tiene a los autores. Velarde y Yabarrena (2018), en su tesis titulada: "Sistema de reconocimiento facial para el control de la trata de personas en Perú", Universidad Andina de Cusco, Cusco Perú 2018. Tuvo como objetivo implementar un aplicativo que les permita reconocer a los ciudadanos que se encuentran perdidos, debido a secuestros o trata de personas que existe en la localidad, dicho aplicativo ayudara a reconocer los rostros para obtener un mejor control y de esta manera reducir los tiempos de búsqueda para los casos de pérdida de personas, la problemática fue la trata de personas y secuestros en la localidad de Cusco. La justificación fue que con esta innovación tecnológica se agilizará los procesos que existen cuando se logra capturar a un delincuente y el aplicativo tendrá conexión con varias entidades del estado. En cuanto a la metodología de la investigación que se usó, fue aplicada y en cuanto al desarrollo se utilizó la

metodología XP. La población que se usó en el presente trabajo tuvo una muestra de 50 ciudadanos buscados por secuestro de las mafias que fueron sacadas de la base de datos del ministerio del interior, esto fue para obtener los resultados, la identificación y reconocimiento de una persona extraviada, dado esto se concluyó que el aplicativo ayudará en la identificación de ciudadanos buscados o no habidos.

Becerra (2019) por otro lado, su investigación titulada "Patrones de conducta facial, para identificar accesos informáticos no autorizados". El fin del proyecto es implementar un sistema que se adecue y brinde seguridad al momento del control del personal por medio del reconocimiento facial. Finalizando, la utilidad depende mucho como el algoritmo o patrón de reconocimiento facial identifique y genere un mejor acceso de seguridad en los aplicativos de reconocimiento facial.

Según Vejarano (2018), en su tesis titulada: "Reconocimiento Facial mediante Imágenes Estereoscópicas", para optar el grado de Título Profesional elaborada en la Universidad Señor de Sipán, Pimentel Perú, tuvo como objetivo aprender varias caras por medio de un aplicativo de algoritmos para reconocimientos faciales, su problemática fue el bajo nivel de precisión del reconocimiento facial frente a diferentes factores como la el tipo de luz, la postura y los múltiples ademanes que realiza la persona y muchas veces eso no permite que pueda ser reconocido por el aplicativo. La justificación fue poder comparar las imágenes en 2D y las 3D que son propuestas en el aplicativo. La metodología que se usó fue cuasi- experimental, en cuanto al método de investigación que se desarrolló se tuvo a la observación y captura de imágenes. Se utilizaron varias imágenes en formato RGB, utilizando una cantidad de píxeles, y gracias a esos requisitos se obtuvo como muestra 348 imágenes. Se tuvo como resultado que el 94.56 % fue eficaz y el 92 % fue robusto, se tuvo como conclusión corregir y seleccionar los diferentes algoritmos del aplicativo nos ayudará a mejorar el reconocimiento obteniendo los resultados previstos. De esta tesis tomamos como referencia los objetivos puesto que nos ayuda a conocer cómo se realiza la implementación de un aplicativo de reconocimiento facial en 3D.

Según Martínez (2017), en su tesis titulada: "Diseño del sistema de control de asistencia del personal en la agencia mercado de la Caja Huancayo aplicando tarjetas de proximidad de tecnología RFID", Universidad Continental, Huancayo Perú, se tuvo como objetivo el diseño de una aplicación que nos ayude a llevar un mejor control de las asistencias de los trabajadores de la caja Huancayo, haciendo uso de la tecnología RFID, en cuanto a la problemática que se tuvo la falta de orden al momento de registrar el control de asistencia, así como la suplantación del trabajador y el retraso al marcar la asistencia de los trabajadores de la agencia, la justificación de la investigación es que la agencia tendrá un nuevo aplicativo de control de asistencia mediante la tecnología RFID, esto ayudará a que el tiempo promedio de retraso sea menor en la agencia cada vez que se marque la debida asistencia. Se tuvo como población y muestra a 22 trabajadores que son todos los que trabajan en la agencia puesto que es menor a 100, también se evaluó el tiempo promedio de retraso con relación a las asistencias de los trabajadores, antes que se usará el sistema el proceso de marcado de asistencia fue de 4.30 minutos y después de usar el aplicativo fue de 2.50 minutos esto nos ayuda a concluir que la implementación de la aplicación mejorará el control de tiempo de atraso, trayéndolo muchos beneficios a la agencia por su bajo costo de implementación.

Según Galindo, Huaranga y Samaniego (2021), en su tesis titulada "Reconocimiento facial para la identificación de los alumnos en exámenes finales en la modalidad presencial de la Universidad Continental – Huancayo, 2021", tuvo como objetivo poder implementar un software de escritorio usando la metodología Kanban para poder controlar al alumnado en sus exámenes y evitar así la suplantación de los estudiantes mediante el reconocimiento facial usando machine learning, la metodología fue Kanban basado en wips armando un tablero Online Trello. La conclusión fue que el programa tuvo un 90% de exactitud y precisión y un 93% de sensibilidad.

En los antecedentes locales tenemos según Yáñez (2019), en su tesis titulada "Sistema de reconocimiento facial para el control de acceso de estudiantes a los laboratorios de la FIIS-UNAC, 2019", en su trabajo de investigación se planteó una problemática interesante, los laboratorios de las FIIS-UNAC tenían una carencia de monitoreo de entrada y salida. Por lo cual, se planteó determinar cuál sería el efecto

de un sistema de reconocimiento facial para los alumnos que entran y salen del laboratorio. Por lo tanto, se demostró que la inteligencia artificial en el campo de reconocimiento facial ayudo a mejorar el control de acceso del alumnado que asiste a los laboratorios. Teniendo como resultado que su indicador acceso autorizados alcanzo el 100% de después de la implementación

Según Alejo (2021), en su tesis que lleva por nombre: “Algoritmo de reconocimiento facial para la Gestión de control de acceso de la empresa Altoque PS S.A”. Universidad Cesar Vallejo, Lima Perú. Esta tesis tuvo como objetivo poder determinar la influencia que tiene el algoritmo para el control de acceso de los trabajadores de la empresa Altoque y así mismo poder determinar en cuanto se pudo reducir el tiempo de verificación, como problemática se tuvo el inadecuado control de acceso al área de almacén y que muchas veces perjudicaban los pedidos ya que las diferentes personas que ingresaban no estaban autorizadas y solo generaban retrasos y equivocaciones, en esta tesis se usó la metodología Aplicada, Experimental del tipo Pre-Experimental, como conclusión se tuvo que él algoritmo pudo reducir en un 47% el acceso no autorizado del personal, de la misma manera se redujo el tiempo de verificación en un 1 minuto 52 segundos llegando afirmar que el sistema de reconocimiento facial si mejora la gestión de control de acceso en la empresa.

Según Aquijes (2021), en su tesis que lleva por nombre: “Implementación de un Sistema de Reconocimiento Facial para el control de acceso del personal en la empresa GUIMARTBOT S.A.C” de la Universidad Cesar Vallejo. Esta tesis tuvo como objetivo desarrollar un Sistema de Reconocimiento Facial que gestione eficientemente el control de acceso del personal en la empresa GUIMARTBOT S.A.C. En cuanto a su problemática es que cuentan con la presencia de ciertos procesos inadecuados de seguridad de la información en los sistemas informáticos relacionado al control de acceso del personal para el acceso a la información de la empresa, usaron la metodología aplicada y el tipo de investigación es experimental y el diseño de estudio es pre-empirico. Tuvo como conclusión que el sistema de reconocimiento facial mejoro el control de acceso en un 37% y la precisión en un 18%.

Python es un lenguaje de programación de fácil sintaxis, se puede ejecutar en diferentes plataformas como Windows, Linux, Mac y es un lenguaje orientado a objetos, una de sus ventajas es que Python tiene incluidas muchas bibliotecas y no solo se utiliza para operar archivos, sino también para elaborar sitios web que pueden requerir IA (Gowrishankar & Veena 2019, p1).

El autor define que el reconocimiento facial es un sistema de identificación avanzada por la tecnología, ya que permite identificar al sujeto por medio de una imagen, vídeo o cualquier parte del rostro (Moreno 2021, p145).

Sistema de reconocimiento facial cada vez es más aceptado en las ciudades para proteger su entorno y familias de la inseguridad que se vive en las calles, sugiere que sea enfocado para el uso del bien, ya que puede traer rastreos de personas sin su permiso, por lo cual se evidenció la utilidad del reconocimiento facial (Bravo 2018, p.186).

Reconocimiento facial puede tener muchas utilidades y aplicaciones en la empresa dando beneficios a sus procesos que puedan mantenerse firmes y brindando todo tipo de seguridad dentro de la organización. (Huamaní 2020, p.20),

El reconocimiento facial tiene varios tipos de utilidades y es usado en diferentes soluciones como en la medicina, detectando el movimiento del rostro por cada punto, así logrando una detección del estado mental de las personas, logrando inducir con que tipo personas se puede estar en contacto (Alcaraz, 2020, p.250).

El reconocimiento facial en cámaras permite identificar a las personas de forma biométrica, para ello, se necesita un sistema de software que tenga la capacidad de almacenar los rostros de las personas para así poder comprarlas con el detector de reconocimiento facial (Lozano, 2018, p.203).

La tecnología de reconocimiento facial (FRT) surge a base de una necesidad que se tiene en el momento o la urgencia de poder identificar a la persona o individuo mediante patrones extrayendo datos y características del rostro por medio de una videocámara y comparándolo con la base de datos de los rostros con sus respectivos nombres asociados (Mohammad, 2020).

Sistema de seguridad se define como un conjunto de elementos e instalaciones que se relacionan entre sí, para brindar protección a las personas o bienes materiales que se encuentren en el sitio específico (Ferro, 2020, p.22).

Define la biometría, como una tecnología que permite identificar al usuario o sujeto base a sus características físicas e intransferibles propias de cada persona (Iñiguez, 2020, p.109).

Define la seguridad biométrica como un sistema para controlar el acceso del personal o usuario a una cierta área o lugar específico de manera eficiente por medio de la identificación basada en características únicas de la persona (Ferro, 2020, p.5).

Define control de acceso como un medio o sistema que responde mediante autorización y denegación para dar acceso a un lugar, recurso o bien específico previo asignación (Vega, 2021, p.47).

El Ministerio de Tecnologías de la Información y las Comunicaciones, menciona que el control de acceso se considera como lógico y físico, como se ve en la norma ISO/IEC 27002:2013 en dominio de Seguridad física y ambiental.

Un sistema Biométrico se puede definir como una disciplina científica que se encarga de la medición y el despliegue de los diferentes atributos que tiene el ser humano, que puede permitir identificarlos de manera individual y única (Fairhust, 2019, p.10).

Cualquier característica humana puede ser usada como datos biométricos siempre y cuando cumpla con 4 criterios básicos los cuales son: Universalidad, Singularidad, Permanencia y Colectabilidad. (Fairhust, 2019, p.11).

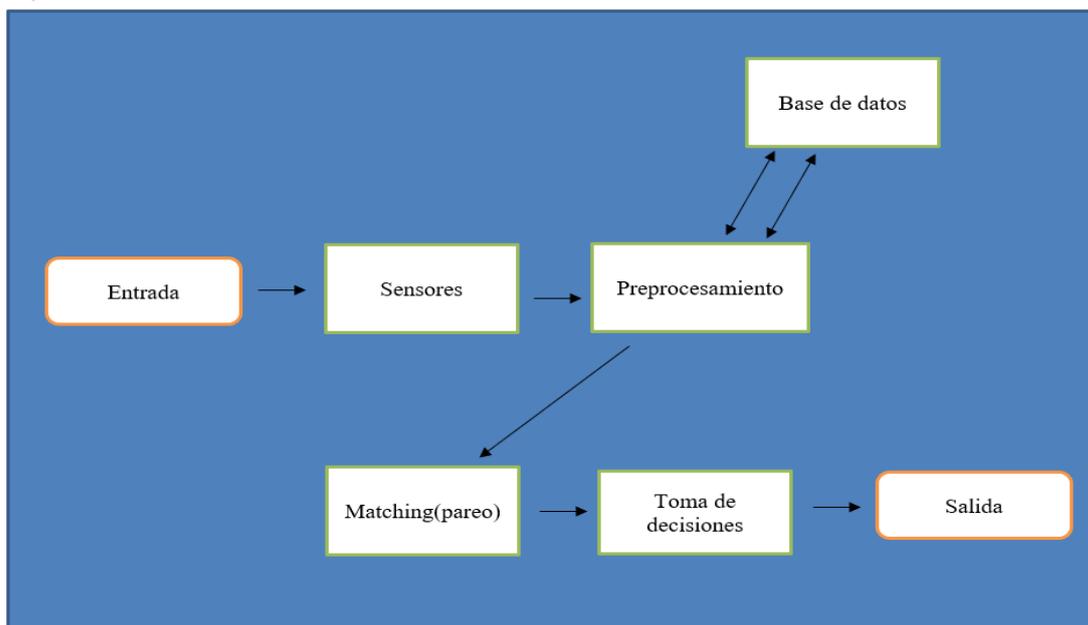
Tabla 1: Criterios básicos

Universalidad	Singularidad	Permanencia	Colectabilidad
-Todas las personas deben contar con la característica elegida, ya que debe ser inclusivo y puedan ser usado por todas las personas	-No debe haber dos personas que sean iguales en la característica elegida.	- La característica elegida debe ser permanente en el tiempo, la característica que elijamos debe ser la misma cuando se mida.	-La característica debe permitir ser medida cuantitativamente, debe estar debidamente definida para evitar ambigüedades.

Fuente: Fairhust

Mas allá de estos cuatro criterios básicos como la Universalidad, Singularidad, Permanencia y Colectabilidad, existen otros elementos que son citados algunas veces como la resistencia a la elusión (difícil de engañar), también tenemos a la noción de aceptabilidad (Fairhust, 2019, p.13).

Figura 1: Componentes de los sistemas biométricos



Fuente: Fairhust

En el tema de control de acceso el autor nos dice que es de suma importancia y sobre todo muy necesario hoy en día por diversos factores, en situaciones que generan desorden, caos e inseguridad se puede implementar esta tecnología ya que es muy beneficiosa, tenemos como ejemplo los sistemas biométricos tales como huellas, reconocimiento de voz y facial y otros, son ágiles para poder identificar a las personas sin preguntarles (Salvatierra, 2019, p. 12).

Recepción de alarmas está ubicada en lugar específico de la organización y consiste en recibir la activación de la alarma y comunicar al encargado específico de la activación (Ferro, 2020, p.29).

Según el CSIRT del Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia, menciona que el control de acceso se considera como lógico y físico, como se ve en la norma ISO/IEC 27002:2013 en dominio de Seguridad física y ambiental (2021, p.3).

Según Calder (2017), la norma ISO/IEC 27001:2013, en su dominio de seguridad física y entorno, en Áreas seguras en controles de ingreso físico, maneja como objetivo de control que las áreas deben ser seguras y protegidas por medio de controles establecidos que permitan el acceso del personal autorizado (p.59).

Según Calder (2017), la norma ISO/IEC 27002:2013, en su dominio de seguridad física y entorno, en Áreas seguras en controles de ingreso físico, menciona la guía de implementación con las directrices a considerar. De manera que, se debe registrar fecha y hora de las personas entrantes, solo debe dar autorización para el propósito específico establecido y la entidad del personal debe ser autenticada por los medios adecuados, el acceso al área debe estar controlado y restringido solo al personal autorizado por medio de un identificador, se debe monitorear de manera segura en un libro físico o electrónico los reportes, todos los empleados deben tener un identificación y notificar al encargado de seguridad si no tiene su respectiva identificación(p.60).

Según Calder (2017), la norma ISO/IEC 27004:2013, proporciona directrices destinadas para evaluar el rendimiento de la seguridad de la información mediante la medición de los objetivos de control. Además, la medición es una actividad para determinar un valor, estado o tendencia en el rendimiento. Por lo cual, la

organización debe definir que supervisar, medir, analizar y evaluar, con la finalidad de cumplir el grupo u objetivo de control (p.18).

Según Bearmud (2016), hace referencia el indicador en su elaboración de un plan de implementación de la ISO/IEC 27001:2013, en su gestión de indicadores aplicados en la organización. (p.46):

Figura 2: Formula de acceso autorizado

$$PAA = \frac{NAA}{NAT} \times 100$$

Fuente: Bearmud

En cual:

PAA= Porcentaje de acceso autorizado.

NAA= Número de acceso autorizado.

NAT= Número de acceso totales.

Las empresas han adquirido inteligencia artificial para incrementar su eficiencia, intentando adquirir autonomía, movilidad y agilidad, buscando cambios constantes y dinámicos en su entorno. (Valbuena, 2021, p.110)

Las empresas están utilizando inteligencia artificial para obtener incremento en su eficiencia, tales como: reconocimiento de imágenes, desempeño comercial, mantenimiento predictivo, detección y clasificación de objetos, etc. (Rouhiainen, 2018, p.36)

La aplicación de la inteligencia artificial en la administración pública mejora e incrementa la eficiencia, obteniendo una mejora de capacidades de las máquinas en el sector público. (Filgueiras, 2021, p.10)

La eficiencia es la capacidad de obtener lo que se espera o lo que se pretende de manera que utiliza menos recursos para alcanzar el objetivo. (Patienten 2020, p.130)

La precisión es una métrica que se utiliza mucho en los sistemas de inteligencia artificial ya que da respuestas precisas muchas veces como un cociente que indica

una predicción precisa tal como el verdadero positivo y falso positivo. (Berryhill, 2019, p.78)

La precisión viene a ser la proporción de cada observación predicha como positiva que es en realidad positiva. (Albon, 2018, p.187)

Figura 3: Formula de Precisión

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

Figura 3: Formula de precisión

Fuente: Albon

En cual:

P= Precisión.

VP= Verdadero Positivo, predice correcto.

FP= Falso Positivo, predice incorrecto.

Para el indicador de Precisión estamos usando la matriz de confusión.

Tabla 2: Matriz de Confusión

		PREDICCIONES	
		(+)	(-)
OBSERVACION	(+)	Verdaderos (+) (VP)	Falsos (-) (FN)
	(-)	Falsos (+) (FP)	Verdaderos (-) (VN)

Fuente: BerreHill

La metodología XP junta muchas buenas prácticas, que se centran en tener una gran calidad y sobre todo eficiente. Las buenas prácticas que tiene la metodología XP se dividen en: las prácticas relacionadas con el diseño y desarrollo que están supeditadas a la elaboración del software y las prácticas donde se está presente la planificación y organización del proyecto. Esta metodología se basa en la codificación puesto que su concepto tiene solo una especificación formal, dado que revisa la codificación que se reutiliza, se conceptualiza y minimiza el análisis y el diseño para posteriormente usarla en la programación del sistema (Ruiz, 2017, p.280).

La metodología Scrum está dentro de las metodologías ágiles, esta metodología no solo se limita para poder desarrollar software, sino para cualquier otro proyecto, si se desea usar la metodología scrum el equipo de trabajo debe poseer las habilidades requeridas. Unos de los pilares de scrum es la transparencia, donde los resultados son visibles para todos, la inspección debe ser recurrente para poder detectar algunas variaciones que se puedan dar e influir negativamente en el desarrollo del proyecto. La metodología scrum tiene los siguientes roles, Scrum Master (el responsable), Product owner (propietario del producto) y el Team Scrum (Ramos, 2017, p.101).

Porque decidimos usar la metodología Xp para este proyecto, cuadro comparativo:

Tabla 3: Cuadro comparativo de metodología Xp y Scrum

Metodología Scrum	Metodología Xp
Puede utilizarse no solo para elaborar software sino para otros proyectos	Su eje principal es la elaboración del Software
En la metodología Scrum normalmente se trabaja individualmente.	En la metodología xp normalmente se trabaja en parejas.
Habitualmente los tiempos de entrega de iteraciones son más largos.	Normalmente los tiempos de entrega de cada iteración son más cortos.
Las tareas realizadas y revisadas por el Scrum master si da su visto bueno, ya no se modifican.	Las tareas realizadas si se pueden modificar en cualquier momento.

Elaboración Propia

El OpenCV es una librería de multiplataforma de visión artificial que permite el reconocimiento de gestos, captura de movimiento, realidad aumentada y comprensión de movimiento (Molloy, 2019, p.416).

El autor define OpenCV como una librería que contiene un conjunto de procedimientos y análisis de imágenes, siendo las más solicitadas y utilizadas en la actualidad para aplicaciones de visión artificial (Domínguez, 2021, p.4).

Eigenface es un algoritmo que tiene como objetivo solucionar el problema de gestos y usa la técnica LDA (análisis discriminante lineal) que tiene como fin juntar las imágenes que serán entrenadas para cada persona individualmente también

llamada clase, esta clase genera dos subclases como son: la inter clase(diferentes posturas de la cara de la misma persona) y la extra clase(diferentes posturas de diferentes personas), es vital el entrenamiento de imágenes pero en diferentes contextos como luz o gestos.(Galindo 2017, p.5).

III. Metodología.

3.1 Tipo y diseño de investigación

Tipo de investigación: Aplicada

Diseño de investigación: Experimental de grado preexperimental.



Figura 4: Diseño de investigación

Fuente: Elaboración propia

Dónde:

O_0 : El control de acceso antes del Sistema del reconocimiento facial

X: El sistema de reconocimiento facial

O_1 : El control de acceso después del Sistema del reconocimiento facial

3.2 Variable y Operacionalización

Control de acceso (Variable cuantitativa dependiente)

● Definición conceptual

Según Vega (2021), es un medio o sistema que responde mediante autorización y denegación para dar acceso a un lugar, recurso o bien específico previo asignación (p.47).

● Definición operacional

Se utiliza el instrumento ficha de registro para la recolección de datos donde se obtendrá los datos de los indicadores que se sugirieron en la investigación, adhiriendo una escala de razón. Por lo cual, se observa en la tabla de operacionalización de variable en el anexo 1.

● Indicador

El indicador escogido para medir la variable dependiente fue: control de acceso autorizado y precisión de acceso.

Tabla 4: Matriz de Operacionalización

Variable	Definición Conceptual	Definición Operacional	Dimensión	Indicador	Fórmula	Instrumento	Escala
Variable dependiente: Control de acceso	Según Vega (2021), es un medio o sistema que responde mediante autorización y denegación para dar acceso a un lugar, recurso o bien específico previo asignación (p.47).	Se utiliza el instrumento ficha de registro para la recolección de datos donde se obtendrá la información de los indicadores planteados de la investigación, adhiriendo una escala de razón.	Seguridad Física	Control de acceso autorizado	$PAA = \frac{NAA}{NAT} * 100$ <p>PAA: Porcentaje de accesos autorizados NAA: Número de accesos autorizados NAT: Número de accesos totales.</p>	Ficha de registro	RAZÓN
				Precisión de acceso	Según Albon: Precisión $P = \frac{VP}{VP+FP}$ <p>P= Precisión VP=Verdadero Positivo, predice correcto. FP=Falso Positivo, predice incorrecto.</p>	Ficha de registro	RAZÓN

Fuente: Elaboración propia

● Escala de medición

La escala de medición que se ha usado para medir la variable dependiente es la razón, puesto que son datos que tendrán un punto de cero absoluto y no hay valor numérico negativo.

3.3 Población, muestra y muestreo

● Población

Hernández y Coello (2020), manifestaron que es parte de un grupo de elementos o toda la realidad que tengan uno o más atributos en común que hayan sido recalculadas por el investigador. (p. 59).

Con lo que esto respecta, la población del estudio fueron 19 personas que son trabajadores de la Clínica Multident Buenos Aires, como se muestra en la siguiente tabla.

Tabla 5: población

INDICADOR	POBLACIÓN	CANTIDAD	TIEMPO
Control de acceso autorizado	trabajadores de la Clínica	19	1 mes
Precisión de acceso	trabajadores de la Clínica	19	1 mes

Fuente: Elaboración propia

● Muestra

Según Carrasco (2019), en cuanto a la muestra viene a ser parte de una población con singularidades objetivas importantes y ajustadas a la fecha para que el resultado que se ha logrado obtener de la muestra nos sirva para generalizar a todos los componentes de la población. (p.37)

Por consiguiente, Castro (2003), manifiesta " La muestra es equivalente a la población cuando los elementos que integran son menores a 50, por ende, la muestra es igual a la población"(p.69). Por lo cual, la población es menor a 50, no se obtendrá un subgrupo y se utilizó toda la población total.

• Muestreo

En este caso, el muestro no será utilizado en el estudio, ya que la muestra es inexistente debido que el número de integrantes de la población es menor a 50. Por lo tanto, el muestreo no será aplicado.

3.4 Técnica de instrumento de recolección de datos

Humberto [et al.] (2019), redactaron que las técnicas de investigación son una agrupación de normas y procedimientos para organizar un proceso en particular y alcanzar un objetivo en particular, además que los instrumentos de investigación son las recursos conceptuales o materiales que, mediante ítems, se puede recopilar los datos e información del investigado. (p. 273)

• Validez

Según Sánchez (2018), nos dice que la validez es la forma correcta de medir el estudio que se está realizando, ya que, mide los requerimientos de la investigación con evidencias de aplicación del instrumento medición (p.124).

Por lo cual, se consiguió 3 juicios de expertos para la validación de los instrumentos, tal como sostuvo Sánchez (2018), manifiesta que la validez por medio de expertos consta en verificar que el criterio de la aplicación se ha correctamente usado de tal grado que sea pertinente, relevante y claro p.124).

Tabla 6: Juicios de expertos

Experto	Grado	Juicio
Ángeles Pinillos, Daniel Orlando	Magíster	Aplicable
Ortega Vargas, Christian Víctor	Magíster	Aplicable
Ventocilla Aguado, Cristian	Magíster	Aplicable

Fuente: Elaboración propia

• Fichaje

Para Ñaupas (2018), en la investigación existen diferentes técnicas, el fichaje es una de las técnicas que más valoración tiene para la recopilación de documentos, información y datos de documentos a mano. (p.255).

Para Carrasco (2019), esta técnica es utilizada mayormente en fichas de varios tamaños donde se registrarán datos que puedan servir para el objetivo que busca el investigador (p. 280).

Tabla 7: Técnica e instrumentos utilizados.

Indicador	Técnica	Instrumento
1.- Control de acceso autorizado	- Fichaje	- Ficha de Registro
2.- Precisión de acceso	- Fichaje	- Ficha de Registro

Fuente: Elaboración Propia

• Confiabilidad

Para Hernández (2014), existen diferentes procedimientos para hallar la confiabilidad del instrumento, uno de ellos es el Test-Retest donde se repite la ejecución de dos o más grupos en diferentes periodos, logrando así los parámetros para evaluar si el instrumento es confiable o no. (p294).

Para Carrasco (2019), nos dice que la confiabilidad es parte de un instrumento que nos permitirá poder medir en diferentes tiempos al mismo grupo. Por medio de las pruebas de correlación se puede saber si el instrumento a utilizar es confiable o no (p.339).

Tabla 8: Medidas para test y retest

Nombre de Prueba	Momento	Resultado
Prueba A	1 momento	Coeficiente de Correlación
Prueba A	2 momento	

Fuente: Elaboración Propia

3.5 Procedimientos

En esta tesis se planteó y se formuló el problema que tiene la Clínica Multident Buenos Aires, para después justificar y utilizar como guía algunos trabajos previos para poder tener un mejor marco de referencia para la solución al problema sobre el inadecuado control de acceso al área de almacén, también se plantearon las Hipótesis y finalmente detallamos la metodología de la tesis.

En este estudio se han aplicado ficha de registro para medir los indicadores que habían sido validados por ingenieros de sistemas, dando la veracidad de los mismos. Los instrumentos fueron tomados para 19 trabajadores en la Clínica Multident Buenos Aires por ello tenemos las fichas de registro del Pre-test y Post-test.

En este estudio se usa la herramienta Spss para poder procesar los datos que hemos podido recolectar para el Pre-test (antes de la implementación) y Post-test (después de la implementación).

Se realiza el análisis descriptivo e inferencial de la tesis. También se realiza el contraste para la aceptación de las hipótesis específicas mediante la prueba de T Student. La variable independiente Control de acceso, se ha medido a través del indicador: Control de acceso autorizado y precisión de acceso. Además, se adjunta en anexos la autorización de la empresa que permite hacer la investigación.

Finalmente se realiza las conclusiones, discusiones y recomendaciones correspondientes de la presente tesis.

3.6 Métodos de Análisis de Datos

Este estudio es de enfoque cuantitativo, por lo que el método de análisis de datos que se usó fue de grado experimental, pre experimental. Se utilizó un Pre-test y Pos-test para medir la influencia que tiene el Sistema de reconocimiento facial para el control de acceso en el almacén de la Clínica Multident Buenos Aires.

Galindo (2020), menciona que para saber si la procedencia de la muestra es normal se tiene que aplicar la prueba de Shapiro-Wilk o kolmogorov-Smirnov, si la muestra es menor a 50 se aplica Shapiro-Wilk, en caso contrario, si es mayor a 50 se aplica Kolmogórov-Smirnov (p.37).

En este caso, se aplicará la de Shapiro-Wilk por que la población es 20 y menor a 50, por ende, se utilizará el programa Spss para obtener la prueba de normalidad si el resultado para el nivel de confianza es mayor a 0.05 estaríamos hablando de una distribución normal.

Análisis Descriptivo

En el presente trabajo de investigación se implementa un sistema de reconocimiento facial para poder analizar el control de acceso autorizado y la precisión del acceso, dado el caso se realizó la prueba del pre-test sin el reconocimiento facial implementado y post-test con el reconocimiento facial implementado, en el punto de Resultados se aprecian las siguientes figuras en base a los indicadores.

Análisis Inferencial

Se obtuvo los datos del pre-test y post-test de las fichas de registro para luego realizar la prueba de normalidad en los indicadores de control de acceso autorizado y precisión de acceso, obteniendo que los datos provienen de una distribución normal.

Los indicadores de Precisión de Acceso y Control de Acceso autorizado antes y después de la implementación del sistema web de Reconocimiento Facial se verán reflejados en el punto de resultados.

Prueba de hipótesis.

Puesto que nuestros datos provienen de una distribución normal, utilizaremos la prueba de T Student para contrastar las Hipótesis planteadas.

Hipótesis específica 1:

El sistema de reconocimiento facial mejora el control de acceso del personal en el área de almacén en la Clínica Multident Buenos Aires

Indicador: Control de acceso autorizado

Las Variables que se definieron son las siguientes:

CAAAI: Control de acceso autorizado antes de la implementación.

CAADI: Control de acceso autorizado después de la implementación.

Hipótesis H10: El sistema de reconocimiento facial no mejora el control de acceso del personal en el área de almacén en la Clínica Multident Buenos Aires.

CAAAI \geq CAADI

Hipótesis H1a: El sistema de reconocimiento facial mejora el control de acceso del personal en el área de almacén en la Clínica Multident Buenos Aires.

CAAAI $<$ CAADI

Hipótesis específica 2:

El sistema de reconocimiento facial mejora la precisión de acceso del personal en el área de almacén, en la Clínica Multident Buenos Aires.

Indicador: Precisión de Acceso

Las Variables que se definieron son las siguientes:

PAAI: Precisión de acceso autorizado antes de la implementación.

PADI: Precisión de acceso autorizado antes de la implementación.

Hipótesis H20: El sistema de reconocimiento facial no mejora la precisión de acceso del personal en el área de almacén, en la Clínica Multident Buenos Aires.

PAAI \geq PADI

Hipótesis H2a: El sistema de reconocimiento facial mejora la precisión de acceso del personal en el área de almacén, en la Clínica Multident Buenos Aires.

PAAI $<$ PADI

3.7 Aspectos Éticos

Esta investigación está basada en los reglamentos y lineamientos de la Universidad César Vallejo para así poder realizar una correcta investigación.

Además, se contó con los siguientes principios éticos:

- **Beneficencia:** Los involucrados en la investigación contaron con beneficios y ningún tipo de daño.

- No maleficencia: Ningún involucrado en la investigación fue herido o dañado durante el estudio.
- Autonomía: Cada involucrado en la investigación fue informado del procedimiento y ninguno fue forzado a participar.

IV RESULTADOS

RESULTADO ANÁLISIS DESCRIPTIVO

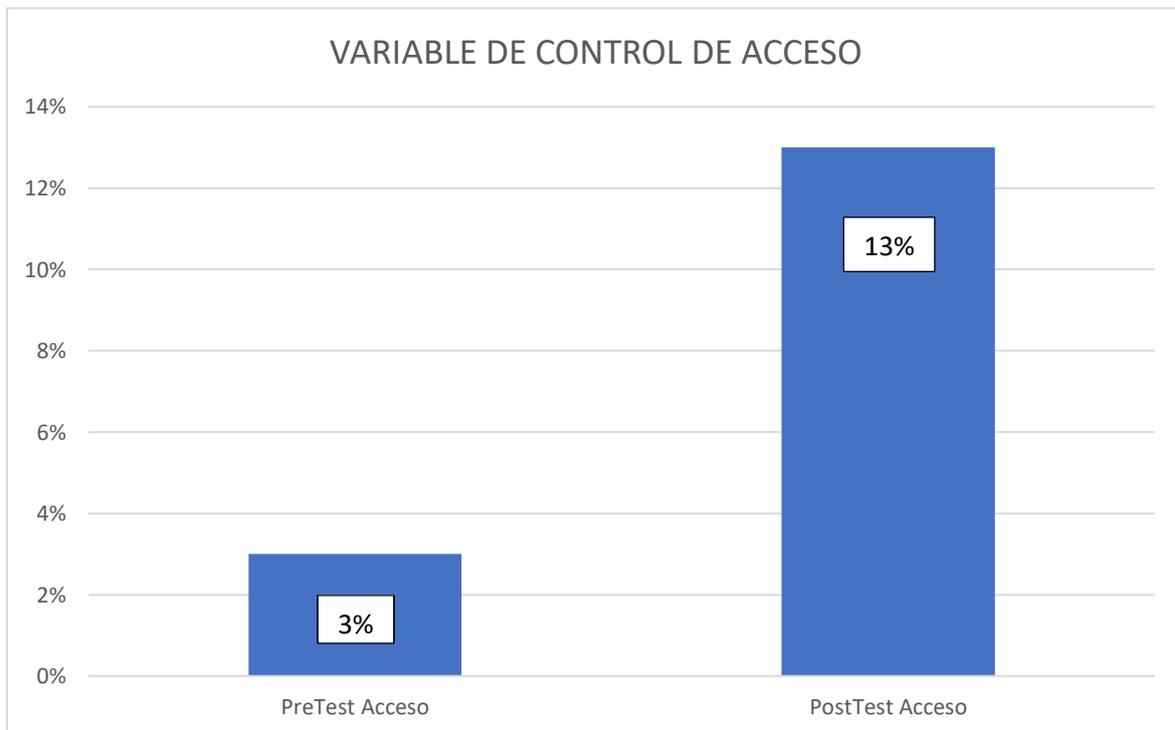
- Indicador: Control de Acceso Autorizado.

