Servicio de Software Factory para los OEE en 4 Lotes - ID 410299

Documento Técnico conteniendo Análisis de librerías de reconocimiento facial y prueba de vida con licenciamiento o suscripción local y nube.

CENTRO DE DESARROLLO SOSTENIBLE SA

23/FEB/2024

ÍNDICE DE CONTENIDOS

1. INTRODUCCIÓN.....3
2. GLOSARIO DE TÉRMINOS.....3
3. RELEVAMIENTO Y ANÁLISIS TÉCNICO SOBRE EL ESTADO DEL ARTE PARA LAS TECNOLOGÍAS DE RECONOCIMIENTO FACIAL Y PRUEBAS DE VIDA, PARA INTERACCIONES DE APLICACIONES MÓVILES Y APLICACIONES WEB.....4
3.1. Características del Face Recognition.....4
3.2. Técnicas de reconocimiento facial.....6
3.3. Prueba de vida.....6
3.4. Estado del arte de tecnologías de Face Recognition.....8
3.5. Experiencias de la región.....18
4. ARQUITECTURAS TECNOLÓGICAS QUE SE AJUSTEN A LA NECESIDAD IDENTIFICADA, TENDIENTE A DAR RESPUESTA A SISTEMAS DE SERVICIOS LOCALES, EN LA NUBE Y APLICACIONES MÓVILES, QUE INCLUYA LAS RECOMENDACIONES DE STACK TECNOLÓGICO.....22
5. DIFERENTES OPCIONES DE MECANISMOS DE MONETIZACIÓN Y PAGO PARA LOS SERVICIOS QUE PUEDA PROVEER EL MITIC A OTRAS ENTIDADES POR MEDIO DEL FACERECOGNITIONCORE.....29
6. EETT FUNCIONALES DE LAS APPS A SER MODIFICADAS.....31
7. EETT NO FUNCIONALES DE LAS APPS A SER MODIFICADAS.....32
8.1. REGISTRO DE USUARIO.....32
8.2. INICIO DE SESIÓN CON RECONOCIMIENTO FACIAL.....37
8.3. ACTUALIZACIÓN DE PERFIL PARA RECONOCIMIENTO FACIAL.....42
9. CONCLUSIONES Y RECOMENDACIONES FINALES.....45
10. REFERENCIAS.....46
11. PLANIFICACIÓN DE ENTREGA DE LA OT.....46
12. PERFILES PARA EL DESARROLLO DE LA OT.....47

1. INTRODUCCIÓN

En el marco de los servicios de Software Factory para los OEE en 4 Lotes - ID 410299, Orden de Trabajo Nro 4 recibida, fueron convocados los expertos claves por parte de la empresa Centro de Desarrollo Sostenible S.A para Realizar un relevamiento y análisis técnico del estado del arte y las aplicaciones específicas para la aplicación de reconocimiento facial y pruebas de vida en aplicaciones móviles para realizar OnBoarding digital en las aplicaciones móviles del estado. La misma, funcionará como un núcleo de reconocimiento facial, permitiendo a los usuarios acceder a funcionalidades de identificación biométrica desde dispositivos inteligentes como smartphones y otros, autenticados por medio de la Identidad Electrónica de la aplicación móvil (PortalParaguay).

Este documento presenta el producto entregable de la orden de trabajo Nro 4, el cual incluye en las siguientes secciones: i) relevamiento y análisis técnico sobre el estado del arte para las tecnologías de reconocimiento facial y pruebas de vida, para interacciones de aplicaciones móviles y aplicaciones web, ii) arquitecturas tecnológicas que se ajusten a la necesidad identificada, tendiente a dar respuesta a sistemas de servicios locales, en la nube y aplicaciones móviles, que incluya las recomendaciones de stack tecnológico, iii) diferentes opciones de mecanismos de monetización y pago para los servicios que pueda proveer el MITIC a otras entidades por medio del FaceRecognitionCore, iv) EETT Funcionales de las Apps a ser modificadas, y v) EETT No funcionales de las Apps a ser modificadas.

2. GLOSARIO DE TÉRMINOS

Computer vision: Es un campo de Inteligencia Artificial e Informática que enseña a los ordenadores a 'ver' y entender el contenido de las imágenes digitales.

Face recognition: El reconocimiento facial es una tecnología potencialmente capaz de comparar un rostro humano a partir de una imagen digital contra una base de datos de rostros e identificar a una persona.

Machine learning: Es una disciplina del campo de la Inteligencia Artificial que, a través de algoritmos, dota a los ordenadores de la capacidad de identificar patrones en datos masivos y elaborar predicciones

Deep learning: es un tipo de machine learning que entrena a una computadora para que realice tareas como las hacemos los seres humanos, como el reconocimiento del habla, la identificación de imágenes o hacer predicciones.

Deepfake: Es una noticia o nota falsa que a simple vista se ve que es real pero solo engaña.

Tensorflow: Es una biblioteca de código abierto para aprendizaje automático a través de un rango de tareas, y desarrollado por Google para satisfacer sus necesidades de sistemas capaces de construir y entrenar redes neuronales para detectar y descifrar patrones y correlaciones, análogos al aprendizaje y razonamiento usados por los humanos

3. *RELEVAMIENTO Y ANÁLISIS TÉCNICO SOBRE EL ESTADO DEL ARTE PARA LAS TECNOLOGÍAS DE RECONOCIMIENTO FACIAL Y PRUEBAS DE VIDA, PARA INTERACCIONES DE APLICACIONES MÓVILES Y APLICACIONES WEB*

El reconocimiento facial se ha convertido en una tecnología importante para diversas aplicaciones, como vigilancia, control de acceso, análisis de multitudes y más. Con el reconocimiento facial en tiempo real, los rostros se pueden detectar e identificar instantáneamente mediante la transmisión de una cámara o una transmisión de video. Esto permite casos de uso interesantes, como permitir el acceso autorizado a instalaciones seguras, identificar personas incluidas en listas negras y recopilar datos demográficos de multitudes.

Un analizador facial es un software que identifica o confirma la identidad de una persona a partir del rostro. Funciona mediante la identificación y medición de los rasgos faciales en una imagen. Los sistemas de seguridad biométricos utilizan el reconocimiento facial para identificar de forma exclusiva a las personas durante la incorporación o el inicio de sesión de los usuarios, así como para reforzar la actividad de autenticación de estos. Los dispositivos móviles y personales también utilizan con frecuencia la tecnología de los analizadores faciales para proteger los dispositivos.

De todas las mediciones biométricas, el reconocimiento facial se considera el más natural. Esto sigue una lógica intuitiva, ya que normalmente nos reconocemos a nosotros mismos y a los demás mirando las caras, en lugar de las huellas digitales y los iris.

3.1. Características del Face Recognition

Como en los últimos años la capacidad de procesamiento informático ha aumentado considerablemente, los métodos convencionales de reconocimiento facial aplican modelos de Deep Learning para entrenar los sistemas de detección.

Los sistemas de tecnología facial pueden variar, pero en general tienden a funcionar de la siguiente manera:

3.1.1. Paso 1: Reconocimiento facial

La cámara detecta y ubica la imagen de un rostro, ya sea de forma independiente o como parte de una muchedumbre. La imagen puede mostrar a la persona de frente o de perfil.

3.1.2. Paso 2: Análisis facial

A continuación, se captura y analiza una imagen del rostro. La mayor parte de la tecnología de reconocimiento facial depende de imágenes 2D en lugar de 3D, ya que se puede comparar de manera más fácil una imagen 2D con las fotos públicas o las de una base de datos. El software lee la geometría de tu rostro. Los factores clave incluyen la distancia entre los ojos, la profundidad de las cuencas de los ojos, la distancia desde la frente hasta el mentón, la forma de los pómulos y el contorno de los labios, las orejas y el mentón. El objetivo es identificar los puntos de referencia faciales que son clave para distinguir un rostro.

3.1.3. Paso 3: Conversión de la imagen a datos

El proceso de captura de rostro transforma la información analógica (un rostro) en un conjunto de información digital (datos) basado en los rasgos faciales de la persona. Básicamente, el análisis del rostro se convierte en una fórmula matemática. El código numérico se denomina huella facial. De la misma manera en que las huellas dactilares son únicas, cada persona tiene su propia huella facial.

3.1.4. Paso 4: Búsqueda de una coincidencia

El reconocimiento facial puede identificar a una persona al comparar los rostros de dos o más imágenes y evaluar la probabilidad de que coincidan. Por ejemplo, puede verificar que el rostro mostrado en una foto tomada con la cámara de un móvil coincide con el rostro de una imagen de un documento de identidad emitido por el gobierno, como un permiso de conducir o un pasaporte, así como verificar que el rostro que aparece en la foto no coincide con un rostro de un conjunto de rostros capturados previamente.

3.1.5. Validación y Seguridad

Si bien, por lo general, los datos biométricos se consideran como uno de los métodos de autenticación más confiables, también conllevan un riesgo importante. Esto se debe a que, si alguien es víctima del pirateo de los detalles de su tarjeta de crédito, esa persona tiene la opción de congelar su crédito y tomar medidas para cambiar la información personal que se infringió. Este mismo riesgo debemos considerar en los casos en que una persona pierda su “huella facial” digital o la misma sea generada de manera artificial.

En todo el mundo, la información biométrica se está capturando, almacenando y analizando en cantidades cada vez mayores, a menudo por parte de organizaciones y gobiernos, con un historial mixto de ciberseguridad. Una pregunta que se hace cada vez con mayor frecuencia es qué tan segura es la infraestructura que almacena y procesa todos estos datos.

Como el software de reconocimiento facial aún se encuentra en una etapa relativamente temprana, las leyes que rigen el área están evolucionando y en algunos países, pueden no existir aún. Los ciudadanos comunes cuya información está comprometida tienen pocas vías legales para apelar. A medida que el uso del reconocimiento facial se populariza, aumenta el alcance que los hackers malintencionados tienen para robar los datos faciales con el fin de cometer fraudes.

Es por eso que la información biométrica almacenada de los usuarios debe ser almacenada en un ambiente seguro, minimizando el riesgo de hurto o extracción de dicha información.

Los sistemas de reconocimiento de rostros humanos utilizan patrones matemáticos únicos para almacenar los datos biométricos. Por lo tanto, son uno de los métodos de identificación más seguros y eficaces de la tecnología biométrica. Los datos faciales se pueden anonimizar y mantener en privado para reducir el riesgo de acceso no

autorizado. La tecnología de detección de actividad vital distingue entre usuarios vivos y sus imágenes faciales. Esto evita que el sistema sea engañado con la fotografía de un usuario vivo.

3.2. Técnicas de reconocimiento facial

Hay diferentes tipos de técnicas utilizadas para el reconocimiento facial

3.2.1. Holísticas

Se tienen en cuenta los datos que aporta la cara al completo. Se insertan algunas imágenes en una base de datos para utilizarlas de comparación; las caras propiamente se crean extrayendo los rasgos más característicos y se representan como un vector de pesos; estos vectores son comparados con las imágenes de la base de datos y se determina si la identidad coincide.

3.2.2. Geométricas

Se usa en el reconocimiento facial 2D. Las imágenes se representan mediante una estructura geométrica o codificando sus valores de intensidad. La imagen, localizando los rasgos más distintivos y midiendo algunos parámetros, se transforma en primitivas geométricas (como puntos, líneas y curvas). A partir de aquí se crean unas plantillas con estadísticas que sirven para comparar. En el reconocimiento facial 3D se capta información sobre la forma de la cara y se analiza la coincidencia con los metadatos extraídos. Se busca siempre la mejor coincidencia por encima de un umbral, es decir, se compara con todos los elementos de la base de datos.

3.2.3. Análisis de la textura de la piel

Esta técnica se basa en la apariencia y analizan el espacio. Se puede aplicar a imágenes de baja resolución o mala calidad. Sin embargo, se requiere un conjunto de muestras considerable y los cambios en la iluminación o expresividad influyen considerablemente en el análisis.

3.2.4. Basadas en vídeos

Consiste en identificar a una persona entre varias presentes en una grabación en función de sus datos biométricos faciales. La ventaja es que la imagen no es fija, sino dinámica y capta muy bien los cambios en las expresiones. Permite construir un modelo 3D y analizar también características y cambios temporales. Esta técnica es especialmente útil en la vigilancia.

