DESARROLLO DE UN SISTEMA DE CONTROL DE ACCESO MEDIANTE VISIÓN POR COMPUTADORA PARA LA TERAPIA COGNITIVA EN PACIENTES CON ENFERMEDAD DE ALZHEIMER

Daniel Esteban Maya Portillo

Trabajo de investigación para optar al título de Bioingeniero

Modalidad de Práctica

Proyecto de investigación

Asesor

John Fredy Ochoa Gómez, Doctor (PhD) en Ingeniería Electrónica

Asesor

Claudia Patricia Ramos Pérez, Especialista (Esp) en Psiquiatría

Universidad de Antioquia

Facultad de Ingeniería

Bioingeniería

Medellín, Antioquia, Colombia

2024

Cita	Maya Portillo [1]
Referencia Estilo IEEE (2020)	[1] D. Maya Portillo, “Desarrollo de un sistema control de acceso mediante visión por computadora para la terapia cognitiva en pacientes con enfermedad de Alzheimer”, Proyecto de investigación en Bioingeniería, Universidad de Antioquia, Medellín, Colombia, 2024.

Grupo de Investigación Neuropsicología y Conducta (GRUNECO).

Dedicatoria

Dedico este trabajo a mis padres y a mis abuelos, quienes, con su amor y apoyo incondicional, me han sido un faro de motivación y orgullo en cada paso de mi camino. Sus palabras de aliento y admiración, en cada regreso a mi pueblo, me han llenado de fuerza y determinación para seguir adelante. También dedico este trabajo a mis hermanos, a quienes, como les digo, “mis chiquillos”, me han dado la responsabilidad de ser un modelo a seguir. Saber que vienen detrás de mí y que me ven con admiración, me ha dado la motivación para esforzarme y alcanzar mis metas.
A todos ellos, gracias por estar siempre presente en mi vida y por creer en mí. Este trabajo es un reflejo de su apoyo y amor.

Agradecimientos

Expreso mi más profundo agradecimiento a la Universidad de Antioquía, que me ha brindado un espacio de crecimiento académico y personal, lleno de conocimientos y lecciones valiosas para la vida. Agradezco especialmente a las personas que han dejado una huella imborrable en mi camino:

- A mis amigos y familiares, por su incansable apoyo emocional y motivación en momentos de dificultad.
- A mis tutores, John Fredy y Claudia Patricia, por su guía y confianza en mis capacidades, lo que me ha permitido crecer y desarrollarme.
- Al grupo GRUNECO, por la oportunidad de participar en este proyecto y confiar en mí.
- A Isabella Ariza, por su invaluable amistad y recomendación, que ha sido fundamental en mi camino.
- A todas las personas que han sido parte de mi carrera de Bioingeniería, con quienes he compartido momentos de estudio, risas, lágrimas y crecimiento. Estoy agradecido por su presencia en mi vida y por haber contribuido a mi formación como persona.

TABLA DE CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

SIGLAS, ACRÓNIMOS Y ABREVIATURAS

Esp.	Especialista
PhD	Philosophiae Doctor
UdeA	Universidad de Antioquia
TNM	Trastorno Neurocognitivo Mayor
EA	Enfermedad de Alzheimer
DSM-5	Manual Diagnóstico y Estadístico de los Trastornos Mentales
IA	Inteligencia Artificial
AA	Aprendizaje Automático
DOM	Document Object Model
TIC	Tecnologías de la Información y la Comunicación
SSD	Single Shot Multibox Detector
CDR	Clinical Dementia Rating Scale
DRY	Don´t repeat yourself

RESUMEN

El presente proyecto de investigación, enmarcado en la iniciativa "*Desarrollo de una intervención multimodal con énfasis en la anosognosia para el tratamiento de la enfermedad de Alzheimer a través de Tecnologías de información y Comunicación"* de Minciencias, exploró cómo los sistemas de control de acceso a plataforma web haciendo uso de tecnologías de la información y la comunicación, pueden mejorar la autonomía y calidad de vida de sus usuarios en primeras etapas de enfermedad de Alzheimer, así como aliviar la carga de sus cuidadores.