Tabla 9: Estadística descriptiva Control de Acceso Autorizado

Estadísticos descriptivos					
	N	Mínimo	Máximo	Media	Desv. Desviación
PREAcceso	19	,00	,12	,0332	,04164
POSTAcceso	19	,00	,30	,1326	,10969
N válido (por lista)	19				

Fuente Spss

Figura 5: Gráficos de Control de Acceso autorizado Pre y Post Test



Fuente Elaboración Propia

El resultado para el indicador de control de Acceso autorizado obtenido en el Pre-Test es de una media del 3% en comparación con el resultado obtenido en el Post-Test el cual la media fue de 13%. De acuerdo a los resultados se llega a la

conclusión que existe una diferencia antes y después de la implementación del Sistema de Reconocimiento Facial puesto que el porcentaje máximo después de implementar el sistema es de 30% y antes de implementar el sistema es de 12%.

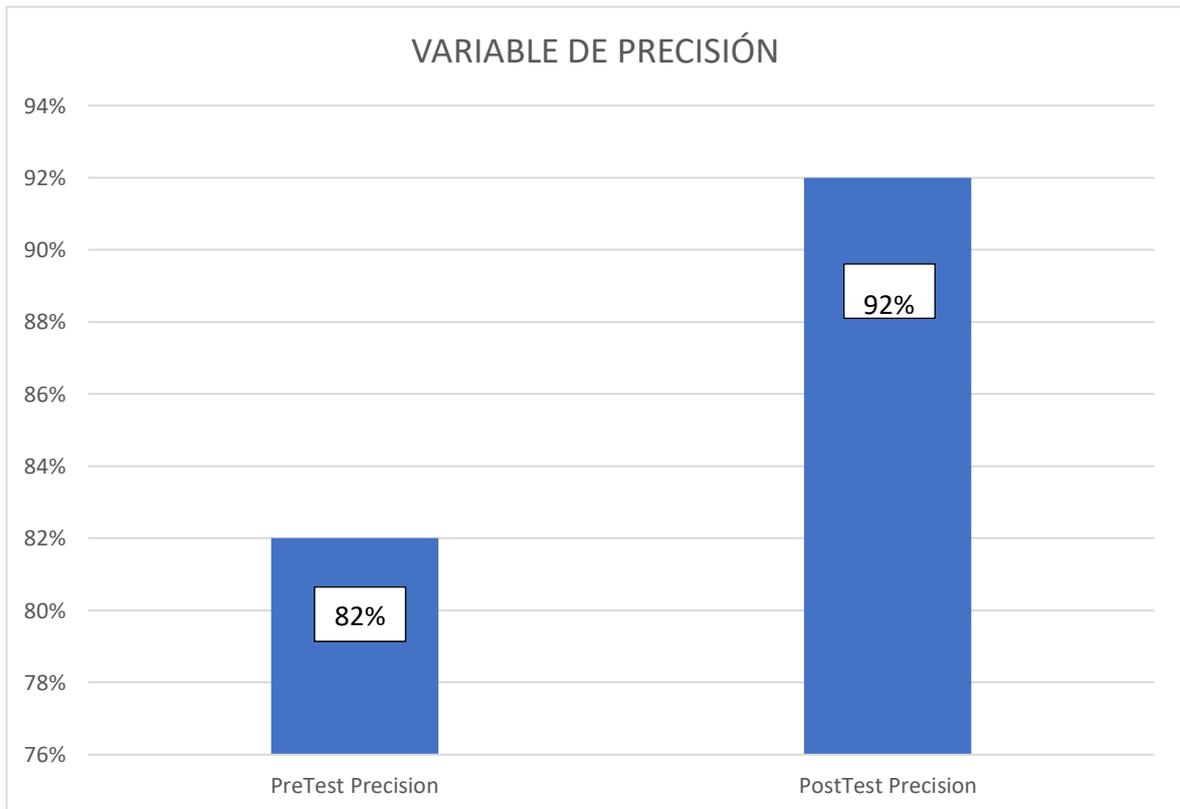
- Indicador: Precisión de Acceso Autorizado.

Tabla 10: Estadística descriptiva Precisión de Acceso

Estadísticos descriptivos					
	N	Mínimo	Máximo	Media	Desv. Desviación
PREPrecision	19	,70	,92	,8274	,05373
POSTPrecision	19	,81	1,00	,9279	,06373
N válido (por lista)	19				

Fuente Sps

Figura 6: Gráficos de Precisión de Acceso Pre y Post Test



Fuente Elaboración Propia

El resultado para el indicador de precisión de Acceso obtenido en el Pre-Test de la media es de 82% en comparación con el resultado obtenido en el Post-Test de la media el cual fue de 92%. De acuerdo a los resultados se llega a la conclusión que existe una diferencia antes y después de la implementación del Sistema de Reconocimiento Facial puesto que el porcentaje mínimo antes de implementar el sistema es de 70% y después de implementar el sistema es de 81%.

RESULTADO ANÁLISIS INFERENCIAL

Si:

Sig. < 0.05 distribución no normal.

Sig. \geq 0.05 distribución normal.

- Indicador: Control de Acceso Autorizado.

Tabla 11: Prueba de Normalidad Control de Acceso Autorizado

Pruebas de normalidad						
	Kolmogorov-Smirnov			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
PREAcceso	,308	19	,000	,749	19	,000
POSTAcceso	,265	19	,001	,817	19	,002

Fuente Spss

En la figura se puede apreciar el Sig. del indicador de Control de Acceso autorizado, teniendo como resultados en el Pre- Test un 0,000 y el en Post-Test un 0,02 entonces se puede concluir que los datos vienen de una distribución no normal al ser menores a 0,05. A continuación, se presentan los histogramas de la distribución normal de cada indicador

Figura 7: Histograma de Control de Acceso Autorizado Pre-Test

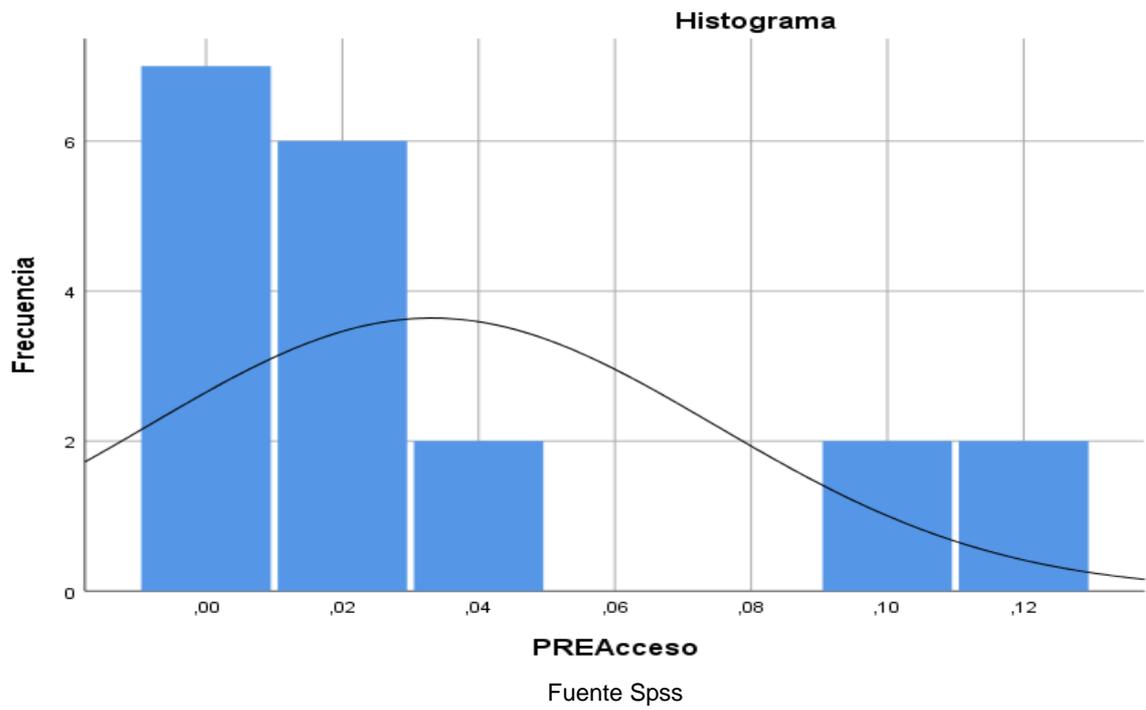
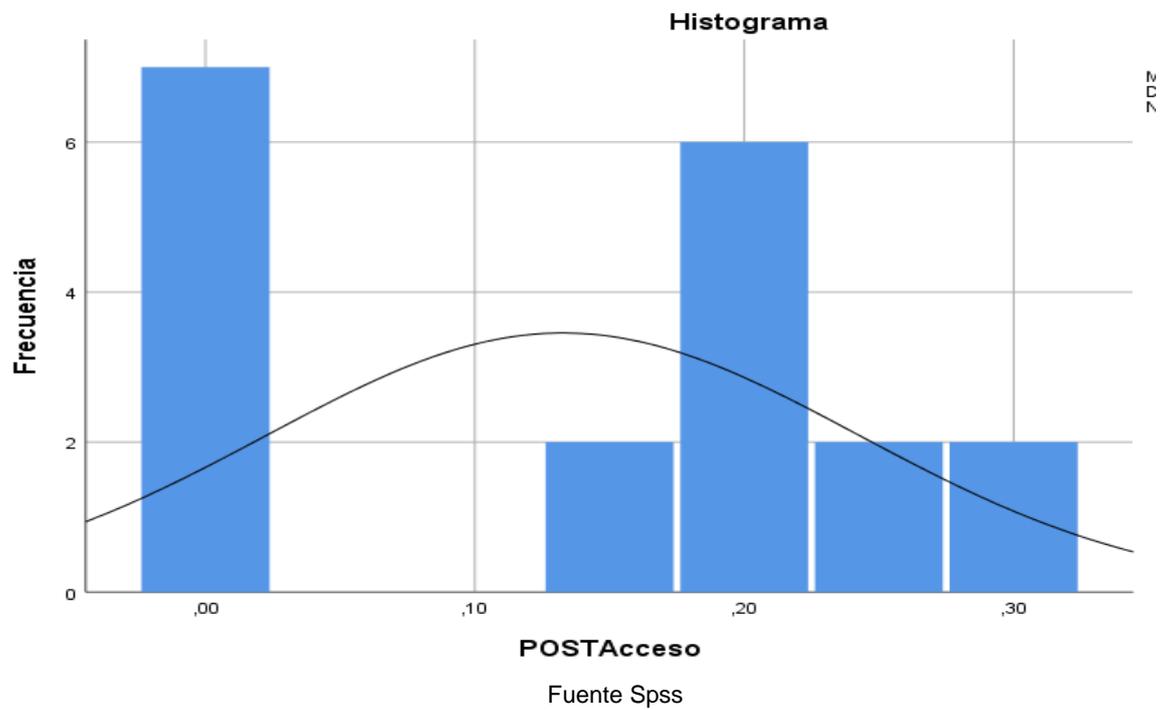


Figura 8: Histograma de Control de Acceso Autorizado Post-Test



- Indicador: Precisión de Acceso.

Tabla 12: Prueba de Normalidad Precisión de Acceso

Pruebas de normalidad						
	Kolmogorov-Smirnov ^a			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
PREPrecision	,186	19	,082	,923	19	,130
POSTPrecision	,167	19	,174	,903	19	,055

a. Corrección de significación de Lilliefors

Fuente Spss

En la figura se puede apreciar el Sig. del indicador de Control de Acceso autorizado, teniendo como resultados en el Pre- Test un 0,130 y el en Post-Test un 0,055 entonces se puede concluir que los datos vienen de una distribución normal al ser mayores a 0,05. A continuación, se presentan los histogramas de la distribución normal de cada indicador

Figura 9: Histograma de Precisión de Acceso Pre-Test

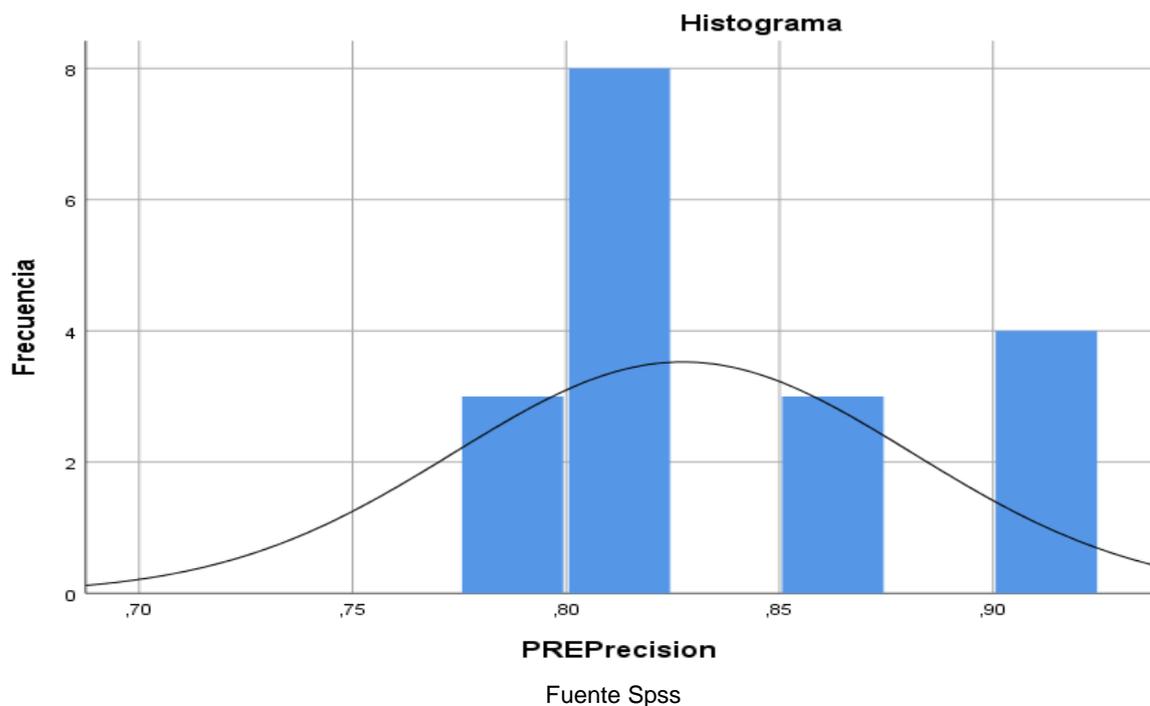
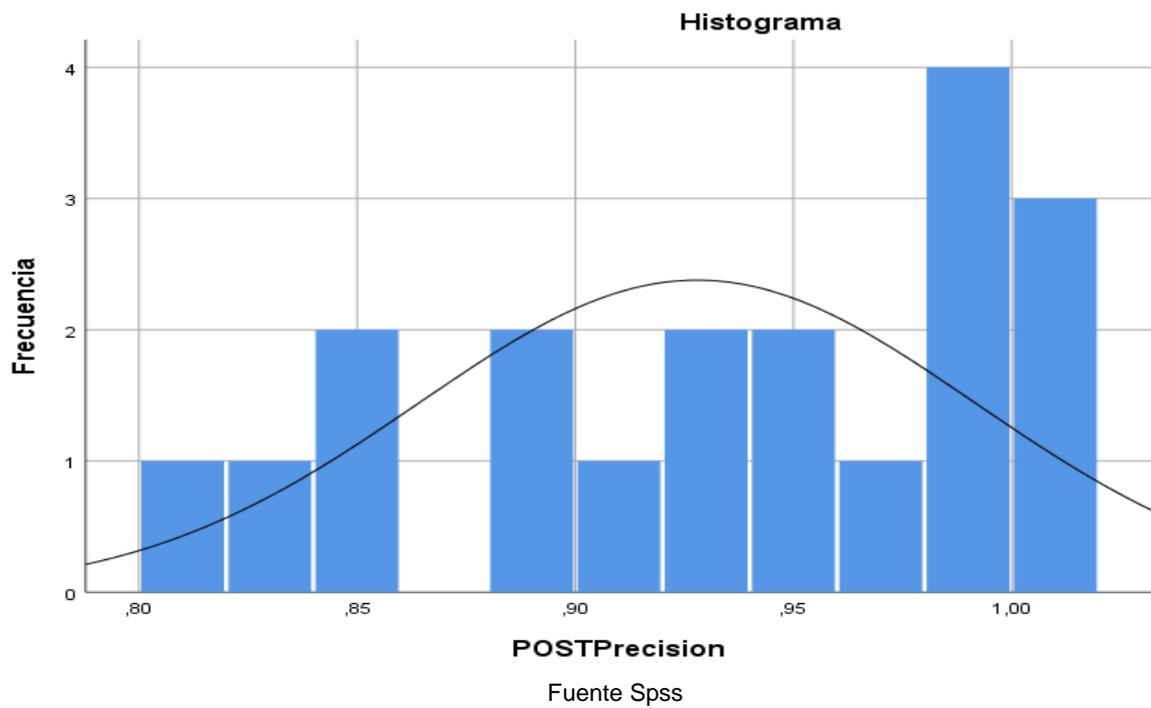


Figura 10: Histograma de Precisión de Acceso Post-Test



En este caso se puede observar que nuestros datos para el indicador de control de acceso autorizado no son normales, utilizaremos la prueba estadística de Wilcoxon para contrastar la Hipótesis. Para nuestro indicador de Precisión de acceso ya que los datos provienen de una distribución normal usaremos la prueba de T student para contrastar la Hipótesis con muestreo aleatorio simple.

RESULTADO HIPÓTESIS

Para realizar la prueba de Hipótesis ejecutamos los resultados de las pruebas de normalidad donde se obtuvo que los datos tanto del pre-test como del post- test del indicador de Control de Acceso autorizado no son normales por tanto utilizaremos la prueba de Wilcoxon y para el indicador de Precisión de acceso al ser datos de distribución normal usaremos la prueba de T Student para dar los resultados correspondientes para las hipótesis que hemos planteado.

HIPÓTESIS ESPECÍFICA 1:

Hipótesis H10: El sistema de reconocimiento facial no mejora el control de acceso del personal en el área de almacén en la Clinica Multident Buenos Aires.

Hipótesis H1a: El sistema de reconocimiento facial mejora el control de acceso Autorizado del personal en el área de almacén en la Clinica Multident Buenos Aires.

Indicador:

Control de Acceso Autorizado.

Donde:

CAAAI: Control de acceso autorizado antes de la implementación.

CAADI: Control de acceso autorizado después de la implementación.

Tabla 13: Prueba de Rangos Wilcoxon para el Control de Acceso Autorizado

		Rangos		
		N	Rango promedio	Suma de rangos
POSTAcceso - PREAcceso	Rangos negativos	0 ^a	,00	,00
	Rangos positivos	12 ^b	6,50	78,00
	Empates	7 ^c		
	Total	19		

Fuente Spss

Tabla 14: Prueba Wilcoxon para el Control de Acceso Autorizado

Estadísticos de prueba	
	POSTAcceso - PREAcceso
Z	-3,077
Sig. asintótica(bilateral)	,002

a. Prueba de rangos con signo de Wilcoxon

Fuente Spss

Entonces, sabiendo que el P valor al estar por debajo del nivel de significancia que es 0,05 rechaza la Hipótesis Nula y se acepta la Hipótesis Alternativa. El sistema de reconocimiento facial mejora el control de acceso autorizado del personal en el área de almacén en la Clinica Multident Buenos Aires.

HIPÓTESIS ESPECÍFICA 2:

Hipótesis H20: El sistema de reconocimiento facial no mejora la precisión de acceso del personal en el área de almacén, en la Clinica Multident Buenos Aires.

Hipótesis H2a: El sistema de reconocimiento facial mejora la precisión de acceso del personal en el área de almacén, en la Clinica Multident Buenos Aires.

Indicador:

Precisión de Acceso

Donde:

PAAI: Precisión de acceso autorizado antes de la implementación.

PADI: Precisión de acceso autorizado antes de la implementación.

Teniendo en cuenta el valor t-student obtenido de la prueba t-student que es 4.262, se hace el contraste con el valor t obtenido de la tabla t-student 1.7341 (Figura 12), entonces se infiere que el valor obtenido de la prueba es mayor por lo que se encuentra en zona de rechazo.

Tabla 15: Prueba T para la Precisión de Acceso

		Prueba de muestras emparejadas							
		Diferencias emparejadas							
		Media	Desv. Desviación n	Desv. Error promedio	95% de intervalo de confianza de la diferencia		t	gl	Sig. (bilateral)
					Inferior	Superior			
Par 1	POSTPrecision - PREPrecision	,1005	,10282	,02359	,05097	,15008	4,262	18	,000

Fuente Spss

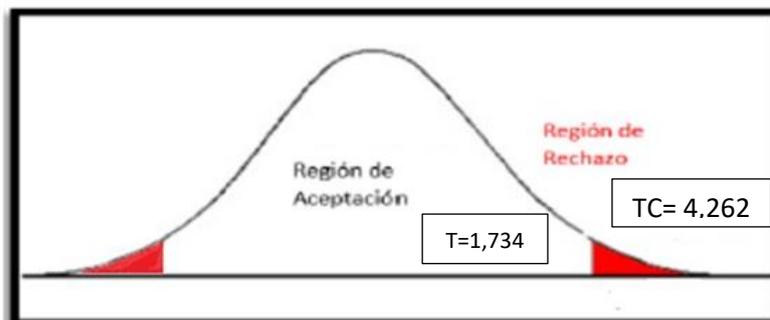
Aplicando la fórmula de T student

$$TC = \frac{x - u}{\frac{s}{\sqrt{n}}}$$

$$TC = 4,26$$

$$TC = \frac{0,10053}{\frac{0,10282}{\sqrt{19}}}$$

Figura 11: Zona de Rechazo



Fuente Elaboración Propia

Figura 12: Tabla de T student 2

α	0.45	0.40	0.35	0.25	0.20	0.15	0.10	0.05	0.025	0.01	0.005	0.0005
1	0.1584	0.3249	0.5095	1.0000	1.3764	1.9626	3.0777	6.3138	12.7062	31.8205	63.6567	636.6192
2	0.1421	0.2887	0.4447	0.8165	1.0607	1.3862	1.8856	2.9200	4.3027	6.9646	9.9248	31.5991
3	0.1366	0.2767	0.4242	0.7649	0.9785	1.2498	1.6377	2.3534	3.1824	4.5407	5.8409	12.9240
4	0.1338	0.2707	0.4142	0.7407	0.9410	1.1896	1.5332	2.1318	2.7764	3.7469	4.6041	8.6103
5	0.1322	0.2672	0.4082	0.7267	0.9195	1.1558	1.4759	2.0150	2.5706	3.3649	4.0321	6.8688
6	0.1311	0.2648	0.4043	0.7176	0.9057	1.1342	1.4398	1.9432	2.4469	3.1427	3.7074	5.9588
7	0.1303	0.2632	0.4015	0.7111	0.8960	1.1192	1.4149	1.8946	2.3646	2.9980	3.4995	5.4079
8	0.1297	0.2619	0.3995	0.7064	0.8889	1.1081	1.3968	1.8595	2.3060	2.8965	3.3554	5.0413
9	0.1293	0.2610	0.3979	0.7027	0.8834	1.0997	1.3830	1.8331	2.2622	2.8214	3.2498	4.7809
10	0.1289	0.2602	0.3966	0.6998	0.8791	1.0931	1.3722	1.8125	2.2281	2.7638	3.1693	4.5869
11	0.1286	0.2596	0.3956	0.6974	0.8755	1.0877	1.3634	1.7959	2.2010	2.7181	3.1058	4.4370
12	0.1283	0.2590	0.3947	0.6955	0.8726	1.0832	1.3562	1.7823	2.1788	2.6810	3.0545	4.3178
13	0.1281	0.2586	0.3940	0.6938	0.8702	1.0795	1.3502	1.7709	2.1604	2.6503	3.0123	4.2208
14	0.1280	0.2582	0.3933	0.6924	0.8681	1.0763	1.3450	1.7613	2.1448	2.6245	2.9768	4.1405
15	0.1278	0.2579	0.3928	0.6912	0.8662	1.0735	1.3406	1.7531	2.1314	2.6025	2.9467	4.0728
16	0.1277	0.2576	0.3923	0.6901	0.8647	1.0711	1.3368	1.7459	2.1199	2.5835	2.9208	4.0150
17	0.1276	0.2573	0.3919	0.6892	0.8633	1.0690	1.3334	1.7396	2.1098	2.5669	2.8982	3.9651
18	0.1274	0.2571	0.3915	0.6884	0.8620	1.0672	1.3304	1.7341	2.1009	2.5524	2.8784	3.9216
19	0.1274	0.2569	0.3912	0.6876	0.8610	1.0655	1.3277	1.7291	2.0930	2.5395	2.8609	3.8834
α	0.45	0.40	0.35	0.25	0.20	0.15	0.10	0.05	0.025	0.01	0.005	0.0005
20	0.1273	0.2567	0.3909	0.6870	0.8600	1.0640	1.3253	1.7247	2.0860	2.5280	2.8453	3.8495
21	0.1272	0.2566	0.3906	0.6864	0.8591	1.0627	1.3232	1.7207	2.0796	2.5176	2.8314	3.8193
22	0.1271	0.2564	0.3904	0.6858	0.8583	1.0614	1.3212	1.7171	2.0739	2.5083	2.8188	3.7921
23	0.1271	0.2563	0.3902	0.6853	0.8575	1.0603	1.3195	1.7139	2.0687	2.4999	2.8073	3.7676
24	0.1270	0.2562	0.3900	0.6848	0.8569	1.0593	1.3178	1.7109	2.0639	2.4922	2.7969	3.7454
25	0.1269	0.2561	0.3898	0.6844	0.8562	1.0584	1.3163	1.7081	2.0595	2.4851	2.7874	3.7251
26	0.1269	0.2560	0.3896	0.6840	0.8557	1.0575	1.3150	1.7056	2.0555	2.4786	2.7787	3.7066
27	0.1268	0.2559	0.3894	0.6837	0.8551	1.0567	1.3137	1.7033	2.0518	2.4727	2.7707	3.6896
28	0.1268	0.2558	0.3893	0.6834	0.8546	1.0560	1.3125	1.7011	2.0484	2.4671	2.7633	3.6730

Entonces, sabiendo que el P valor al estar por debajo del nivel de significancia que es 0,05 rechaza la Hipótesis Nula y se acepta la Hipótesis Alternativa. También podemos afirmar que el valor obtenido de la prueba t se encuentra en la zona de rechazo, donde no se acepta la hipótesis nula y se acepta la hipótesis alterna con un porcentaje de 95% de confianza. Por estas dos razones, El sistema de reconocimiento facial mejora la precisión de acceso del personal en el área de almacén en la Clínica Multident Buenos Aires.

HIPÓTESIS GENERAL:

De acuerdo a los resultados obtenidos para los indicadores Control de Acceso autorizado y Precisión de acceso, se rechaza la hipótesis nula y se acepta la hipótesis alternativa, toda vez que los resultados obtenidos se encuentran en la región de rechazo. Es por ello se acepta la Hipótesis alterna la cual es El Sistema de Reconocimiento Facial mejora el control de acceso del personal en el almacén de la Clínica Multident Buenos Aires

V DISCUSIÓN

Este trabajo de se realizó, con el objetivo de poder determinar la influencia que tiene el sistema de reconocimiento facial con aprendizaje profundo para el control de acceso, en el almacén de la Clínica Odontológica Multident Buenos Aires.

En base a los resultados obtenidos en la investigación, se obtuvo como resultado que el sistema de reconocimiento facial con aprendizaje profundo ayudo a mejorar el indicador de control de acceso autorizados de un 3% a un 13%, lo que equivale a un aumento del 10%. Ahora bien, al realizar la comparación con el indicador de acceso autorizado en la investigación del autor Yáñez (2019) titulada “Sistema de reconocimiento facial para el control de acceso de estudiantes a los laboratorios de la FIIS-UNAC, 2019”, donde su indicador alcanzo el 100% de acceso autorizados después de la implementación. Por otro lado, al realizar la comparación del mismo indicador del autor Aquijes (2021) titulada “Implementación de un Sistema de Reconocimiento Facial para el control de acceso del personal en la empresa GUIMARTBOT S.A.C” su indicador de control de acceso autorizado alcanzo un incremento del 18%. Podemos deducir que el sistema de reconocimiento facial mejora significativamente el control de acceso autorizados y por otro lado disminuye los no autorizados.

Por otro lado, según los resultados obtenidos en la investigación con el sistema de reconocimiento facial con aprendizaje profundo también ayudo a mejorar el indicador de precisión de acceso autorizado de un 82% a un 92%, lo que nos da entender que el indicador mejoro en un 10% en cuanto a su precisión. Ahora bien, al realizar la comparación con el indicador de precisión de acceso autorizado en la investigación de los autores Galindo, Huaranga y Samaniego (2021), en su tesis titulada “Reconocimiento facial para la identificación de los alumnos en exámenes finales en la modalidad presencial de la Universidad Continental – Huancayo, 2021”, donde su indicador de precisión alcanzo el 90% de precisión después de la implementación, podemos deducir que el sistema de reconocimiento facial mejora significativamente la precisión de acceso.

VI CONCLUSIONES

Se concluyo que el sistema de reconocimiento facial con aprendizaje profundo mejoro el control de acceso en el área de almacén de la Clinica Odontológica Multident Buenos Aires, dado que nos ayudó a minimizar el control de acceso de las personas no autorizadas y mejoro la precisión de acceso autorizado, permitiendo así poder alcanzar las metas de este trabajo de Tesis.

Se concluyo que el sistema de reconocimiento facial con aprendizaje profundo mejoró el indicado de control de acceso autorizado en un 10%. Antes de la implementación tuvo un resultado de 3% y ya con la implementación un 13%. En base a esto podemos afirmar que el sistema de reconocimiento facial mejora el control de acceso autorizado minimizando los accesos no autorizados en la Clinica Odontológica Multident Buenos Aires.

Se concluyo que el sistema de reconocimiento facial con aprendizaje profundo mejoro el indicador de precisión de acceso en un 10%. Antes de la implementación tuvo un 82% y ya con la implementación un 92%. En base a esto podemos afirmar que el sistema de reconocimiento facial con aprendizaje profundo mejora la precisión de acceso en Clinica Odontológica Multident Buenos Aires.

Finalmente, después de obtener resultados satisfactorios en los indicadores planteados en esta Tesis se llega a la conclusión que el sistema de reconocimiento facial con aprendizaje profundo mejora el control de acceso autorizado y la precisión de acceso en el almacén de la Clinica Odontológica Multident Buenos Aires.

VII RECOMENDACIONES

Al tener como fuente principal la implementación del sistema de reconocimiento facial con aprendizaje profundo para el control de acceso en el almacén de la Clínica Odontológica Multident Buenos Aires y después de demostrar la optimización del proceso, se recomienda para las futuras investigaciones lo siguiente:

- Se recomienda llevar el reporte de nivel de acceso del personal con el fin de llevar un control de acceso autorizado para acceder al almacén del personal de la Clínica Multident Buenos Aires.
- Se recomienda poder realizar una capacitación para los usuarios en cuanto al manejo del sistema de reconocimiento facial para el momento en que haya nuevo personal autorizado o no autorizado en la Clínica Multident Buenos Aires.
- Se recomienda llevar el reporte de precisión de acceso con el fin de llevar un control adecuado y en cuanto mejora la precisión de acceso del personal de la Clínica Multident Buenos Aires.
- Manejo de software de manera correcta para evitar posibles complicaciones a nivel lógico.
- Se recomiendan cámaras de video Ip cableadas ya que nos darán una mejor cobertura, puesto que las cámaras con wifi tienden a no tener un buen control ya que dependen de la cobertura del wifi.
- A los estudios siguientes que deseen implementar un sistema de reconocimiento facial con aprendizaje profundo esta investigación puede servir como guía en estudios futuros que así requieran.

REFERENCIAS

ALBON, Cris. Python Machine Learning Cookbook: Practical Solutions from Preprocessing to Deep Learning. 1er ed. U.S.A: O'Reilly Media. 2018. 366 pp. ISBN10: 1491989386, ISBN13: 9781491989388.