3.3. Prueba de vida

El mundo virtual es escenario de constantes ataques, fraudes y suplantaciones de identidad. Para que un proceso de verificación de identidad sea seguro y fiable, tiene que completarse con una prueba de vida.

La prueba de vida es una parte del proceso de verificación de identidad que asegura que la persona que realiza el proceso no está cometiendo algún tipo de fraude de identidad. Es decir, verifica que se trata de una persona real y no un intento de fraude como fotos, máscaras 3D o técnicas de deepfake. Esto se logra mediante algoritmos que analizan los

datos recopilados de los sensores biométricos, para determinar si la fuente es real o reproducida.

Existen dos categorías principales de detección de prueba de vida:

Activa: Las soluciones de prueba de vida activa buscan principalmente signos de vida. Solicitan al usuario que realice una acción que no se puede replicar fácilmente con una suplantación. También pueden incorporar varias modalidades, como el análisis de pulsaciones de teclado o el reconocimiento de voz o movimientos corporales. Este último puede analizar el movimiento de la boca para determinar qué se trata de una persona viva. Dado que el usuario debe mostrar signos de vida, estos métodos a menudo presentan problemas de usabilidad, son menos precisos y requieren interacción del usuario.

Pasiva: Los algoritmos de prueba de vida pasiva buscan principalmente signos de suplantación, pero también pueden identificar pasivamente signos de vida. En ambos casos, no dependen de la participación activa del usuario. Pueden ser más poderosos debido a que pueden emplear varios algoritmos de manera no intrusiva para los usuarios, proporcionando sistemas altamente utilizables que también pueden adaptarse con el tiempo a los entornos de clientes.

3.3.1. Importancia de la Detección de Prueba de Vida

La detección de prueba de vida es crucial por las siguientes razones clave:

Prevención del Fraude:
Sin detección de prueba de vida, un atacante podría engañar fácilmente un sistema biométrico utilizando una fotografía de alta calidad o un video del rostro, huella dactilar u otras características biométricas del usuario autorizado. La detección de prueba de vida ayuda a prevenir tales intentos fraudulentos.

Seguridad Reforzada:
Al agregar una capa adicional de seguridad, la detección de prueba de vida fortalece el entorno general de seguridad de los sistemas biométricos, haciéndolos más confiables para aplicaciones como la banca móvil, el control de acceso y la autenticación segura.

Protección de la Privacidad:
La detección de prueba de vida garantiza que solo se capturen los datos biométricos genuinos necesarios para la identificación, reduciendo el riesgo de violaciones de la privacidad mediante el uso de materiales o imágenes no autorizadas.

3.3.2. Funcionamiento de la Detección de Prueba de Vida

La detección de prueba de vida emplea varias técnicas y tecnologías para determinar si los datos biométricos presentados provienen de un ser humano vivo o de una fuente fraudulenta. Aquí hay algunos métodos comunes utilizados en la detección de prueba

de vida:

Análisis de Movimiento:
Este método depende del seguimiento y análisis del movimiento del sujeto. Por ejemplo, al utilizar el reconocimiento facial, el sistema puede instruir al usuario a parpadear, sonreír o mover la cabeza. Los usuarios genuinos responderán con movimientos naturales e involuntarios que pueden detectarse, mientras que las imágenes estáticas o los videos no pueden replicar estos movimientos.

Detección de Profundidad 3D:
Actualmente, hay muy pocos teléfonos móviles habilitados para la detección de profundidad 3D en el mercado, todos con una resolución bastante baja. Sin embargo, esto probablemente cambie en el futuro. La mayoría de los fabricantes que afirman tener detección de 3D en soluciones móviles en realidad utilizan distorsión de perspectiva u otros métodos para inferir la estructura 3D. Los algoritmos no tienen una comprensión real de la estructura 3D y requieren interacción del usuario. No obstante, el avance del hardware 3D permitirá aplicaciones de prueba de vida y correspondencia más sofisticadas a medida que la tecnología evoluciona.

Análisis de Textura:
El análisis de textura implica examinar los detalles finos y texturas de la piel o la huella dactilar del sujeto. La piel genuina exhibirá características únicas y patrones de transpiración difíciles de replicar con una foto o material sintético.

Pruebas de Desafío-Respuesta:
La detección de prueba de vida también puede involucrar pruebas de desafío-respuesta, en las cuales el sistema le pide al usuario que realice acciones específicas, como girar la cabeza o decir una frase aleatoria. El sistema luego analiza las respuestas para determinar la presencia de vida.

Aprendizaje Automático con IA:
Potentes enfoques de aprendizaje automático utilizando técnicas avanzadas de IA han permitido algoritmos sofisticados, capaces de detectar transformaciones sutiles en la imagen que provienen de ataques de presentación. Esto incluye inferir la estructura 3D y detectar diferencias texturales sutiles en suplantaciones invisibles al ojo humano.

3.4. Estado del arte de tecnologías de Face Recognition

La tecnología de reconocimiento facial recopila un conjunto de datos biométricos, como las características y proporciones del rostro o las expresiones faciales, únicos de cada persona, por lo que se puede llevar a cabo una identificación o autenticación de la persona bastante precisa. Al igual que las huellas dactilares, la forma de nuestra cara, los gestos y expresiones en ella y nuestros rasgos fisiológicos nos hacen únicos.

Hoy en día existen muchas bibliotecas y herramientas sólidas tanto de código abierto

como comercial, que facilitan la integración de capacidades de reconocimiento facial en tiempo real en aplicaciones móviles y Web.

A continuación se especifican los rasgos principales de algunas soluciones disponibles en el mercado.

3.4.1. Librerías con licenciamiento de código abierto

3.4.1.1. OpenCV

Es probablemente la librería de *computer vision* de código abierto más popular que existe. Utilizado por empresas como Google, Yahoo y Microsoft, OpenCV contiene algoritmos altamente optimizados para el procesamiento de imágenes y vídeos.

Utilizando los detectores y reconocedores faciales de OpenCV, la identificación y verificación facial en tiempo real se pueden incorporar a proyectos con bastante facilidad. Las capacidades en tiempo real hacen que OpenCV sea excelente para sistemas de control de acceso, monitoreo de transmisiones de CCTV y cualquier aplicación que requiera reconocimiento facial instantáneo.

El último lanzamiento registrado en su repositorio es del 2023-12-28:
https://opencv.org/
https://pypi.org/project/opencv-python/

3.4.1.2. DLib

DLib es un potente conjunto de herramientas C++ de código abierto que contiene algoritmos de aprendizaje automático para resolver problemas del mundo real. Entre sus muchas características, DLib contiene herramientas para construir sistemas de reconocimiento facial en tiempo real. Esto incluye detectores de puntos de referencia faciales para encontrar partes de la cara.

Los modelos DLib se utilizan a menudo para crear aplicaciones Python utilizando los enlaces DLib Python. Para casos de uso en tiempo real, las implementaciones de C++ de alto rendimiento disponibles en DLib son ideales. Las capacidades de análisis facial en tiempo real han hecho que el kit de herramientas sea popular para aplicaciones de control de acceso, autenticación de usuarios y videovigilancia.

El último lanzamiento registrado en su repositorio es del 2022-05-08:
http://dlib.net/
https://pypi.org/project/dlib/

3.4.1.3. Face Recognition

Face Recognition es una librería de reconocimiento facial simple para Python construida sobre DLib y OpenCV. El objetivo de la librería es proporcionar una API fácil de usar para tareas de reconocimiento facial. Las características clave incluyen detección, alineación e identificación de rostros impulsadas por algoritmos que utilizan la técnica de Deep Learning.

Como sugiere el nombre, el reconocimiento facial facilita la integración de identificación facial en tiempo real en aplicaciones Python. Oculta las complejidades de llamar a DLib y OpenCV y proporciona una API limpia. La sencilla interfaz ha hecho que la biblioteca sea popular para implementar sistemas de control de acceso y otros proyectos de reconocimiento facial.

La última actualización registrada en el repositorio de código abierto GitHub es del 2018-04-02:
https://github.com/ageitgey/face_recognition
https://pypi.org/project/face-recognition/

3.4.1.4. FaceNet

Desarrollado por investigadores de Google, FaceNet utiliza Tensorflow (una aplicación desarrollada por Google para aprendizaje de máquina) para aprender incrustaciones de rostros. Las incrustaciones se pueden comparar utilizando una métrica de distancia para verificar la similitud de las caras. Para casos de uso en tiempo real, los modelos de FaceNet se han optimizado para ejecutarse en dispositivos periféricos, teléfonos móviles y navegadores.

La última actualización registrada en el repositorio de código abierto GitHub es del 2018-04-10:
https://github.com/davidsandberg/facenet

3.4.1.5. LUNA SDK

LUNA SDK de VisionLabs proporciona a los desarrolladores un conjunto completo de API y herramientas para crear sistemas de reconocimiento facial de un extremo a otro. Permite la detección de rostros en tiempo real, el seguimiento, la detección de puntos de referencia, la codificación de rostros, la identificación, la verificación y más.

Las bibliotecas C++ optimizadas ofrecen el rendimiento necesario para las tareas de análisis facial. El SDK se puede utilizar para agregar capacidades de reconocimiento facial a la infraestructura de vigilancia, sistemas de control de acceso y cualquier aplicación que requiera la identificación de rostros.

La última actualización registrada en el repositorio de código abierto GitHub es del 2021-04-12:
https://github.com/VisionLabs/FaceEngine/commits/master/setup.py
https://visionlabs.ai/solutions/luna-sdk/

3.4.2. Aplicaciones comerciales

3.4.2.1. Kairos

Kairos proporciona potentes API de reconocimiento facial que se pueden utilizar para integrar capacidades de reconocimiento facial en aplicaciones. Su API de reconocimiento facial permite la comparación de rostros 1:1 para verificación y la

comparación 1:N para identificar rostros desconocidos.

La API ofrece alta precisión y rápida velocidad de coincidencia para satisfacer las demandas de los casos de uso en tiempo real. Kairos también proporciona SDK para varios lenguajes de programación que permiten la integración en aplicaciones iOS, Android, web y IoT. Hay disponible un plan inicial gratuito para probar la API, lo que hace que Kairos sea excelente para la creación de prototipos y pruebas de conceptos.

Enlace al sitio oficial:
https://face.kairos.com/

3.4.2.2. Amazon Rekognition

Amazon Rekognition es un servicio de *computer vision* que forma parte de Amazon Web Services (AWS). Proporciona capacidades de reconocimiento facial y análisis facial en tiempo real altamente escalables a través de simples llamadas API.

Rekognition ofrece reconocimiento facial de baja latencia y análisis de transmisiones de video. Puede detectar, rastrear y analizar rostros y buscar instantáneamente en una colección de rostros para identificar personas de interés. Esto lo hace adecuado para aplicaciones de seguridad, vigilancia y control de acceso.

Enlace al sitio oficial:
https://aws.amazon.com/es/rekognition/

3.4.2.3. Microsoft Azure Face API

Microsoft Azure Face API es parte de Microsoft's Cognitive Services. Proporciona algoritmos avanzados de detección, identificación, verificación y análisis facial. Para escenarios en tiempo real, ofrece API de baja latencia con alta capacidad de rendimiento.

Funciones clave como la coincidencia cara a cara, la identificación de personas y la detección de vida hacen que la API sea ideal para implementar soluciones de vigilancia y control de acceso en tiempo real. También proporciona capacidades de agrupación de rostros para rastrear individuos a través de múltiples transmisiones de cámaras.

Enlace al sitio oficial:
https://azure.microsoft.com/es-es/products/ai-services/ai-vision/

3.4.2.4. DOT Innovatics

El kit de herramientas de incorporación digital (DOT) de Innovatrics es una oferta tecnológica completa para el desarrollo de aplicaciones de verificación de la identidad remota. Los componentes del DOT incluyen biometría facial de primer nivel, verificación del documento de identidad y detección de vida acreditada. Cada componente se desarrolla a nivel interno y está bien documentado para que la integración sea fácil.

El kit de herramientas de incorporación digital permite almacenar y gestionar datos biométricos de los clientes para la autenticación y prevención del fraude de identidad.