Se siguió una estructura de trabajo dividida en fases de desarrollo cortas que priorizaron las tareas más importantes con el objetivo de realizar entregas frecuentemente para obtener una retroalimentación constante y realizar ajustes en el proceso. Para el desarrollo de la tecnología se hizo una revisión de tecnologías y herramientas, luego se seleccionó el framework de node.js y express para trabajar en conjunto en el backend y la librería React en el frontend. Además, se implementó el flujo de reconocimiento facial con la librería de face-api.js tanto en el backend como en el frontend. Finalmente, se evaluó la usabilidad del sistema a través de la estrategia "*piensa en voz alta*" y aplicando la métrica estándar de experiencia de usuario "*Single Ease Question"*.

El proyecto logró desarrollar un sistema de control de acceso mediante visión por computadora que se integra satisfactoriamente en la plataforma web especializada en la terapia cognitiva de pacientes con enfermedad de Alzheimer. Este sistema brinda a los usuarios con Alzheimer una alternativa segura, eficiente e intuitiva para acceder a plataformas web, otorgándoles mayor autonomía y seguridad en su interacción digital.

Palabras clave — **Enfermedad de Alzheimer, desarrollo de software, plataforma web, biometría, reconocimiento facial.**

ABSTRACT

The present research project, framed within the initiative "*Development of a multimodal intervention with an emphasis on anosognosia for the treatment of Alzheimer's disease through Information and Communication Technologies*" by Minciencias, explored how access control systems for web platforms using Information and Communication Technologies can improve the autonomy and quality of life of users in the early stages of Alzheimer's disease, as well as alleviate the burden on their caregivers.

The work followed a structure divided into short development phases that prioritized the most important tasks to allow for frequent deliveries, enabling constant feedback and adjustments throughout the process. For the technology development, a review of technologies and tools was conducted, after which the Node.js and Express framework was selected for the backend, and the React library for the frontend. Additionally, the facial recognition flow was implemented using the Face-api.js library in both the backend and frontend. Finally, the system's usability was evaluated through the *"think aloud"* strategy and by applying the standard user experience metric *"Single Ease Question."*

The project successfully developed an access control system using computer vision that integrates seamlessly into the web platform specialized in cognitive therapy for Alzheimer's patients. This system provides users with Alzheimer's a safe, efficient, and intuitive alternative to access web platforms, granting them greater autonomy and security in their digital interactions.

Keywords — **Alzheimer's disease, software development, web platform, biometrics, facial recognition.**

I. INTRODUCCIÓN

El Alzheimer es un trastorno neurodegenerativo progresivo que afecta a la memoria, la cognición y el comportamiento. A medida que la enfermedad progresa, las personas con Alzheimer pueden experimentar dificultades en diversos aspectos de su vida cotidiana, como la comunicación, la toma de decisiones y la vida independiente [1]. Este panorama resulta preocupante, debido a que la Organización Mundial de la Salud [OMS], en su informe de marzo de 2023 sobre la demencia, indica que el número de casos diagnosticados de la enfermedad de Alzheimer en todo el mundo se sitúa entre el 60 % y el 70 % del total de casos de pacientes con demencia, es decir, que afecta a unos 55 millones de personas y cada año se registran 10 millones de nuevos casos, lo que supone un aumento de 82 millones de adultos en 2030 y de 152 millones en 2050 [2].

Dado el aumento previsto en el número de personas con enfermedad de Alzheimer, existe una necesidad de investigación que explore enfoques innovadores para mejorar su calidad de vida y apoyar su tratamiento cognitivo. Es aquí donde la tecnología adquiere un papel más influyente en la mejora de la vida de los adultos mayores afectados por el Alzheimer, acompañándolos en todas las etapas, desde las más tempranas hasta las más avanzadas de la enfermedad [2].

El Alzheimer afecta significativamente la capacidad cognitiva de los individuos, por lo que los métodos convencionales de acceso a plataformas con autenticación de usuario, que requieren recordar nombres de usuario y contraseñas, sean particularmente desafiantes. Estos métodos pueden resultar complicados para los pacientes debido al deterioro de la memoria y de la capacidad de concentración, lo que puede llevar a errores de entrada y frustración.

Para abordar este desafío, la siguiente propuesta de investigación busca investigar el impacto de los métodos de control de acceso a plataformas web utilizando tecnologías de la información y la comunicación (TIC) en las primeras fases de la enfermedad de Alzheimer.