ALCARAZ, M. 2020. Head-tracking as an interface device for image control in digital pathology: a comparative study. Murcia, España: Servicio de Anatomía Patológica, 2020. ISSN: 16998855

ALEJO, Paul. (2021) Algoritmo de reconocimiento facial para la gestión del control de acceso de la empresa Altoque PS S.A. Previo a Tesis de Título (Ingeniero de Sistemas de información y comunicaciones). Perú: Universidad Cesar Vallejo, Lima, 2021. Disponible en: https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/84197/Alejo_CPS-SD.pdf?sequence=1&isAllowed=y

AQUIJEZ, Ronny. 2021. Implementación de un Sistema de Reconocimiento Facial para el control de acceso del personal en la empresa GUIMARTBOT S.A.C. Tesis de Título (Ingeniero de Sistemas). Perú: Universidad Cesar Vallejo, Lima, 2021. Disponible en: https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/83111/Aquijez_CRD-Ampuero_ML-SD.pdf?sequence=1&isAllowed=y

BEARMUD, Soraya. Elaboración de un Plan de Implementación de la ISO/IEC 27001:2013. Tesis (Máster Interuniversitario en Seguridad de las Tecnologías de la Información y de las Comunicaciones). España: Universidad Oberta de Catalunya, 2016. Disponible en: <https://openaccess.uoc.edu/bitstream/10609/53528/7/sjimenezbeTFM0616mem%C3%B2ria.pdf>

BECERRA, Fray. Patrones de conducta facial, para identificar accesos informáticos no autorizados. Trabajo de Titulación. Perú. Universidad Señor de Sipán, Facultad de Ingeniería, Arquitectura y Urbanismo. 2019. 110 pp.

Berryhill, J. 2019. La Inteligencia artificial y su uso en el sector público. Paris, Francia: OECD Working Paper, 2019. ISSN: 19934351.

BRAVO, CJ. 2018. Aceptación del reconocimiento facial como medida de vigilancia y seguridad: un estudio empírico en Chile. Coquimbo, Chile: s.n., 2018. ISSN:07168756

CACERES, Mariño. “Aplicación Móvil de Reconocimiento Facial en Personas con Antecedentes de Abuso Sexual en la Provincia de Andahuaylas, Apurímac- 2018”, tesis de título, Univ. Nacional José María Arguedas, 2018 [En línea]. Disponible en: http://repositorio.unajma.edu.pe/bitstream/handle/123456789/358/Ervin_Lewis_Tesis_Bachiller_2018.pdf?sequence=1&isAllowed=y.

CALDER, Alan. ISO27001/ISO27002: Una guía de bolsillo. Inglaterra: IT Governance Publishing. 2017. 83 pp. ISBN: 9781849289184

CALLES, Marco. Sistema informático de reconocimiento facial para el registro y control de asistencia de los socios de la cooperativa de taxis y camionetas Puyo. Previa a Tesis de Título (Ingeniero de Sistemas e Informático). Ecuador: Universidad Regional Autónoma de los Andes, Puyo, 2019. Disponible en: <https://n9.cl/bTSc>

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

CASTRO, Fernando. El proyecto de investigación y su esquema de elaboración. Caracas: Uyapar, 2003, 144pp. ISBN: 9806629000

COSTA, Mari, Análisis de un Sistema de reconocimiento facial a partir de una base de datos realizada mediante Python. Tesis (Obtención de grado en Ingeniería Electrónica Industrial y Automática. Barcelona. Universidad Politécnica de Catalunya BarcelonaTech, Escola d’Enginyeria de Barcelona Est, 2020. 99. P.

DOMINGUEZ, Tomás. Visión artificial: Aplicaciones prácticas con OpenCV - Python. 1 era ed. España: Marcombo, 2021. 388 pp. ISBN: 9788426733474

ESTREMADOYRO Lam, Ignacio. Modelo propuesto para la toma de asistencia con reconocimiento facial en imágenes capturadas con múltiples rostros en la escena. Tesis (Ingeniero de Sistemas). Arequipa: Universidad Católica de Santa María, 2016. 76 pp. <http://tesis.ucsm.edu.pe/repositorio/handle/UCSM/5265>

FAIRHUST, Michael. Biometrics: A Very Short Introduction (Very Short Introductions). 1er ed. U.S.A: Oxford University Press, 2019. 143 pp. ISBN10: 0198809107, ISBN13: 9780198809104.

FERRO, José. SISTEMAS DE SEGURIDAD. 1 era ed. España: José Manuel Ferro Veiga, 2020. 357 pp. ISBN: 9756301724386

FILGUERAS, Fernando. Inteligencia Artificial en la administración pública: ambigüedad y elección de sistemas de IA y desafíos de gobernanza digital. Brasil: Revista del CLAD Reforma y Democracia, 2021, 38 pp. ISSN 1315-2378

FUNDACIÓN TELEFÓNICA. Sociedad Digital en España 2020-2021: El año en que todo cambió. 1 era ed. España: Fundación Telefónica, 2021. 637 pp. ISBN: 9788430624386

GALINDO, Jenny. Control de Acceso a Archivos y Carpetas a través del reconocimiento Facial [En línea]. Agosto 2017 N°1 [Fecha de consulta: 16 de abril del 2022]. Disponible en: <http://investigacionsis.fuac.edu.co/html/RepositorioOJS/ojsfuac/ojs/index.php/UAC SIS/article/download/27/32>

ISSN: 2346-3562

GOWRISHANKAR S, y VEENA A. Introduction to Python Programming. Editorial CRC, 2019. 465 pp. ISBN13: 9780815394372, ISBN10: 0815394373

HUAMANI, P. 2020. Enfoque Práctico de la aplicación del Toolbox Deep Learning del Matlab en el reconocimiento Facial de estudiantes. Lima, Perú: Universidad Ricardo Palma, 2020. ISBN: 978-958520714-1

HUERTA, Marcos. Porque fracasan las Organizaciones.1°. Ediciones Pirámide, 2013, 256 pp ISBN 978-84-368-2987-7

IÑIGUEZ, Hector. SEGURIDAD INFORMÁTICA Y PROTECCIÓN DE DATOS PERSONALES. Bolivia: Hector Giuseppe Iñiguez Estrada, 2020. 115 pp. ISBN: 9789917004936

IRIZARRY, Rafael. Introduction to Data Science. Estados Unidos: Chapman & Hall, 2019. 743 pp. ISBN 9780367357986

LAI, K. Multi-Spectral Facial Biometrics in Access Control. Universidad of Drive NW. Calgary: Canadá, 2020. 99pp. Disponible en <https://arxiv.org/pdf/2007.11318.pdf>

LOZANO, José Luis. Cámaras de reconocimiento facial en el arte contemporáneo: la obra del colectivo Sven de España. Valencia: Universidad Miguel Hernández Altea 6 (2): 203-212, 2018. ISSN 2340-8510

MARTINEZ, Rodolfo. Diseño del Sistema de Control de Asistencia en la Agencia Mercado de la Caja Huancayo aplicando Tarjetas de Proximidad de Tecnología RFID. Tesis (Ingeniero en Sistemas e Informática). Perú: Universidad Continental, 2017. Disponible en: <https://n9.cl/V9wl>

Ministerio de Tecnologías de la Información y las Comunicaciones. Organización de la Seguridad de la Información. Colombia: Bogotá, 2021. Disponible en: <https://www.csirt.gob.cl/estadisticas/el-control-de-la-semana-no-2-organizacion-de-la-seguridad-de-la-informacion/>

MOHAMMAD, Sikender. Facial Recognition Technology [en Línea]. 2020. [Fecha de Acceso: 05 de mayo 2021]. Disponible en SSRN: <https://ssrn.com/abstract=3622882> or <http://dx.doi.org/10.2139/ssrn.3622882>

MOLLOY, Derek. Raspberry Pi® a fondo para desarrolladores. España: Marcombo, 2019. 696 pp. ISBN: 9788426727800

MORENO, Mar. Inteligencia artificial (Umbralés éticos, Derecho y Administraciones Públicas). 9 na ed. España: Aranzadi / Civitas, 2021. 144p. ISBN: 9788413910284

Ñaupas, H. 2018. Metodología de la investigación cuantitativa-cualitativa y redacción de la tesis. Bogotá, Colombia: Ediciones de la U, 2018. 538 p. ISBN:978-958-762-876-0.

OTZEN, T. y MANTEROLA, C. 2017. Técnicas de Muestreo sobre una Población a Estudio. Int. J. Morphol. 35(1), pp.227-232. ISSN 0717-9502

Patienten, S. 2020. Inhibitor May Promote Better Responses to Abiraterone inmCRPC. Oxford, Reino Unido: s.n., 2020. DOI: 10.1093/annonc

RAMIREZ Cáceres, Robert. Análisis y diseño de un sistema web de reconocimiento facial para la autenticación y control de personal del Cisea Palmira, Huaraz – 2017.

Tesis (Ingeniero de Sistemas e Informática).
<http://repositorio.unasam.edu.pe/handle/UNASAM/1156?show=full>

Ramos, Daniel. Curso de Ingeniería de Software. 2ª edición. España: 3Ciencias, 2017. 339 pp. ISBN 9781544132532.

ROUHIANEN, Lasse. Inteligencia artificial: 101 cosas que debes saber hoy sobre nuestro futuro. España: Alienta, 2018. 352 pp. ISBN: 9788417568122

RUIZ, Elena. Nuevas tendencias en los sistemas de información. Madrid: Editorial Universitaria Ramón Areces, 2017. 332 pp. ISBN: 978-84-9961-269- 0

SALVATIERRA T. Desarrollo de un sistema de control de asistencia estudiantil mediante reconocimiento facial. Tesis (Master en Ingeniería de Software y sistemas informáticos). Ecuador: Universidad Internacional de la Rioja, 2018. Disponible en: <https://n9.cl/RINv>

TAYLOR, B.S. Setting intentions: considering racial justice implications of facial recognition technology. Degree of Master of Arts in Communication, Culture and Technology. Georgetown University. 2020. 57 pp.

VALBUENA, Roiman. Inteligencia Artificial: Investigación Científica Avanzada Centrada en Datos. España: Cencal Press, 2021. 499 pp. ISBN: 9789801815297

VEGA, Edgar. Seguridad de la información. 1 era ed. España: 3Ciencias, 2021. 112 pp. ISBN: 9788412209365

VELARDE, Olenka y YABARRENA, Josué. Sistema de reconocimiento facial para el control de la trata de personas en Perú. Tesis (Ingeniero de Sistemas). Perú: Universidad Andina del Cusco, 2018. Disponible en: <http://repositorio.uandina.edu.pe/handle/UAC/2047>

VEJARANO, Martín (2018). Reconocimiento Facial mediante Imágenes Estereoscópicas. Tesis (Ingeniero de Sistemas). Perú: Universidad Señor de Sipán, 2018. Disponible en: <https://repositorio.uss.edu.pe/handle/20.500.12802/5339>

WARDEN, Pete Machine Learning with TensorFlow Lite on Arduino and Ultra Low-Power Microcontrollers. EEUU: Editorial "O'Reilly Media, Inc.", 2019. 504 pp. ISBN: 9781492052012

YAÑEZ, Margarita. Sistema de reconocimiento facial para el control de acceso de estudiantes a los laboratorios de la FIIS-UNAC, 2019. Trabajo para titulación. Perú. Universidad César Vallejo, Facultad de Ingeniería de Sistemas.2019. 220 pp.

ANEXOS

ANEXO 1: Matriz de operacionalización de variable

Variable	Definición Conceptual	Definición Operacional	Dimensión	Indicador	Fórmula	Instrumento	Escala
Variable independiente: Sistema de reconocimiento facial	Según Moreno (2021), define que el reconocimiento facial es un sistema de identificación avanzada, ya que, permite identificar al sujeto por medio de una imagen, vídeo o cualquier parte del rostro.						
Variable dependiente: Control de acceso	Según Vega (2021), es un medio o sistema que responde mediante autorización y denegación para dar acceso a un lugar, recurso o bien específico previo asignación (p.47).	Se utiliza el instrumento ficha de registro para la recolección de datos donde se obtendrá la información de los indicadores planteados de la investigación, adhiriendo una escala de razón.	Seguridad Física	Control de acceso autorizado	$PAA = \frac{NAA}{NAT} * 100$ <p>PAA: Porcentaje de accesos autorizados NAA: Número de accesos autorizados NAT: Número de accesos totales.</p>	Ficha de registro	RAZÓN
				Precisión de acceso	<p>Según Albon: Precisión</p> $P = \frac{VP}{VP+FP}$ <p>P= Precisión VP=Verdadero Positivo, predice correcto. FP=Falso Positivo, predice incorrecto.</p>	Ficha de registro	RAZÓN

ANEXO 2: Matriz de consistencia

Sistema de Reconocimiento Facial con aprendizaje profundo para el control de acceso del almacén de la Clínica Multident Buenos Aires					
Problema	Objetivos	Hipótesis	Indicador	Fórmula	Metodología
<p>General</p> <p>¿De qué manera influye el Sistema de Reconocimiento Facial con aprendizaje profundo para mejorar el control de acceso de la Clínica Multident Buenos Aires?</p>	<p>General</p> <p>Desarrollar un Sistema de Reconocimiento Facial con aprendizaje profundo para mejorar el control de acceso en el almacén de la Clínica Multident Buenos Aires</p>	<p>General</p> <p>El Sistema de Reconocimiento Facial con aprendizaje profundo mejora el control de acceso en el almacén de la Clínica Multident Buenos Aires</p>			
<p>Específico</p> <p>¿Cuál será el efecto del Sistema de Reconocimiento Facial con aprendizaje profundo para el control de acceso autorizado en el área de almacén de la Clínica Multident Buenos Aires?</p>	<p>Específico</p> <p>Determinar la influencia de un Sistema de Reconocimiento Facial con aprendizaje profundo en el control de acceso autorizado del área de almacén en la Clínica Multident Buenos Aires</p>	<p>Específico</p> <p>El Sistema de Reconocimiento Facial con aprendizaje profundo mejora el control de acceso del personal en el área de almacén en la Clínica Multident Buenos Aires</p>	<p>Control de acceso autorizado</p>	$PAA = \frac{NAA}{(NAT)} * 100$	<p>Tipo de investigación: Aplicada</p> <p>Diseño de investigación: Experimental Preexperimental</p>
<p>Específico</p> <p>¿Cuál será la precisión de un Sistema de Reconocimiento Facial con aprendizaje profundo en el control de acceso de la Clínica Multident Buenos Aires?</p>	<p>Específico</p> <p>Calcular la precisión del Sistema de Reconocimiento Facial con aprendizaje profundo del personal en el área de almacén en la Clínica Multident Buenos Aires</p>	<p>Específico</p> <p>El Sistema de Reconocimiento Facial con aprendizaje profundo mejora la precisión del reconocimiento del personal en el área de almacén en la Clínica Multident Buenos Aires</p>	<p>Precisión de acceso</p>	$P = \frac{VP}{VP+FP}$	

ANEXO 3: Validación de juicios de expertos



CERTIFICADO DE VALIDEZ DE CONTENIDO DEL INSTRUMENTO QUE MIDE LA VARIABLE CONTROL DE ACCESO

N.º	INDICADORES / ITEMS	Pertinencia ¹		Relevancia ²		Claridad ³		Sugerencias
		Si	No	Si	No	Si	No	
	DIMENSION 1							
1.	Control de acceso autorizado	x		x		x		
	DIMENSION 2							
2.	Precisión de acceso	x		x		x		

Observaciones (precisar si hay suficiencia): _____

Opinión de aplicabilidad: Aplicable Aplicable después de corregir No aplicable

Apellidos y nombres del juez validador. Mg: Angeles Pinillos, Daniel Orlando

DNI:46442421

¹Pertinencia: El ítem corresponde al concepto teórico formulado.

²Relevancia: El ítem es apropiado para representar al componente o dimensión específica del constructo

³Claridad: Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo

Nota: Suficiencia, se dice suficiencia cuando los ítems planteados son suficientes para medir la dimensión

25 de junio del 2022



Firma del Experto Informante



CERTIFICADO DE VALIDEZ DE CONTENIDO DEL INSTRUMENTO QUE MIDE LA VARIABLE CONTROL DE ACCESO

N.º	INDICADORES / ITEMS	Pertinencia ¹		Relevancia ²		Claridad ³		Sugerencias
		Si	No	Si	No	Si	No	
	DIMENSION 1							
1.	Control de acceso autorizado	x		x		x		
	DIMENSION 2							
2.	Precisión de acceso	x		x		x		

Observaciones (precisar si hay suficiencia): _____

Opinión de aplicabilidad: Aplicable [**X**] Aplicable después de corregir [] No aplicable []

Apellidos y nombres del juez validador. **Mg: Christian Víctor Ortega Vargas**

DNI: 43989724

¹Pertinencia: El ítem corresponde al concepto teórico formulado.

²Relevancia: El ítem es apropiado para representar al componente o dimensión específica del constructo

³Claridad: Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo

Nota: Suficiencia, se dice suficiencia cuando los ítems planteados son suficientes para medir la dimensión

9 de julio del 2022

Firma del Experto Informante



CERTIFICADO DE VALIDEZ DE CONTENIDO DEL INSTRUMENTO QUE MIDE LA VARIABLE CONTROL DE ACCESO

N°	INDICADORES / ITEMS	Pertinencia ¹		Relevancia ²		Claridad ³		Sugerencias
		Si	No	Si	No	Si	No	
	DIMENSION 1							
1.	Control de acceso autorizado	x		x		x		
	DIMENSION 2							
2.	Precisión de acceso	x		x		x		

Observaciones (precisar si hay suficiencia): _____

Opinión de aplicabilidad: Aplicable Aplicable después de corregir

No aplicable

Apellidos y nombres del juez validador. Mg: Ventocilla Aguado, Cristian

DNI: 15760318

¹Pertinencia: El ítem corresponde al concepto teórico formulado.

²Relevancia: El ítem es apropiado para representar al componente o dimensión específica del constructo

³Claridad: Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo

Nota: Suficiencia, se dice suficiencia cuando los ítems planteados son suficientes para medir la dimensión

25 de junio del 2022

Firma del Experto Informante

ANEXO 4: ASPECTOS ADMINISTRATIVOS

Recursos y Presupuestos

a. Recursos Humanos

Recursos Humanos									
Nombres y apellidos	Función / Rol	N° de meses	Costo Total (s/.)	Entidades				Total	
				Propio		Aporte empresa		Aporte monetario	Aporte no monetario
				Aporte monetario	Aporte no monetario	Aporte monetario	Aporte no monetario		
- Nicolas Chavez Vásquez	Investigador	4	2000	S/ .0	S/ .2000	S/ .0	S/ .2000	S/ .0	S/ .2000
-Armando Valentín Arana	Investigador	4	2000	S/ .0	S/ .2000	S/ .0	S/ .2000	S/ .0	S/ .2000
Total, S/.				S/ .0	S/.4000	S/ .0	S/.4000	S/ .0	S/.4000

Tabla 4: Recurso Humanos
Fuente: Elaboración propia

b. Equipos y bienes duraderos

Equipos y bienes duraderos										
Descripción	Unidad de medida	Cantidad	Costo Unitario (s/.)	Costo Total (s/.)	Entidades				Total	
					Propio		Aporte empresa			
					Aporte monetario	Aporte no monetario	Aporte monetario	Aporte no monetario	Aporte monetario	Aporte no monetario
Laptop HP- Core i5	UND	2	3500	7000	S/ .0	S/ .7000	S/ .0	S/ .0	S/ .0	S/ .7000
CPU	UND	1	1200	1200	S/ .0	S/ .0	S/ .1200	S/ .0	S/ .1200	S/ .0
Cámara	UND	1	250	250	S/ .0	S/ .0	S/ .250	S/ .0	S/ .250	S/ .0
Disco externo	UND	1	400	400	S/ .0	S/ .0	S/ .400	S/ .0	S/ .400	S/ .0
Cable UTP	UND	2	30	60	S/ .0	S/ .0	S/ .60	S/ .0	S/ .60	S/ .0
USB Kingston de 64	UND	2	69	138	S/ .138	S/ .0	S/ .0	S/ .0	S/ .138	S/ .0
Celular Samsung Galaxy A30s	UND	1	1299	1299	S/ .0	S/ .1299	S/ .0	S/ .0	S/ .0	S/ .1299
Celular Vivo 21	UND	1	1199	1199	S/ .0	S/ .1199	S/ .0	S/ .0	S/ .0	S/ .1199
Impresora multifuncional EPSON L375	UND	1	649	S/ .649	S/ .0	S/ .649	S/ .0	S/ .0	S/ .0	S/ .649
Total, S/.					S/ .138	S/ .10796	S/ .1910	S/ .0	S/ .2048	S/ .10147

Tabla 5: Equipos y bienes duraderos
Fuente: Elaboración propia

c. Materiales e insumos

Materiales e insumos										
Descripción	Unidad de medida	Cantidad	Costo Unitario (s/.)	Costo Total (s/.)	Entidades empresa				Total	
					Propio		Aporte Empresa		Aporte monetario	Aporte no monetario
					Aporte monetario	Aporte no monetario	Aporte monetario	Aporte no monetario		
Papel bond	PK	1	17	17	S/ .0	S/ .0	S/ .17	S/ .0	S/ .17	S/ .0
Lapicero	UND	3	6	18	S/ .0	S/ .0	S/ .18	S/ .0	S/ .18	S/ .0
Licencia Office 365	UND	1	249	249	S/ .0	S/ .0	S/ .249	S/ .0	S/ .249	S/ .0
Licencia Visual Studio	UND	2	132	264	S/ .0	S/ .0	S/ .264	S/ .0	S/ .264	S/ .0
Tinta para impresora	UND	10	45	450	S/ .0	S/ .0	S/ .450	S/ .0	S/ .450	S/ .0
Folders	UND	4	0.5	2	S/ .0	S/ .0	S/ .2	S/ .0	S/ .2	S/ .0
Total, S/.					S/ .0	S/ .0	S/ .1000	S/ .0	S/ .1000	S/ .0

Tabla 6: Materiales e insumos
Fuente: Elaboración propia

d. Asesorías especializadas y servicios

Asesorías especializadas y servicios										
Descripción	Unidad de medida	Cantidad	Costo Unitario (s/.)	Costo Total (s/.)	Entidades				Total	
					Propio		Aporte Empresa		Aporte monetario	Aporte no monetario
					Aporte monetario	Aporte no monetario	Aporte monetario	Aporte no monetario		
Servicio de telefonía	UND	2	25	50	S/ .0	S/ .50	S/ .0	S/ .0	S/ .0	S/ .50
Servicio de internet	UND	2	40	80	S/ .0	S/ .80	S/ .0	S/ .0	S/ .0	S/ .80
Servicio de hosting	Mes	2	80	160	S/ .0	S/ .160	S/ .0	S/ .0	S/ .0	S/ .160
Servicio de empastado	UND	2	8	16	S/ .0	S/ .16	S/ .0	S/ .0	S/ .0	S/ .16
Servicio de anillado	UND	2	9	18	S/ .0	S/ .18	S/ .0	S/ .0	S/ .0	S/ .18
Servicio de energía eléctrica	UND	2	100	200	S/ .0	S/ .200	S/ .0	S/ .0	S/ .0	S/ .200
Servicio de autobús	UND	15	12	180	S/ .0	S/ .180	S/ .0	S/ .0	S/ .0	S/ .180
Total					S/ .0	S/ .704	S/ .0	S/ .0	S/ .0	S/ .704

Tabla 7: Asesorías especializadas y servicio
Fuente: Elaboración propia

Financiamiento

Con recurso universitario:

S/. 0.00 (0 %)

Con recurso de la empresa:

S/. 2910 (20%)

Autofinanciamiento

S/. 11.638 (80%)

Cronograma de ejecución

Se ha optado de utilizar el cronograma de Gantt para tener las fechas y tiempos que se desarrollara en el proyecto, se puede observar en el anexo 9.

ANEXO 5: PRE-TEST Control de acceso autorizado

FICHA DE REGISTRO					
INVESTIGADORES		Chavez Vasquez, Nicolas Valentin Arana, Jean Pierre		Tipo de Prueb	PRE TEST
EMPRESA		Clínica Multident Buenos Aires			
DIRECCION		Av. Wiese Mza. D1 Lt. 27 Lima-San Juan de Lurigancho			
FECHA DE INICIO		25/07/2022	FECHA FINAL		24/08/2022
VARIABLE		INDICADOR	MEDIDA	FORMULA	
Control de Acceso		Control de acceso autorizado	Porcentual	$PAA = \frac{NAA}{NAT} * 100$	
N°	Nombre Personal	Fecha	PAA: Porcentaje de Accesos autorizados	NAA: Numero de acceso autorizados	NAT: Numeros de acceso totales
1	Personal 1	25/07/2022 24/08/2022	4%	30	727
2	Personal 2	25/07/2022 24/08/2022	4%	40	998
3	Personal 3	25/07/2022 24/08/2022	2%	25	1107
4	Personal 4	25/07/2022 24/08/2022	2%	10	420
5	Personal 5	25/07/2022 24/08/2022	2%	12	490
6	Personal 6	25/07/2022 24/08/2022	10%	115	1107
7	Personal 7	25/07/2022 24/08/2022	11%	125	1107
8	Personal 8	25/07/2022 24/08/2022	10%	117	1107
9	Personal 9	25/07/2022 24/08/2022	12%	135	1107
10	Personal 10	25/07/2022 24/08/2022	2%	21	850
11	Personal 11	25/07/2022 24/08/2022	2%	21	854
12	Personal 12	25/07/2022 24/08/2022	2%	27	1080
13	Personal 13	25/07/2022 24/08/2022	0%	0	638
14	Personal 14	25/07/2022 24/08/2022	0%	0	628
15	Personal 15	25/07/2022 24/08/2022	0%	0	590
16	Personal 16	25/07/2022 24/08/2022	0%	0	629
17	Personal 17	25/07/2022 24/08/2022	0%	0	636
18	Personal 18	25/07/2022 24/08/2022	0%	0	602
19	Personal 19	25/07/2022 24/08/2022	0%	0	638

ANEXO 7: PRE-TEST Precisión de acceso autorizado

FICHA DE REGISTRO					
INVESTIGADORES		Chavez Vasquez, Nicolas Valentin Arana, Jean Pierr		Tipo de Prue	PRE TEST
EMPRESA		Clínica Multident Buenos Aires			
DIRECCION		Av. Wiese Mza. D1 Lt. 27 Lima-San Juan de Lurigancho			
FECHA DE INICIO		25/07/2022	FECHA FINAL		24/08/2022
VARIABLE		INDICADOR	MEDIDA	FORMULA	
Control de Acceso		Precisión de acceso	Decimal	$P = \frac{VP}{VP + FP}$	
N°	Nombre Persona	Fecha	P: Precisión	VP: Verdadero Positivo	FP: Falso Positivo
1	Personal 1	25/07/2022 24/08/2022	0,8	24	6
2	Personal 2	25/07/2022 24/08/2022	0,82	33	7
3	Personal 3	25/07/2022 24/08/2022	0,92	23	2
4	Personal 4	25/07/2022 24/08/2022	0,9	9	1
5	Personal 5	25/07/2022 24/08/2022	0,91	11	1
6	Personal 6	25/07/2022 24/08/2022	0,82	96	21
7	Personal 7	25/07/2022 24/08/2022	0,90	113	15
8	Personal 8	25/07/2022 24/08/2022	0,82	97	20
9	Personal 9	25/07/2022 24/08/2022	0,85	115	20
10	Personal 10	25/07/2022 24/08/2022	0,85	18	3
11	Personal 11	25/07/2022 24/08/2022	0,80	17	4
12	Personal 12	25/07/2022 24/08/2022	0,85	23	4
13	Personal 13	25/07/2022 24/08/2022	0,80	61	15
14	Personal 14	25/07/2022 24/08/2022	0,79	58	15
15	Personal 15	25/07/2022 24/08/2022	0,80	68	16
16	Personal 16	25/07/2022 24/08/2022	0,78	52	14
17	Personal 17	25/07/2022 24/08/2022	0,82	75	16
18	Personal 18	25/07/2022 24/08/2022	0,79	64	17
19	Personal 19	25/07/2022 24/08/2022	0,70	70	18

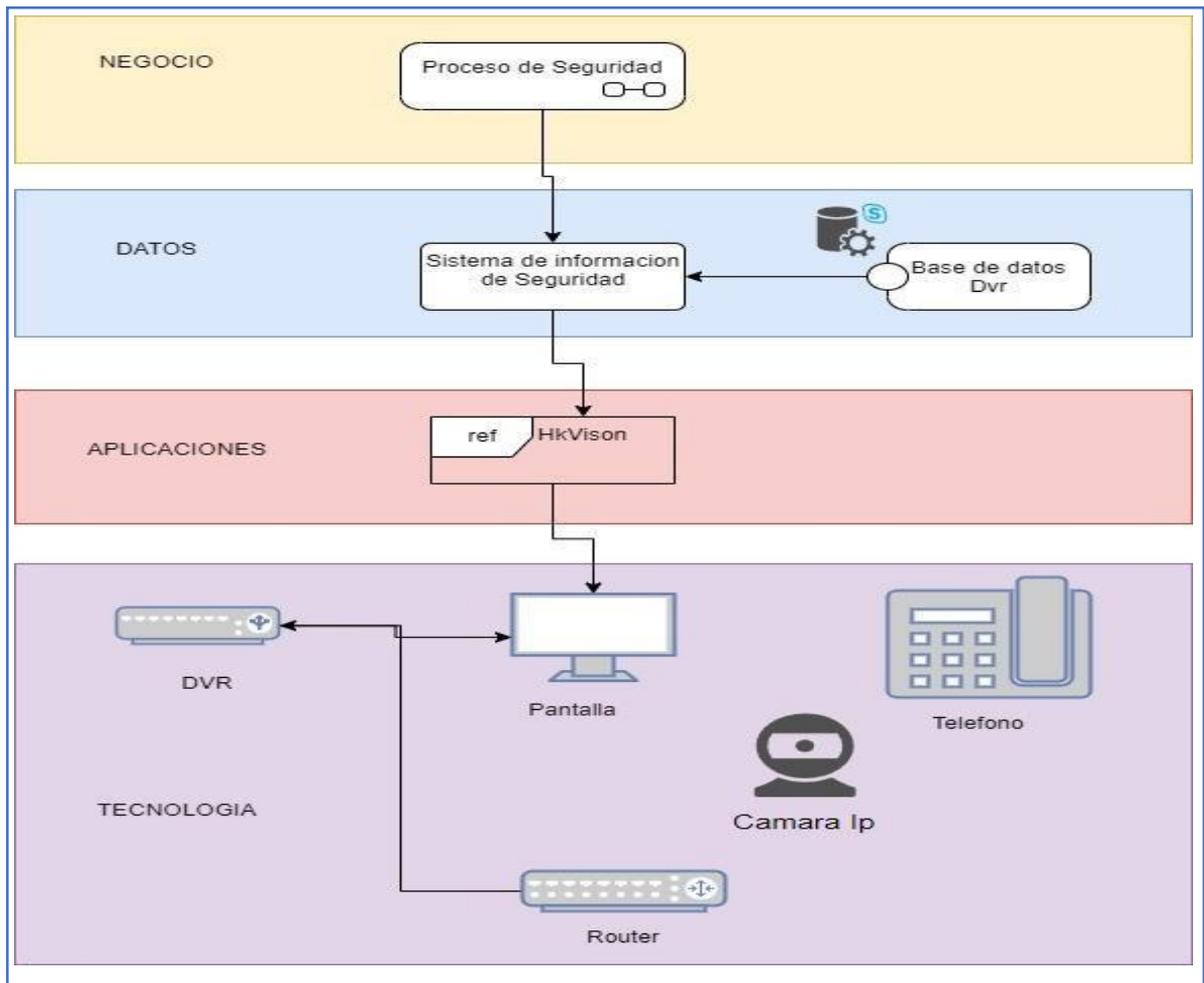
ANEXO 9: POST-TEST Control de acceso autorizado

FICHA DE REGISTRO					
INVESTIGADORES		Chavez Vasquez, Nicolas Valentin Arana, Jean Pierre		Tipo de Prueb	POST TEST
EMPRESA		Clínica Multident Buenos Aires			
DIRECCION		Av. Wiese Mza. D1 Lt. 27 Lima-San Juan de Lurigancho			
FECHA DE INICIO		26/09/2022	FECHA FINAL		26/10/2022
VARIABLE		INDICADOR	MEDIDA	FORMULA	
Control de Acceso		Control de acceso autorizado	Porcentual	$PAA = \frac{NAA}{NAT} \cdot 100$	
N°	Nombre Personal	Fecha	PAA: Porcentaje de Accesos autorizados	NAA: Numero de acceso autorizados	NAT: Numeros de acceso totales
1	Personal 1	26/09/2022 26/10/2022	19%	24	125
2	Personal 2	26/09/2022 26/10/2022	18%	44	253
3	Personal 3	26/09/2022 26/10/2022	17%	27	158
4	Personal 4	26/09/2022 26/10/2022	18%	24	135
5	Personal 5	26/09/2022 26/10/2022	19%	20	105
6	Personal 6	26/09/2022 26/10/2022	25%	165	667
7	Personal 7	26/09/2022 26/10/2022	23%	152	667
8	Personal 8	26/09/2022 26/10/2022	30%	197	667
9	Personal 9	26/09/2022 26/10/2022	28%	134	667
10	Personal 10	26/09/2022 26/10/2022	17%	25	145
11	Personal 11	26/09/2022 26/10/2022	19%	26	134
12	Personal 12	26/09/2022 26/10/2022	19%	25	130
13	Personal 13	26/09/2022 26/10/2022	0%	0	250
14	Personal 14	26/09/2022 26/10/2022	0%	0	268
15	Personal 15	26/09/2022 26/10/2022	0%	0	287
16	Personal 16	26/09/2022 26/10/2022	0%	0	298
17	Personal 17	26/09/2022 26/10/2022	0%	0	178
18	Personal 18	26/09/2022 26/10/2022	0%	0	234
19	Personal 19	26/09/2022 26/10/2022	0%	0	320

ANEXO 10: POST-TEST Precisión de acceso

FICHA DE REGISTRO					
INVESTIGADORES		Chavez Vasquez, Nicolas Valentin Arana, Jean Pierr		Tipo de Prue	POST TEST
EMPRESA		Clínica Multident Buenos Aires			
DIRECCION		Av. Wiese Mza. D1 Lt. 27 Lima-San Juan de Lurigancho			
FECHA DE INICIO		26/09/2022		FECHA FINAL	
				26/10/2022	
VARIABLE		INDICADOR	MEDIDA	FORMULA	
Control de Acceso		Precisión de acceso	Decimal	$P = \frac{VP}{VP + FP}$	
N°	Nombre Persona	Fecha	P: Precisión	VP: Verdadero Positivo	FP: Falso Positivo
1	Personal 1	26/09/2022 26/10/2022	1	24	0
2	Personal 2	26/09/2022 26/10/2022	0,97	43	1
3	Personal 3	26/09/2022 26/10/2022	0,92	25	2
4	Personal 4	26/09/2022 26/10/2022	0,95	23	1
5	Personal 5	26/09/2022 26/10/2022	0,81	16	4
6	Personal 6	26/09/2022 26/10/2022	1	165	0
7	Personal 7	26/09/2022 26/10/2022	0,89	135	17
8	Personal 8	26/09/2022 26/10/2022	0,82	163	34
9	Personal 9	26/09/2022 26/10/2022	0,89	120	14
10	Personal 10	26/09/2022 26/10/2022	0,85	21	4
11	Personal 11	26/09/2022 26/10/2022	0,90	24	2
12	Personal 12	26/09/2022 26/10/2022	0,84	21	4
13	Personal 13	26/09/2022 26/10/2022	0,98	24	1
14	Personal 14	26/09/2022 26/10/2022	0,98	26	1
15	Personal 15	26/09/2022 26/10/2022	0,92	22	2
16	Personal 16	26/09/2022 26/10/2022	0,94	19	1
17	Personal 17	26/09/2022 26/10/2022	1	15	0
18	Personal 18	26/09/2022 26/10/2022	0,96	22	1
19	Personal 19	26/09/2022 26/10/2022	1	14	0

ANEXO 11: AIS IS Proceso de control de acceso





Autorización para el Proyecto de Tesis

Por medio del presente documento, hacemos constar que el sr(a) **Jean Pierre Valentín Arana**, identificado con D.N.I. N° 74885113 (como invitado) y el sr(a) **Nicolas ChávezVásquez**, identificado con D.N.I. N° 41401083 que actualmente labora en la empresa Multident Buenos Aires con razón social **Odonto.bk e.i.r.l**, identificada con RUC N° 20603153104 y con dirección en **Av. Wiese Mz D1 Lt27 San Juan de Lurigancho, Lima -Perú**, están realizando su trabajo de Tesis con el nombre "Sistema de Reconocimiento facial con aprendizaje profundo para el control de acceso del almacén, en la Clínica Multident Buenos Aires, 2022" que se implementara en el área de almacén.