Enlace al sitio oficial:
https://www.innovatrics.com/es/dot-kit-de-herramientas-de-onboarding-digital/

3.4.2.5. VU Security

VU Security provee soluciones de Seguridad de la Información contra varios ataques de seguridad dirigidos a individuos, empresas y organismos gubernamentales. VU Security tiene como misión mantener la confidencialidad, integridad y disponibilidad antes, durante y luego de realizar una transacción de validación de credenciales.

La solución Onboarding Management se encarga de validar la identidad de las personas para prevenir la suplantación de la identidad. El módulo Face® constituye la primera plataforma de implementación masiva de autenticación facial. El reconocimiento de los individuos se realiza mediante el análisis de los rostros de las personas valiéndose de puntos de referencia y la distancia entre estos puntos. A su vez, se utiliza el registro de movimientos y acciones, como un guiño o una sonrisa, para evitar la suplantación de la identidad. Es multiplataforma y puede integrarse con sistemas de Microsoft y Cisco. Se puede implementar en segundo plano, sin incomodar al usuario.

Enlace al sitio oficial:
https://www.vusecurity.com/es/

3.4.3. Inconvenientes en la detección de rostros

Es posible que algunas caras no se reconozcan debido a la composición de fotos, como:

- Imágenes con iluminación extrema, por ejemplo, fuerte contraluz.
- Obstáculos que bloquean uno o los dos ojos.
- Diferencias en el tipo de pelo o vello facial.
- Cambios en la apariencia facial debido a la edad.
- Expresiones faciales extremas.

Es importante destacar que es mucho más probable que estos inconvenientes afecten en major medida a los procesos de reconocimiento facial de 1 a N, es decir, la búsqueda de coincidencia de una rostro entre una base de datos de conocimiento de cientos, miles o millones de rostros.

3.4.4. Tabla comparativa entre soluciones analizadas

Producto	Integración	Fortalezas	Prueba de Vida	Última Actualización y Precio
OpenCV	Librería	Tiene más de 2500 algoritmos optimizados. Entre los cuales se incluyen algoritmos de face recognition Tiene más de 47 mil personas en la comunidad de usuarios. Hay numerosos ejemplos de utilización de la librería para reconocimiento facial y prueba de vida, incluso en combinación con otras herramientas de Inteligencia Artificial de código abierto como Tensorflow. La biblioteca se utiliza ampliamente en empresas, grupos de investigación y organismos gubernamentales. Dispone de interfaces para C++, Python, Java y MATLAB. Compatible con Windows, Linux, Android y Mac OS	Debe ser programada analizando las características faciales detectadas por la librería, rastreando las distancias relativas entre estas características. Por ejemplo, utilización algoritmos basados en heurísticas, que incluyen el movimiento de los ojos, el movimiento de los labios y la detección de parpadeo. Este conjunto de algoritmos intenta rastrear el movimiento de los ojos y los parpadeos para garantizar que el usuario no esté sosteniendo una foto de otra persona (ya que una foto no parpadeará ni moverá los labios). El sistema debe ser previamente entrenado, para ello se debe proveer ejemplos de rostros reales, y rostros falsos.	2023-12-28 Producto Open Source sin costo de licencia de uso

DLib	Librería	Proporciona documentación completa y precisa para cada clase y función Se proporcionan muchos programas de ejemplo. La librería es probada periódicamente en sistemas MS Windows, Linux y Mac OS X. No se requieren instalar otros paquetes para usar la librería. Incluye una amplia gama de algoritmos para aprendizaje automático y manejo de imágenes.	Debe ser programada analizando las características faciales detectadas por la librería, rastreando las distancias relativas entre estas características. Por ejemplo, utilización algoritmos basados en heurísticas, que incluyen el movimiento de los ojos, el movimiento de los labios y la detección de parpadeo. Este conjunto de algoritmos intenta rastrear el movimiento de los ojos y los parpadeos para garantizar que el usuario no esté sosteniendo una foto de otra persona (ya que una foto no parpadeará ni moverá los labios). El sistema debe ser previamente entrenado, para ello se debe proveer ejemplos de rostros reales, y rostros falsos.	2022-05-08 Producto Open Source sin costo de licencia de uso
Face Recognition	Librería	Reconoce y manipula caras desde Python o desde la línea de comandos Utiliza el reconocimiento facial de última generación de DLib creado con Deep Learning. El modelo tiene una precisión del 99,38%	Debe ser programada analizando las características faciales detectadas por la librería, rastreando las distancias relativas entre estas características. Por ejemplo, utilización algoritmos basados en heurísticas, que incluyen el movimiento de los ojos, el movimiento de	2018-04-02 Producto Open Source sin costo de licencia de uso

		en Labeled Faces in the Wild. [2] (un punto de referencia público para la verificación facial) También proporciona una herramienta simple de línea de comando face_recognition que le permite realizar reconocimiento facial en una carpeta de imágenes desde la línea de comando	los labios y la detección de parpadeo. Este conjunto de algoritmos intenta rastrear el movimiento de los ojos y los parpadeos para garantizar que el usuario no esté sosteniendo una foto de otra persona (ya que una foto no parpadeará ni moverá los labios). El sistema debe ser previamente entrenado, para ello se debe proveer ejemplos de rostros reales, y rostros falsos.	
FaceNet	Librería	Es un sistema basado en redes neuronales que utiliza algoritmos de Deep Learning para reconocer rostros. El sistema FaceNet logró una precisión del 99,63% en Labeled Faces in the Wild. [2] (un punto de referencia público para la verificación facial)	Debe ser programada analizando las características faciales detectadas por la librería, rastreando las distancias relativas entre estas características. Por ejemplo, utilización algoritmos basados en heurísticas, que incluyen el movimiento de los ojos, el movimiento de los labios y la detección de parpadeo. Este conjunto de algoritmos intenta rastrear el movimiento de los ojos y los parpadeos para garantizar que el usuario no esté sosteniendo una foto de otra persona (ya que una foto no parpadeará ni moverá los labios).	2018-04-10 Producto Open Source sin costo de licencia de uso

			El sistema debe ser previamente entrenado, para ello se debe proveer ejemplos de rostros reales, y rostros falsos.	
LUNA SDK	Librería	Contiene varias implementaciones y fábricas de detectores de rostros para crear una puntuación de detección precisa. Su motor de prueba de vida determina si un rostro detectado es una imagen fija o está en una secuencia de imágenes, es decir, una transmisión de video de una cámara o un archivo de video. Extrae y combina un amplio conjunto de características que describen el rostro (incluido el tamaño, el ángulo y otras medidas) para determinar si dos imágenes de rostro pertenecen a la misma persona.	Debe ser programada analizando las características faciales detectadas por la librería, rastreando las distancias relativas entre estas características. Por ejemplo, utilización algoritmos basados en heurísticas, que incluyen el movimiento de los ojos, el movimiento de los labios y la detección de parpadeo. Este conjunto de algoritmos intenta rastrear el movimiento de los ojos y los parpadeos para garantizar que el usuario no esté sosteniendo una foto de otra persona (ya que una foto no parpadeará ni moverá los labios). El sistema debe ser previamente entrenado, para ello se debe proveer ejemplos de rostros reales, y rostros falsos.	2021-04-12 Producto Open Source sin costo de licencia de uso
Kairos	Nube On-Premise	Facilidad de integración con la API Precisión considerable Alto nivel de seguridad	Incluida	On-Premise 20.000 USD anuales, uso ilimitado

Amazon Rekognition Face Liveness	Nube	Reconocimiento facial en tiempo real Precisión Máxima en el mercado a la fecha Escalable	Incluida	Primeras 500 mil comprobaciones 0,0150 USD por comprobación Siguientes 2,5 millones de comprobaciones 0,0125 USD por comprobación Más de 3 millones de comprobaciones 0,0100 USD por comprobación
Microsoft Azure Face API	Nube	Fácil integración con otros productos de Microsoft Precisión considerable Alto nivel de seguridad Existen recomendaciones de Microsoft para mitigar problemas de rendimiento, en especial en la transmisión de la fotografía al servicio alojado en la nube de Azure [1]	NO Incluida, existe una solución pero está en Beta y aún no está siendo comercializada	**Gratis - Web** 30.000 transacciones gratis por mes **Estándar - Web** 0-1M transacciones - $1 por 1000 transacciones 1-10M transacciones - $0,65 por 1000 transacciones 10-100M transacciones - $0,60 por 1000 transacciones 100M+ transacciones - $0,40 por 1000 transacciones
DOT Innovatrics	Nube On-Premise	Facilidad de integración con la API Precisión considerable Alto nivel de seguridad	Incluida	Se solicitó presupuesto al proveedor, sin respuesta a la fecha.
VU Security	Nube	Facilidad de	Incluida	On-Premise

	On-Premise	integración con la API Precisión considerable Alto nivel de seguridad		Presupuesto aproximado, no incluye instalación: $1.5 por registro de usuario $0.50 anual por usuario

3.5. Experiencias de la región

3.5.1. Argentina

SID - Sistema de Identidad Digital

El Sistema de Identidad Digital es la primera herramienta tecnológica desarrollada por el Estado Argentino que, mediante la validación de la identidad por rostro, le permitirá al ciudadano acceder a servicios públicos y privados sin necesidad de trasladarse a una oficina

Es una validación remota de identidad en tiempo real con el Renaper mediante factores de autenticación biométrica (reconocimiento facial) y fotografía del DNI. Es producto de un trabajo conjunto entre el Ministerio del Interior y la Secretaría de Innovación Pública con el objetivo de poner la tecnología e innovación al alcance de todos los ciudadanos argentinos para que tengan la posibilidad de acceder a servicios o realizar trámites desde cualquier dispositivo electrónico con conectividad móvil.

3.5.1.1. Seguridad

La solución cuenta con características que garantizan su nivel de seguridad preservando los datos suministrados por el ciudadano. La preponderancia de la seguridad y de la privacidad del ciudadano al momento de transaccionar con la plataforma, sumado a políticas de privacidad, son pilares sólidos para la validación segura y confiable.

El reconocimiento facial posee controles de detección de vivacidad para corroborar que el rostro capturado corresponde al de una persona viva y anti-spoofing (suplantación de identidad) para evitar que un posible impostor engañe al sistema.

Los valores biométricos de los ciudadanos no salen del entorno seguro del RENAPER ni son almacenados en el dispositivo.

Una característica adicional de la solución es que cuenta con Timestamping para poder validar las diferentes instancias de la transacción.

La seguridad de la solución SID está basada en las siguientes características:

- La solución cuenta con un Firewall a nivel aplicación (firewall capa 7).

- La información almacenada en base de datos, se encuentra cifrada por el algoritmo AES256.
- Para la validación de legitimidad de los consumidores desde la API, se utilizan API Keys. Las mismas podrán gestionarse desde el portal de autogestión.
- Todas las comunicaciones a nivel red se hacen por canales HTTPS TLS 1.2
- La conectividad entre Azure y Renaper está asegurada por un túnel VPN del tipo Ipsec.

3.5.1.2. Proceso de Validación del SID

El proceso de verificación es aquel mediante el cual se verifica que la imagen del rostro del ciudadano coincide en rasgos con las tomadas al momento de la generación del DNI.

Utilizando la aplicación móvil de RENAPER o implementando el SDK provisto en una aplicación móvil se podrán llevar adelante los siguientes pasos para completar el proceso de verificación:

Identificación con documento de identidad, vigencia del mismo y biometría facial
Para completar el proceso de identificación digital, el ciudadano debe realizar los siguientes pasos luego de abrir la aplicación móvil mediante la cual va a llevar adelante el proceso de verificación de su identidad digital.

- Tomar una fotografía del frente de su documento de identidad
- Tomar una fotografía del dorso de su documento de identidad
- Obtener una fotografía del tipo SELFIE con prueba de vida, donde se le pedirá que efectúe dos gestos de forma aleatoria.
- El SDK evalúa las fotografías de frente y dorso del documento, para establecer un porcentaje de veracidad del plástico del documento de identidad, realiza la consulta al servicio de biometría facial de Renaper.
- Entrega el resultado de validación positivo o negativo.