Es por esto por lo que en el proyecto aprobado por MinCiencias "*Desarrollo de una intervención multimodal con énfasis en la anosognosia para el tratamiento de la Enfermedad de Alzheimer, a través de Tecnologías de Información y Comunicación (TIC)*", se busca abordar esta compleja problemática mediante una intervención integral que aproveche los avances en TIC. Esta

intervención tiene como objetivo principal mejorar la funcionalidad de los pacientes con Alzheimer y disminuir la sensación de sobrecarga en los cuidadores, al proporcionar herramientas que faciliten el manejo de los síntomas neuropsiquiátricos y la carga emocional asociada a la enfermedad. En línea con este enfoque y para complementar y fortalecer la intervención del proyecto mencionado, este proyecto se centra en mejorar el acceso y la usabilidad de las herramientas tecnológicas utilizadas en el tratamiento del Alzheimer. El objetivo de este proyecto de investigación es mejorar la experiencia de usuario de los pacientes al simplificar el proceso de registro e inicio de sesión, garantizando una accesibilidad óptima.

Para abordar esta propuesta, es necesario dividir el problema en dos componentes principales. En primer lugar, se encuentra el desarrollo web, que implica la utilización de una amplia gama de herramientas y frameworks basados en el lenguaje de programación Javascript, así como HTML y CSS. Estas tres tecnologías se combinan de manera sinérgica para crear sitios web dinámicos y visualmente atractivos.

Por otro lado, se encuentra la implementación del control de acceso mediante datos biométricos faciales. Este método se basa en algoritmos especializados que reconocen y verifican la identidad de una persona a través de características faciales únicas. En este proceso, cuando un usuario intenta acceder a la página web, su rostro es capturado por una cámara y se compara con los patrones faciales almacenados en una base de datos. Si se encuentra una coincidencia, se autoriza el acceso al sistema.

Así, el objetivo de este proyecto de investigación buscó determinar si el reconocimiento facial facilita el registro e inicio de sesión para personas con Alzheimer en comparación con métodos tradicionales basados en contraseñas. Para lograrlo se realizaron pruebas piloto para ajustar y validar el diseño experimental.

Los resultados preliminares de este proyecto indican que el reconocimiento facial ofrece una mejor alternativa para la autenticación de usuarios con Alzheimer. En las pruebas realizadas los usuarios reportaron una mayor facilidad de uso y una menor frustración en comparación con los métodos tradicionales. Estos resultados sugieren que el reconocimiento facial puede ser una

herramienta valiosa para mejorar la accesibilidad a las tecnologías de la información y la comunicación para personas con Alzheimer.

La investigación muestra que esta tecnología podría transformar la manera en que los pacientes con Alzheimer interactúan con la tecnología, promoviendo su autonomía y mejorando su calidad de vida. Al simplificar el proceso de inicio de sesión, el reconocimiento facial no solo ayuda los pacientes, sino que también podría reducir la carga de trabajo de los cuidadores, mejorando así el bienestar general de ambas partes.

II. OBJETIVOS

A. Objetivo general

Desarrollar un sistema de control de acceso basado en la biometría facial, utilizando herramientas de visión por computadora, para simplificar el registro e inicio de sesión en una plataforma dedicada a personas en etapa temprana de Alzheimer.

B. Objetivos específicos

- Realizar una revisión de las herramientas y tecnologías disponibles para la implementación de la biometría facial.

- Implementar un sistema de control de acceso basado en la biometría facial utilizando herramientas de visión por computadora, integrándolo de manera efectiva en la interfaz web.

- Ajustar y validar la efectividad y accesibilidad de la interfaz web y el sistema de control de acceso mediante pruebas piloto con individuos en primeras etapas de Alzheimer.

III. MARCO TEÓRICO

I. Alzheimer

El Alzheimer es una enfermedad neurodegenerativa que afecta principalmente a los adultos mayores, es decir, personas con 60 o más años, y se caracteriza por la pérdida progresiva de la memoria, el lenguaje y otras habilidades cognitivas. En las etapas tempranas, los efectos cognitivos pueden ser menos pronunciados y pueden incluir dificultades para recordar cosas, problemas con el sentido del olfato, y cambios en el comportamiento y la personalidad. Estos síntomas pueden interferir con la vida diaria, pero generalmente no son tan severos como en etapas más avanzadas de la enfermedad [3].