Se expide la presente a solicitud de los interesados para los fines que estimen convenientes.


ODONTO.BK E.I.R.L.
LUIS A. VÁSQUEZ ZEGARRA
GERENTE GENERAL

Lima, 16 de Setiembre del 2022

Gerente General
Luis Alberto Vásquez Zegarra
DNI: 10168349
Cel: 995 629 260



ANEXO 14: Metodología XP para el Sistema de Reconocimiento Facial

Planificación:

Es la Fase inicial de la metodología XP, donde se establece una comunicación continua entre el equipo de desarrollo y el cliente, para obtener principalmente los requerimientos del sistema. Además, permite establecer el alcance del proyecto y fechas de entrega del sistema, tomando en cuenta en la prioridad y tiempo estimado para el desarrollo de cada historia de usuario.

Historia de usuario

Las historias de usuario deben describirse en un lenguaje común para que sea comprensible para todos (clientes, programadores y usuarios), representando los requerimientos que debe cumplir el sistema.

Las Historias de Usuarios de la Clínica Multident Buenos Aires son las siguientes:

- Registro "Login del sistema web"
- Registro "Administración de Personal"
- Registro "Administración de Usuario"
- Registro "Administración de Cámara"
- Registro "Administración de Reporte"

A continuación, se muestra las historias de usuario donde se realiza una breve descripción de las funciones que realiza el sistema.

Tabla 1 Historia de usuario Login del Sistema web

HISTORIA DE USUARIO	
Numero: 1	Nombre: Login del sistema web.
Usuario: Administrador	Iteración Asignada: 1
Prioridad en Negocio: Baja	Puntos Estimados: 1
Riesgo en Desarrollo: Bajo	
Descripción: Los tipos de usuario del sistema tendrán que tener un nombre de usuario y clave única con la que pueden ingresar.	
Observaciones: Solo los usuarios que estén definidos en el sistema tendrán acceso a la aplicación web.	

Tabla 2 Historia de usuario Administración de Usuario

HISTORIA DE USUARIO	
Numero: 2	Nombre: Administración de usuario.
Usuario: Administrador	Iteración Asignada: 1
Prioridad en Negocio: Media	Puntos Estimados: 3
Riesgo en Desarrollo: Medio	
Descripción: Cuando se necesite que una persona nueva acceda a la aplicación web se deberá comunicar con el administrador para brindar sus datos personales y las funciones que desea utilizar de la aplicación web.	
Observaciones: Esto se realizará cuando ingrese un nuevo trabajador ya sea doctores, recepcionista, almacén	

Tabla 3 Historia de usuario Administración de Personal.

HISTORIA DE USUARIO	
Numero: 3	Nombre: Administración de Personal.
Usuario: Administrador	Iteración Asignada: 1
Prioridad en Negocio: Alta	Puntos Estimados: 3
Riesgo en Desarrollo: Alto	
Descripción: Todo el Personal que laboran en la Clinica deben proporcionar su información para su registro.	
Observaciones: El personal no tendrá acceso al Sistema solo el Administrador	

Tabla 4 Historia de usuario Administración de Reportes.

HISTORIA DE USUARIO	
Numero: 4	Nombre: Administración de Reportes.
Usuario: Administrador	Iteración Asignada: 1
Prioridad en Negocio: Alta	Puntos Estimados: 3
Riesgo en Desarrollo: Alto	
Descripción: El Administrador creara la interfaz de reportes de acuerdo a lo estipulado por el administrador que este a cargo de la empresa.	
Observaciones: Cada Reporte tendrá una identificación del Personal como la hora y el acceso autorizado o no autorizado.	

Tabla 5 Historia de usuario Administración de Cámara.

HISTORIA DE USUARIO	
Numero: 5	Nombre: Administración de Cámara.
Usuario: Administrador	Iteración Asignada: 1
Prioridad en Negocio: Alta	Puntos Estimados: 3
Riesgo en Desarrollo: Alto	
Descripción: El Administrador creara la interfaz donde se podrán visualizar la cámara de acuerdo a lo estipulado por el administrador que está a cargo de la Clínica.	
Observaciones: Esta cámara será la única que permitirá el reconocimiento Facial	

ROLES DE USUARIOS:

En cuanto a los roles tenemos 2 tipos de usuarios

Código	0
Tipo de usuario	Administrador
Área Funcional	Seguridad
Actividades	Realiza las configuraciones generales del sistema web

Código	1
Tipo de usuario	Usuario
Área Funcional	Seguridad
Actividades	Visualización del sistema web

PLAN DE ENTREGA:

ITERACIONES	ORDEN DE LA HIST. DE USUARIO	Prioridad	DURACION
1	Administración de Login	Media	2 semanas
2	Administración de configuración para el personal	Media	2 semanas
3	Administración y configuración de usuario	Alta	2 semanas
4	Administración y configuración de reportes	Alta	2 semanas
5	Administración y configuración de cámaras	Alta	2 semanas

PLAN DE ITERACIONES:

ITERACION 1.

Toda tarea y trabajo de cada iteración del proyecto es expresado en tareas de diseño y programación, cada una de estas tareas es asignada a un diseñador o programador correspondiente. A continuación, se detallan las tareas de la 1ra iteración del Sistema web:

TAREA			
Numero:	1	Numero de Historia de usuario:	1
Nombre:	Diseño de la interfaz para el login		
Tipo:	Diseño	Iteración:	1
Responsable	Autor	Puntos estimados:	0.5
Fecha de inicio:		Fecha de fin:	
Descripción	Diseñar la interfaz para el login de la aplicación web,		

TAREA			
Numero:	2	Numero de Historia de usuario:	1
Nombre:	Codificación de la interfaz para el login		
Tipo:	Desarrollo	Iteración:	1
Responsable	Autor	Puntos estimados:	0.5
Fecha de inicio:		Fecha de fin:	
Descripción	Codificar las funciones para el login de la aplicación web,		

ITERACION 2.

Esta tarea contribuye a poder alcanzar el objetivo de las historias de usuario del Sistema web, esta asignada a un diseñador o programador responsable. A continuación, se detallan las tareas de la 2da iteración del Sistema web.

TAREA			
Numero:	3	Numero de Historia de usuario:	2
Nombre:	Diseño de la interfaz para la administración del Personal		
Tipo:	Diseño	Iteración:	2
Responsable	Autor	Puntos estimados:	0.5
Fecha de inicio:		Fecha de fin:	
Descripción	Diseñar la interfaz para la administración del personal acorde a cada historia de usuario		

TAREA			
Numero:	4	Numero de Historia de usuario:	2
Nombre:	Codificación de la administración del Personal		
Tipo:	Desarrollo	Iteración:	2
Responsable	Autor	Puntos estimados:	1
Fecha de inicio:		Fecha de fin:	
Descripción	Codificar las funciones de crear, modificar y eliminar de la administración del personal.		

ITERACION 3.

Esta tarea contribuye a poder alcanzar el objetivo de las historias de usuario del Sistema web, esta asignada a un diseñador o programador responsable. A continuación, se detallan las tareas de la 3da iteración del Sistema web

TAREA			
Numero:	5	Numero de Historia de usuario:	3
Nombre:	Diseño de la interfaz para la administración de usuarios		
Tipo:	Diseño	Iteración:	2
Responsable	Autor	Puntos estimados:	0.5
Fecha de inicio:		Fecha de fin:	
Descripción	Diseñar la interfaz de usuario para la administración de usuarios acorde a cada historia de usuario		

TAREA			
Numero:	6	Numero de Historia de usuario:	3
Nombre:	Codificación para la administración de usuarios		
Tipo:	Desarrollo	Iteración:	2
Responsable	Autor	Puntos estimados:	3
Fecha de inicio:		Fecha de fin:	
Descripción	Codificar las funciones de crear, modificar y eliminar de la administración de usuarios.		

ITERACIÓN 4.

Esta tarea contribuye a poder alcanzar el objetivo de las historias de usuario del Sistema web, esta asignada a un diseñador o programador responsable. A continuación, se detallan las tareas de la 4da iteración del Sistema web

TAREA			
Número:	7	Numero de Historia de usuario:	4
Nombre:	Diseño de la interfaz para la administración de reportes		
Tipo:	Diseño	Iteración:	4
Responsable	Autor	Puntos estimados:	0.5
Fecha de inicio:		Fecha de fin:	
Descripción	Diseñar la interfaz de reportes para la administración de reportes acorde a cada historia de usuario		

TAREA			
Número:	8	Numero de Historia de usuario:	4
Nombre:	Codificación para la administración de reportes		
Tipo:	Desarrollo	Iteración:	4
Responsable	Autor	Puntos estimados:	5
Fecha de inicio:		Fecha de fin:	
Descripción	Codificar las funciones de crear y eliminar de la administración de reportes.		

ITERACIÓN 5.

Esta tarea contribuye a poder alcanzar el objetivo de las historias de usuario del Sistema web, esta asignada a un diseñador o programador responsable. A continuación, se detallan las tareas de la 2da iteración del Sistema web

TAREA			
Número:	9	Numero de Historia de usuario:	5
Nombre:	Diseño de la interfaz para la administración cámara		
Tipo:	Diseño	Iteración:	5
Responsable	Autor	Puntos estimados:	0.5
Fecha de inicio:		Fecha de fin:	
Descripción	Diseñar la interfaz de donde se visualizarán la cámara		

TAREA			
Número:	10	Numero de Historia de usuario:	5
Nombre:	Codificación para la administración de cámara		
Tipo:	Desarrollo	Iteración:	5
Responsable	Autor	Puntos estimados:	5
Fecha de inicio:		Fecha de fin:	
Descripción	Codificar las funciones para la visualización y administración de la cámara de video.		

DISEÑO UI

Interfaz de Login

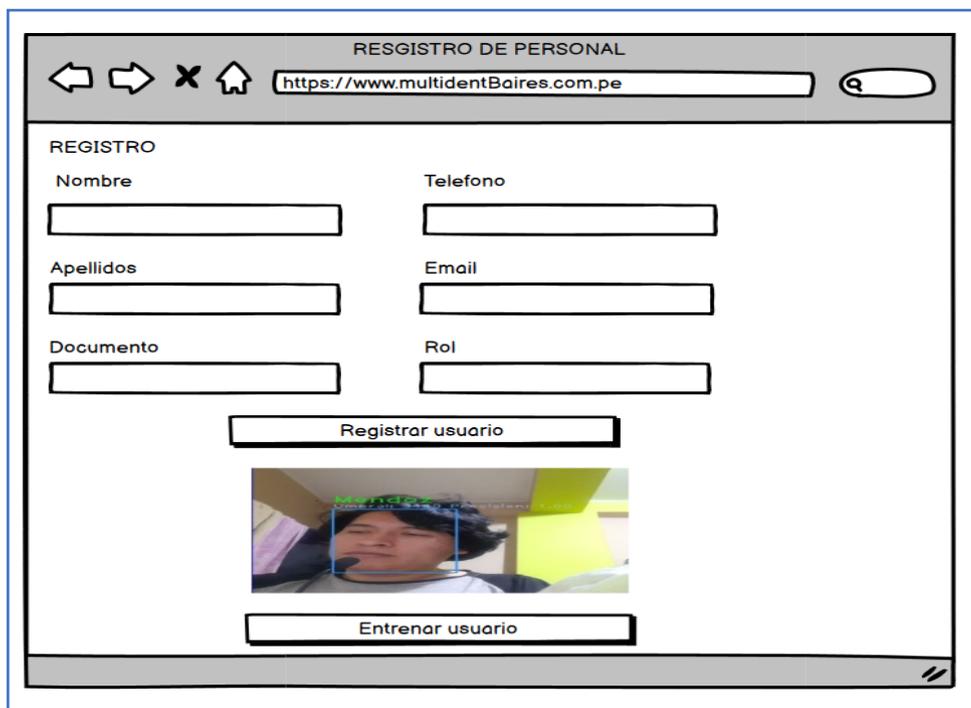
The image shows a wireframe of a login page. At the top, there is a browser header with navigation icons and a search bar containing the URL 'https://www.multidentBaires.com.pe'. Below the header is the Multident logo, which consists of the word 'MULTIDENT' in a stylized font above 'BUENOS AIRES - S/RL'. The main content area contains the following elements:

- A label 'Usuario' above a text input field.
- A label 'Contraseña' above a text input field.
- A button labeled 'Iniciar Sesión'.
- A link labeled 'Olvide la contraseña' below the button.

Interfaz del Menú



Interfaz de Registro



Interfaz de Editar

REGISTRO DE PERSONAL

https://www.multidentBaires.com.pe

EDITAR

Nombre

Telefono

Apellidos

Email

Documento

Rol

Interfaz de Reporte

REPORTE

AGREGAR USUARIO

Mostrar Registro

Nombre	Apellidos	Correo	Telefono	Rol	Estatus	Foto	Opciones
Nicolas	Chavez Vasquez	nicox24@hotmail.com	951007606	Asistente	Activo	Activo	Editar Eliminar
Nicolas	Chavez Vasquez	nicox24@hotmail.com	951007606	Asistente	Activo	Activo	Editar Eliminar
Nicolas	Chavez Vasquez	nicox24@hotmail.com	951007606	Asistente	Activo	Activo	Editar Eliminar

Creación de Tarjetas CRC

Las tarjetas CRC permiten mantener un registro de las clases utilizadas para el desarrollo de la aplicación web, así como también de sus métodos y atributos. El diseño de estas tarjetas es funcional para mejorar la comprensión del diseño.

Tabla 1 Tarjeta CRC de Login

TARJETA CR	
Login	
Responsabilidades	Colaboradores
Iniciar Sesión Validar Usuario	Administrador

Tabla 2 Tarjeta CRC de Usuario

TARJETA CR	
Usuario	
Responsabilidades	Colaboradores
Crear usuario Modificar usuario Eliminar usuario	Administrador

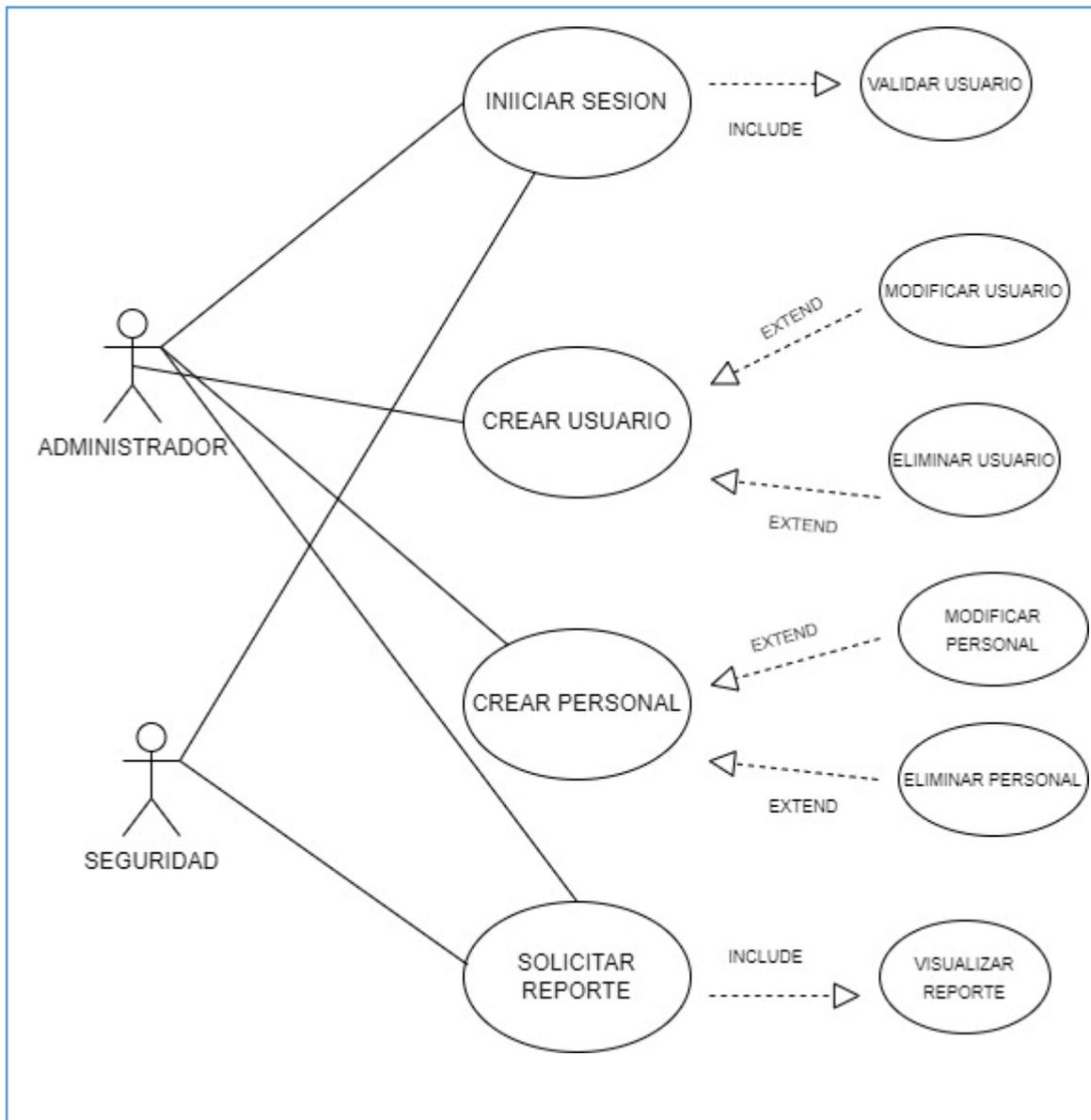
Tabla 3 Tarjeta CRC del Personal

TARJETA CR	
Personal	
Responsabilidades	Colaboradores
Crear Personal Editar Personal Eliminar Personal	Administrador

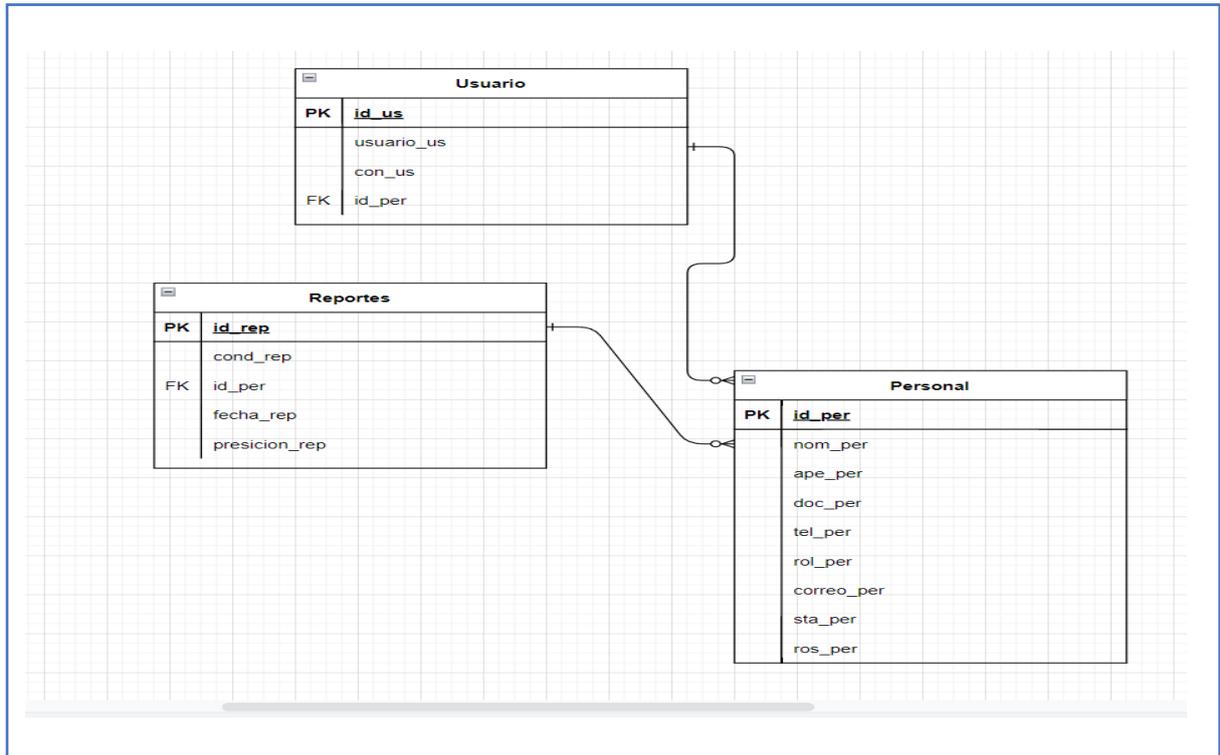
Tabla 4 Tarjeta CRC del Reporte

TARJETA CR	
Reporte	
Responsabilidades	Colaboradores
Visualizar reporte	Administrador

CASOS DE USO



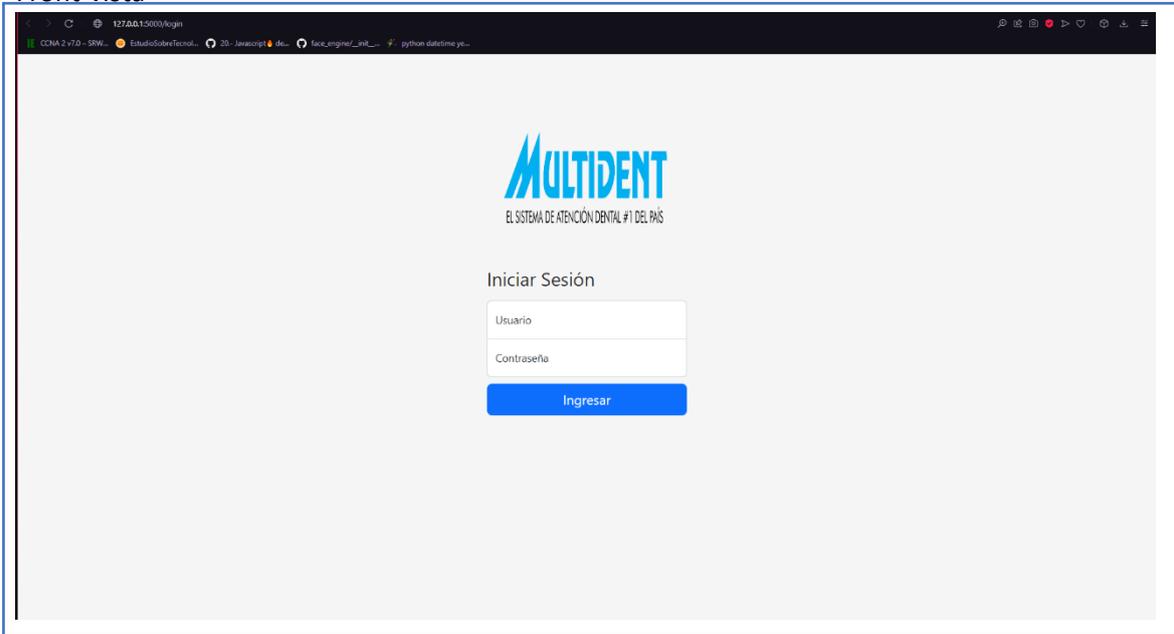
MODELO ENTIDAD RELACION



CODIFICACION:

H1: Login del Sistema web

Front-vista



HTML

```
src > templates > auth > login.html > form.form-signin
1  {% extends './baseLogin.html' %}
2  {% block title %}login{% endblock %}
3  {% block customCSS %}
4  <link rel="stylesheet" href="{{ url_for('static', filename='css/login.css') }}">
5  {% endblock %}
6  {% block body %}
7  <form class="form-signin" action="/login" method="POST">
8  
9  {% with messages = get_flashed_messages() %}
10  {% if messages %}
11  <br />
12  {% for message in messages %}
13  <div class="alert alert-primary alert-dismissible" role="alert">
14  <strong>
15  {{message}}
16  </strong>
17  <button type="button" class="btn-close" data-bs-dismiss="alert" aria-label="Close">
18  </button>
19  </div>
20  {% endfor %}
21  {% endif %}
22  {% endwith %}
23  <h1 class="h3 mb-3 fw-normal">Iniciar Sesión</h1>
24  <input type="hidden" name="csrf_token" value="{{ csrf_token() }}">
25  <div class="form-floating">
26  <input type="text" class="form-control" id="username" name="username" placeholder="Username">
27  <label for="username">Usuario</label>
28  </div>
29  <div class="form-floating">
30  <input type="password" class="form-control" name="password" placeholder="Password">
31  <label for="password">Contraseña</label>
32  </div>
33  <button class="w-100 btn btn-lg btn-primary" type="submit">Ingresar</button>
34  </form>
35  {% endblock %}
```

BACKEND

```
@login_manager_app.user_loader
def load_user(id):
    return ModelUser.get_by_id(db,id)

@app.route('/')
def index():
    return redirect(url_for('login'))

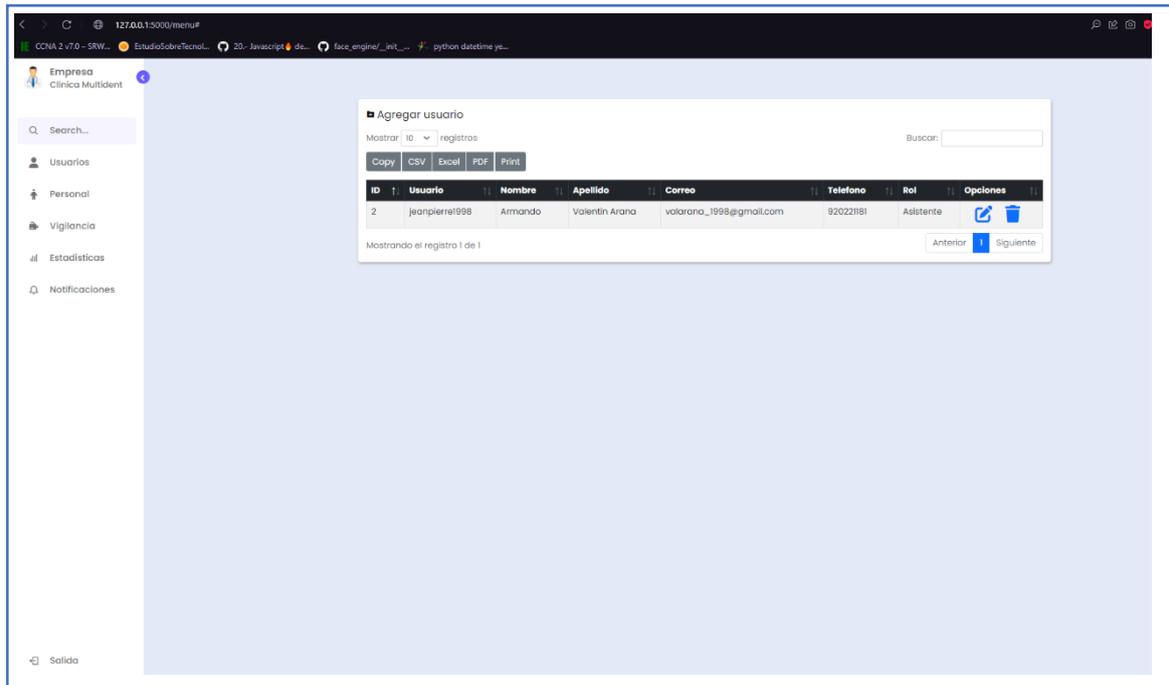
@app.route('/login', methods=['GET', 'POST'])
def login():
    if request.method=='POST':
        user=User(1,request.form['username'],request.form['password'])
        logged_user=ModelUser.login(db,user)
        if logged_user != None:
            if logged_user.password:
                login_user(logged_user)
                return redirect(url_for('menu'))
            else:
                flash("Contraseña equivocada")
                return render_template('auth/login.html')
        else:
            flash("Usuario no encontrado")
            return render_template('auth/login.html')
    else:
        return render_template('auth/login.html')
```

CSS

```
src > static > css > # login.css > ...
 1  html,
 2  body {
 3      height: 100%;
 4  }
 5  body {
 6      display: flex;
 7      align-items: center;
 8      padding-bottom: 250px;
 9      background-color: #f5f5f5;
10  }
11  .form-signin {
12      width: 100%;
13      max-width: 330px;
14      padding: 15px;
15      margin: auto;
16  }
17  .form-signin .form-floating:focus-within {
18      z-index: 2;
19  }
20  .form-signin input[type="text"] {
21      margin-bottom: -1px;
22      border-bottom-right-radius: 0;
23      border-bottom-left-radius: 0;
24  }
25  .form-signin input[type="password"] {
26      margin-bottom: 10px;
27      border-top-left-radius: 0;
28      border-top-right-radius: 0;
29  }
30
31
```

H3: Administración de USUARIO

HTML



CSS

```
src > static > css > # tablaUsuario.css > h1
1
2  html {
3      scroll-behavior: smooth;
4  }
5
6  html ::-webkit-scrollbar {
7      width: 10px;
8      background-color: #111d2c;
9      cursor: pointer;
10 }
11
12 html ::-webkit-scrollbar-thumb {
13     background: linear-gradient(160deg, #3c76ba, #1e428b);
14     width: 10px;
15     border-radius: 5px;
16 }
17
18 html ::-webkit-scrollbar-thumb:hover {
19     background: #379dc3;
20     cursor: pointer;
21 }
22
23 body {
24     background: #eee;
25     font-family: 'Raleway', sans-serif;
26     font-family: 'Roboto', sans-serif;
27     font-family: 'Poppins', sans-serif;
28     font-family: 'Rubik', sans-serif;
29     padding: 100px 0;
30 }
31
32 h1,
33 h2,
34 h3,
35 h4,
36 h5,
37 h6,
38 p,
39 a,
40 ol,
```

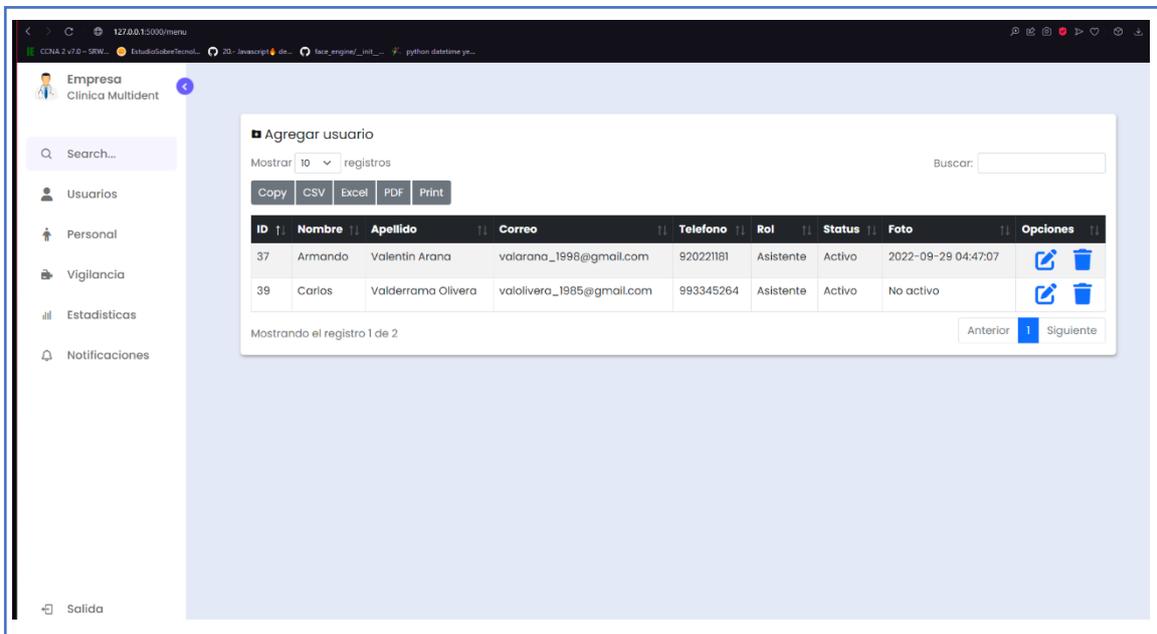
BACKEND

```
@classmethod
def get_tabla(self, db):
    try:
        cursor= db.connection.cursor()
        sql="Select id_us,usuario_us,nom_per,ape_per,correo_per,tel_per,rol_per FROM user INNER JOIN personal ON user.id_per = personal.id_per"
        cursor.execute(sql)
        row= cursor.fetchall()
        if row != None:
            return row
    except Exception as ex:
        raise Exception(ex)
```

```
@app.route('/crudUsuarioMenu')
def crudUsuarioMenu():
    usuario= ModelUser.get_tabla(db)
    return render_template('auth/crudUsuarioMenu.html', datosusuario= usuario)
```

H3: Administración de Personal

VISTA-ADM



Empresa
Clínica Multident

Search...