Identificación con biometría facial sin tarjeta DNI

- El ciudadano ingresa de forma manual el número de su documento y género en la aplicación móvil.
- El ciudadano se toma una fotografía del tipo SELFIE con prueba de vida, donde se le pedirá que efectúe dos gestos aleatorios.
- El SDK utiliza el número de documento y género obtenidos, y la fotografía con gesto neutral capturada, y envía la información al sistema biométrico de RENAPER para obtener el porcentaje de validación exitoso o no.

Identificación mediante vigencia del documento con tarjeta DNI

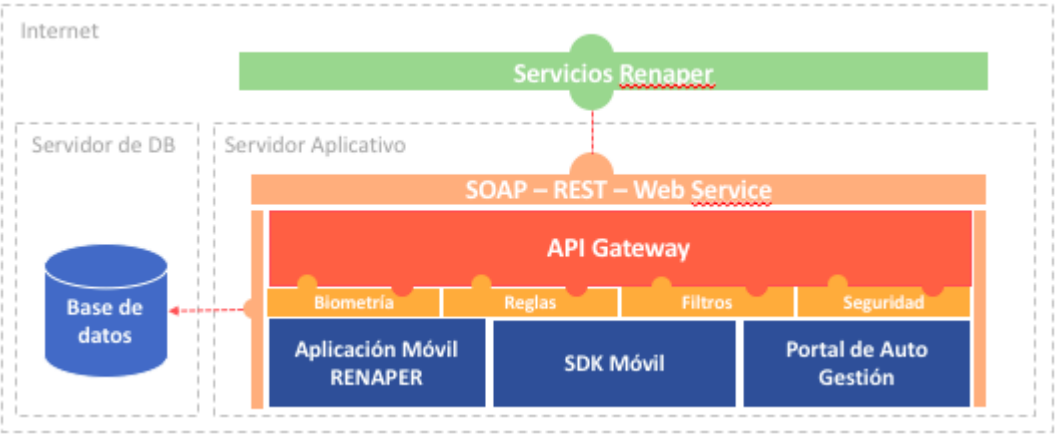
- El ciudadano ingresa de forma manual el número de su documento, género y

número de trámite que figura en su DNI.

- El SDK utiliza el número de documento, género y número de trámite obtenidos, y envía la información al sistema de datos de RENAPER para obtener la vigencia del documento de identidad.

3.5.1.3. Tecnologías soportadas por el SID

El sistema de integración provisto por Identidad Digital basada en reconocimiento facial, es a través de servicios web REST, por lo tanto, cualquier tecnología que permita consumir dichos servicios podrá ser utilizada, se ilustra a continuación un diagrama de despliegue resumido de la arquitectura de RENAPER:



Fuente: https://www.argentina.gob.ar/interior/renaper/sid-sistema-de-identidad-digital

3.5.2. Brasil

Biovalid

Es una solución digital desarrollada por el Servicio Federal de Procesamiento de Datos (Serpro), permite el uso de biometría facial a través del teléfono celular para validar la identidad, como alternativa al uso de un certificado digital.

Biovalid está disponible en una aplicación para dispositivos móviles iOS y Android y es parte de las acciones del Gobierno Federal del Brasil para impulsar la transformación digital del país. Al brindar soluciones como Biovalid, el Estado Federal refuerza su compromiso de ser el motor de la transformación digital en el país buscando cada vez más reducir la burocracia y modernizar los servicios públicos y privados a través de la inteligencia digital. Esta tecnología trae grandes avances para el Brasil al garantizar reducción de costos y tiempos en las gestiones tanto públicas como privadas.

Utiliza tecnología **pasiva de prueba de vida** que no requiere que el usuario realice movimientos para la validación. Todo lo que tiene que hacer es ponerse frente a la cámara y listo, la captura de vivacidad está hecha. La tecnología pasiva aporta mejor rendimiento, mejor usabilidad y mejor experiencia de usuario. También es posible realizar la validación

facial mediante una fotografía de referencia enviada por el cliente.

3.5.2.1. Beneficios y características

- *Token biométrico de seguridad:* firmado con certificado y sello de tiempo.
- *Movilidad:* Usuarios validados de forma segura independientemente de su ubicación.
- *Flexibilidad de acceso:* Uso de la aplicación BioValid (menor costo de desarrollo) o aplicación de empresa mediante acceso a la API (mayor flexibilidad).
- *Garantía y confiabilidad:* La base biométrica es la base oficial del gobierno, sin intermediarios, minimizando los riesgos de fraude.

3.5.2.2. Costo

Utilización gratuita hasta por 30 días o hasta llegar a 3000 consultas. Dentro de este plazo o límite de consultas se podrá cancelar el contrato sin coste alguno, en caso de superarlo se cobrará el servicio según la siguiente tabla de precios.

Consulta	Precio (US$)
Rango 1 - 1 a 149	3,69 / solicitud
Rango 2: 150 a 9999	3.19 / solicitud
Rango 3: 10 000 a 49 999	2,39 / solicitud
Rango 4: 50 000 a 99 999	1,67 / solicitud
Rango 5 - desde 100.000	1,42 / solicitud

Para fines de facturación se cuentan todas las solicitudes que devolvieron el código 200. El código 200 se devuelve cuando el usuario pasó la prueba de vida y fue posible realizar la validación facial en la base de datos (se devolvió la puntuación de similitud facial).

El retorno de las validaciones biométricas se define por rango y porcentaje. Según el porcentaje de similitud se identifica el rango de probabilidad. Los rangos se aplican tanto a la validación facial como a la digital.

Probabilidad	Porcentaje
Probabilidad muy alta	100% - 93%
Probabilidad alta	92,99% - 85%
Baja probabilidad	84,99% - 32%
Probabilidad muy baja	31,99% - 0%

4. *ARQUITECTURAS TECNOLÓGICAS QUE SE AJUSTEN A LA NECESIDAD IDENTIFICADA, TENDIENTE A DAR RESPUESTA A SISTEMAS DE SERVICIOS LOCALES, EN LA NUBE Y APLICACIONES MÓVILES, QUE INCLUYA LAS RECOMENDACIONES DE STACK TECNOLÓGICO*

El Core de Servicios en la Nube para el estado (FaceRecognitionCore) debe estar disponible para el acceso de forma simple, ágil y segura. Debe ser independiente del lenguaje en el que estén programados las aplicaciones clientes que desean invocar sus servicios.

Las APIS REST son una solución sencilla para la manipulación de datos de forma segura. De esta forma se separa totalmente la interfaz de usuario del servidor y el almacenamiento de datos. Esto resulta en una mejora en la portabilidad de la interfaz a otro tipo de plataformas, aumenta la escalabilidad de los proyectos y permite que los distintos componentes de los desarrollos se puedan evolucionar de forma independiente.

La separación entre cliente y servidor tiene una ventaja y es que cualquier equipo de desarrollo puede escalar el producto sin excesivos problemas. Se puede migrar a otros servidores o realizar todo tipo de cambios en la base de datos, siempre y cuando los datos de cada una de las peticiones se envíen de forma correcta. Esta separación facilita tener en servidores distintos el front y el back y eso convierte a las aplicaciones en productos más flexibles a la hora de trabajar.

La API REST siempre se adapta al tipo de sintaxis o plataformas con las que se esté trabajando, lo que ofrece una gran libertad a la hora de cambiar o probar nuevos entornos dentro del desarrollo. Lo único que es indispensable es que las respuestas a las peticiones se hagan siempre en el lenguaje de intercambio de información usado

Para FaceRecognitionCore la sugerencia es utilizar una API REST con intercambio de información en formato JSON.

4.1. Propuesta de API REST

- **Inscripción/Enroll**

  Para inscribir a alguien, todo lo que se necesita hacer es enviar una foto JPG o PNG. Se puede enviar la foto como una URL de acceso público o como una foto codificada en Base64.

  Se debe enviar también un identificador (subject_id) para la persona que se va a inscribir. El identificador podría ser cualquier cosa significativa para identificar de manera única a la persona.

  Se pueden inscribir varias imágenes de la misma persona (también conocida como subject_id) para mejorar la precisión de las coincidencias. La cantidad óptima de imágenes registradas por persona dependería de los algoritmos de reconocimiento facial que sean implementados, pero el reconocimiento debería funcionar bien con solo 1.

Parámetros requeridos
image = URL de acceso público o foto codificada en Base64.
subject_id = Se utiliza como identificador del rostro.

Http Headers
content-yype = application/json
liveness=true (opcional si se desea realizar prueba de vida)

Parámetros retornados
face_id = identificador del rostro registrado

- **Verificación**

Para verificar una cara que haya sido registrada previamente, todo lo que se necesita hacer es enviar una foto JPG o PNG. Se puede enviar la foto como una URL de acceso público o codificada en Base64.

Además se debe enviar el subject_id para verificar que la foto enviada corresponde con la persona registrada previamente.

Siempre que la solicitud pueda realizar una coincidencia, se recibirá un estado de "éxito". Se retorna además el valor de "confianza" para determinar si la comparación es válida para su aplicación. Los valores de confianza superiores al 60% son casi siempre de la misma persona.

Parámetros requeridos
image = URL de acceso público o foto codificada en Base64.
subject_id = Se utiliza como identificador del rostro.

Http Headers
content-type = application/json
liveness=true (opcional si se desea realizar prueba de vida)

Parámetros retornados
status = identificador de éxito de la operación
subject_id = identificador del rostro.
confidence = porcentaje de confianza de la validación (valor decimal entre 1 y 0)

- **Eliminación**

Elimina un rostro (subject_id) de la base de datos

Parámetros requeridos
subject_id = Se utiliza como identificador del rostro.

Http Headers
Content-Type = application/json

Parámetros retornados
status = identificador de éxito de la operación

4.2. Mecanismos de seguridad

- Las invocaciones a la api se realizarán únicamente de forma segura mediante el protocolo HTTPS

- Las invocaciones deben estar autenticadas mediante una API key. Se enviarán los datos de la API key en cada invocación mediante cabeceras HTTP

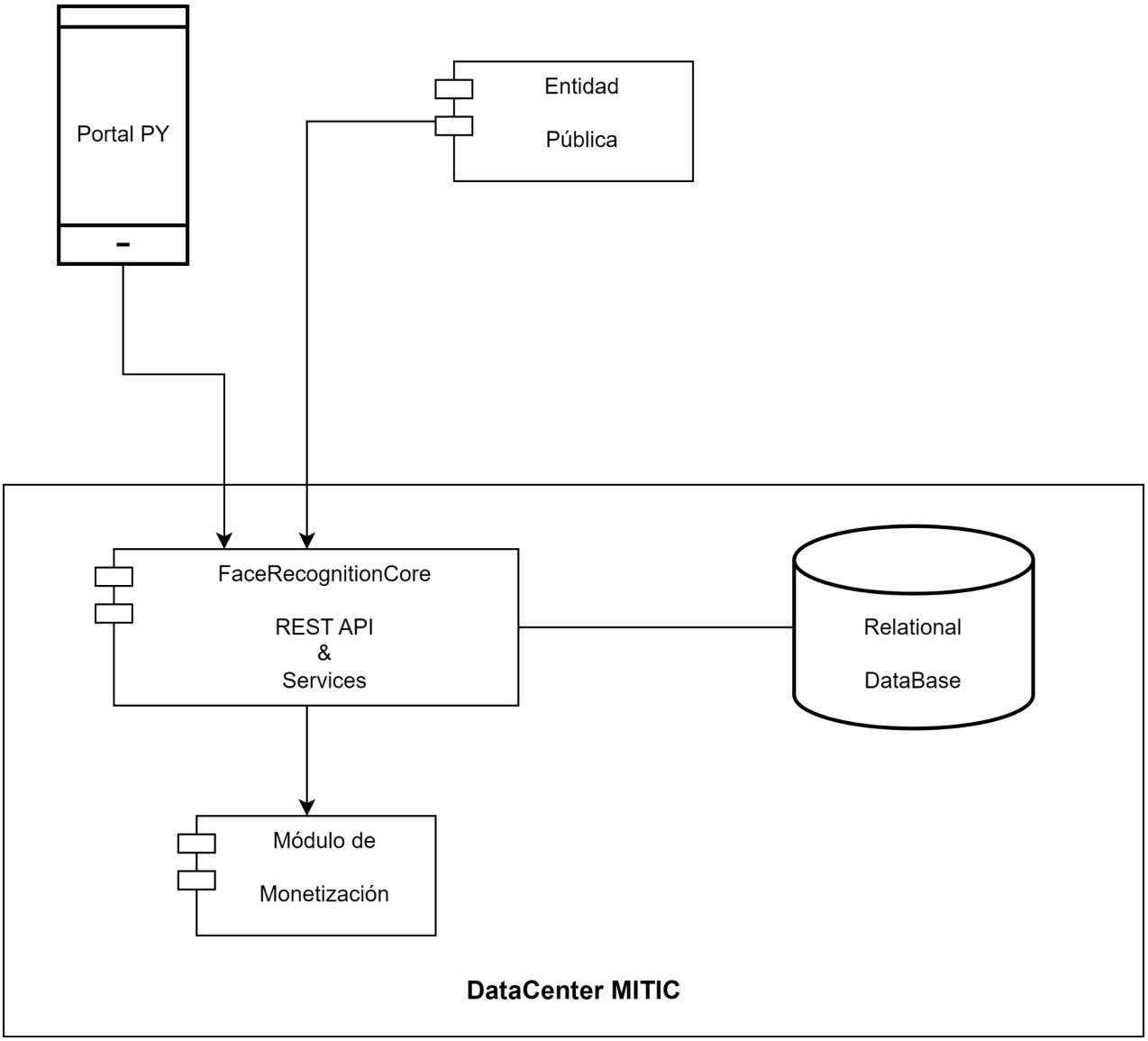
  app_id: "El identificador de la aplicación"
  app_key: "la clave de la aplicación"

- El método de generación de la API key estará condicionada según el método de monetización seleccionado.