Dado que los síntomas y el avance de la enfermedad varían de persona a persona, es fundamental implementar enfoques de tratamiento que respondan a las necesidades particulares de cada paciente. En su artículo sobre el manejo conductual multimodal para personas con demencia, Allen [4] sostiene que las estrategias más eficaces para mantener la funcionalidad de los pacientes con EA se derivan de la adaptación a las necesidades individuales de cada paciente y la oferta de opciones interdisciplinarias y transdisciplinarias, es decir, intervenciones multimodales.

La EA es una enfermedad dinámica que cambia constantemente, por lo que el tratamiento debe ser flexible para adaptarse y responder a las necesidades cambiantes de la persona con demencia [5]. Ya que la demencia no solo afecta a quien la padece, sino también a sus seres queridos. Las personas con demencia pueden experimentar cambios drásticos en su personalidad, y los cuidadores y familiares deben ajustarse a estos cambios, ayudar en el autocuidado y manejar las responsabilidades económicas del hogar, lo que puede causar estrés emocional y financiero [4].

El tratamiento de la EA puede ser de dos tipos:

- Farmacológico: Se plantea como estrategia inicial en pacientes con EA leve o moderada con carácter sintomático.
- No farmacológico: Incluye aspectos como la estimulación cognitiva, una intervención estructurada que pretende entrenar las habilidades cognitivas y mejorar la calidad de vida repitiendo actividades cognitivas graduadas de forma terapéutica.

La intervención más eficaz combina el tratamiento farmacológico con el no farmacológico. Entre las intervenciones no farmacológicas, la terapia ocupacional (TO) es una alternativa eficaz para mantener la independencia funcional en las actividades diarias. Además, la terapia asistida por ordenadores (TAO) es un campo de intervención que combina la actividad del sujeto con el uso de aplicaciones informáticas [4].

Aunque no existe un tratamiento médico que frene o cure el Alzheimer, los medicamentos disponibles pueden atenuar o retrasar la mayoría de los síntomas, y en algunos casos, invertir estos procesos deterioradores. El manejo multimodal, que incluye tratamientos farmacológicos y no farmacológicos, puede proporcionar comodidad, dignidad e independencia a las personas con esta enfermedad durante un período mayor y ayudar a sus cuidadores a lidiar con los desafíos asociados [4].

II. Biometría

Cada ser humano en nuestro planeta posee características morfológicas únicas, como la forma del rostro, la geometría de las manos, los ojos, el iris y las huellas digitales. Estos rasgos permiten a nuestro cerebro y a sistemas tecnológicos especializados identificar y distinguir a individuos específicos [6]. La biometría se deriva de "bio", que significa vida, y "metron", medida, y en un contexto más amplio, se refiere a la aplicación de técnicas estadísticas basadas en matemáticas que analizan datos de las ciencias biológicas. Estos análisis se aplican en tecnología para diseñar dispositivos y algoritmos utilizados en la identificación, autenticación y certificación de personas [7]. De esta forma los sistemas biométricos automatizan la medición de características físicas o de comportamiento de individuos para obtener autenticación, es decir, para reconocer si una persona está presente en un lugar y momento determinados, activando así un mecanismo, típicamente un sistema de seguridad [7].

Sistemas biométricos

A continuación, se presenta una descripción de los principales sistemas biométricos:

1. Huella dactilar

Este sistema tiene como principio de funcionamiento el análisis de los patrones únicos de las crestas y surcos presentes en la piel de los dedos. Un sensor captura la imagen de la huella y

la compara con una plantilla almacenada en una base de datos para verificar la identidad del usuario [8].

Dentro de sus ventajas esta que consta de una alta precisión, además de una amplia aceptación entre los usuarios que se encuentran familiarizados con smartphones, no obstante, dentro de sus desventajas está que requiere de contacto físico con el dispositivo, por lo que entra en conflicto si se requiere para un aplicativo web puesto a que no todos los usuarios podrán contar con un lector de huella digital, además es vulnerable a heridas en los dedos y a posibles falsificaciones [8].

2. Reconocimiento facial

El reconocimiento facial utiliza cámaras y algoritmos de software para analizar las características faciales de una persona, como la forma de la cara, la distancia entre los ojos, la nariz y la boca, y la textura de la piel. La información obtenida se compara con una plantilla facial almacenada en una base de datos para verificar la identidad del usuario [9].