Usuarios

Personal

Vigilancia

Estadísticas

Notificaciones

Salida

Agregar usuario

Mostrar 10 registros

Buscar:

Copy CSV Excel PDF Print

ID	Nombre	Apellido	Correo	Telefono	Rol	Status	Foto	Opciones
37	Armando	Valentin Arana	valarana_1998@gmail.com	920221181	Asistente	Activo	2022-09-28 04:47:07	 
39	Carlos	Valderrama Olivera	valolivera_1985@gmail.com	993345264	Asistente	Activo	No activo	 

Mostrando el registro 1 de 2

Anterior 1 Siguiete

HTML

```
src > templates > auth > tablaUsuario.html > ...
1  {% extends './baseContenedor.html'%}
2  {% block title%}Login{% endblock %}
3  {% block customCSS%}
4  <link href="https://fonts.googleapis.com/css?family=Poppins:wght@300;400;500;600&display=swap" rel="stylesheet">
5  <link rel="stylesheet" href="{{ url_for('static', filename='css/tablaUsuario.css')}}">
6  <link rel="stylesheet" href="{{ url_for('static', filename='css/datatables.min.css')}}">
7  <link rel="stylesheet" href="{{ url_for('static', filename='css/bootstrap.min.css')}}">
8  <link rel="stylesheet" href="https://cdnjs.cloudflare.com/ajax/libs/font-awesome/6.2.0/css/all.min.css" integrity="sha512-xh60/CkQoP0MDDyTDqerRDPcVd1SpvCA90"
9  {% endblock %}
10 {% block body%}
11 <!-- ===== Data-Table = Start ===== -->
12 <div class="container">
13 <div class="row">
14 <div class="col-12">
15
16 <div class="data_table" style="margin-top: 5%;>
17 <div class="button" style="margin-bottom: 1%; id="btn-agregarTrabajador">
18 <button style="color: #151515; border: 0; background-color: white; ">
19 <i class="bx bxs-folder-plus"></i>
20 <span class="btn-text" user-select="none" style="font-size: 20px;">Agregar usuario</span>
21 </button>
22 </div>
23 <table id="example" class="table table-striped table-bordered" style="margin-top: 5%;>
24 <thead class="table-dark">
25 <tr>...
26 </tr>
27 </thead>
28 <tbody id="color">...
29 </tbody>
30 </table>
31 <meta type="hidden" name="csrf-token" content="{{ csrf_token() }}">
32 </div>
33 </div>
34 <div>
35 <meta type="hidden" name="csrf-token" content="{{ csrf_token() }}">
36 </div>
37 </div>
38 </div>
39 </div>
40 </div>
41 </div>
42 </div>
43 </div>
44 </div>
45 </div>
46 </div>
47 </div>
48 </div>
49 </div>
50 </div>
51 </div>
52 </div>
53 </div>
54 </div>
55 </div>
56 </div>
57 </div>
58 </div>
59 </div>
60 </div>
61 </div>
62 </div>
63 </div>
64 </div>
65 </div>
```

JAVASCRIPT

```
<script>
var csrftoken = $('meta[name=csrf-token]').attr('content')
$.ajaxSetup({
  beforeSend: function(xhr, settings) {
    if (!/^GET|HEAD|OPTIONS|TRACE$/i.test(settings.type)) {
      xhr.setRequestHeader("X-CSRFToken", csrftoken)
    }
  }
})
$("#btn-agregarTrabajador").click(function() {
  tipoCrud("Registro", " ")
})

$(".editar").click(function() {
  let id=$(this).attr("id");
  tipoCrud("Editar",id);
})
$(".eliminar").click(function() {...
function tipoCrud(tipo,id){...
</script>
<script src="https://cdn.jsdelivr.net/npm/sweetalert2@11.4.35/dist/sweetalert2.all.min.js"></script>
<script src="{{ url_for('static', filename='javascript/bootstrap.bundle.min.js')}}"></script>
<script src="{{ url_for('static', filename='javascript/datatables.min.js')}}"></script>
<script src="{{ url_for('static', filename='javascript/pdfmake.min.js')}}"></script>
<script src="{{ url_for('static', filename='javascript/vfs_fonts.js')}}"></script>
<script src="{{ url_for('static', filename='javascript/custom.js')}}"></script>
<script src="{{ url_for('static', filename='javascript/tablaTrabajador.js')}}"></script>
```

CSS

```
src > static > css > # tablaUsuario.css > h1
1
2  html {
3      |   scroll-behavior: smooth;
4      | }
5
6  html::-webkit-scrollbar {
7      |   width: 10px;
8      |   background-color: #111d2c;
9      |   cursor: pointer;
10     | }
11
12  html::-webkit-scrollbar-thumb {
13     |   background: linear-gradient(160deg, #3c76ba, #1e428b);
14     |   width: 10px;
15     |   border-radius: 5px;
16     | }
17
18  html::-webkit-scrollbar-thumb:hover {
19     |   background: #379dc3;
20     |   cursor: pointer;
21     | }
22
23  body {
24     |   background: #eee;
25     |   font-family: 'Raleway', sans-serif;
26     |   font-family: 'Roboto', sans-serif;
27     |   font-family: 'Poppins', sans-serif;
28     |   font-family: 'Rubik', sans-serif;
29     |   padding: 100px 0;
30     | }
31
32  h1,
33  h2,
34  h3,
35  h4,
36  h5,
37  h6,
38  p,
39  a,
40  ol,
```

BACKEND

```
src > models > ModelTrabajador.py > ModelTrabajador > buscar_id
1
2  from .entities.trabajador import Trabajador
3
4  class ModelTrabajador():
5      @classmethod
6      def get_tabla(self, db):
7          try:
8              cursor= db.connection.cursor()
9              sql="Select * FROM personal"
10             cursor.execute(sql)
11             row= cursor.fetchall()
12             if row != None:
13                 return row
14
15             except Exception as ex:
16                 raise Exception(ex)

```

```
@app.route('/tablaUsuario')
def tablaUsuario():
    trabajador= ModelTrabajador.get_tabla(db)
    return render_template('auth/tablaUsuario.html', datosTrabajador= trabajador)
```

VISTA-REGISTRO PERSONAL

The screenshot displays a web application interface for 'Empresa Clínica Multident'. The browser's address bar shows the URL '127.0.0.1:5000/menu'. The left sidebar contains a search bar and navigation links for 'Usuarios', 'Personal', 'Vigilancia', 'Estadísticas', 'Notificaciones', and 'Salida'. The main content area is titled 'Registro' and contains a form with the following fields:

- Nombre: Ingrese el nombre
- Apellido: Ingrese el apellido
- Correo: Ingrese el correo
- Numero de celular: Ingrese el numero
- Documento de Identidad: Ingrese el numero
- Rol de trabajador: Asistente (dropdown menu)

Below the form is a blue button labeled 'Registrar usuario'. Underneath is a video feed showing a person's face with a green bounding box and the text 'Cf:1.00' in the top left corner. Below the video is a purple button labeled 'Registrar sin mascarilla'.

HTML

```
src > templates > auth > crudUsuario.html > div.container > div.content > form#formulario > div#animacion
1  {% extends './baseContenedor.html'%}
2  {% block title%}Login{% endblock %}
3  {% block customCSS%}
4  <link rel="stylesheet" href="{{ url_for('static', filename='css/registroUsuario.css')}}">
5  <!--<script src="https://cdnjs.cloudflare.com/ajax/libs/jquery/3.5.1/jquery.min.js"></script-->
6  <link rel="stylesheet" href="{{ url_for('static', filename='css/iziToast.min.css')}}">
7  {% endblock %}
8  {% block body%}
9  <div class="container" style="margin:auto; margin-top: 2%;">
10     <div id="tipo" class="title">{{tipo}}</div>
11     <div class="content">
12         <form id="formulario" action="">
13             <div class="user-details">
14                 <div class="input-box">
15                     <span class="details">Nombre</span>
16                     <input type="text" id="nom" placeholder="Ingrese el nombre" required >
17                 </div>
18                 <div class="input-box">
19                     <span class="details">Apellido</span>
20                     <input type="text" id="ape" placeholder="Ingrese el apellido" required>
21                 </div>
22 > <div class="input-box">...
25 </div>
26 > <div class="input-box">...
29 </div>
30 > <div class="input-box">...
33 </div>
34 > <div class="input-box">...
43 </div>
44 > <div class="input-box" id="sta_hide" style="display: none;">...
50 </div>
51 </div >
52 <meta type="hidden" name="csrf-token" content="{{ csrf_token() }}">
53 > <div class="button">...
55 </div>
56 > <div id="animacion" style="display: none;">...
63 </div>
64 </form>
65 </div>
66 </div>
```

CSS

```
1 @import url('https://fonts.googleapis.com/css2?family=Poppins:wght@200;300;400;500;600;700&display=swap');
2 > *{...
7 }
8 > body{...
15 }
16 > .container{...
23 }
24 > .container .title{...
28 }
29 > .container .title::before{...
38 }
39 > .content form .user-details{...
44 }
45 > form .user-details .input-box{...
48 }
49 > form .input-box span.details{...
53 }
54 > .user-details .input-box input,select{...
54 }
55 .user-details .input-box input:focus,
56 .user-details .input-box input:valid{...
58 }
59 > form .gender-details .gender-title{...
72 }
73 > form .category{...
78 }
79 > form .category label{...
83 }
84 > form .category label .dot{...
92 }
93 #dot-1:checked ~ .category label .one,
94 #dot-2:checked ~ .category label .two,
95 #dot-3:checked ~ .category label .three{...
98 }
99 > form input[type="radio"]{...
101 }
102 > form .button{...
105 }
106 > form .button1{...
109 }
```

JSCRIPT

```
<script >
var csrfToken = $('meta[name=csrf-token']).attr('content')
> $.ajaxSetup({...
> if(document.getElementById("tipo").firstChild.nodeValue=="Actualizar"){...
var docImg=""
var count=101
> $('#formulario').on('submit',function(event) {...
> $("#registrar_usuario_imagen1").click(function() {...
> $("#registrar_usuario_imagen2").click(function() {...
> $("#entrenar_modelo").click(function() {...
</script>
```

BACKEN

INSERTAR DATOS PEROSNAL

```
@classmethod
def insertar_usuario(self, db,nom,ape,doc,correo,tel,rol,status):
    try:
        cursor= db.connection.cursor()
        sql="""INSERT INTO personal (nom_per, ape_per,doc_per,correo_per,tel_per,rol_per,sta_per)
VALUES ('{0}','{1}','{2}','{3}','{4}','{5}','{6}')""".format(nom,ape,doc,correo,tel,rol,status)
        cursor.execute(sql)
        db.connection.commit()
        return True
    except Exception as ex:
        raise Exception(ex)
```

```
@classmethod
def get_doc(self, db,doc):
    try:
        cursor= db.connection.cursor()
        sql="Select doc_per FROM personal WHERE doc_per='{0}'".format(doc)
        cursor.execute(sql)
        row= cursor.fetchall()
        if row != None:
            return row
        else:
            return False
    except Exception as ex:
        raise Exception(ex)
```

```
return False
@app.route('/modeloUsuario',methods=['POST'])
def modeloUsuario():
    msn=""
    id=request.form["id"]
    tipo=request.form["tipo"]
    nom=request.form["nom"]
    ape=request.form["ape"]
    doc=request.form["doc"]
    correo=request.form["correo"]
    tel=request.form["tel"]
    rol=request.form["rol"]
    status=request.form["sta"]
    if(tipo=="Registro"):
        if(ModelTrabajador.get_doc(db,doc)):
            msn="True"
        else:
            if(ModelTrabajador.insertar_usuario(db,nom,ape,doc,correo,tel,rol,status)):
                msn="True1"
            else:
                msn="Error al registrar"
```

BACKEND INSERTAR IMAGEN PERSONAL

```
@classmethod
def actualizarFechaFoto(self, app,db,fecha,id):
    with app.app_context():
        try:
            cursor= db.connection.cursor()
            sql="UPDATE personal SET fecha_ros_per='{0}' WHERE id_per='{1}'".format(fecha,id)
            cursor.execute(sql)
            db.connection.commit()
            return True
        except Exception as ex:
            raise Exception(ex)
```

```
def dnn_mostrar_rostro_reg():
    prototxt='src/DnnLibreria/Deploy_protobxt.txt'
    model='src/DnnLibreria/res10_300x300_ssd_iter_140000.caffemodel'
    net=cv2.dnn.readNetFromCaffe(prototxt,model)
    cap=cv2.VideoCapture(1,cv2.CAP_DSHOW)
    this_count=1
    while True:
        ret, frame = cap.read()
        if ret == False: break
        height, width, _ =frame.shape
        frame_resized = cv2.resize(frame, (300,300))
        blob=cv2.dnn.blobFromImage(frame_resized,1, (300,300), (104,117,123))
        net.setInput(blob)
        detections=net.forward()
        auxFrame = frame.copy()
        for detection in detections[0][0]:
            if detection[2]>0.7:
                box= detection[3:7] * [width, height, width, height]
                x_start, y_start, x_end, y_end = int(box[0]),int(box[1]),int(box[2]),int(box[3])
                if(this.inciar=="True1"):
                    if this.count >= 101:
                        this.inciar=""
                        this.id=""
                        break
                    else:
                        personDoc = this.id
                        dataPath = 'C:/Users/USUARIO/Desktop/flask-login/src/Rostros'
                        personPath = dataPath + '/' + personDoc
                        if not os.path.exists(personPath):
                            os.makedirs(personPath)
                        rostro = auxFrame[y_start:y_end,x_start:x_end]
                        rostro = cv2.resize(rostro,(150,150),interpolation=cv2.INTER_CUBIC)
                        cv2.imwrite(personPath + '/rostro_{}.jpg'.format(this.count),rostro)
                        cv2.rectangle(frame, (x_start, y_start),(x_end,y_end), (0,255,0),1)
                        cv2.putText(frame,"DI: "+personDoc+" Foto: {}".format(this.count),(x_start, y_start - 5),1,1.2,(0,255,255),2)
                        this.count = this.count + 1
                elif(this.inciar=="True2"):
                    if this.count >= 201:
                        msn=ModelTrabajador.actualizarFechaFoto(app,db,str(datetime.now().replace(microsecond=0).isoformat(' ')),this.id)
                        this.inciar=""
                        this.id=""
                        break
                    else:
                        personDoc = this.id
                        dataPath = 'C:/Users/USUARIO/Desktop/flask-login/src/Rostros'
                        personPath = dataPath + '/' + personDoc
                        if not os.path.exists(personPath):
                            os.makedirs(personPath)
                        rostro = auxFrame[y_start:y_end,x_start:x_end]
                        rostro = cv2.resize(rostro,(150,150),interpolation=cv2.INTER_CUBIC)
                        cv2.imwrite(personPath + '/rostro_{}.jpg'.format(this.count),rostro)
                        cv2.rectangle(frame, (x_start, y_start),(x_end,y_end), (0,255,0),1)
                        cv2.putText(frame,"DI: "+personDoc+" Foto: {}".format(this.count),(x_start, y_start - 5),1,1.2,(0,255,255),2)
                        this.count = this.count + 1
                else:
                    cv2.rectangle(frame, (x_start, y_start),(x_end,y_end), (0,255,0),1)
                    cv2.putText(frame,"CF: {:.2f}".format(detection[2]),(x_start, y_start - 5),1,1.2,(0,255,255),2)
        (flag, encodedImage) = cv2.imencode(".jpg", frame)
```

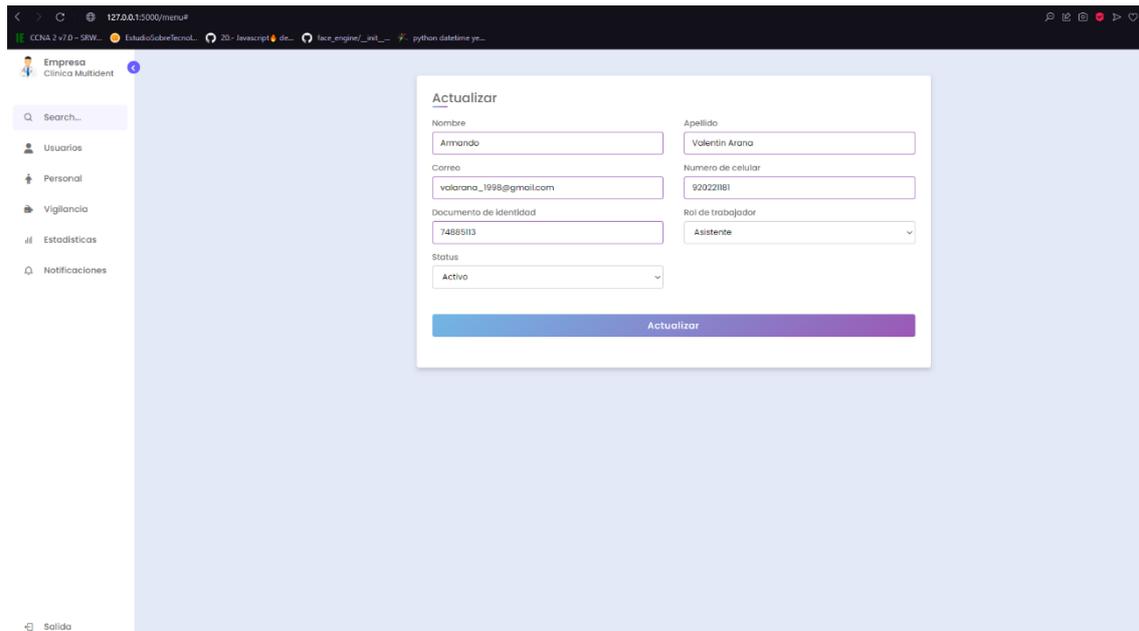
```
@app.route("/video_dnn_mostrar_rostro_reg")
def video_dnn_mostrar_rostro_reg():
    return Response(dnn_mostrar_rostro_reg(),
                    mimetype = "multipart/x-mixed-replace; boundary=frame")
```

BACKEND ENTRENAR MODELO

```
@app.route('/entrenar_modelo')
def entrenar_modelo():
    xmlRuta='C:/Users/USUARIO/Desktop/flask-login/modeloEigenFace.xml'
    if os.path.exists(xmlRuta):
        os.remove(xmlRuta)
    dataPath = 'C:/Users/USUARIO/Desktop/flask-login/src/Rostros'
    peopleList = os.listdir(dataPath)
    labels = []
    facesData = []
    label = 0
    for nameDir in peopleList:
        personPath = dataPath + '/' + nameDir
        print('Leyendo las imágenes')
        for fileName in os.listdir(personPath):
            print('Rostros: ', nameDir + '/' + fileName)
            labels.append(label)
            facesData.append(cv2.imread(personPath+'/'+fileName,0))
            label = label + 1
    face_recognizer = cv2.face.EigenFaceRecognizer_create()
    print("Entrenando...")
    face_recognizer.train(facesData, np.array(labels))
    face_recognizer.write('modeloEigenFace.xml')
    print("Modelo almacenado...")
    return True
```

VISTA-EDITAR PERSONAL

VISTA EDITAR DATOS



The screenshot shows a web browser window with a URL of 127.0.0.1:5000/menu#. The page title is "Empresa Clínica Multident". On the left, there is a sidebar menu with options: "Usuarios", "Personal", "Vigilancia", "Estadísticas", and "Notificaciones". The main content area displays a form titled "Actualizar" for editing user data. The form fields are as follows:

Actualizar	
Nombre	Apellido
<input type="text" value="Amrondo"/>	<input type="text" value="Valentin Arana"/>
Correo	Numero de celular
<input type="text" value="valarana_1998@gmail.com"/>	<input type="text" value="92022181"/>
Documento de Identidad	Rol de trabajador
<input type="text" value="7488513"/>	<input type="text" value="Asistente"/>
Status	
<input type="text" value="Activo"/>	
<input type="button" value="Actualizar"/>	

VISTA EDITAR FOTO

Empresa Clínica Multident

Search...

- Usuarios
- Personal
- Vigilancia
- Estadísticas
- Notificaciones

Salida

Actualizar

Nombre Ingrese el nombre	Apellido Ingrese el apellido
Correo Ingrese el correo	Numero de celular Ingrese el numero
Documento de identidad Ingrese el numero	Rol de trabajador Asistente
Status Activo	

Actualizar



Registrar sin mascarilla

HTML

```
src > templates > auth > crudUsuario.html > div.container > div.content > form#formulario > div#animacion
1  {% extends './baseContenedor.html'%}
2  {% block title%}Login{% endblock %}
3  {% block customCSS%}
4  <link rel="stylesheet" href="{{ url_for('static', filename='css/registroUsuario.css')}}">
5  <!--<script src="https://cdnjs.cloudflare.com/ajax/libs/jquery/3.5.1/jquery.min.js"></script-->
6  <link rel="stylesheet" href="{{ url_for('static', filename='css/iziToast.min.css')}}">
7  {% endblock %}
8  {% block body%}
9  <div class="container" style="margin:auto; margin-top: 2%;>
10     <div id="tipo"class="title">{{tipo}}</div>
11     <div class="content">
12         <form id="formulario" action="">
13             <div class="user-details">
14                 <div class="input-box">
15                     <span class="details">Nombre</span>
16                     <input type="text" id="nom" placeholder="Ingrese el nombre" required >
17                 </div>
18                 <div class="input-box">
19                     <span class="details">Apellido</span>
20                     <input type="text" id="ape" placeholder="Ingrese el apellido" required>
21                 </div>
22 > <div class="input-box">...
25 </div>
26 > <div class="input-box">...
29 </div>
30 > <div class="input-box">...
33 </div>
34 > <div class="input-box">...
43 </div>
44 > <div class="input-box" id="sta_hide" style="display: none;">...
50 </div>
51 </div >
52 <meta type="hidden" name="csrf-token" content="{{ csrf_token() }}">
53 > <div class="button">...
55 </div>
56 > <div id="animacion" style="display: none;">...
63 </div>
64 </form>
65 </div>
66 </div>
```

CSS

```
1 @import url('https://fonts.googleapis.com/css2?family=Poppins:wght@200;300;400;500;600;700&display=swap');
2 > *{...
7 }
8 > body{...
15 }
16 > .container{...
23 }
24 > .container .title{...
28 }
29 > .container .title::before{...
38 }
39 > .content form .user-details{...
44 }
45 > form .user-details .input-box{...
48 }
49 > form .input-box span.details{...
53 }
54 > .user-details .input-box input,select{...
54 }
55 .user-details .input-box input:focus,
56 > .user-details .input-box input:valid{...
58 }
59 > form .gender-details .gender-title{...
72 }
73 > form .category{...
78 }
79 > form .category label{...
83 }
84 > form .category label .dot{...
92 }
93 #dot-1:checked ~ .category label .one,
94 #dot-2:checked ~ .category label .two,
95 > #dot-3:checked ~ .category label .three{...
98 }
99 > form input[type="radio"]{...
101 }
102 > form .button{...
105 }
106 > form .button1{...
109 }
```

JSCRIPT

```
<script >
var csrftoken = $('meta[name=csrf-token]').attr('content')
> $.ajaxSetup({...
> if(document.getElementById("tipo").firstChild.nodeValue=="Actualizar"){...
var docImg=""
var count=101
> $('#formulario').on('submit',function(event) {...
> $("#registrar_usuario_imagen1").click(function() {...
> $("#registrar_usuario_imagen2").click(function() {...
> $("#entrenar_modelo").click(function() {...
</script>
```

BACKEND-EDITAR

SQL

```
@classmethod
def actualizar_usuario(self, db, id, nom, ape, doc, correo, tel, rol, status):
    try:
        cursor= db.connection.cursor()
        sql="UPDATE personal SET nom_per='{0}', ape_per='{1}',doc_per='{2}',correo_per='{3}',tel_per='{4}',rol_per='{5}',sta_per='{6}' WHERE id_per='{7}'"
        cursor.execute(sql)
        db.connection.commit()
        return True
    except Exception as ex:
        raise Exception(ex)
```

```
@app.route('/modeloUsuario',methods=['POST'])
def modeloUsuario():
    msn=""
    id=request.form["id"]
    tipo=request.form["tipo"]
    nom=request.form["nom"]
    ape=request.form["ape"]
    doc=request.form["doc"]
    correo=request.form["correo"]
    tel=request.form["tel"]
    rol=request.form["rol"]
    status=request.form["sta"]
    if(tipo=="Registro"):
        if(ModelTrabajador.get_doc(db,doc)):
            msn="True"
        else:
            if(ModelTrabajador.insertar_usuario(db,nom,ape,doc,correo,tel,rol,status)):
                msn="True1"
            else:
                msn="Error al registrar"
    elif(tipo=="Editar"):
        if(ModelTrabajador.actualizar_usuario(db,id,nom,ape,doc,correo,tel,rol,status)):
            msn="True2"
        else:
            msn="True3"
    return msn
```

BACKEND EDITAR IMAGEN PEROSNAL

```
@classmethod
def actualizarFechaFoto(self, app,db,fecha,id):
    with app.app_context():
        try:
            cursor= db.connection.cursor()
            sql="UPDATE personal SET fecha_ros_per='{0}' WHERE id_per='{1}'".format(fecha,id)
            cursor.execute(sql)
            db.connection.commit()
            return True
        except Exception as ex:
            raise Exception(ex)
```

```
def dnn_mostrar_rostro_reg():
    prototxt='src/DnnLibreria/Deploy_prototxt.txt'
    model='src/DnnLibreria/res10_300x300_ssd_iter_140000.caffemodel'
    net=cv2.dnn.readNetFromCaffe(prototxt,model)
    cap=cv2.VideoCapture(1,cv2.CAP_DSHOW)
    this.count=1
    while True:
        ret, frame = cap.read()
        if ret == False: break
        height, width, _ =frame.shape
        frame_resized = cv2.resize(frame, (300,300))
        blob=cv2.dnn.blobFromImage(frame_resized,1, (300,300), (104,117,123))
        net.setInput(blob)
        detections=net.forward()
        auxFrame = frame.copy()
        for detection in detections[0][0]:
            if detection[2]>0.7:
                box= detection[3:7] * (width, height, width, height)
                x_start, y_start, x_end, y_end = int(box[0]),int(box[1]),int(box[2]),int(box[3])
                if(this.inciar=="True1"):
                    if this.count >= 101:
                        this.inciar=""
                        this.id=""
                        break
                    else:
                        personDoc = this.id
                        dataPath = 'C:/Users/USUARIO/Desktop/Flask-login/src/Rostros'
                        personPath = dataPath + '/' + personDoc
                        if not os.path.exists(personPath):
                            os.makedirs(personPath)
                        rostro = auxFrame[y_start:y_end,x_start:x_end]
                        rostro = cv2.resize(rostro,(150,150),interpolation=cv2.INTER_CUBIC)
                        cv2.imwrite(personPath + '/rostro_{}.jpg'.format(this.count),rostro)
                        cv2.rectangle(frame, (x_start, y_start),(x_end,y_end),(0,255,0),1)
                        cv2.putText(frame,"DI: "+personDoc+" Foto: {}".format(this.count),(x_start, y_start - 5),1,1.2,(0,255,255),2)
                        this.count = this.count + 1
                elif(this.inciar=="True2"):
                    if this.count >= 201:
                        msn=ModelTrabajador.actualizarFechaFoto(app,db,str(datetime.now().replace(microsecond=0).isoformat(' ')),this.id)
                        this.inciar=""
                        this.id=""
                        break
                    else:
                        personDoc = this.id
                        dataPath = 'C:/Users/USUARIO/Desktop/Flask-login/src/Rostros'
                        personPath = dataPath + '/' + personDoc
                        if not os.path.exists(personPath):
                            os.makedirs(personPath)
                        rostro = auxFrame[y_start:y_end,x_start:x_end]
                        rostro = cv2.resize(rostro,(150,150),interpolation=cv2.INTER_CUBIC)
                        cv2.imwrite(personPath + '/rostro_{}.jpg'.format(this.count),rostro)
                        cv2.rectangle(frame, (x_start, y_start),(x_end,y_end),(0,255,0),1)
                        cv2.putText(frame,"DI: "+personDoc+" Foto: {}".format(this.count),(x_start, y_start - 5),1,1.2,(0,255,255),2)
                        this.count = this.count + 1
                else:
                    cv2.rectangle(frame, (x_start, y_start),(x_end,y_end),(0,255,0),1)
                    cv2.putText(frame,"CF: {:.2f}".format(detection[2]),(x_start, y_start - 5),1,1.2,(0,255,255),2)
        (flag, encodedImage) = cv2.imencode(".jpg", frame)
```

```
@app.route("/video_dnn_mostrar_rostro_reg")
def video_dnn_mostrar_rostro_reg():
    return Response(dnn_mostrar_rostro_reg(),
                    mimetype = "multipart/x-mixed-replace; boundary=frame")
```

BACKEND ENTRENAR MODELO

```
@app.route('/entrenar_modelo')
def entrenar_modelo():
    xmlRuta='C:/Users/USUARIO/Desktop/flask-login/modeloEigenFace.xml'
    if os.path.exists(xmlRuta):
        os.remove(xmlRuta)
    dataPath = 'C:/Users/USUARIO/Desktop/flask-login/src/Rostros'
    peopleList = os.listdir(dataPath)
    labels = []
    facesData = []
    label = 0
    for nameDir in peopleList:
        personPath = dataPath + '/' + nameDir
        print('Leyendo las imágenes')
        for fileName in os.listdir(personPath):
            print('Rostros: ', nameDir + '/' + fileName)
            labels.append(label)
            facesData.append(cv2.imread(personPath+'/'+fileName,0))
            label = label + 1
    face_recognizer = cv2.face.EigenFaceRecognizer_create()
    print("Entrenando...")
    face_recognizer.train(facesData, np.array(labels))
    face_recognizer.write('modeloEigenFace.xml')
    print("Modelo almacenado...")
    return True
```

VISTA-ELIMINAR PERSONAL

The screenshot shows a web application interface for user management. The main content area displays a table titled "Agregador usuario" with columns for ID, Nombre, Apellido, Correo, Telefono, Rol, Status, Foto, and Opciones. The table contains three records. A confirmation dialog is overlaid on the table, asking "¿Confirmar eliminar el registro? 37" with "Confirmar" and "Cancel" buttons.