4.3. Diagrama de Arquitectura

Se propone que el FaceRecognitionCore esté expuesto al exterior mediante una interfaz REST API, la cual a su vez está conectada con los servicios de reconocimiento facial y prueba de vida internos. Los cuales acceden a una base de datos relacional interna para almacenar la información que sea necesaria para el proceso de enrolamiento y autenticación.

Todo está integrado al módulo de monetización, el cual controlará que la operación de reconocimiento facial esté cubierta financieramente hablando. Los detalles técnicos de este mecanismo de control dependerá en gran medida del tipo de monetización que sea elegido para el proceso de cobro.

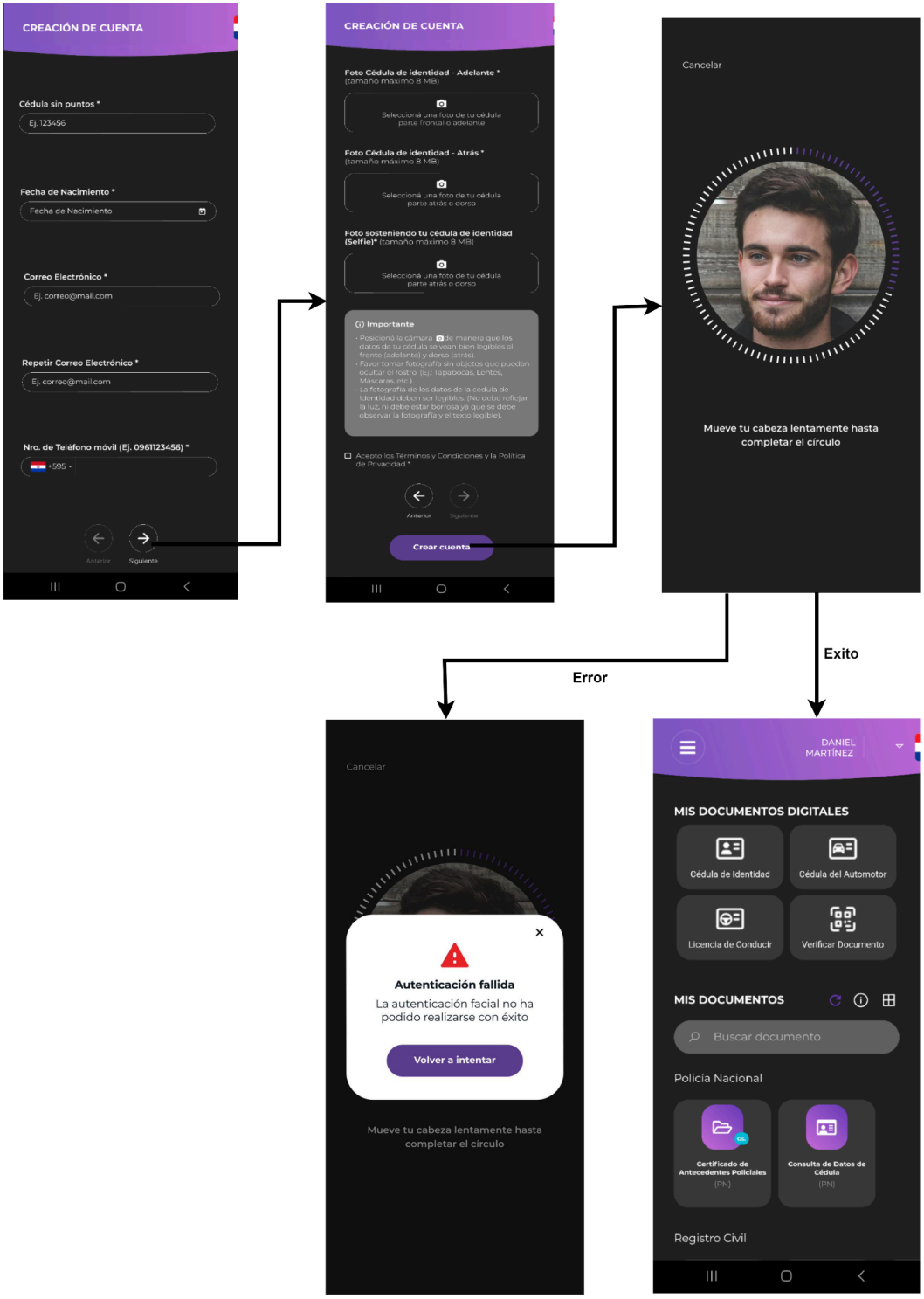


4.4. Flujo de pantallas para la aplicación Portal PY

Los principales flujos que deben ser modificados para incorporar el reconocimiento facial a la aplicación Portal PY son los siguientes: (La pantalla donde se ejemplifica el reconocimiento facial contiene solo una imagen ilustrativa)

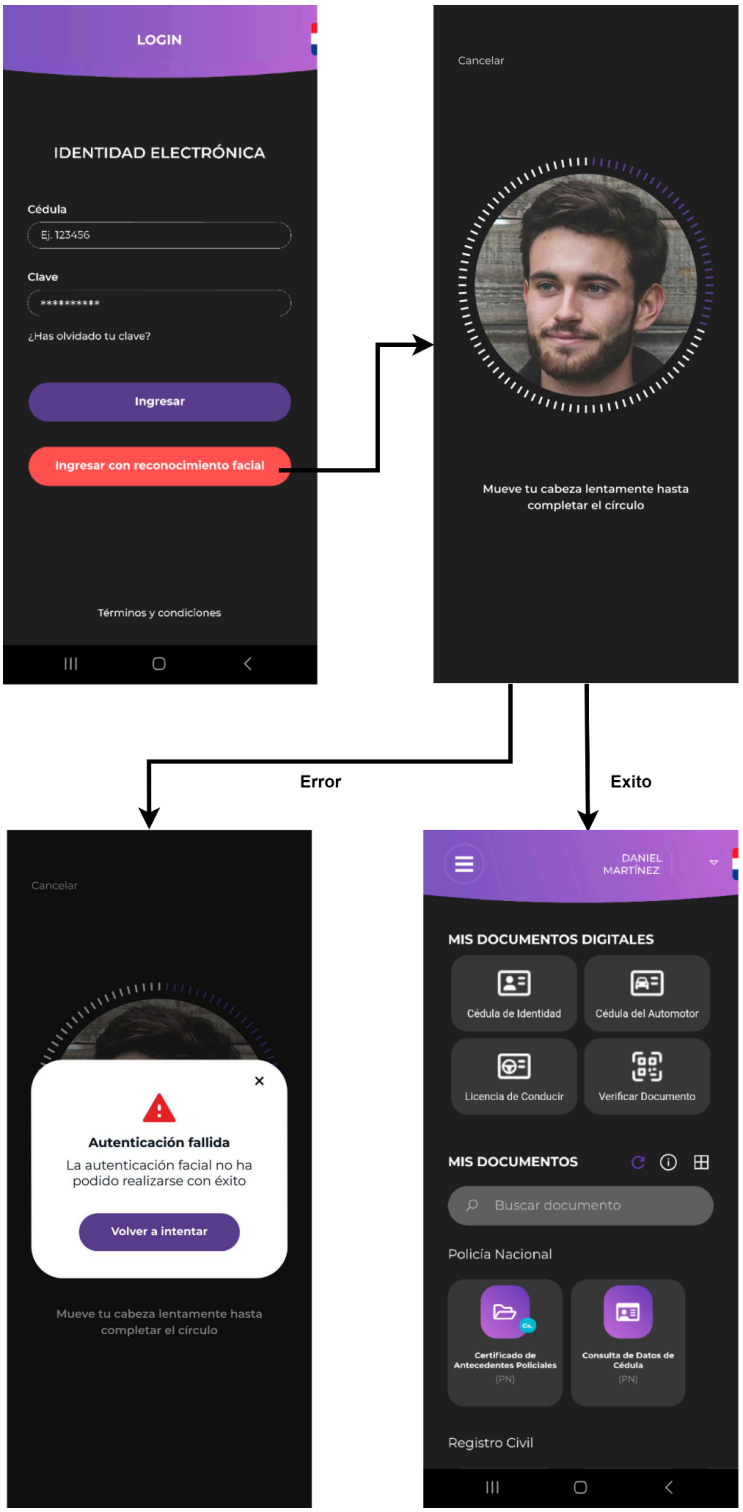
4.4.1. Registro de Usuario

El registro de usuario se realiza ahora por la Web. Para pasar a la aplicación Portal PY se presenta a continuación el flujo propuesto de pantallas:



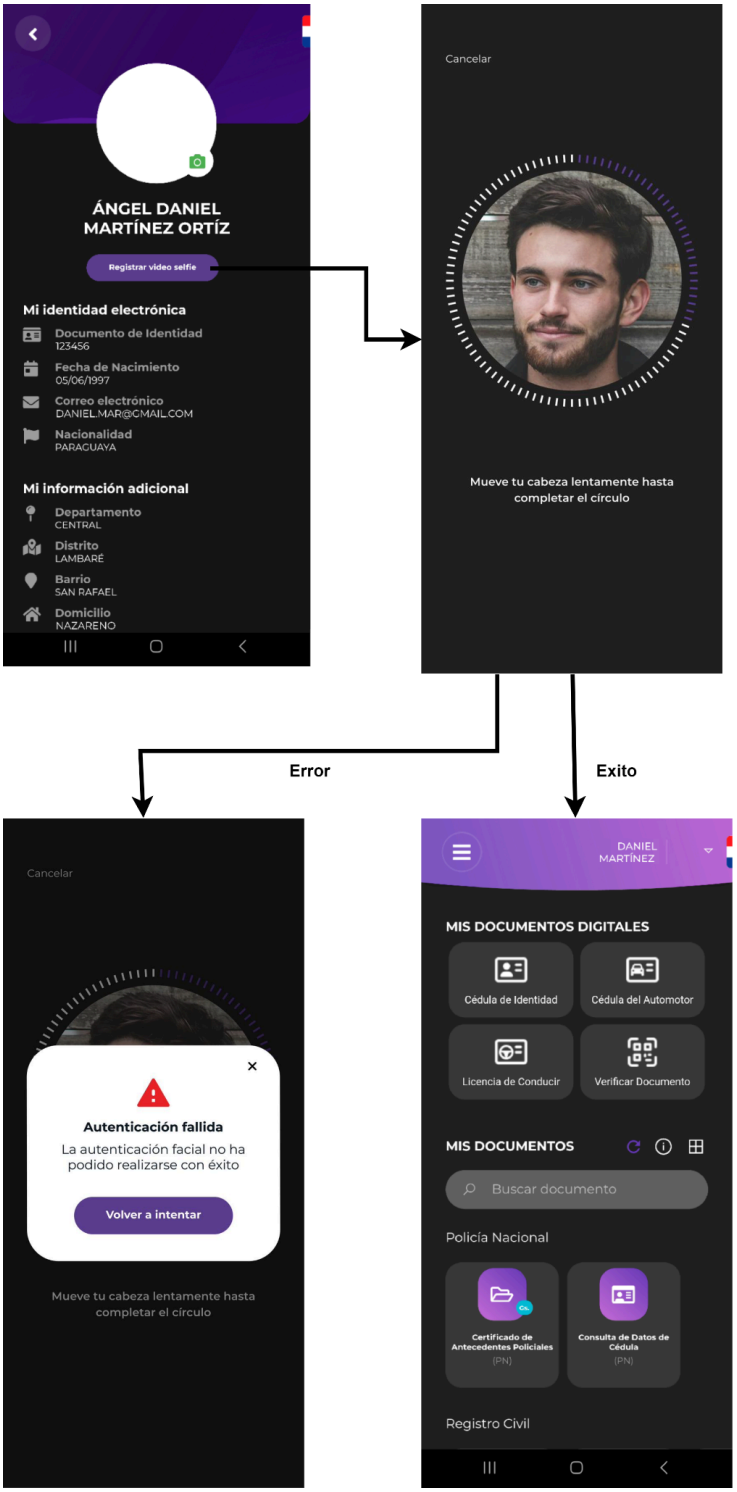
4.4.2. Autenticación

Para la autenticación se agrega un botón adicional para dar la posibilidad de autenticación por reconocimiento facial:



4.4.3. Edición de Perfil

Para los usuarios que ya se encuentran registrados en la aplicación Portal PY, se agrega un botón "Registrar video selfie" en la edición de Perfil para incorporar la funcionalidad de autenticación por reconocimiento facial:



5. *DIFERENTES OPCIONES DE MECANISMOS DE MONETIZACIÓN Y PAGO PARA LOS SERVICIOS QUE PUEDA PROVEER EL MITIC A OTRAS ENTIDADES POR MEDIO DEL FACERECOGNITIONCORE*

En el desarrollo web el término monetización se utiliza para referirse a la capacidad de generar un ingreso a través de un sitio o servicio Web. La monetización puede ser por programas de afiliación, comercio electrónico, poseer contenido premium, por publicidad o por cualquier otra forma de generación de ingresos.

Existen varias opciones a la hora de elegir el mecanismo de monetización para un servicio de reconocimiento facial como FaceRecognitionCore. Se detalla en la tabla a continuación algunos de los métodos de monetización más utilizados por esta clase de servicios. La elección final podría ser una de estas opciones o una combinación de dos o más de ellas.

Nombre	Descripción	Utilidad
Pago por análisis de imagen	Cobra un monto fijo de poco valor cada vez que se analiza una imagen con las API	**Ventajas** El cliente no necesita hacer un desembolso grande para empezar a utilizar el servicio. **Desventajas** Se necesita programar un esquema de débito en cuenta para ir consumiendo un saldo previamente cargado en dicha cuenta. Además de la programación del depósito en cuenta de dicho saldo. O bien, programar un esquema de pago posterior por mes cerrado.
Pago por análisis de prueba de vida	Cobra un monto fijo de poco valor cada vez que se realiza una verificación de prueba de vida	**Ventajas** El cliente no necesita hacer un desembolso grande para empezar a utilizar el servicio. **Desventajas** Se necesita programar un esquema de débito en cuenta para ir consumiendo un saldo previamente cargado en dicha cuenta. Además de la programación del depósito en cuenta de dicho saldo. O bien, programar un esquema de pago posterior por mes cerrado.
Almacenamiento de metadatos de rostros (puede o no	Para habilitar la búsqueda de rostros y usuarios, necesitará	**Ventajas** El cliente no necesita hacer un desembolso grande para empezar a utilizar el servicio.

incluir las fotos o videos)	almacenar un repositorio de objetos de metadatos de rostros (vectores faciales y de usuarios) que FaceRecognitionCore pueda utilizar para buscar coincidencias.	**Desventajas** Se necesita programar un esquema de débito en cuenta para ir consumiendo un saldo previamente cargado en dicha cuenta. Además de la programación del depósito en cuenta de dicho saldo. O bien, programar un esquema de pago posterior por mes cerrado.
Pago fijo anual	Incluye el uso ilimitado del servicio por un pago fijo anual.	**Ventajas** No es necesario implementar un esquema de débito en cuenta o pago por mes cerrado. Si el cliente tiene muchos enrolamientos y/o verificaciones de rostros, el precio no se dispara. **Desventajas** Podría llegar a ser una traba para un cliente que tenga pocos enrolamientos y/o verificaciones totales por año, o para los clientes que quieran ir avanzando en su implementación poco a poco.
Pago fijo por cada registro de rostro	Se cobra un monto fijo de poco valor cada vez que se realiza un enrolamiento de rostro	**Ventajas** El cliente no necesita hacer un desembolso grande para empezar a utilizar el servicio. El cliente no necesita preocuparse por la cantidad de verificaciones faciales que se realicen posterior al enrolamiento. **Desventajas** Si la cantidad de rostros registrados es grande, el precio podría dispararse. Se debe implementar un esquema de cobro cada vez que se realiza en enrolamiento
Pago fijo anual por cada usuario registrado	Se cobra un monto fijo anual por cada usuario registrado.	**Ventajas** No es necesario implementar un esquema de débito en cuenta o pago por mes cerrado. El cliente no necesita preocuparse por la cantidad de verificaciones faciales que realizará anualmente.

		Desventajas Si la cantidad de rostros registrados es grande, el precio podría dispararse.

6. EETT FUNCIONALES DE LAS APPS A SER MODIFICADAS

Lista de requerimientos funcionales para la adecuación de la aplicación móvil PortalParaguay como cliente del FaceRecognitionCore.

6.1. RF1 - Registro de un usuario nuevo

6.1.1. Eliminar el redireccionamiento a la Web para el registro de usuarios

6.1.2. Crear una pantalla de registro de usuario con los siguientes campos:
- Número de cédula de identidad
- Fecha de nacimiento
- Correo electrónico
- Número de teléfono móvil
- Casilla de aceptación de términos y condiciones
- Botón “siguiente”

6.1.3. El avanzar a la siguiente página solicitar que el usuario suba (upload) desde su dispositivo móvil lo siguiente:
- Foto de la parte frontal de su cédula de identidad
- Foto de la parte de atrás de su cédula de identidad
- Una selfie sosteniendo su cédula de identidad
- Botón “iniciar”

6.1.4. Al oprimir el botón “iniciar” se enciende la cámara frontal del dispositivo del usuario y se solicita realizar una determinada acción como prueba de vida.

6.1.5. Realizar la validación de la prueba de vida, contra la selfie y la foto de la parte frontal de la cédula mediante el servicio FaceRecognitionCore.

6.1.6. En caso exitoso, crear el nuevo usuario almacenando en la base de datos toda la información cargada en las pantallas de registro de la aplicación, junto con los datos vectoriales retornados por el reconocimiento facial. Para esto debe invocarse el servicio que debe ser proveído por la API REST que utiliza la aplicación Portal PY.

6.2. RF2 - Registro de rostro para un usuario existente

6.2.1. Modificar la página de perfil del usuario para agregar un botón “Registrar video selfie”.

6.2.2. Al oprimir el botón “Registrar video selfie” se enciende la cámara frontal del dispositivo del usuario y se solicita realizar una determinada acción como prueba de vida.

6.2.3. Realizar la validación de la prueba de vida mediante el servicio FaceRecognitionCore.

6.2.4. En caso exitoso, modificar el registro del usuario para persistir en la base que el usuario ya completó el registro de su rostro. Para esto debe invocarse el servicio que debe ser

proveído por la API REST que utiliza la aplicación Portal PY.

6.3. RF3 - Autenticación por reconocimiento facial

6.3.1. Agregar en la pantalla de inicio de sesión, un botón “Ingresar con reconocimiento facial”.
6.3.2. Al oprimir el botón “Ingresar con reconocimiento facial” se enciende la cámara frontal del dispositivo del usuario y se solicita realizar una determinada acción como prueba de vida.
6.3.3. Realizar la validación de la prueba de vida mediante el servicio FaceRecognitionCore.
6.3.4. En caso de éxito, dar inicio a la sesión del usuario y mostrar la página principal de la aplicación.

7. EETT NO FUNCIONALES DE LAS APPS A SER MODIFICADAS

7.1. RNF1 - Rendimiento

El reconocimiento facial, incluida la prueba de vida, no debería tardar más de cinco segundos en arrojar un resultado positivo o negativo.

7.2. RNF1 - Rendimiento

Para un resultado acertado en el reconocimiento facial se recomienda tomar como coincidencia un porcentaje de confianza superior al 60%.

7.3. RNF3 - Seguridad

Las comunicaciones entre la aplicación y la API REST deben estar siempre encriptadas.

7.4. RNF4 - Intercambio de datos legible

Para el intercambio de datos entre la aplicación de las APIs REST que fueran invocadas, utilizar JSON como estructura de datos compleja.

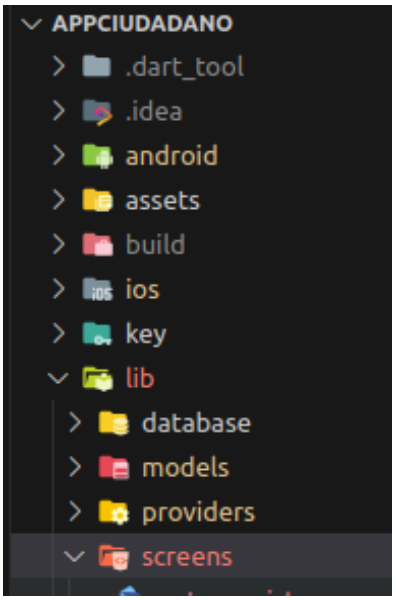
8. MODIFICACIONES NECESARIAS Y ADAPTACIONES REQUERIDAS APLICACIÓN MÓVIL (PORTALPARAGUAY).

Para poder incorporar el módulo de reconocimiento facial con prueba de vida a la aplicación Portal PY, serán necesarias las siguientes modificaciones dentro del código fuente de la misma.

8.1. REGISTRO DE USUARIO

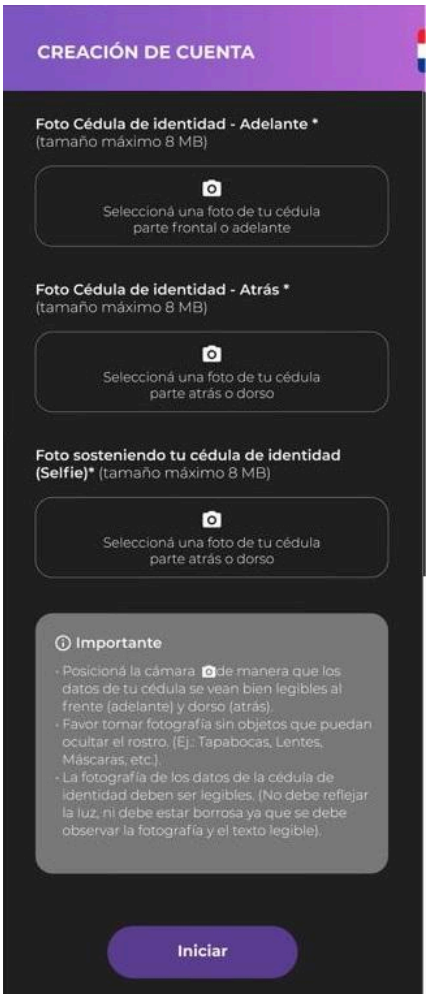
Actualmente para el registro de usuarios se redirige al navegador para pedir la carga de datos al usuario, es decir, la app no tiene una pantalla para el formulario de registro, dicho esto lo que se necesita hacer es lo siguiente:

8.1.1. Crear una nueva pantalla para el registro de usuarios en la carpeta screens del proyecto.



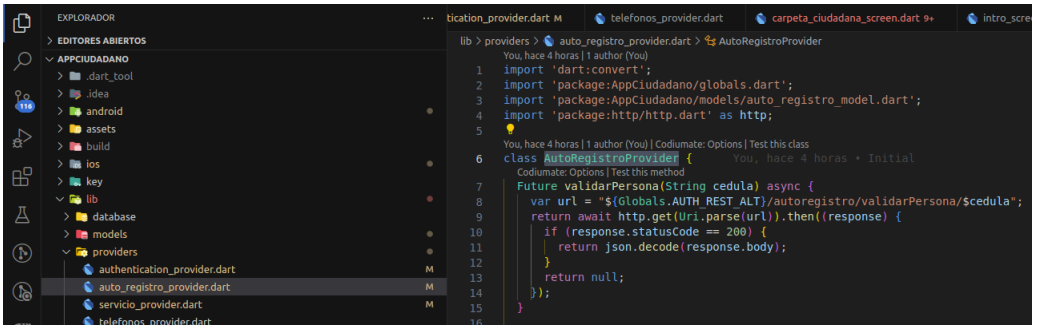
8.1.2. En este nueva pantalla replicar el formulario de la web para el registro de usuario y también el botón “Iniciar”, para el video selfie para verificar la prueba de vida

CREACIÓN DE CUENTA
Cédula sin puntos *
Ej. 123456
Fecha de Nacimiento *
Fecha de Nacimiento
Correo Electrónico *
Ej. correo@mail.com
Repetir Correo Electrónico *
Ej. correo@mail.com
Nro. de Teléfono móvil (Ej. 0961123456) *
+595
Anterior
Siguiente


CREACIÓN DE CUENTA
Foto Cédula de identidad - Adelante *
(tamaño máximo 8 MB)
Seleccioná una foto de tu cédula parte frontal o adelante
Foto Cédula de identidad - Atrás *
(tamaño máximo 8 MB)
Seleccioná una foto de tu cédula parte atrás o dorso
Foto sosteniendo tu cédula de identidad (Selfie)* (tamaño máximo 8 MB)
Seleccioná una foto de tu cédula parte atrás o dorso
Importante
• Posicioná la cámara de manera que los datos de tu cédula se vean bien legibles al frente (adelante) y dorso (atrás).
• Favor tomar fotografía sin objetos que puedan ocultar el rostro. (Ej.: Tapabocas, Lentes, Máscaras, etc.).
• La fotografía de los datos de la cédula de identidad deben ser legibles. (No debe reflejar la luz, ni debe estar borrosa ya que se debe observar la fotografía y el texto legible).
Iniciar

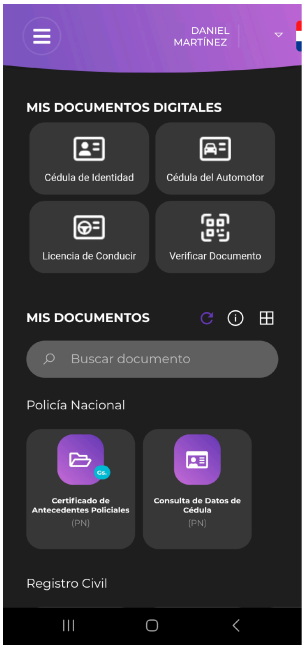
8.1.3. Al hacer click en el botón “Iniciar”, si los datos están correctos, debe mostrar una ventana donde el usuario grabará el video selfie del usuario.

8.1.3.1. En la carpeta providers archivo auto_registro_provider.dart agregar un método a la clase AutoRegistroProvider el cual recibe el video selfie como parámetro para llamar al API de FaceRecognitionCore para las validaciones necesarias. Se sugiere el siguiente nombre para el método: validateAndSaveVideoSelfie

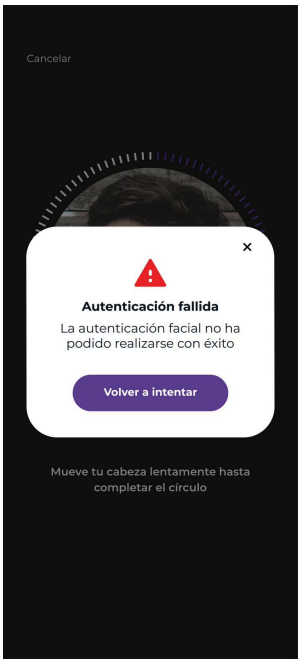


8.1.3.2. Mientras el usuario se graba se debe llamar en tiempo real al método creado en el ítem anterior para hacer la validación del video selfie

8.1.3.3. Si la respuesta de la validación es exitosa el backend guarda en la base de datos todos los campos que cargó el usuario y también los parámetros de reconocimiento facial detectados.



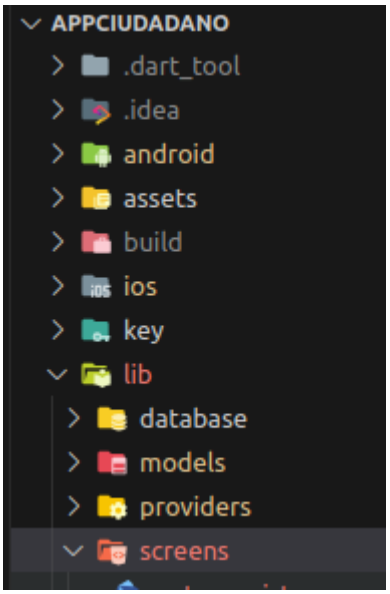
8.1.3.4. Si el resultado de la validación resulta en un error, se muestra la siguiente pantalla de error.



8.2. INICIO DE SESIÓN CON RECONOCIMIENTO FACIAL

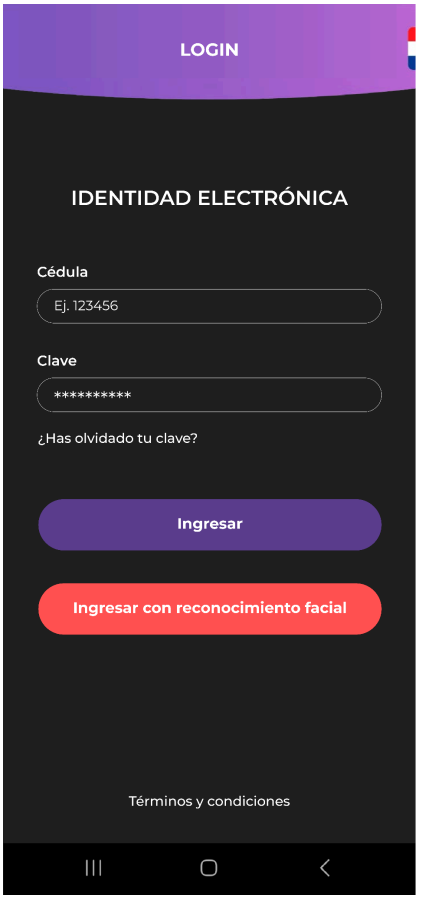
Así como el registro de usuario, la pantalla de Inicio de Sesión es un WebView el cual abre el link del formulario para iniciar sesión a través de la página Web del MITIC. Lo que se requiere hacer es:

8.2.1. Crear una pantalla (nativa, sin WebView) en la carpeta screens del proyecto



8.2.2. Agregar los campos de textos y botón para ingresar como se muestra en la web:

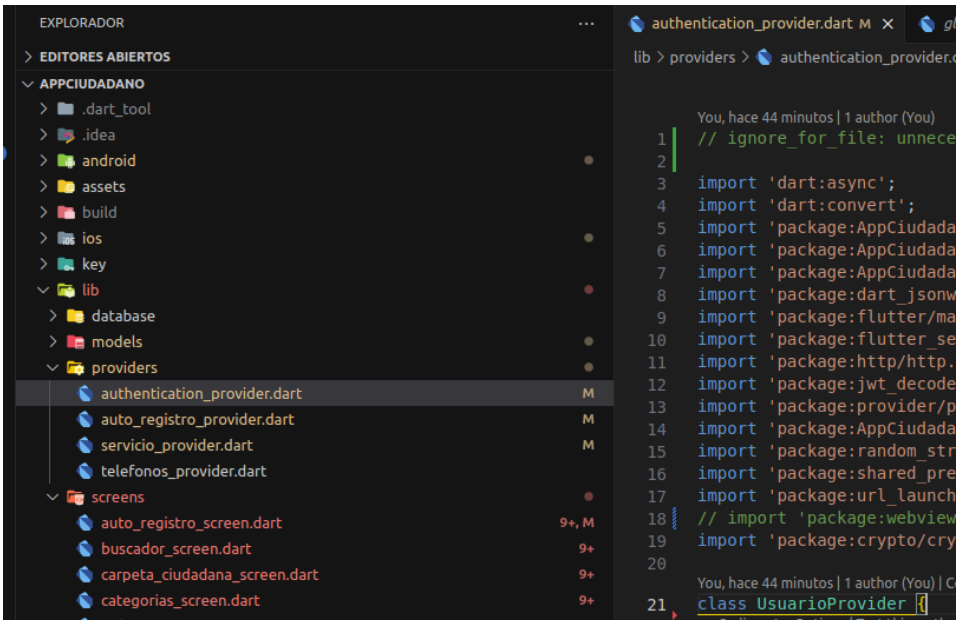
8.2.3. Debajo del botón “Ingresar” agregar un botón extra con el texto “Ingresar con reconocimiento facial”.



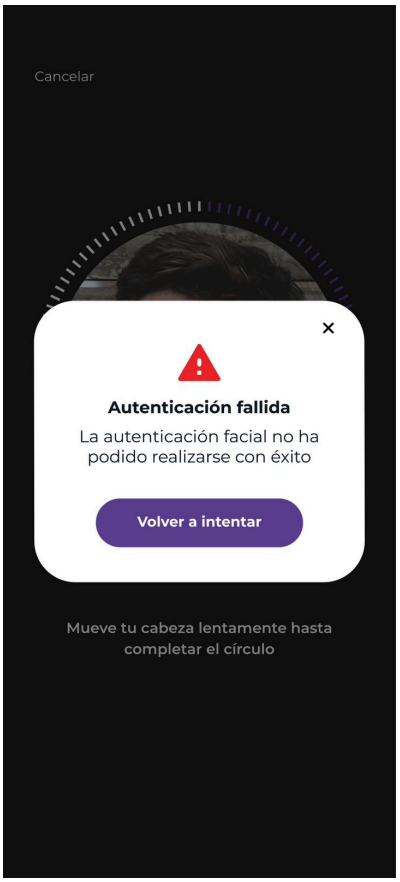
8.2.3.1. El botón “Ingresar con reconocimiento facial” debe abrir una nueva ventana con la vista frontal de la cámara para que el usuario se saque una selfie.