Este sistema tiene como ventaja que el usuario no necesita tener contacto con ningún dispositivo, lo que lo hace más conveniente, además este es un proceso natural e intuitivo para la mayoría de las personas, sumado a esto es un proceso que puede ser muy rápido, especialmente en condiciones de iluminación adecuadas [9].

Dentro de sus desventajas está que la calidad de la imagen facial puede verse afectada por la iluminación, el ángulo de visión, la presencia de sombras y otros factores ambientales

3. ***Reconocimiento de iris***

El reconocimiento de iris utiliza cámaras especiales para capturar imágenes de alta resolución del iris, la parte coloreada del ojo. Un algoritmo analiza los patrones únicos del iris, como la textura y los vasos sanguíneos, para crear una plantilla de iris que se compara con la almacenada en una base de datos para verificar la identidad del usuario [8].

El iris es una característica ocular altamente distintiva, lo que hace que el reconocimiento de iris sea uno de los sistemas biométricos más precisos disponibles. Además, este está protegido por el párpado y otras estructuras oculares, lo que lo hace menos susceptible a falsificaciones que otras modalidades biométricas [8].

En sus desventajas está su alto costo, ya que como se menciona, este es un sistema que requiere de cámaras especializadas lo que lo hace más costoso que otros sistemas biométricos. Además, su proceso de captura puede ser incómodo para algunos usuarios, ya que requiere que se acerquen al dispositivo y mantengan la cabeza quieta, esto sumado a que la calidad de la imagen puede verse afectada por la iluminación y las condiciones ambientales.

4. Reconocimiento de voz

El reconocimiento de voz analiza las características únicas de la voz de una persona, como la frecuencia, el tono, la entonación y la forma de pronunciar las palabras. Un modelo de voz se crea a partir de una muestra de la voz del usuario y se compara con la voz en tiempo real para verificar la identidad [8].

Este sistema ofrece una forma natural e intuitiva de autenticarse y además puede ser implementado en cualquier dispositivo con micrófono, sumado a esto permite autenticación en situaciones donde las manos del usuario están ocupadas o no puede usar métodos de autenticación visuales, no obstante, este se ve afectado por el ruido de fondo y variaciones en la voz lo que lo hace menos preciso que otros métodos biométricos ya que puede llevar a falsos positivos o negativos.

III. Desarrollo web

El desarrollo web es el proceso de crear y mantener sitios web. Abarca desde el diseño de la interfaz de usuario hasta la implementación de la funcionalidad y la gestión de bases de datos.

1. Modelo cliente-servidor

El desarrollo web para reconocimiento facial se sustenta en el modelo cliente-servidor, una arquitectura fundamental en la interacción entre usuarios y páginas web. En este modelo, un

servidor aloja los recursos y procesos que conforman la página web, mientras que un navegador web instalado en el dispositivo del usuario actúa como cliente para solicitar y visualizar esos recursos [9].

a) Cliente

Los clientes envían solicitudes al servidor para acceder a recursos o servicios específicos. Por ejemplo, el navegador web actúa como cliente, interpretando el código HTML, CSS y JavaScript que conforman la página web y presentándola al usuario en una interfaz gráfica. Además, permite al usuario interactuar con la página web mediante la captura de eventos (clics, movimientos del mouse, etc.) y el envío de datos al servidor [9].

b) Servidor

Los servidores están diseñados para ofrecer servicios específicos a los clientes o usuarios. Estos servicios pueden incluir compartir archivos, alojar sitios web, administrar bases de datos, proporcionar acceso a impresoras, entre otros [9].

2. Frontend y backend

El desarrollo web se divide en dos áreas principales:

a) Frontend

El frontend se refiere a la parte de la aplicación web que interactúa directamente con el usuario. Se compone de:

- HyperText Markup Language, HTML: el Lenguaje de Marcado de HiperTexto, define la estructura y el contenido de la página web, incluyendo elementos como títulos, párrafos, imágenes y formularios [10].
- Cascading Style Sheets, CSS: Las Hojas de Estilo en Cascada controlan la apariencia visual de la página web, definiendo colores, tipografías, diseños y animaciones [11].
- JavaScript: Agrega interactividad y dinamismo a la página web, permitiendo la captura de eventos, la manipulación del DOM (Document Object Model) y la comunicación con el backend [12].

b) Backend

El backend es la parte de la aplicación que se ejecuta en el servidor y maneja la lógica de negocio, la autenticación, la gestión de bases de datos y más.