ID	Nombre	Apellido	Correo	Telefono	Rol	Status	Foto	Opciones
37	Armando	Valentin Arana	valarana_1989@gmail.com	920221181	Asistente	Activo	2022-09-29 04:47:07	 
39	Carlos	Valderrama Olivera	valolivera_1985@gmail.com	993345264	Asistente	Activo	No activo	 
40	Carlos	Valderrama Olivera	valolivera_1985@gmail.com	993345264	Doctor	Activo	No activo	 

JAVASCRIPT

```
87  $(".eliminar").click(function() {
88      let id=$(this).attr("id");
89      Swal.fire({
90          title: '¿Confirmar eliminar el registro? '+id,
91          icon: 'warning',
92          showCancelButton: true,
93          confirmButtonColor: '#3085d6',
94          cancelButtonColor: '#d33',
95          confirmButtonText: 'Confirmar',
96      }).then((result) => {
97          if (result.isConfirmed) {
98              var request = $.ajax({
99                  type: 'POST',
100                 url: '/eliminarPersonal',
101                 data: {
102                     id: id
103                 }
104             })
105             .done( function (request) {
106                 if(request=="True"){
107                     Swal.fire('Eliminado!', '', 'success')
108                 }else{
109                     Swal.fire('Error!', '', 'success')
110                 }
111             })
112             .fail( function () {
113                 console.log("error")
114             })
115         }
116     })
117 }
```

BACKEND

```
@classmethod
def eliminar(self, db, id):
    try:
        cursor= db.connection.cursor()
        sql="DELETE FROM personal WHERE id_per='{0}'".format(id)
        cursor.execute(sql)
        db.connection.commit()
        return True
    except Exception as ex:
        raise Exception(ex)
```

```
@app.route('/eliminarPersonal', methods=['POST'])
def eliminarPersonal():
    id=request.form["id"]
    val=ModelTrabajador.eliminar(db, id)
    if(val):
        return "True"
    else:
        return "False"
```

H4: Administración de Reportes

VISTA

Empresa Clínica Multident

Personal detectado: Armando Valerín Arana

Nombre	Apellido	Correo	Telefono	Area	Nivel	Fecha	Precisión
Armando	Valerín Arana	valarana_1998@gmail.com	920221191	Asistente	No autorizado	Thu, 29 Sep 2022 18:28:28 GMT	0.9850765

Mostrando el registro 1 de 1

Anterior | Siguiente

HTML

```
{% extends './baseContenedor.html'%}
{% block title%}Login{% endblock %}
{% block customCSS%}
<link rel="stylesheet" href="{{ url_for('static', filename='css/bootstrap.min.css')}}">
<link rel="stylesheet" href="{{ url_for('static', filename='css/tablaUsuario.css')}}">
<link rel="stylesheet" href="{{ url_for('static', filename='css/datatables.min.css')}}">
<link rel="stylesheet" href="{{ url_for('static', filename='css/iziToast.min.css')}}">
</style>...
</style>
{% endblock %}
{% block body%}
<div class = "container">...
</div>
<div class = "container1">
<table id="mitabla" class="table table-striped table-bordered">
<thead class="table-dark">
<tr>
<th id="nom">Nombre</th>
<th>Apellido</th>
<th>Correo</th>
<th>Telefono</th>
<th>Area</th>
<th>Nivel</th>
<th>Fecha</th>
<th>Precisión</th>
</tr>
</thead>
<tbody id="reporte">
</tbody>
</table>
<meta type="hidden" name="csrf-token" content="{{ csrf_token() }}">
</div>
```

CSS

```
src > static > css > # videoCamara.css > *$.datatable-container .footer-tools .pages ul li span.active
> eliminarPersonal

1  @import url('https://fonts.googleapis.com/css2?family=Noto+Sans&display=swap');
2
3  > :root{ ...
28 }
29 > .material-icons{ ...
31 }
32 > .datatable-container{ ...
40 }
41 > .datatable-container .header-tools{ ...
46 }
47 > .datatable-container .header-tools .search{ ...
49 }
50 > .datatable-container .header-tools .search .search-input{ ...
58 }
59 > .datatable-container .header-tools .tools{ ...
61 }
62 > .datatable-container .header-tools .tools ul{ ...
68 }
69 > .datatable-container .header-tools .tools ul li{ ...
73 }
74 > .datatable-container .footer-tools{ ...
78 }
79 > .datatable-container .footer-tools .list-items{ ...
81 }
82 > .datatable-container .footer-tools .pages{ ...
86 }
87 > .datatable-container .footer-tools .pages ul{ ...
93 }
94 > .datatable-container .footer-tools .pages ul li{ ...
97 }
98 .datatable-container .footer-tools .pages ul li button,
99 .datatable-container .header-tools .tools ul li button{ ...
107 }
108 .datatable-container .footer-tools .pages ul li button:hover,
109 .datatable-container .header-tools .tools ul li button:hover{ ...
112 }
113 > .datatable-container .footer-tools .pages ul li span.active{ ...
116 }
```

JAVASCRIPT

```
function tabla(){
  tablaUsuarios = $('#mitabla').DataTable({
    "ajax":{
      "url": "/obtenerReporte",
      "method": 'POST', //usamos el metodo POST
      "dataSrc":""
    },
    "columns":[ ...
  ]});
}
function alerta(){
  var request =$.ajax({
    type:'POST',
    url:'/buscarAlerta'
  })
  .done( function (request) {
    if(request.response=="False"){
    }else{
      console.log(request.response.length);
      for (var index = 0; index < request.response.length; index++) {
        if(request.response[index][2]=="No autorizado"){
          console.log(request.response[index][2].length)
          iziToast.show({
            title: 'Personal detectado: ',
            titleColor: '#FFFFFF',
            class:'text-success',
            position:'topRight',
            message:request.response[index][0]+" "+request.response[index][1],
            messageColor: '#FFFFFF',
            backgroundColor: '#9E9E9E',
            timeout: 5000,
          });
        }
      }
    }
  })
}
```

BACKEND

B-ALERTA

```
@classmethod
def obtener_alerta(self, db, app, fecha):
    with app.app_context():
        try:
            cursor= db.connection.cursor()
            sql="SELECT nom_per,ape_per,cond_rep FROM reporte INNER JOIN personal ON reporte.id_per = personal.id_per WHERE fecha_rep = DATE_SUB('{0}',
            cursor.execute(sql)
            row= cursor.fetchall()
            if row!= None:
                return row
            else:
                return False
        except Exception as ex:
            raise Exception(ex)
```

```
@app.route('/buscarAlerta',methods=['POST'])
def buscarAlerta():
    fecha=str(datetime.now().replace(microsecond=0).isoformat(' '))
    val=ModelReporte.obtener_alerta(db,app,fecha)
    if(val):
        return jsonify({"response":val})
    else:
        return jsonify({"response":"False"})
```

B-TABLA REPORTE

```
@classmethod
def obtener_tabla(self, db, app, fecha):
    with app.app_context():
        try:
            cursor= db.connection.cursor()
            sql="SELECT nom_per,ape_per,correo_per,tel_per,rol_per,cond_rep,fecha_rep,precision_rep FROM reporte INNER JOIN personal ON reporte.id_per
            cursor.execute(sql)
            row= cursor.fetchall()
            #new_lista.clear()
            new_lista=[]
            new_lista.clear()
            new_lista=[]
            if row != None:
                for i in row:
                    dic={}
                    dic["nombre"]=i[0]
                    dic["apellido"]=i[1]
                    dic["correo"]=i[2]
                    dic["telefono"]=i[3]
                    dic["rol"]=i[4]
                    dic["cond_rep"]=i[5]
                    dic["fecha_rep"]=i[6]
                    dic["precision_rep"]=i[7]
                    new_lista.append(dic)
                return new_lista
            else:
                return False
        except Exception as ex:
            raise Exception(ex)
```

```

@app.route('/obtenerReporte', methods=['POST'])
def obtenerReporte():
    fecha=datetime.now().date()
    reporte=""
    reporte= ModelReporte.obtener_tabla(db,app,fecha)
    if(reporte):
        return jsonify(reporte)
    else:
        dic={}
        dic["nombre"]=" "
        dic["apellido"]=" "
        dic["correo"]=" "
        dic["telefono"]=" "
        dic["rol"]=" "
        dic["cond_rep"]=" "
        dic["fecha_rep"]=" "
        dic["precision_rep"]=" "
        return jsonify(dic)

```

H5: ADMINISTRACIÓN DE CÁMARA

Vista

Personal detectada: Armando Valentin Arana

Nombre	Apellido	Correo	Telefono	Area	Nivel	Fecha	Precisión
Armando	Valentin Arana	valarana_1958@gmail.com	82022181	Asistente	No autorizado	Thu, 20 Sep 2022 15:26:28 GMT	0.9850765

Mostrando el registro 1 de 1

Anterior | Siguiente

HTML

```
{% block title%}Login{% endblock %}
{% block customCSS%}
<link rel="stylesheet" href="{{ url_for('static', filename='css/bootstrap.min.css')}}">
<link rel="stylesheet" href="{{ url_for('static', filename='css/tablaUsuario.css')}}">
<link rel="stylesheet" href="{{ url_for('static', filename='css/datatables.min.css')}}">
<link rel="stylesheet" href="{{ url_for('static', filename='css/iziToast.min.css')}}">
</style>...
</style>
{% endblock %}
{% block body%}
<div class = "container">

</div>
<div class = "container1">
<table id="mitabla" class="table table-striped table-bordered">
<thead class="table-dark">
<tr>
<th id="nom">Nombre</th>
<th>Apellido</th>
<th>Correo</th>
<th>Telefono</th>
<th>Area</th>
<th>Nivel</th>
<th>Fecha</th>
<th>Precisión</th>
</tr>
</thead>
<tbody id="reporte">
</tbody>
</table>
<meta type="hidden" name="csrf-token" content="{{ csrf_token() }}">
</div>
```

CSS

```
src > static > css > # videoCamara.css > # .datatable-container .footer-tools .pages ul li span.active
> eliminarPersonal

1 @import url('https://fonts.googleapis.com/css2?family=Noto+Sans&display=swap');
2
3 > :root{ ...
28 }
29 > .material-icons{ ...
31 }
32 > .datatable-container{ ...
40 }
41 > .datatable-container .header-tools{ ...
46 }
47 > .datatable-container .header-tools .search{ ...
49 }
50 > .datatable-container .header-tools .search .search-input{ ...
58 }
59 > .datatable-container .header-tools .tools{ ...
61 }
62 > .datatable-container .header-tools .tools ul{ ...
68 }
69 > .datatable-container .header-tools .tools ul li{ ...
73 }
74 > .datatable-container .footer-tools{ ...
78 }
79 > .datatable-container .footer-tools .list-items{ ...
81 }
82 > .datatable-container .footer-tools .pages{ ...
86 }
87 > .datatable-container .footer-tools .pages ul{ ...
93 }
94 > .datatable-container .footer-tools .pages ul li{ ...
97 }
98 .datatable-container .footer-tools .pages ul li button,
99 .datatable-container .header-tools .tools ul li button{ ...
107 }
108 .datatable-container .footer-tools .pages ul li button:hover,
109 .datatable-container .header-tools .tools ul li button:hover{ ...
112 }
113 > .datatable-container .footer-tools .pages ul li span.active{ ...
116 }
```

BACKEND

B-VIDEO

```
@app.route('/deteccion_rostro')
def deteccion_rostro():
    dataPath = 'C:/Users/USUARIO/Desktop/flask-login/src/Rostros'
    imagePaths = os.listdir(dataPath)
    print('imagePaths=', imagePaths)
    prototxt='src/DnnLibreria/deploy.prototxt.txt'
    model='src/DnnLibreria/res10_300x300_ssd_iter_140000.caffemodel'
    net=cv2.dnn.readNetFromCaffe(prototxt,model)
    face_recognizer = cv2.Face_EigenFaceRecognizer_create()
    face_recognizer.read('modeloEigenFace.xml')
    cap = cv2.VideoCapture(1)
    while True:
        ret, frame = cap.read()
        gray = cv2.cvtColor(frame, cv2.COLOR_BGR2GRAY)
        auxFrame = gray.copy()
        if ret:
            height, width, _ = frame.shape
            frame_resized = cv2.resize(frame, (300,300))
            blob=cv2.dnn.blobFromImage(frame_resized,1, (300,300), (104,117,123))
            net.setInput(blob)
            detections=net.forward()
            auxFrame = frame.copy()
            for detection in detections[0][0]:
                if detection[2]>0.5:
                    box= detection[3:7] * [width, height, width, height]
                    x_start, y_start, x_end, y_end = int(box[0]),int(box[1]),int(box[2]),int(box[3])
                    rostro = auxFrame[y_start:y_end,x_start:x_end]
                    rostro = cv2.resize(rostro,(150,150), interpolation=cv2.INTER_CUBIC)
                    rostro =cv2.cvtColor(rostro,cv2.COLOR_BGR2GRAY)
                    result = face_recognizer.predict(rostro)
                    exactitud=(int)(result[1])
                    cv2.putText(frame,"Umbral: {}".format(str(exactitud))+" "+"Precision: {}".format(str(detection[2]),(x_start,y_start-5),1,1.3,(255,204,153),1,cv2.LINE_AA)
                    if result[1] < 5500:
                        nomApe=buscar(str(imagePaths[result[0]]))
                        cv2.putText(frame,"{}".format(nomApe[1]),(x_start,y_start-25),2,1.1,(0,255,0),1,cv2.LINE_AA)
                        cv2.rectangle(frame, (x_start,y_start), (x_end,y_end),(255,153,51),2)
                        m=insertarReporte(int(nomApe[0]),(str(datetime.now()).replace(microsecond=0).isoformat(' ')),str(nomApe[2]),str(detection[2]))
                    else:
                        cv2.putText(frame,'Desconocido',(x_start,y_start-20),2,0.8,(0,0,255),1,cv2.LINE_AA)
                        cv2.rectangle(frame, (x_start,y_start), (x_end,y_end),(0,0,255),2)
                    (flag, encodedImage) = cv2.imencode('.jpg', frame)
                    if not flag:
                        continue
                    yield(b'--frame\r\n' b'Content-Type: image/jpeg\r\n\r\n' +
                        bytearray(encodedImage) + b'\r\n')
```

B-INSERTAR REPORTE

```
def insertarReporte(id_trb,fecha_rep,cond_rep,precision_rep):
    this.alerta="False"
    insertar=""
    if(cond_rep=="Almacen"):
        cond_rep="Autorizado"
    else:
        cond_rep="No autorizado"
    val=ModelReporte.verificar_fecha(db,app,id_trb)
    if(val==False):
        insertar=ModelReporte.insertar_moldelo_reporte(db,app,id_trb,fecha_rep,cond_rep,precision_rep)
        this.alerta=cond_rep
    else:
        hora=str(val)
        fecha_rep_1 = datetime.strptime(hora,"%Y-%m-%d %H:%M:%S")
        horaActual=datetime.now().time().hour
        fechaActual=datetime.now().date()
        minutoActual=datetime.now().time().minute
        minReporte=fecha_rep_1.time().minute
        hourReporte=fecha_rep_1.time().hour
        b=0
        if(fechaActual==fecha_rep_1.date()):
            if(horaActual==hourReporte):
                if(minutoActual>minReporte+10 and 50>minReporte):
                    insertar=ModelReporte.insertar_moldelo_reporte(db,app,id_trb,fecha_rep,cond_rep,precision_rep)
                    this.alerta=cond_rep
                else:
                    b=0
            elif(horaActual==hourReporte+1):
                if(minReporte>=50):
                    val=60-minReporte
                    nt=10-val
                    if(minutoActual>nt):
                        insertar=ModelReporte.insertar_moldelo_reporte(db,app,id_trb,fecha_rep,cond_rep,precision_rep)
                        this.alerta=cond_rep
                else:
                    b=5
            else:
                insertar=ModelReporte.insertar_moldelo_reporte(db,app,id_trb,fecha_rep,cond_rep,precision_rep)
                this.alerta=cond_rep
        else:
            insertar=ModelReporte.insertar_moldelo_reporte(db,app,id_trb,fecha_rep,cond_rep,precision_rep)
            this.alerta=cond_rep
    return b
```

```
@app.route("/video_camara")
def video_camara():
    return Response(deteccion_rostro(),
        mimetype = "multipart/x-mixed-replace; boundary=frame")
```

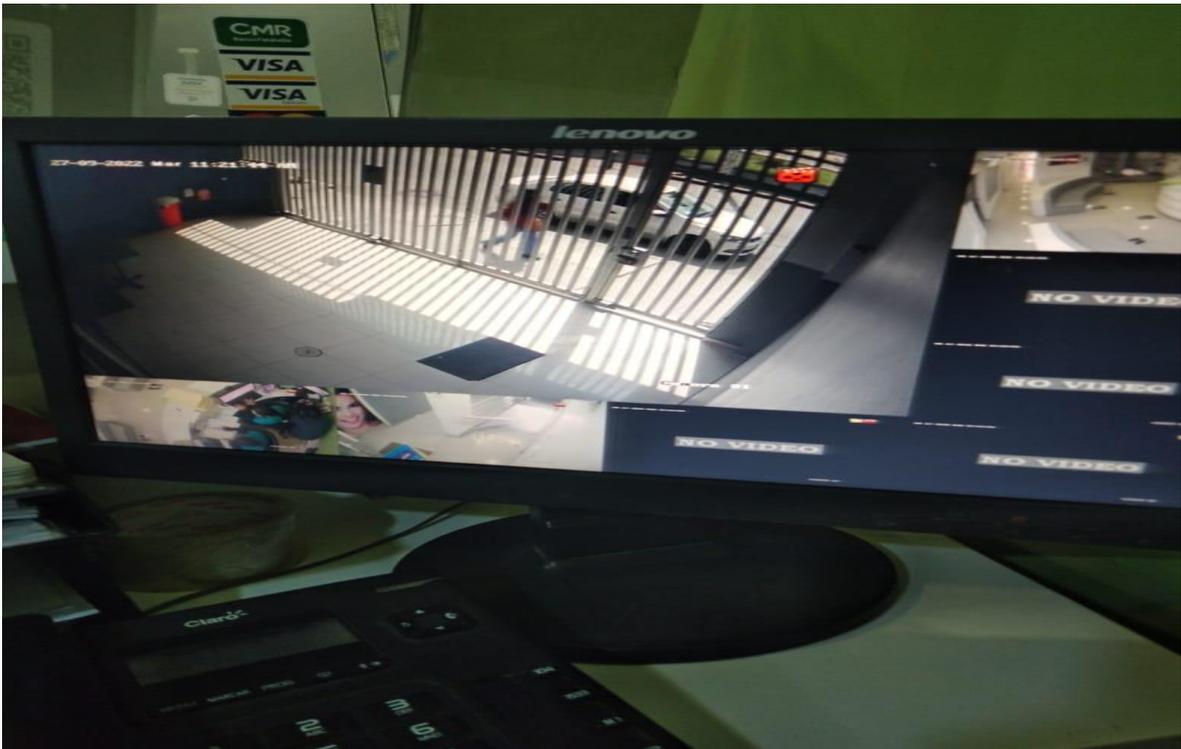
ANEXO 15: EVIDENCIAS

Fotos del Lugar de Aplicación:



Interior de la Clínica





Pasadizos de la Clínica.



Reconocimiento Facial en el almacén

The screenshot shows a web browser window displaying a facial recognition application. The browser address bar shows 'localhost / 127.0.0.1 / api_flask /'. The application interface includes a search bar, a navigation menu on the left, and a central video feed. In the video feed, a person is wearing a teal shirt and a black face mask. A blue bounding box is drawn around the person's face, and text overlay reads 'Velarde Fernar' and 'Umbral: 45'. Below the video feed, there is a table with the following data:

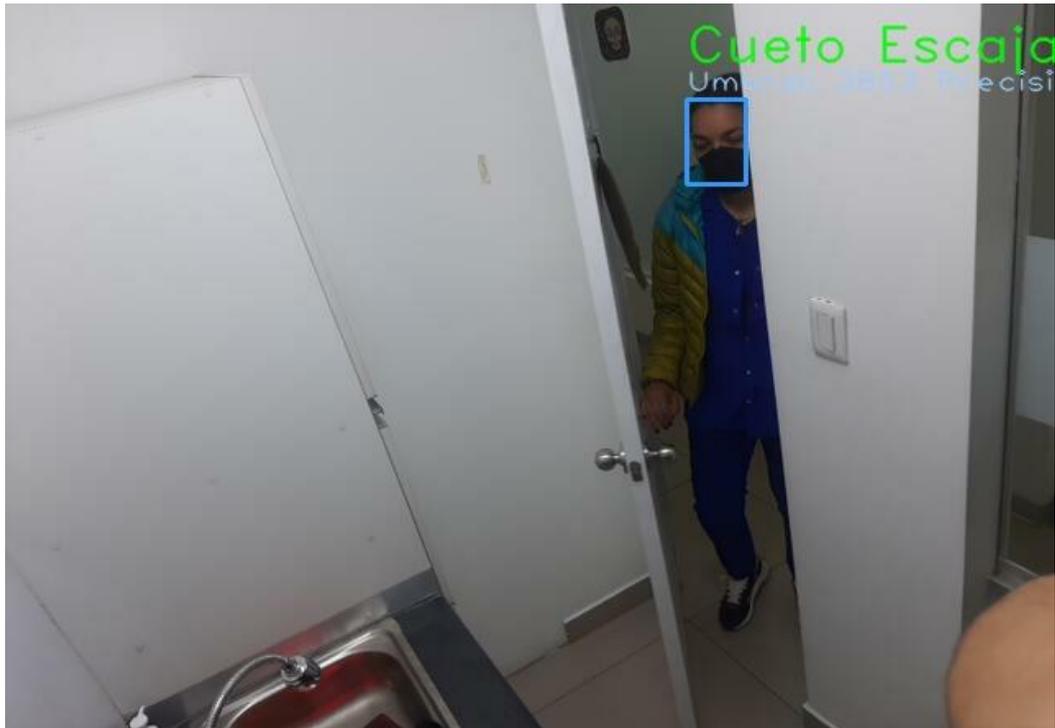
Nombre	Apellido	Correo	Telefono	Area	Nivel	Fecha	Precisión
Katia	Velarde Fernandez	fernandez_katia15@gmail.com	975216485	Doctor	No autorizado	Tue, 27 Sep 2022 14:00:29 GMT	0.5040199

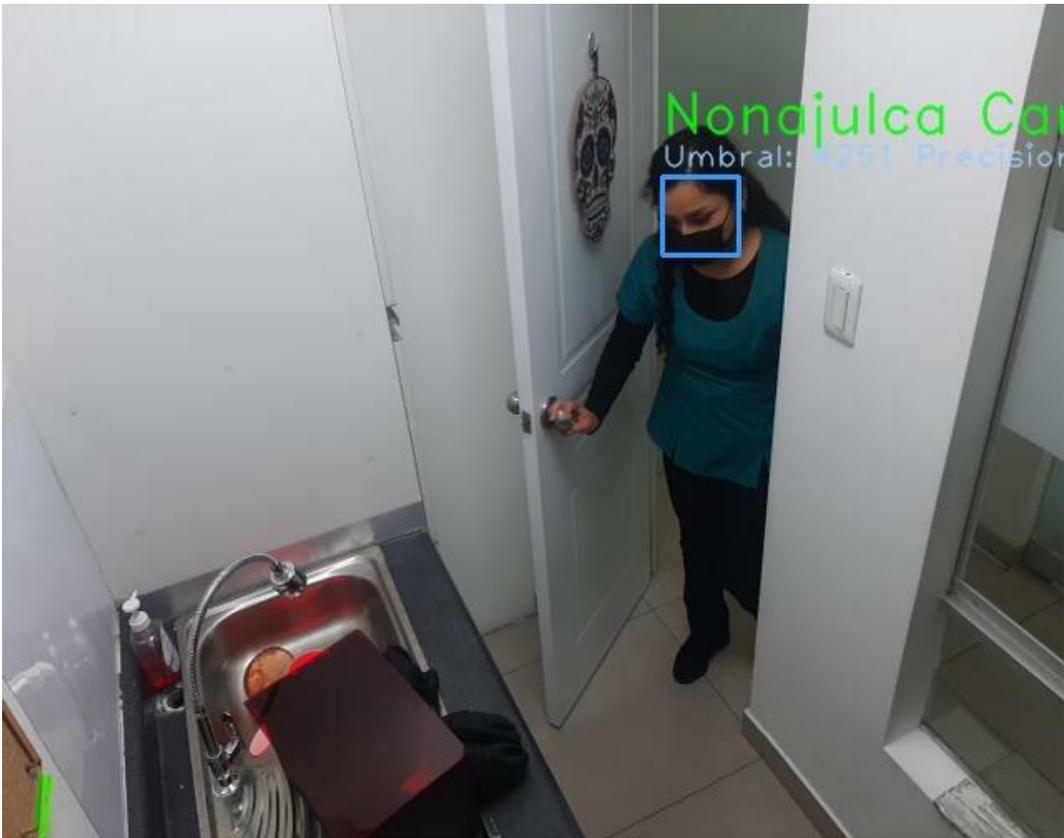
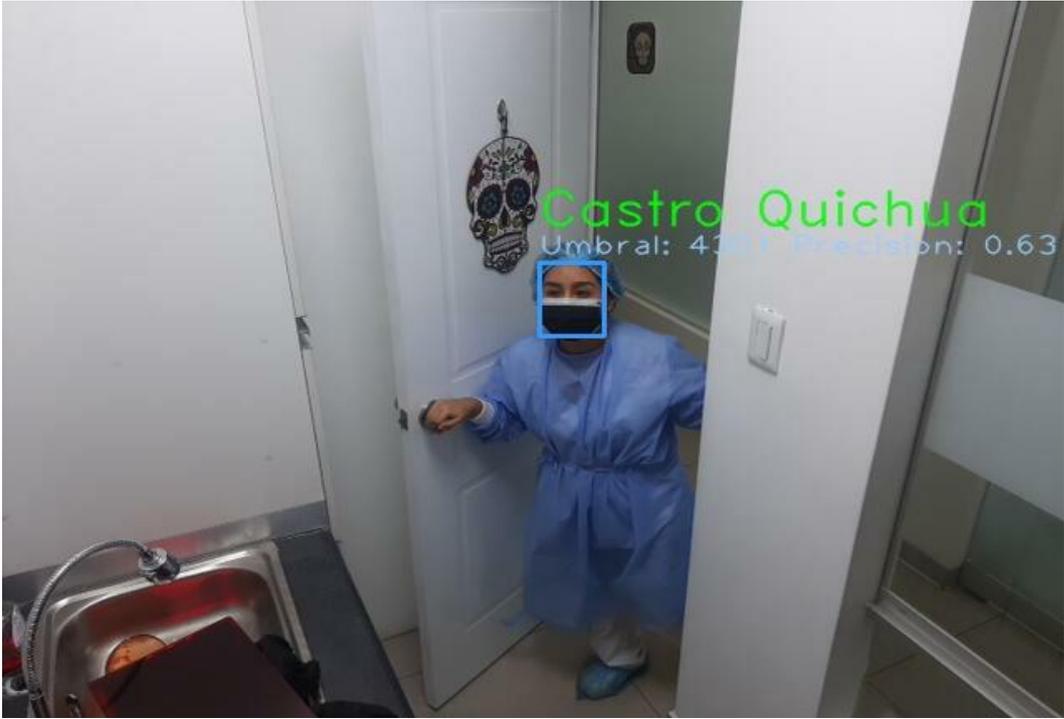
Below the table, it says 'Mostrando el registro 1 de 1'. There are 'Anterior' and 'Siguiente' buttons. The Windows taskbar at the bottom shows the date as 27/09/2022 and time as 14:03.

The screenshot shows the same facial recognition application interface. In the video feed, a person is wearing a blue protective suit and a blue face mask. Two bounding boxes are drawn around the person's face. The top one is red and labeled 'Desconocido' with 'Umbral: 6640 Precision: 0.92'. The bottom one is green and labeled 'Castro Quichua' with 'Umbral: 5426 Precision: 1.00'. Below the video feed, there is a table with the following data:

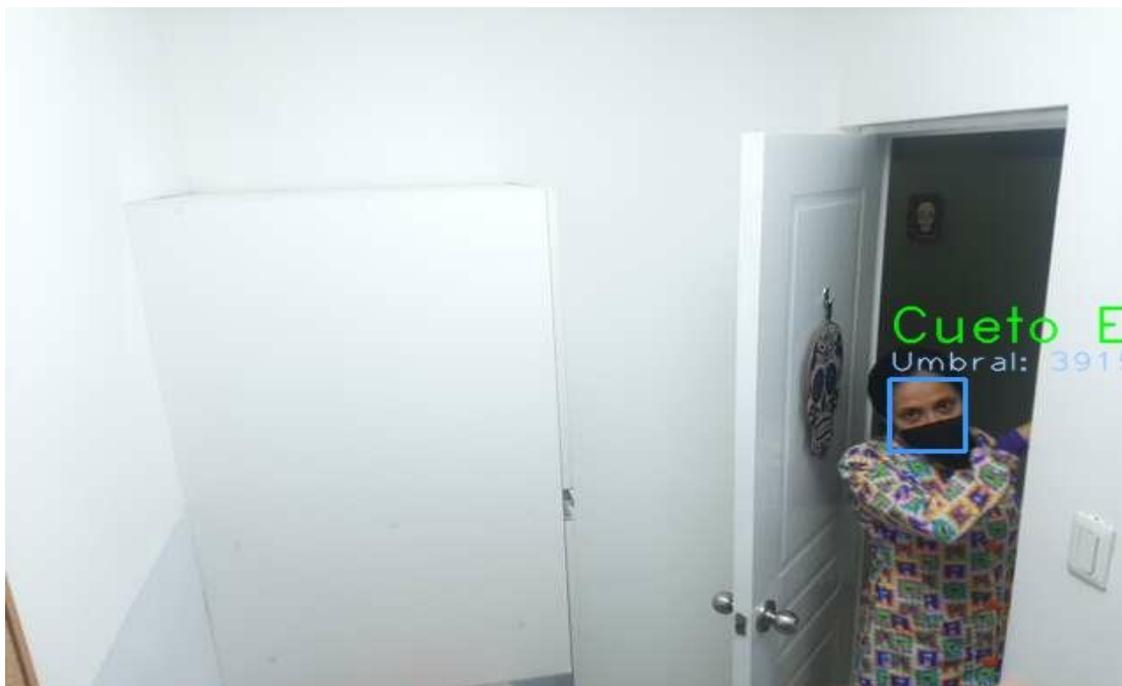
Nombre	Apellido	Correo	Telefono	Area	Nivel	Fecha	Precisión
Jimena	Castro Quichua	quichua_jim_96@gmail.com	942578124	Asistente	No autorizado	Tue, 27 Sep 2022 14:02:25 GMT	0.8374199
Katia	Velarde	fernandez_katia15@gmail.com	975216485	Doctor	No autorizado	Tue, 27 Sep 2022 14:00:29 GMT	0.5040199

The Windows taskbar at the bottom shows the date as 27/09/2022 and time as 14:03.





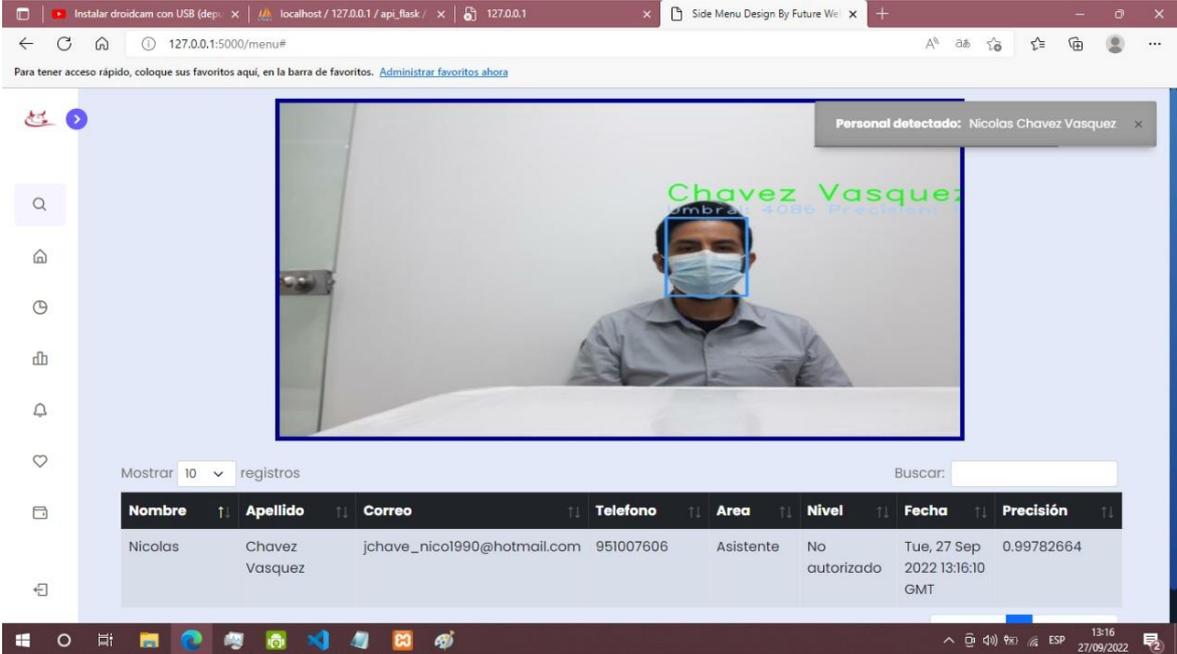
Falso Positivo. Donde el Umbral bajo a 3915 y es por haber realizado un mal entrenamiento del rostro.







Entrenando Imágenes en el Sitio.