8.2.3.2. En la carpeta **providers** archivo **authentication_provider.dart** agregar un nuevo método a la clase **UsuarioProvider** que haga la llamada a llamada al **API FaceRecognitionCore** con el video selfie obtenida del campo de selfie para identificar al usuario. Se sugiere el siguiente nombre para método:

authenticationByFaceRecognition



8.2.3.3. Mostrar mensaje de éxito o error dependiendo de la respuesta del API



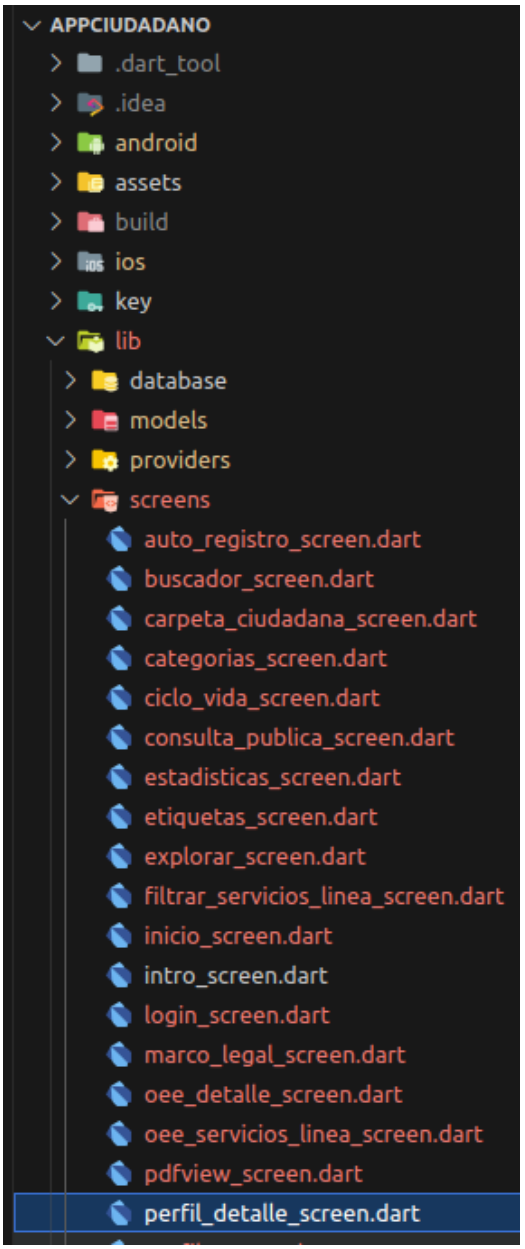
8.2.3.4. En caso de éxito escribir en el storage el token y los datos necesarios. es decir, copiar lo que se hace en el método authentication de la clase UsuarioProvider

```
21  class UsuarioProvider {
55    Future<Map<String, dynamic>?> authentication(
56        BuildContext context, queryParams) async {
57      final params = {'code': queryParams['code'], 'state': queryParams['state']};
58      final headers = {'Content-Type': 'application/json'};
59      final response = await http.post(
60          Uri.parse("${Globals.BASE_URL}/auth/validarAcceso"),
61          headers: headers,
62          body: json.encode(params));
63      if (response.statusCode == 200) {
64        Map<String, dynamic> decodedResp = json.decode(response.body);
65        if (!decodedResp['error']) {
66          var payload = Jwt.parseJwt(decodedResp['token']);
67          final storage = new FlutterSecureStorage();
68          await storage.write(
69            key: Globals.JWT_TOKEN_STORAGE_KEY,
70            value: decodedResp['token'],
71          );
72          await storage.write(
73            key: Globals.JWT_USER_STORAGE_KEY,
74            value: json.encode(decodedResp['ipersona']),
75          );
76          await storage.write(
77            key: Globals.AUTH_PRIMERA_VEZ,
78            value: StatusAccesoPorPrimeraVez.SI.toString(),
79          );
80          await storage.write(key: Globals.AUTH_FECHA_HORA_INACTIVO, value: null);
81          await storage.write(
82            key: Globals.AUTH_LIMITE_INTENTO,
83            value: (payload["authLimiteIntento"] != null
84                ? "${payload["authLimiteIntento"]}"
85                : "${Globals.LIMITE_TIEMPO_EXP_LOCAL}"),
86          );
87          await storage.write(
88            key: Globals.AUTH_TIEMPO_EXP_LOCAL,
89            value: (payload["authTiempoExpLocal"] != null
90                ? "${payload["authTiempoExpLocal"]}"
91                : "${Globals.LIMITE_TIEMPO_EXP_LOCAL}"),
92          );        You, hace 1 segundo • Uncommitted changes
93          var loginInfo = Provider.of<LoginInfoModel>(context, listen: false);
94          await loginInfo.getInfoStorage();
95          print("[DEBUG]: authentication:PAYLOAD $payload");
96          // print("[DEBUG]: authentication:${decodedResp['token']}");
97          return decodedResp;
98        }
99      }
100     return null;
```

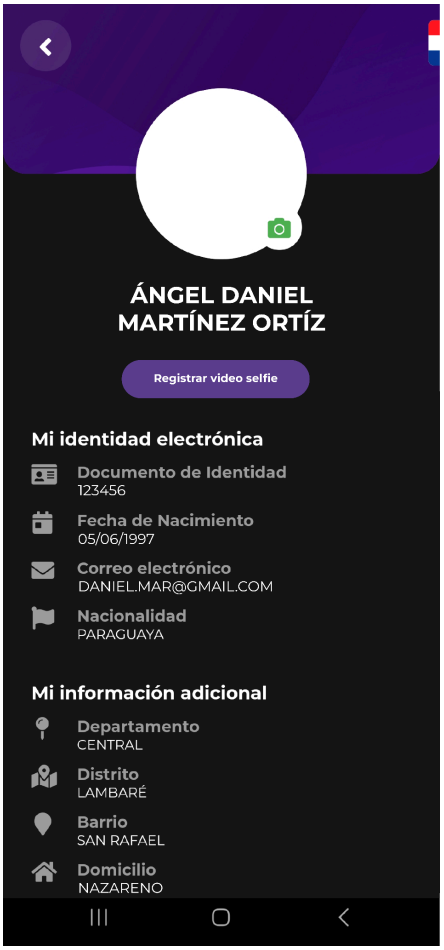
8.3. ACTUALIZACIÓN DE PERFIL PARA RECONOCIMIENTO FACIAL

Para los usuario que ya estén registrados y quieran usar la opción de autenticación por reconocimiento facial se necesita hacer lo siguiente:

8.3.1. En la pantalla de Perfil ubicado en el sistema de archivos dentro de la carpeta screens agregar el botón “Registrar video Selfie” para Reconocimiento Facial



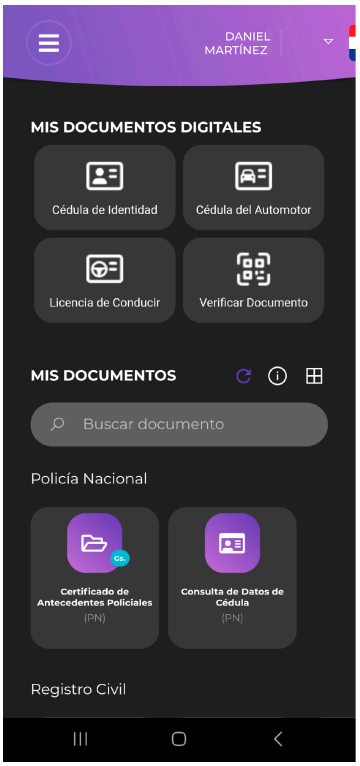
8.3.2. El botón que se sugiere es el siguiente:



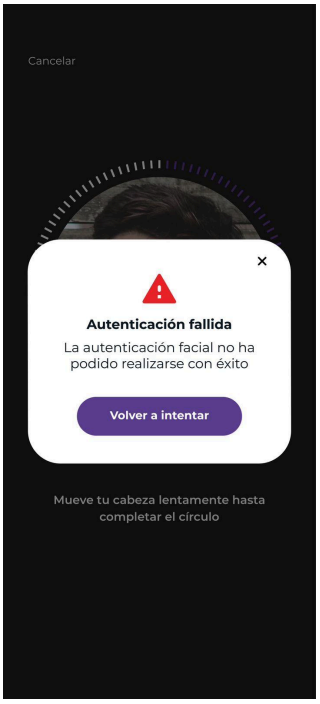
8.3.3. Cuando se hace click a este botón debería llamar al método **validateAndSaveVideoSelfie** de la clase **AutoRegistroProvider**

8.3.4. Se debe llamar en tiempo real al método citado en el ítem anterior para hacer la validación del video selfie

8.3.5. Si la respuesta de la validación es exitosa se realiza el inicio de sesión exitoso y se muestra la página principal de la aplicación.



8.3.6. Si el resultado de la validación resulta en un error, se muestra la pantalla de error.



9. CONCLUSIONES Y RECOMENDACIONES FINALES

En los últimos cincuenta años la aceleración del desarrollo tecnológico ha transformado por completo nuestras sociedades. La hiperconectividad propiciada por el despliegue de las redes de comunicaciones está permitiendo la digitalización de una parte importante de nuestras actividades, aportando numerosos beneficios pero también algunos riesgos que deben ser mitigados.

En esta dualidad analógico-digital uno de los procesos que sigue siendo clave a la hora de aportar seguridad es la verificación de identidad a través del reconocimiento facial. En el mundo físico es una tarea que llevamos a cabo de manera intuitiva en nuestro día a día, reconociendo a personas a simple vista. Cuando esta misma actividad (en absoluto trivial) debe llevarse a cabo de manera automática sin intervención humana es necesario desplegar todo el potencial tecnológico para obtener resultados fiables.

En ese sentido la biometría en conjunción con las tecnologías de inteligencia artificial forman un equipo robusto que nos permite aportar seguridad a los procesos digitales donde sea necesario verificar con garantías la identidad de una persona.

Tanto en el campo del código abierto, como en el campo comercial, existen numerosas soluciones para reconocimiento facial, las cuales incluyen complejos algoritmos de Inteligencia Artificial, como Machine Learning y Deep Learning que son utilizados para lograr un reconocimiento eficiente y preciso del rostro de una persona. Algunas de estas soluciones deben ser previamente entrenadas para lograr una eficiencia deseable de manera a garantizar la identidad de una persona mediante el análisis de su rostro.

En el campo del código abierto, se destaca a la librería OpenCV por contar con numerosos algoritmos para el reconocimiento facial disponibles para la programación de una solución confiable. Además está soportada por una extensa comunidad que comparte en la Web los códigos fuentes de sus soluciones programadas, lo que hace que sea mucho más viable la programación por contar con muchos ejemplos para diversos problemas que deben ser resueltos. A todo esto le sumamos que OpenCV está actualmente en constante actualización por la extensa comunidad que la soporta.

En el campo comercial, existen numerosas soluciones con un porcentaje de confiabilidad bastante alto. Todas se basan en brindar soluciones para el reconocimiento facial a través de una API REST bien documentada, de fácil acceso y utilización. Los mecanismos de monetización que implementan son bien diversos, de manera que es muy probable poder encontrar la solución que mejor se adapte a los requerimientos de los clientes.

10. REFERENCIAS

[1] Microsoft, Mitigate latency and improve performance, url: https://learn.microsoft.com/en-us/azure/ai-services/computer-vision/how-to/mitigate-latency

[2] University of Massachusetts, Labeled Faces in the Wild Home, url: https://vis-www.cs.umass.edu/lfw/

[3] OpenCV Org, url: https://opencv.org/

[4] OpenCV Python, url: https://pypi.org/project/opencv-python/

[5] DLib C++ Library, url: http://dlib.net/

[6] DLib Python, url: https://pypi.org/project/dlib/

[7] GitHub Face Recognition, url: https://github.com/ageitgey/face_recognition

[8] GitHub Face Recognition Python, url: https://pypi.org/project/face-recognition/

[9] Facenet, url: https://github.com/davidsandberg/facenet

[10] VisionLabs, FaceEngine, url: https://github.com/VisionLabs/FaceEngine/commits/master/setup.py

[11] Luna SDK, url: https://visionlabs.ai/solutions/luna-sdk/

[12] Kairos, url: https://face.kairos.com/

[13] Amazon, Amazon Rekognition, url: https://aws.amazon.com/es/rekognition/

[14] Microsoft, Azure AI Vision, url: https://azure.microsoft.com/es-es/products/ai-services/ai-vision/

[15] Innovatrics, url: https://www.innovatrics.com/es/dot-kit-de-herramientas-de-onboarding-digital/

[16] VU Security, url: https://www.vusecurity.com/es/

11. PLANIFICACIÓN DE ENTREGA DE LA OT

Fecha de entrega al MITIC para inicio de las verificaciones	23/Feb/2024
Verificación, ciclo de pruebas y correcciones	11/Mar/2024

Ciclo de pruebas (1er ciclo)	11/Mar/2024
Ciclo de pruebas (2do ciclo)	09/May/2024

12. PERFILES PARA EL DESARROLLO DE LA OT

Coordinador de proyecto	Julio Paciello
Analista Funcional	Marcelo Alvarez

JULIO MANUEL PACIELLO CORONEL

Digitally signed by JULIO MANUEL PACIELLO CORONEL
DN: CN=JULIO MANUEL PACIELLO CORONEL, SERIALNUMBER=CI1490175, G=JULIO MANUEL, SN=PACIELLO CORONEL, OU=F2, O=CERTIFICADO CUALIFICADO DE FIRMA ELECTRONICA, C=PY
Reason: I am the author of this document
Location:
Date: 2024.02.26 15:02:56-03'00'
Foxit PDF Editor Version: 13.0.1

Ing. Julio Paciello Coronel
Coordinador Especialista TIC
Centro de Desarrollo Sostenible