- Lenguajes de programación: Como Python, Java o PHP (Hypertext PreProcessor), se utilizan para desarrollar la lógica de negocio, la interacción con bases de datos y la generación de respuestas al cliente.
- Marcos de trabajo: Facilitan el desarrollo del backend, proporcionando estructuras y herramientas para la gestión de rutas, la autenticación de usuarios, el manejo de errores y la comunicación con el frontend.
- Bases de datos: Almacenan la información persistente de la aplicación, como datos de usuarios, imágenes faciales y configuraciones del sistema.

IV. Interacción humano-computadora

Al diseñar interfaces para el reconocimiento facial en páginas web, es crucial considerar diversos factores de Interacción Humano-Computadora (IHC). Estos factores aseguran que la experiencia del usuario sea intuitiva, accesible y eficiente, especialmente para usuarios con necesidades específicas como los pacientes con Alzheimer en etapas tempranas [13].

Factores de IHC

En el diseño de interfaces para el reconocimiento facial, la simplicidad, consistencia y retroalimentación son elementos esenciales que deben integrarse cuidadosamente. Estos factores son particularmente importantes para usuarios con Alzheimer en etapas tempranas, quienes pueden sentirse abrumados por interfaces complejas y cambios abruptos. A continuación, se exploran estos factores en detalle:

- *Simplicidad:* Las interfaces deben ser lo más sencillas y directas posible. Los pacientes con Alzheimer pueden encontrar las interfaces complejas confusas y frustrantes. Por ello, es fundamental que el diseño sea intuitivo y fácil de navegar, minimizando la cantidad de elementos en la pantalla y priorizando la claridad de las opciones disponibles.

- *Consistencia:* Mantener elementos de diseño coherentes a lo largo de la interfaz, como iconos, colores y fuentes, ayuda a reducir la carga cognitiva de los usuarios. Una interfaz consistente no solo facilita el aprendizaje y la familiarización con el sistema, sino que también promueve la confianza del usuario al ofrecer una experiencia predecible y fiable.
- *Retroalimentación:* Proporcionar retroalimentación inmediata, ya sea visual o auditiva, es crucial para que los usuarios comprendan las consecuencias de sus acciones. Por ejemplo, al lograr un reconocimiento facial exitoso, una respuesta positiva y clara puede ayudar a reforzar la comprensión y la satisfacción del usuario con el sistema.

Pruebas de Usabilidad

Las pruebas de usabilidad son esenciales para evaluar y mejorar la efectividad de las interfaces de reconocimiento facial. Involucran a usuarios reales, en este caso, pacientes con Alzheimer, para obtener comentarios directos y valiosos que guíen el proceso de refinamiento del diseño. Estos son algunos de los aspectos clave en las pruebas de usabilidad:

- *Pruebas con usuarios:* Los pacientes con Alzheimer participan en pruebas de usabilidad. Sus comentarios guían las mejoras.
- *Accesibilidad:* El sistema se adapta a diversas capacidades cognitivas. El tamaño de fuente, el contraste y las opciones de navegación son ajustables.
- *Manejo de errores:* Mensajes de error claros y rutas de recuperación previenen la frustración.

IV. CONSIDERACIONES ÉTICAS

El uso de tecnologías de reconocimiento facial plantea varias consideraciones éticas que deben ser abordadas cuidadosamente para proteger los derechos y la dignidad de los usuarios [14]. Estas consideraciones son particularmente relevantes en el contexto de usuarios vulnerables, como los pacientes con Alzheimer:

- *Privacidad:* La biometría facial plantea preocupaciones de privacidad. La IHC garantiza procesos de consentimiento transparentes y educa a los usuarios sobre el uso de datos.
- *Dignidad:* La IHC promueve interacciones respetuosas. Los pacientes deben sentirse dignos durante los procesos de autenticación.

V. METODOLOGÍA

Este proyecto de investigación utilizó dos metodologías clave para el desarrollo de un sistema de control de acceso intuitivo y accesible para personas en etapas iniciales de la enfermedad de Alzheimer. En una primera fase, se empleó una metodología de cocreación o diseño centrado en el usuario, lo que permitió descubrir que los pacientes con deterioro cognitivo leve (DCL) asociado a la enfermedad de Alzheimer requerían una forma distinta de registro e ingreso al sistema debido a sus dificultades cognitivas. A partir de este hallazgo, se determinó la necesidad de desarrollar un sistema de autenticación mediante reconocimiento facial.