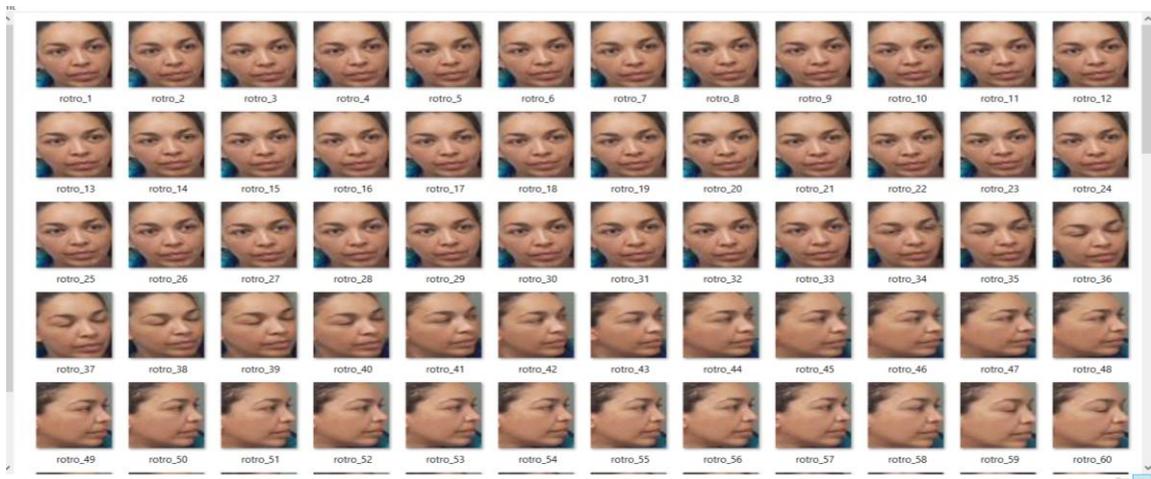
Personal detectado: Nicolas Chavez Vasquez

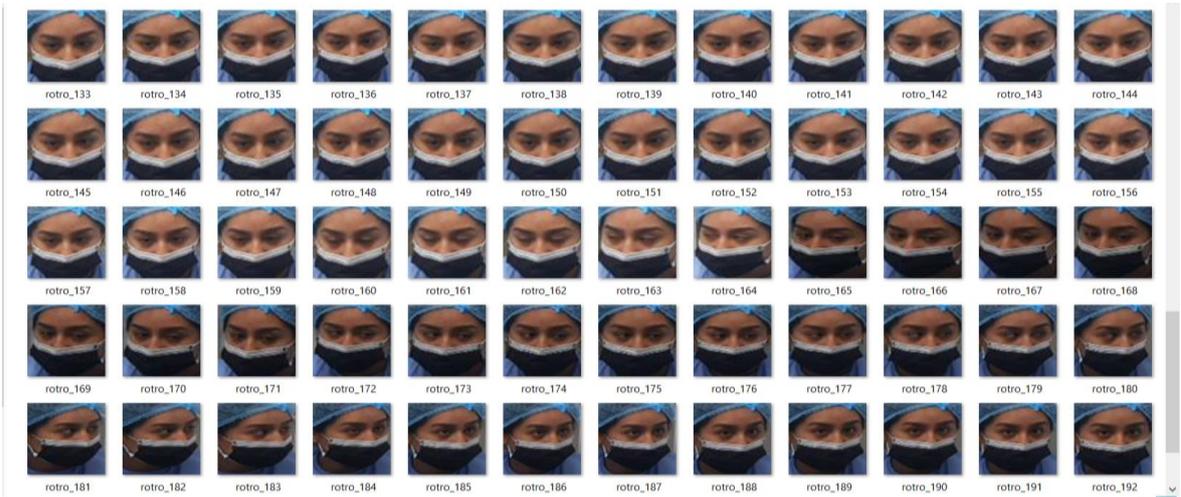
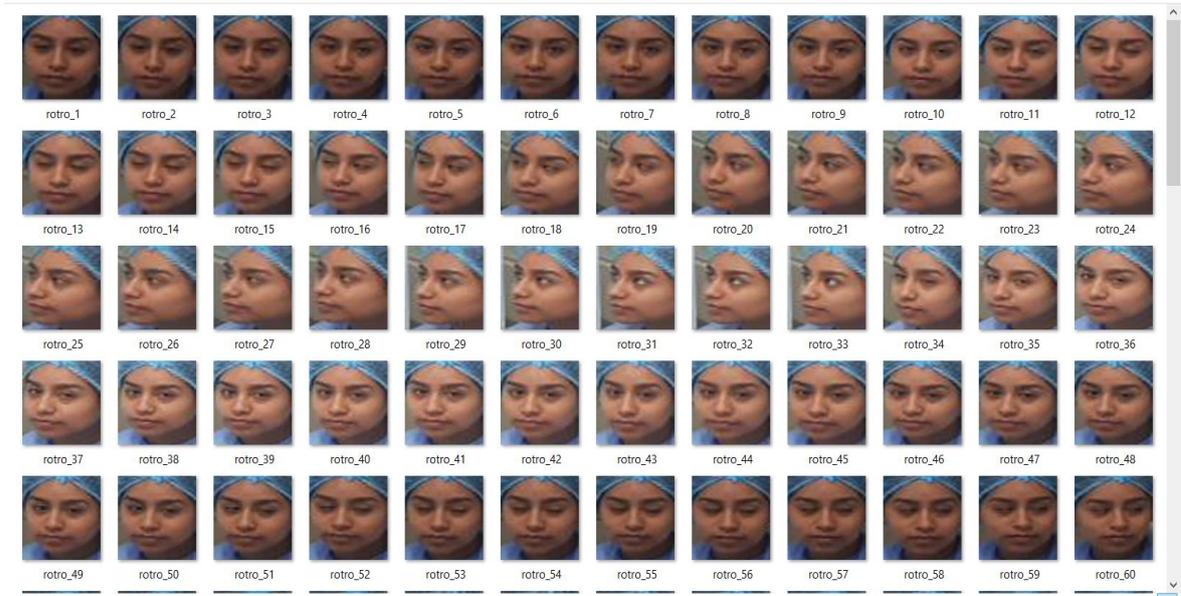
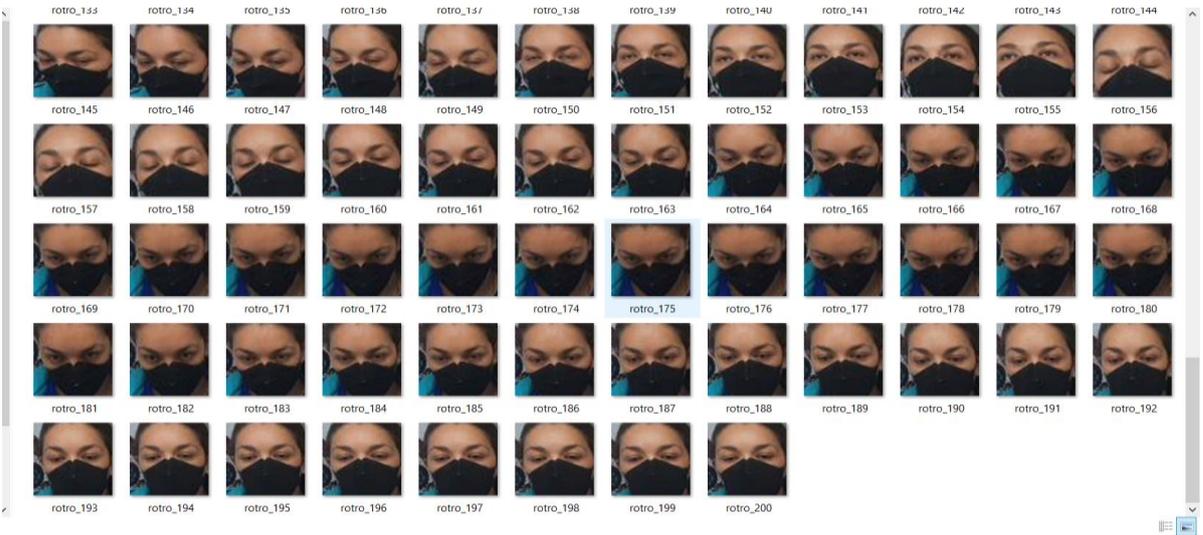
Chavez Vasquez
Cámara 4.08s Precisión

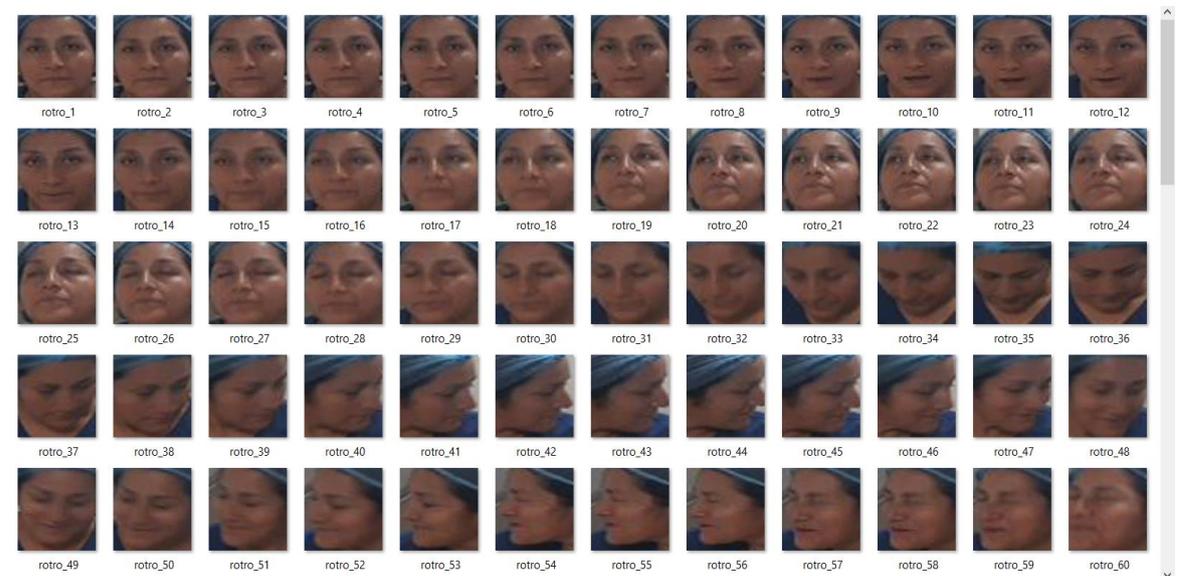
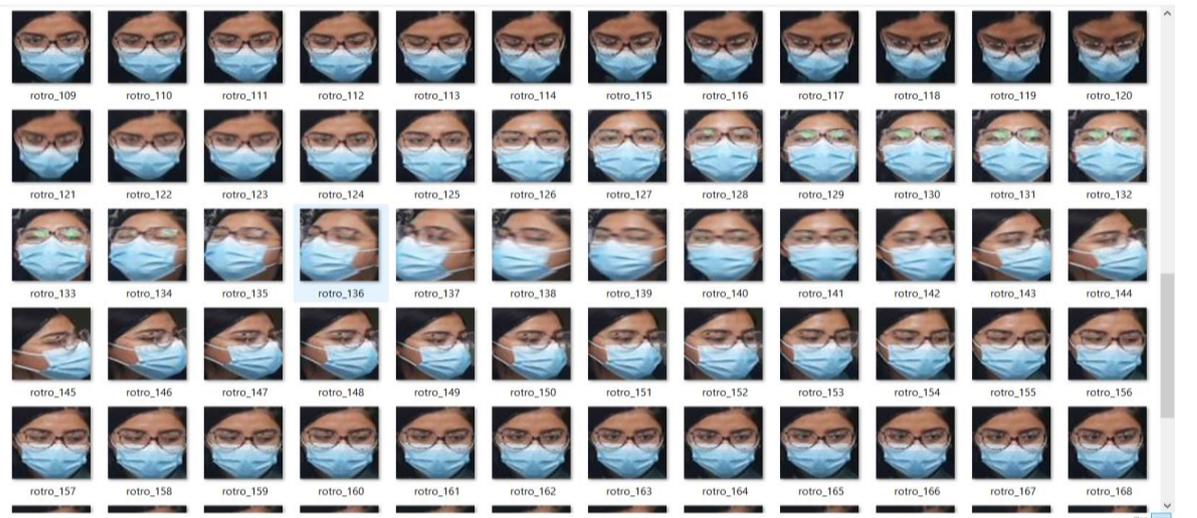
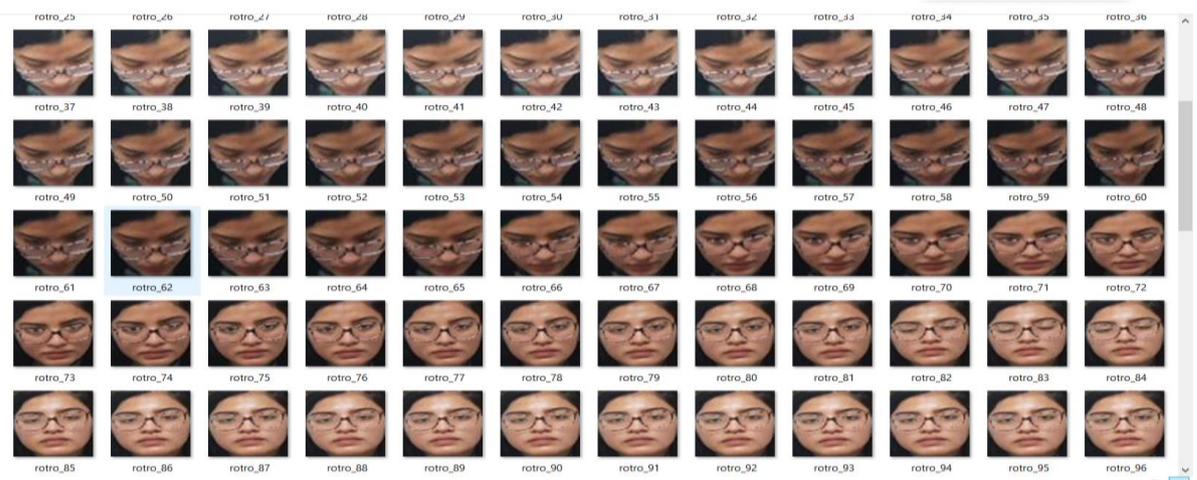
Mostrar 10 registros

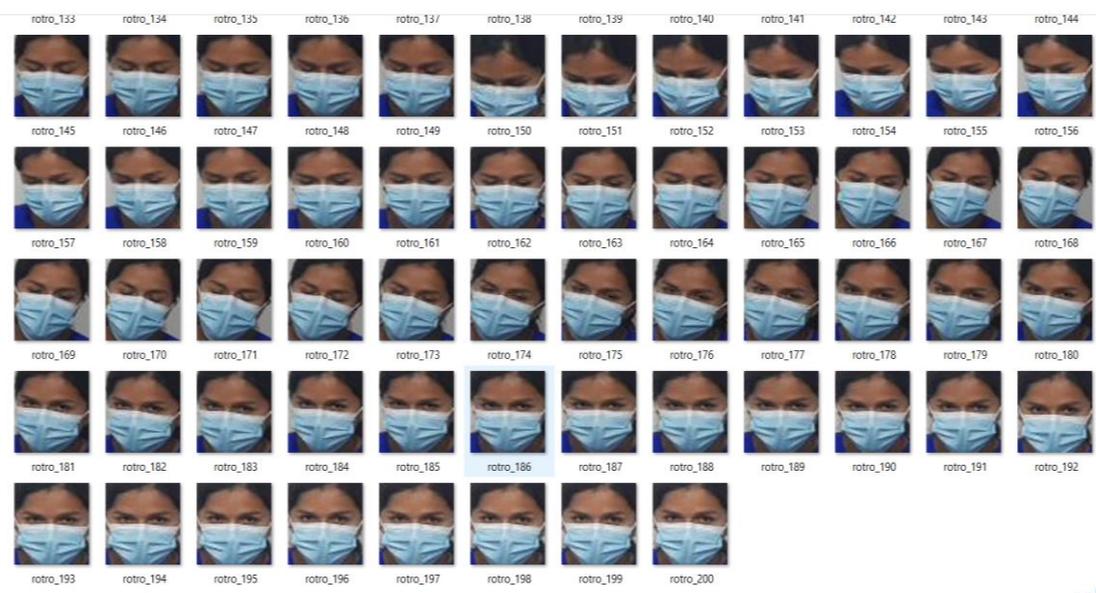
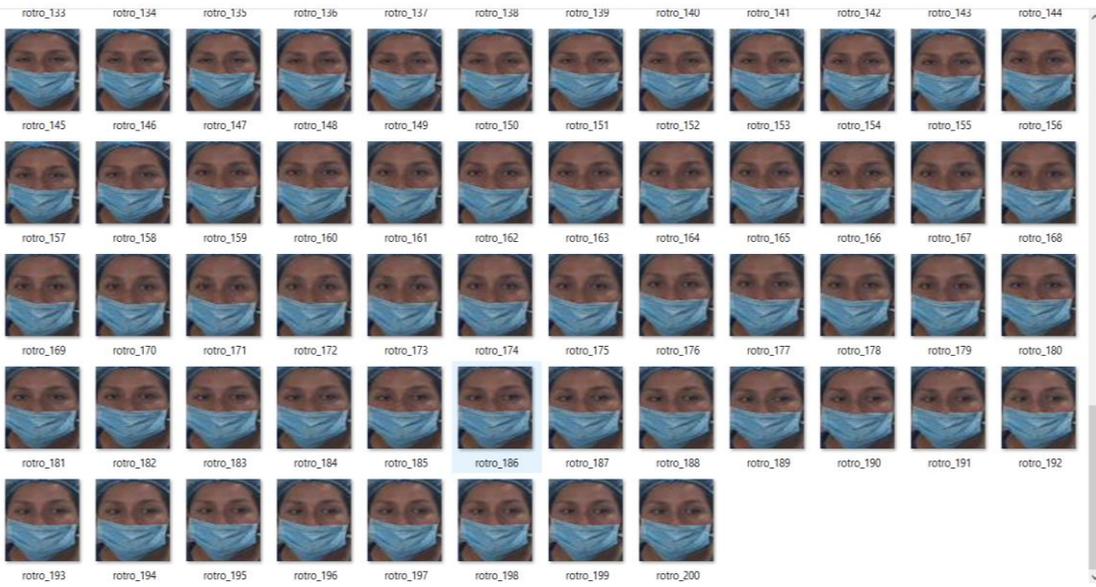
Nombre	Apellido	Correo	Telefono	Area	Nivel	Fecha	Precisión
Nicolas	Chavez Vasquez	jchave_nical990@hotmail.com	951007606	Asistente	No autorizado	Tue, 27 Sep 2022 13:16:10 GMT	0.99782664

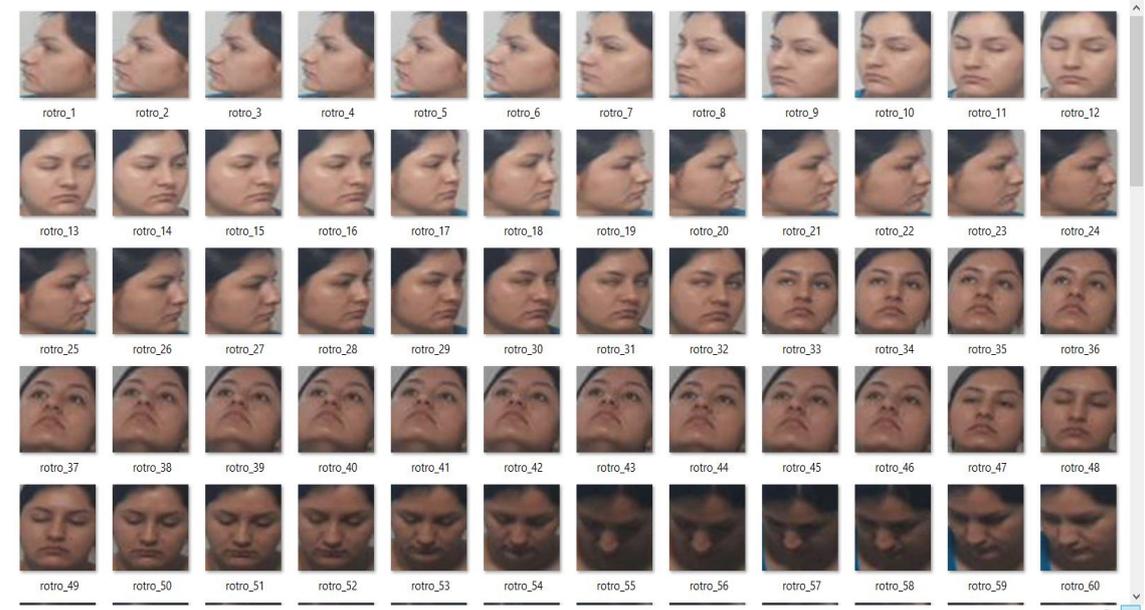
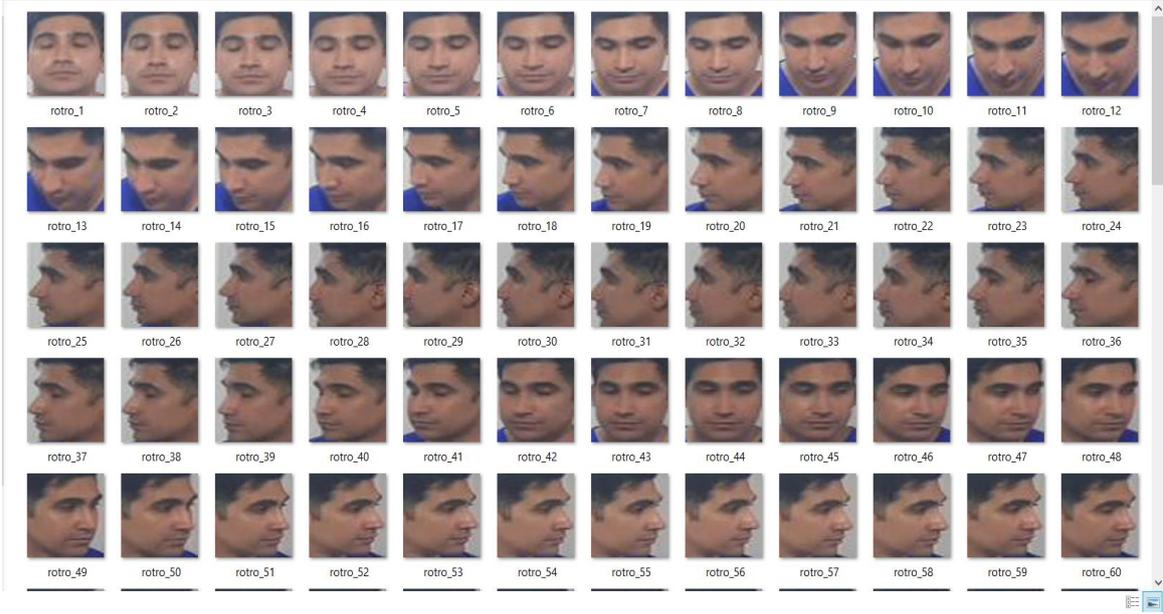
Entrenamiento de Rostros del personal con mascarilla y sin mascarilla.

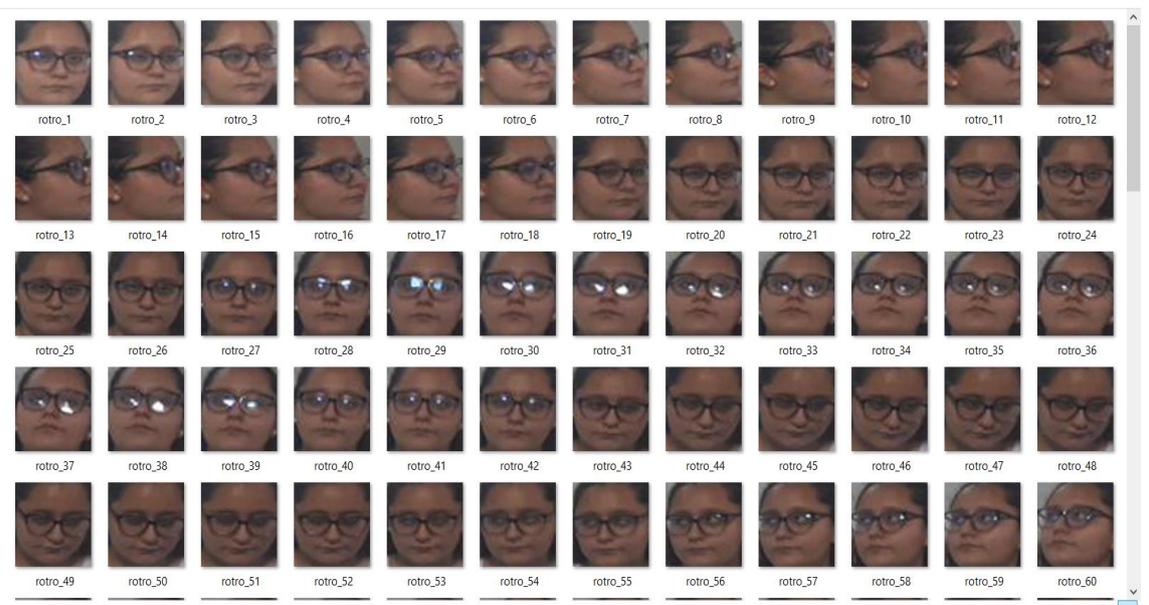
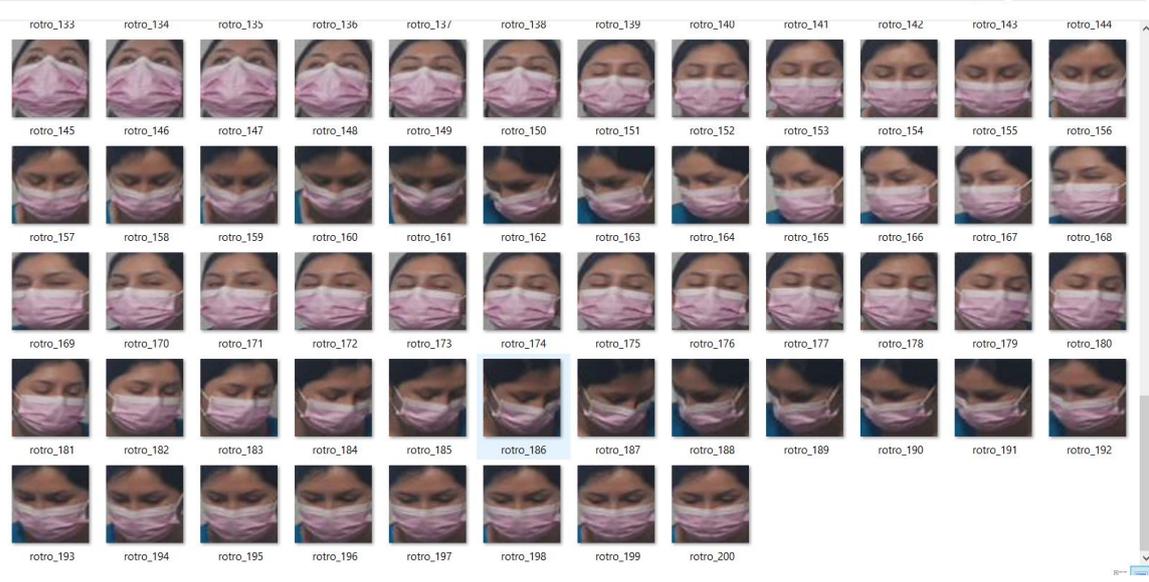


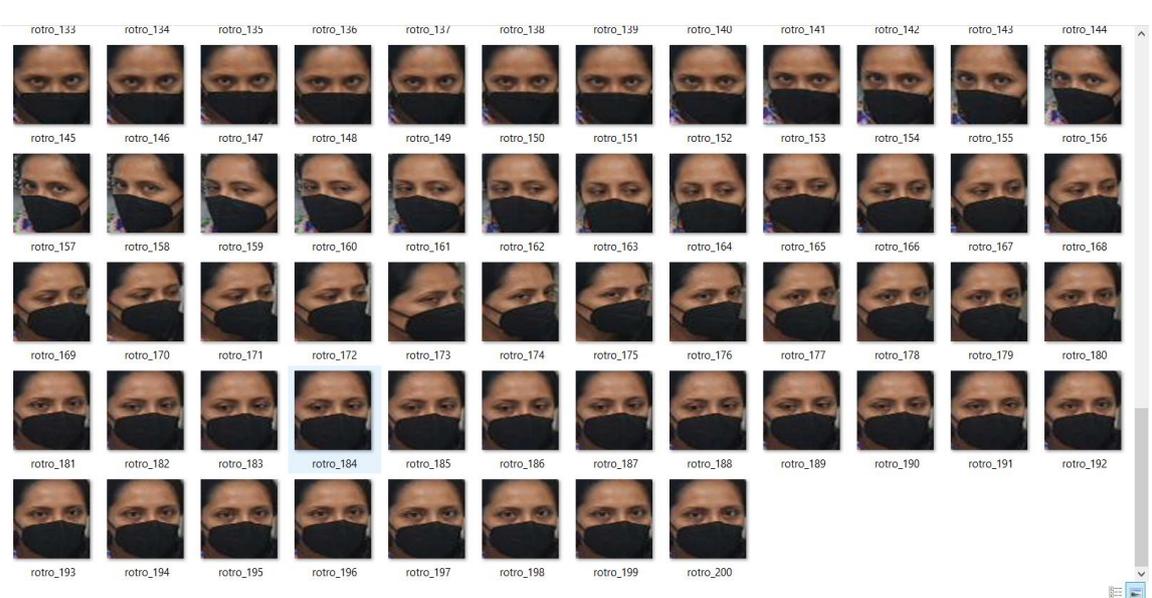
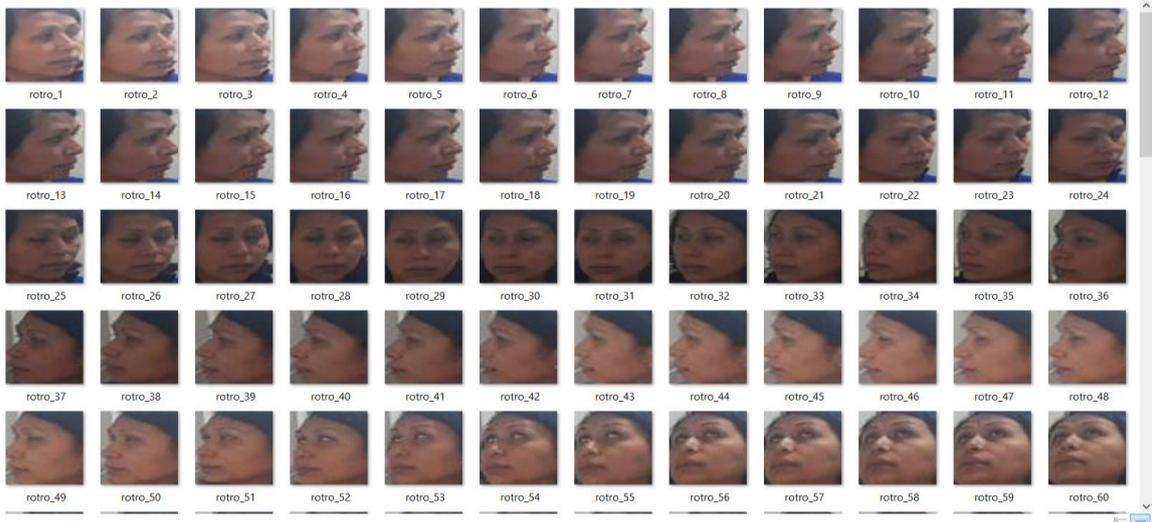


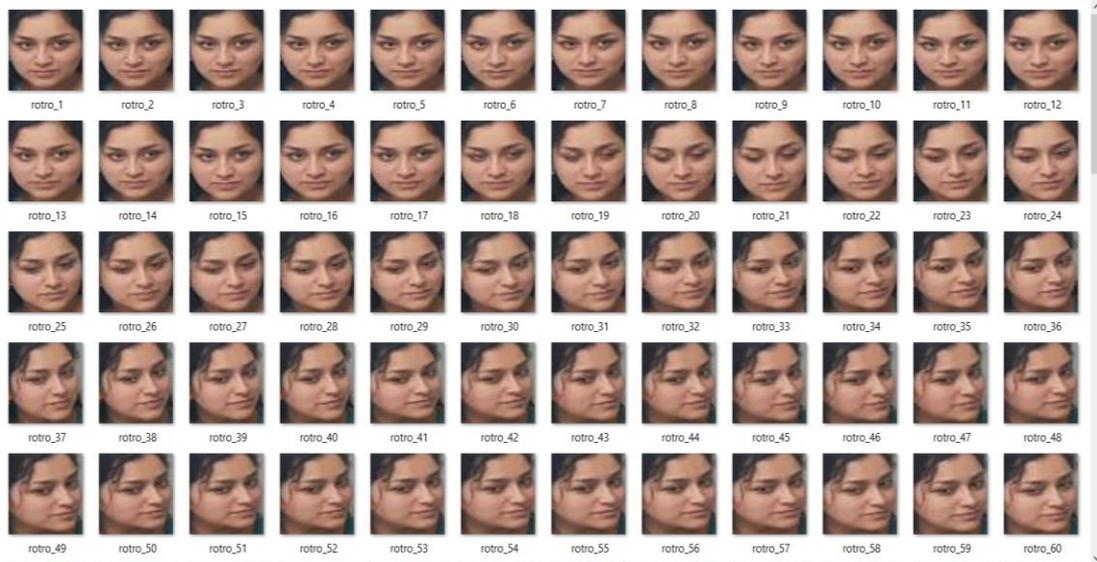
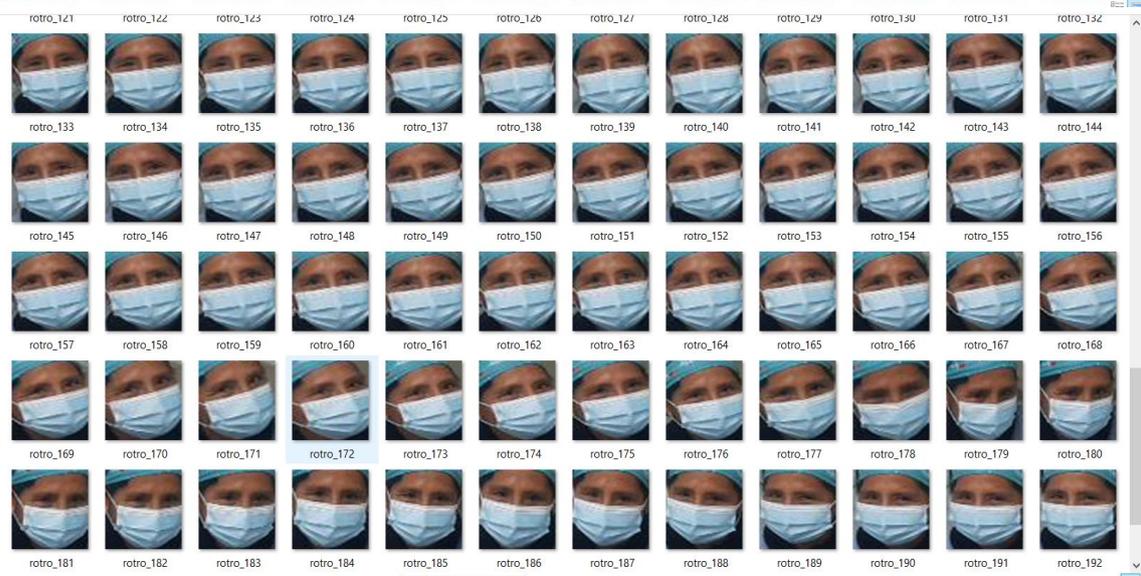


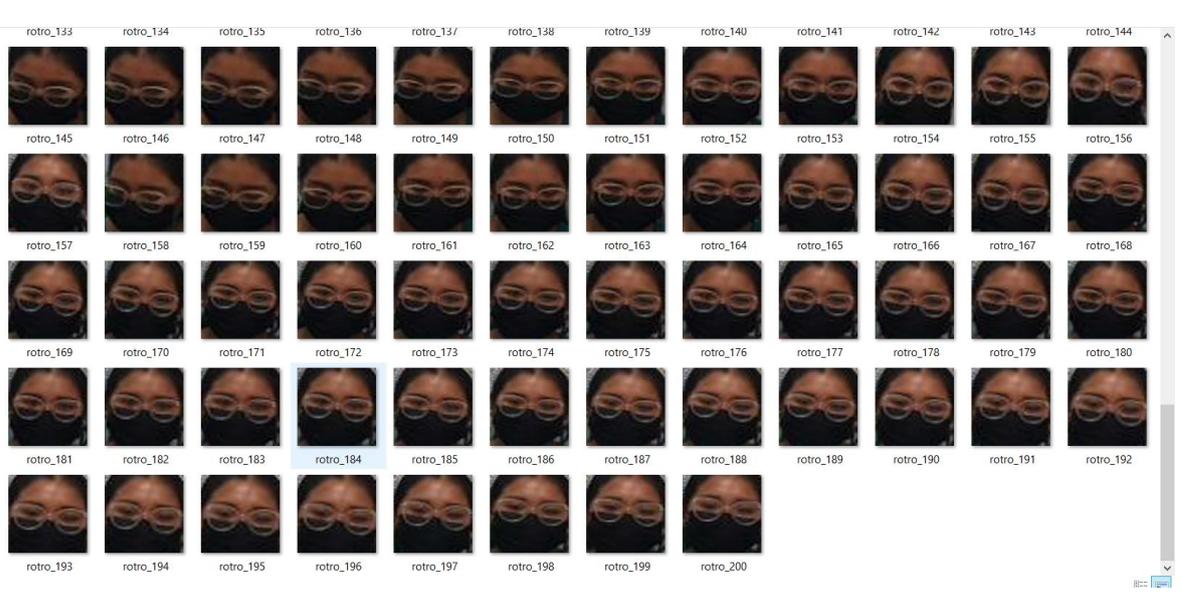
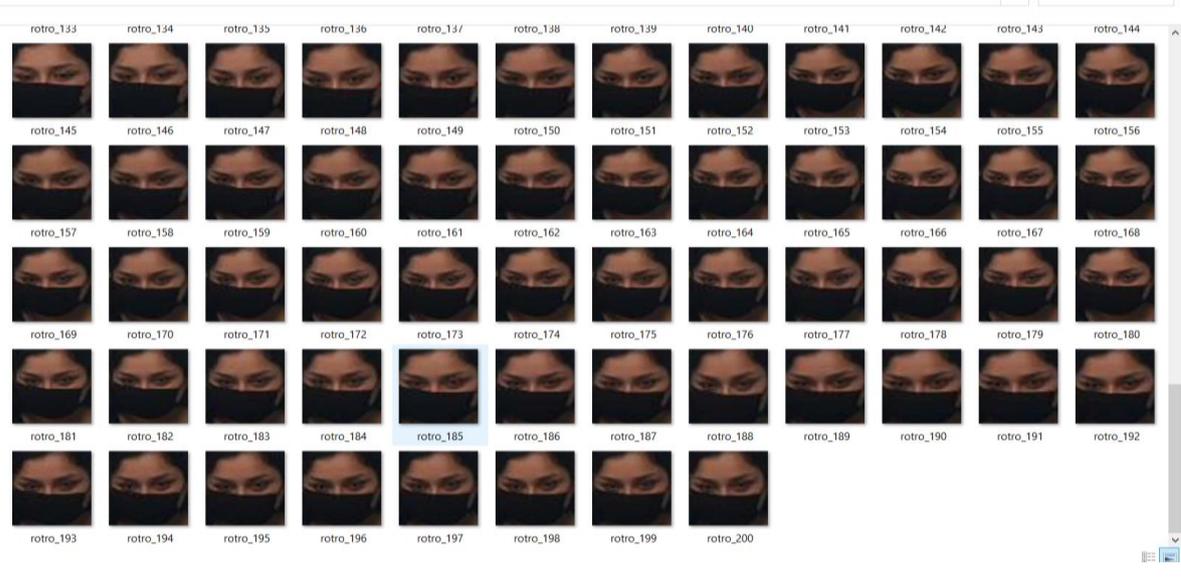


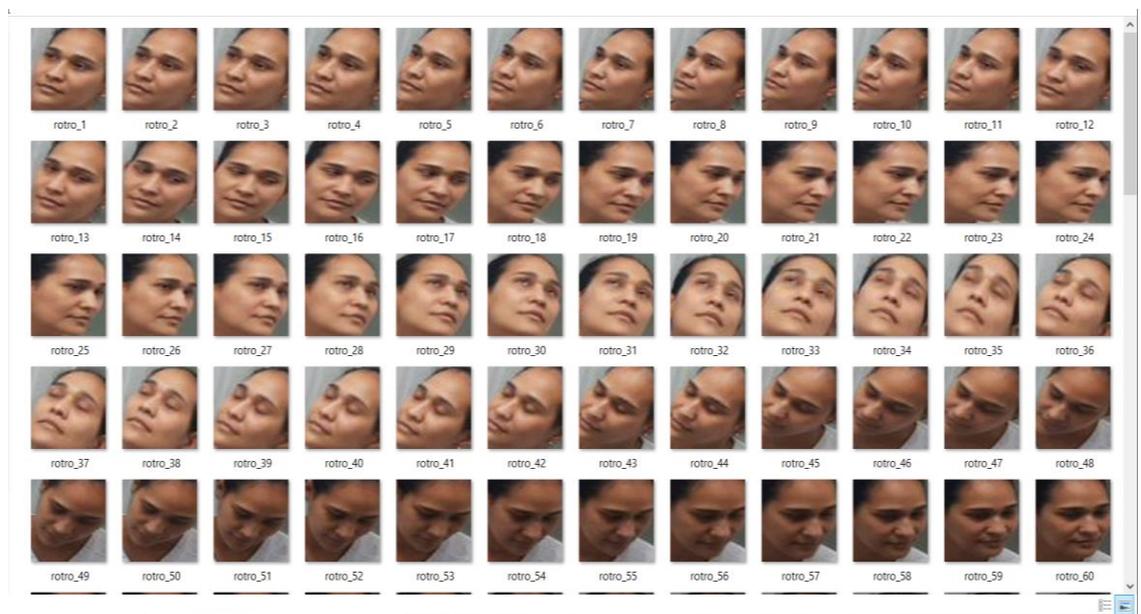


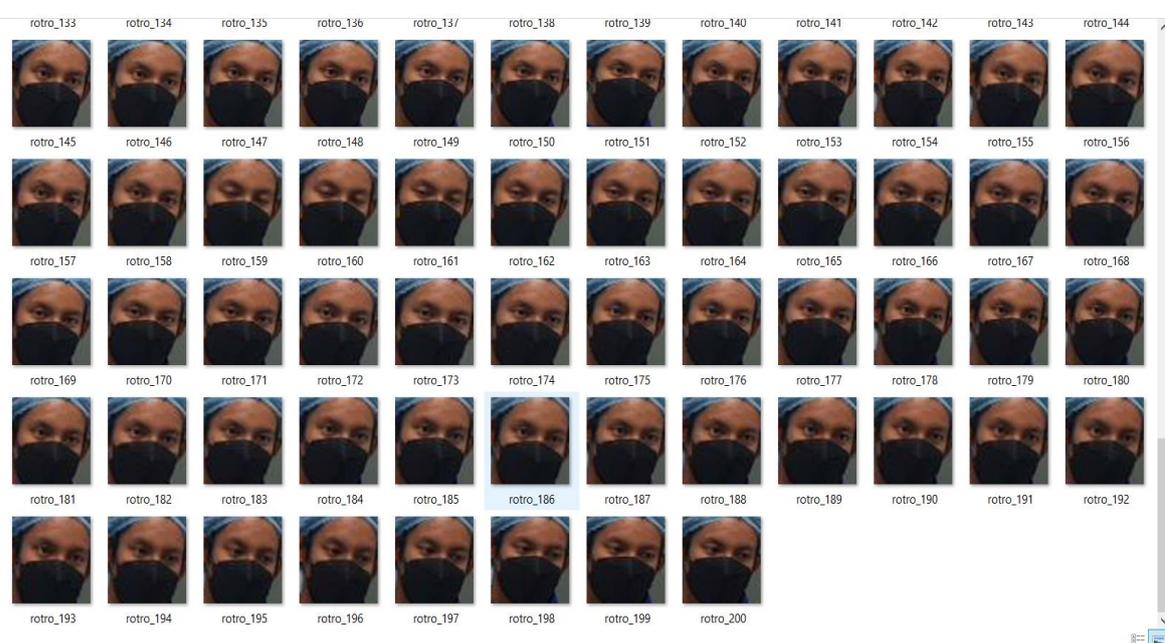
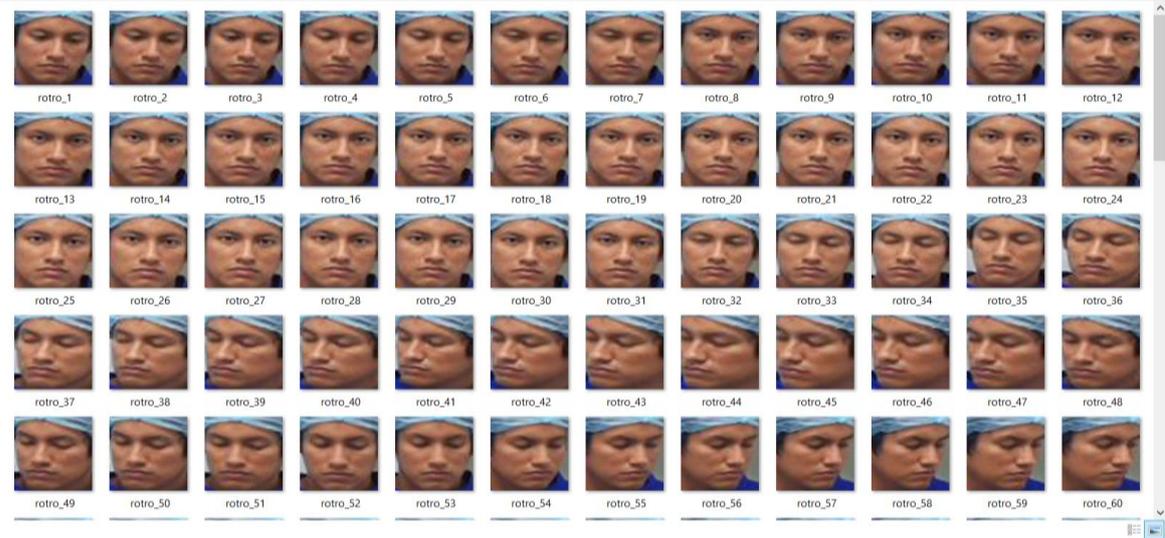
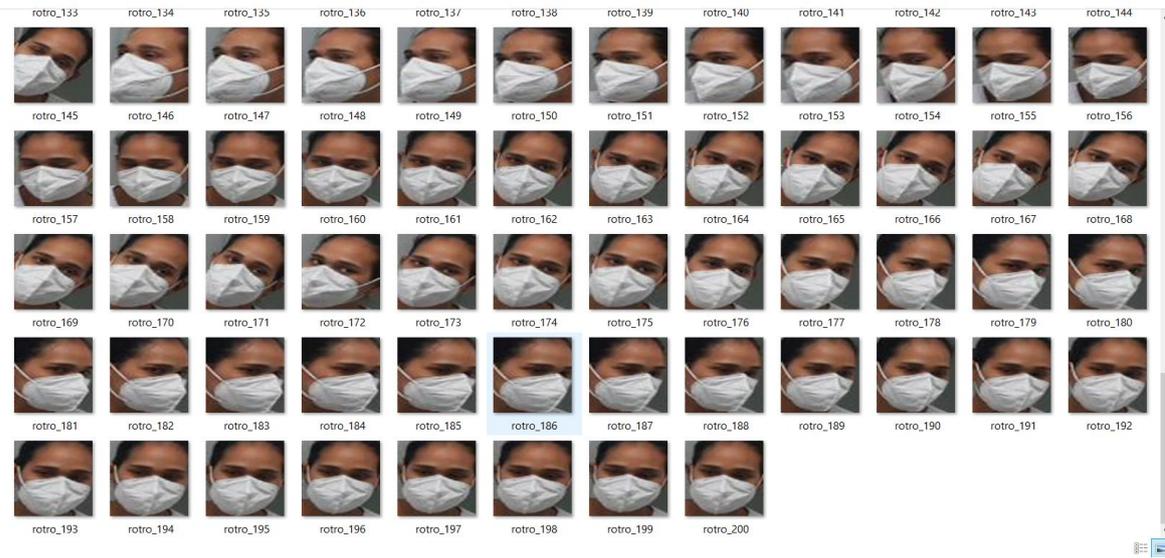


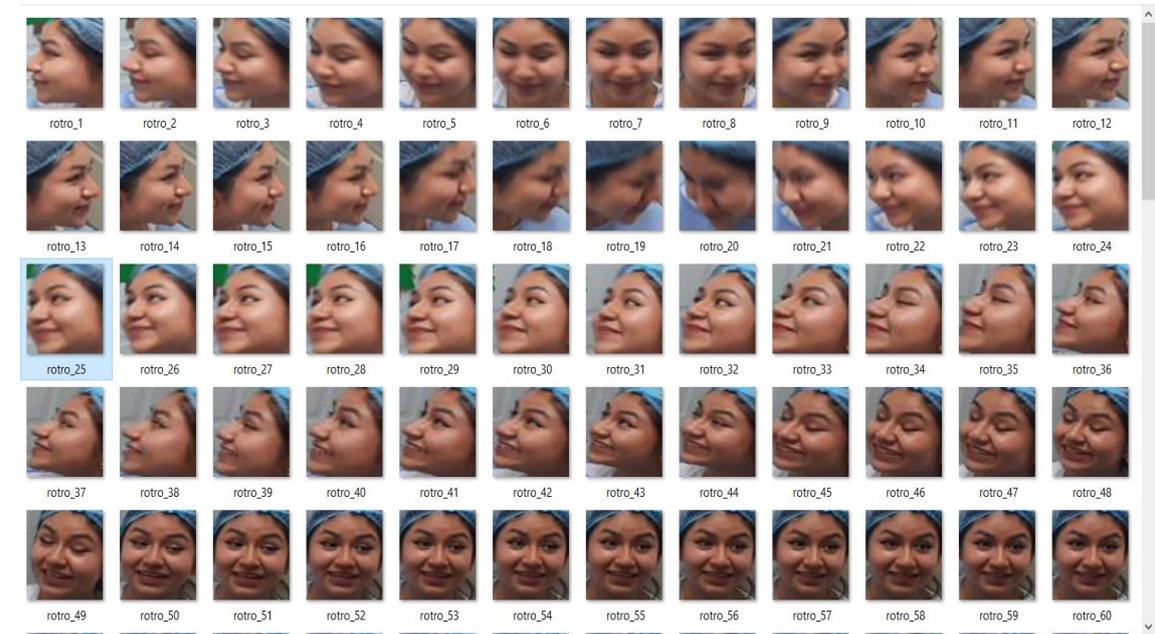
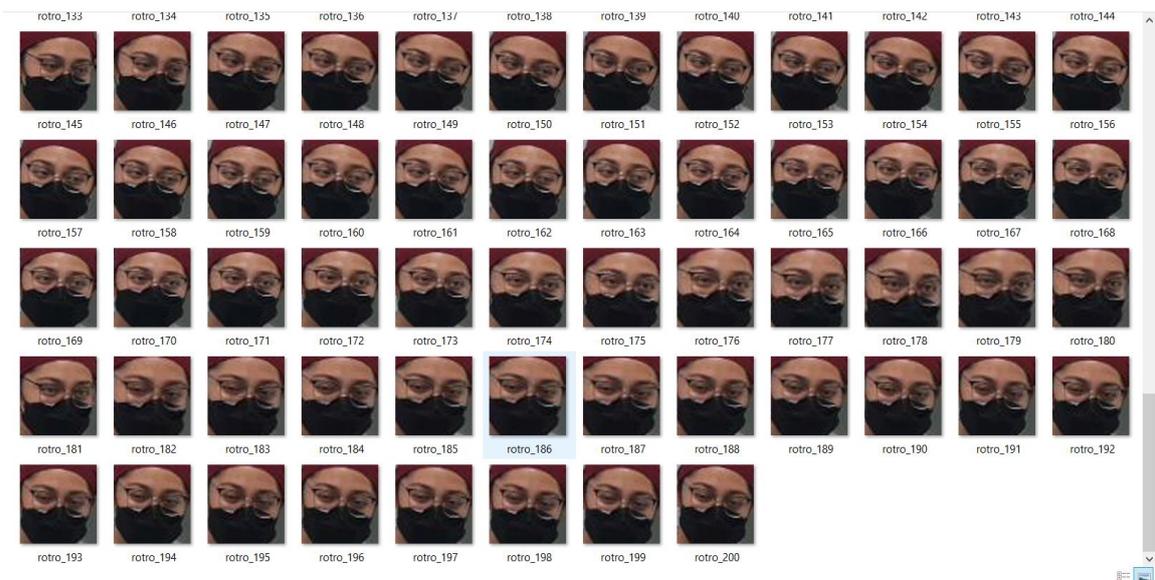


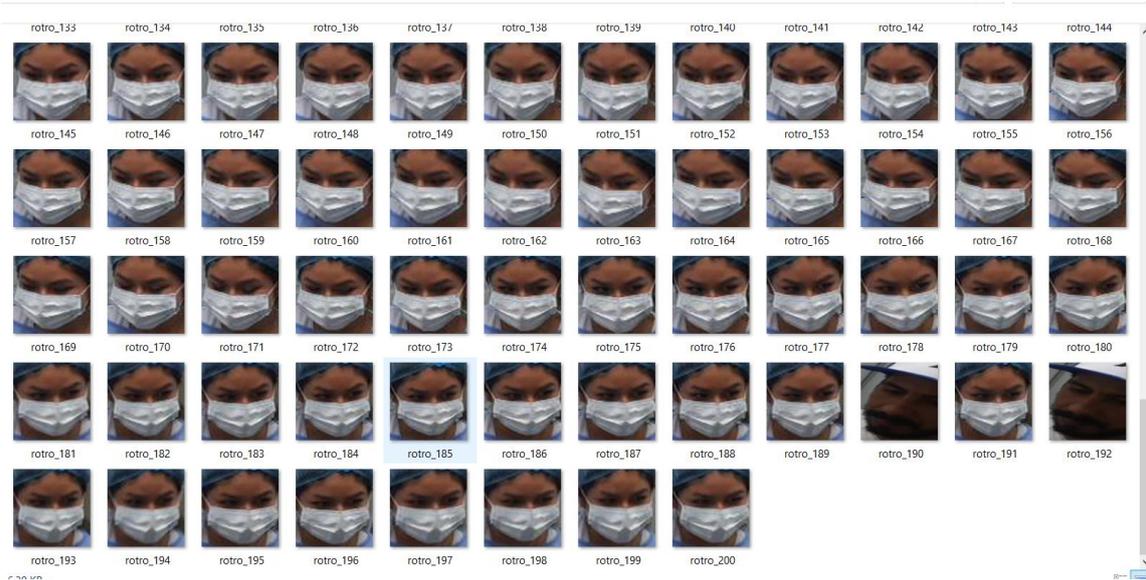




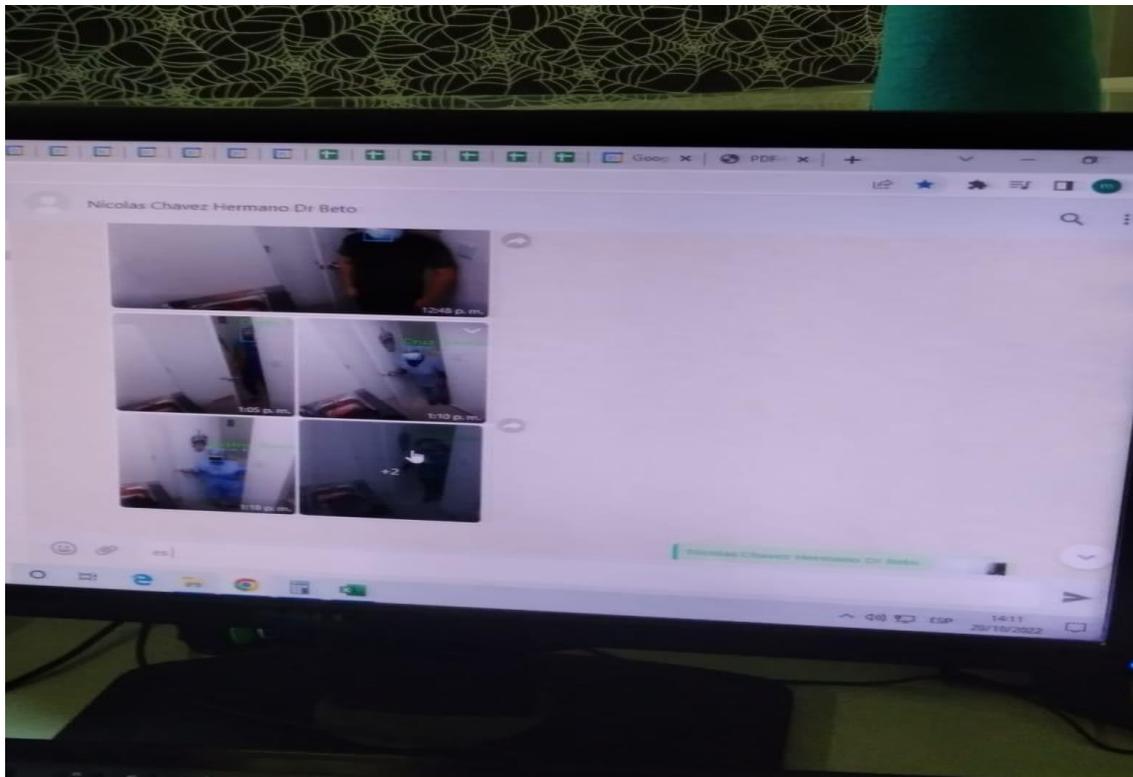


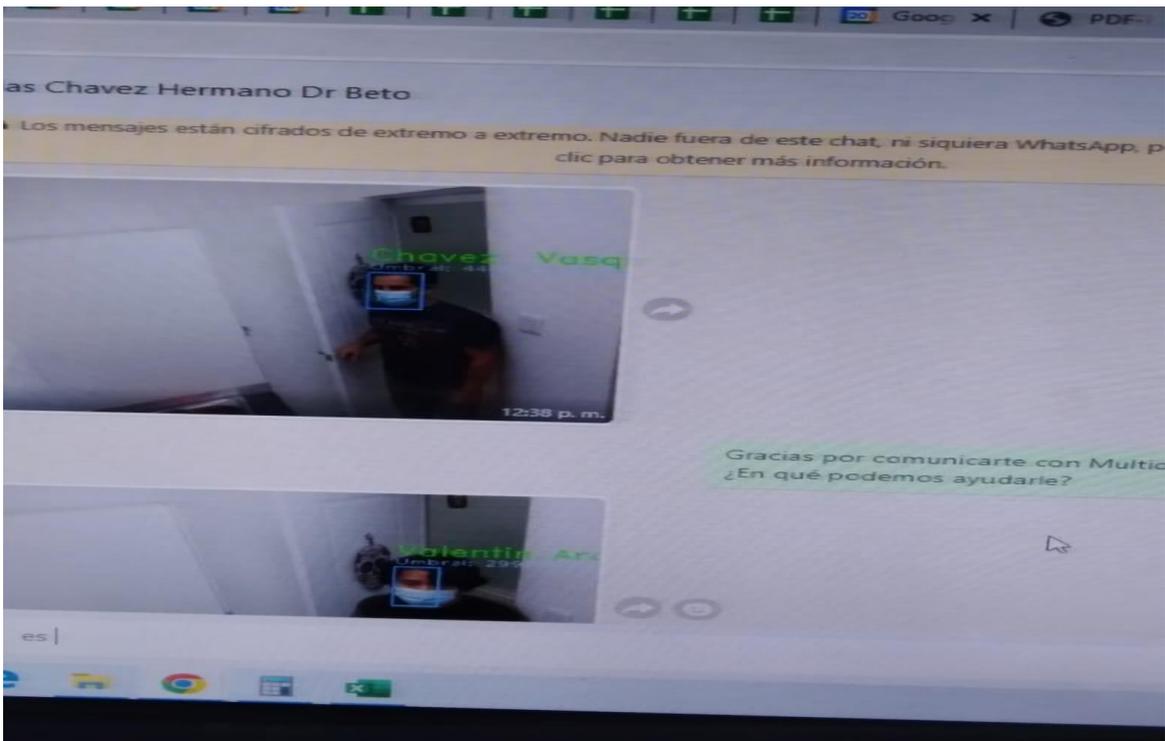
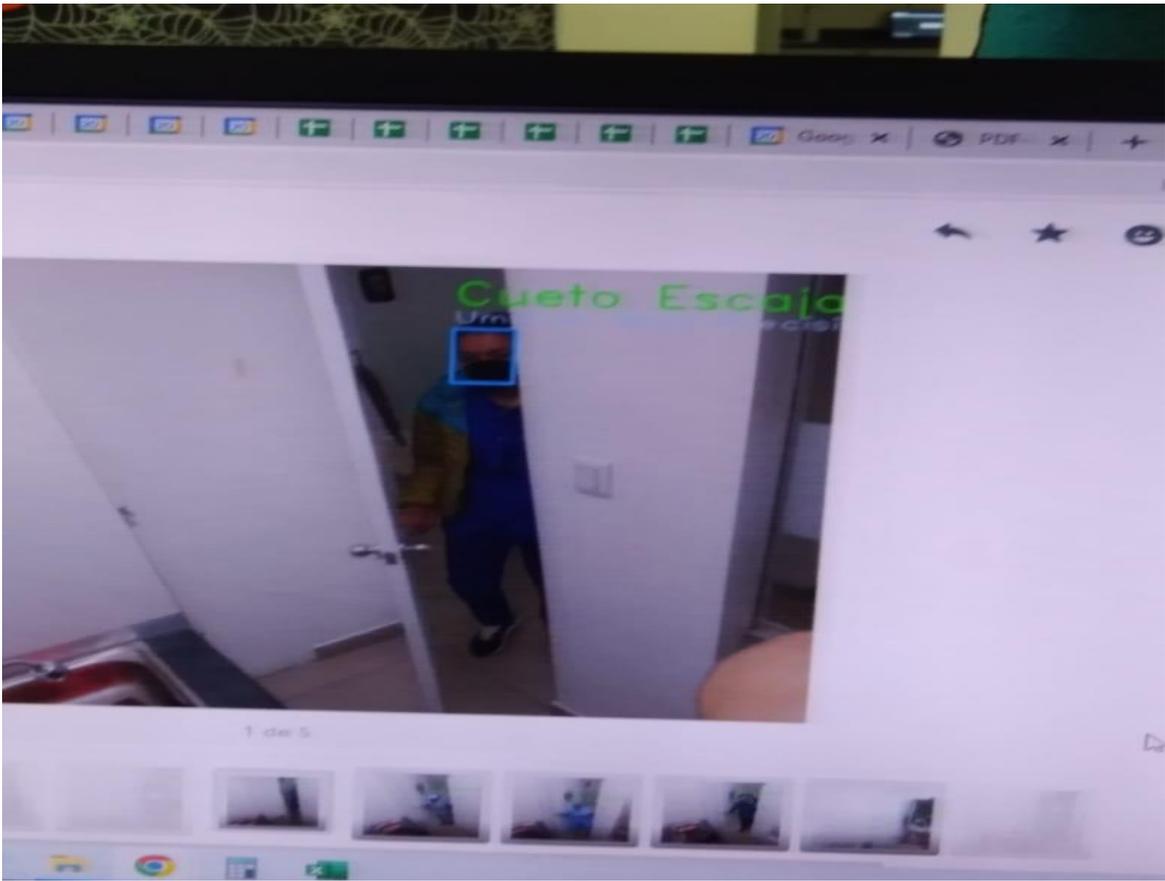






Como aparecen los reportes en el WhatsApp de la Empresa.





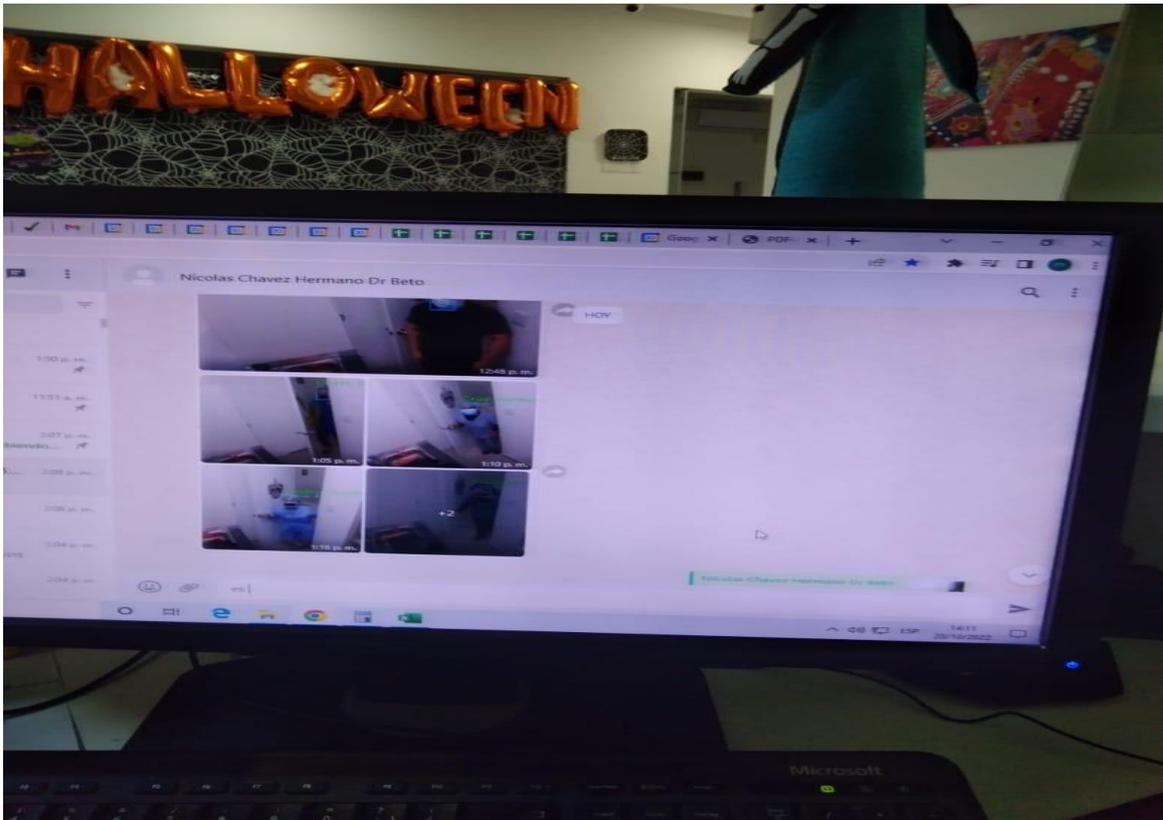


Imagen del Almacén.





Imagen del almacén



Consultorio de la Clínica



Foto con parte del Personal





UNIVERSIDAD CÉSAR VALLEJO

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

Declaratoria de Autenticidad del Asesor

Yo, COHELLO AGUIRRE ROGELIO GONZALO, docente de la FACULTAD DE INGENIERÍA Y ARQUITECTURA de la escuela profesional de INGENIERÍA DE SISTEMAS de la UNIVERSIDAD CÉSAR VALLEJO SAC - LIMA ATE, asesor de Tesis titulada: "Sistema de Reconocimiento facial con aprendizaje profundo para el control de acceso del almacén, en la Clinica Multident Buenos Aires, 2022", cuyos autores son VALENTIN ARANA ARMANDO JEAN PIERRE, CHAVEZ VASQUEZ NICOLAS, constato que la investigación tiene un índice de similitud de 27.00%, 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, 29 de Noviembre del 2022

Apellidos y Nombres del Asesor:	Firma
COHELLO AGUIRRE ROGELIO GONZALO DNI: 07634626 ORCID: 0000-0001-5526-5231	Firmado electrónicamente por: RCOHELLO el 13-12- 2022 21:54:09

Código documento Trilce: TRI - 0462376