Posteriormente, en una segunda fase, el proceso de desarrollo se llevó a cabo con un equipo de desarrolladores asociados al proyecto de MinCiencias, en donde por medio de ciclos de desarrollo cortos y rápidos alineados a la metodología ágil SCRUM se logró determinar un flujo de trabajo que priorizaba las tareas más importantes y así realizar entregas frecuentemente para obtener retroalimentación y realizar ajustes en el proceso.

1. Análisis y planificación

Junto al equipo de desarrolladores, se pudo analizar necesidades iniciales siguiendo una metodología centrada en el usuario llamada método doble diamante [15], que determinó los lineamientos y recomendaciones para diseñar el sistema de control que beneficia al Alzheimer en etapas tempranas.

Con la metodología SCRUM se pudo elaborar una planificación constante y flexible durante el proceso de desarrollo junto con el análisis de necesidades, lo que permitió abordar distintas perspectivas. Por ejemplo, se consideraron las necesidades de los usuarios para garantizar una experiencia intuitiva y accesible, así como los aspectos técnicos y legales del funcionamiento del sistema.

En este sentido, se hizo uso de plataformas como MURAL, Slack y Github Projects para llevar un seguimiento el progreso y facilitar la colaboración entre los miembros del equipo. MURAL permitió la visualización y organización de ideas de manera colaborativa [16]. Slack se

utilizó para la comunicación rápida y eficiente, permitiendo resolver dudas y tomar decisiones en tiempo real [17]. Por otro lado, Github Projects se empleó para la gestión de tareas y el control de versiones del código, asegurando que todos los desarrolladores estuvieran al tanto de los cambios y avances en el proyecto [18].

2. Revisión de metodologías de control de acceso para páginas web

Se realizó una investigación sobre las diversas tecnologías y metodologías de control de acceso, en donde inicialmente se planteó la posibilidad de utilizar un estándar de autenticación utilizando a terceros, tales como Facebook, Google, Github, entre otros, los cuales ofrecían una experiencia de usuario mejorada al simplificar el inicio de sesión con una cuenta aliada. Sin embargo, esta opción presenta desafíos significativos, incluido un control limitado sobre los datos del usuario y posibles riesgos de seguridad si el proveedor de servicios de terceros es comprometido. Además, depender de terceros introduce vulnerabilidades adicionales, como interrupciones del servicio o cambios en las políticas de privacidad que podrían afectar negativamente la experiencia del usuario y la integridad del sistema.

Dadas estas consideraciones, se determinó que un sistema basado en el reconocimiento de características físicas personales podría representar una alternativa que se adecua a las necesidades inherentes del sistema de control de acceso, tales como un alto grado de seguridad y un control personalizado de la información ingresada a la página web. Aunque presenta desafíos adicionales, como preocupaciones de privacidad y la necesidad de requerimientos funcionales, el reconocimiento biométrico puede proporcionar una capa adicional de seguridad que complementa eficazmente las soluciones de autenticación tradicionales.

Es así que teniendo en cuenta las consideraciones detalladas en la (TABLA I), donde se presenta una comparativa entre los diferentes sistemas biométricos existentes, se puede establecer que el reconocimiento facial se destaca como el método biométrico más adecuado para esta plataforma debido a su accesibilidad, conveniencia y eficiencia. La disponibilidad de cámaras en la mayoría de los dispositivos modernos facilita su implementación de manera sencilla y rentable. Además, este método ofrece una experiencia de usuario sin contacto físico, higiénico y cómodo.

TABLA I RESUMEN COMPARATIVO DE SISTEMAS BIOMÉTRICOS

CARACTERÍSTICA	HUELLA DACTILAR	RECONOCIMIENTO FACIAL	RECONOCIMIENTO DE IRIS	RECONOCIMIENTO DE VOZ
Contacto Físico	Requerido	No requerido	No requerido	No requerido
Precisión	Alta	Alta	Alta	Media
Costo	Bajo	Bajo	Alto	Bajo
Facilidad De Uso	Alta	Alta	Media	Alta
Seguridad	Media	Alta	Alta	Media
Privacidad	Media	Baja	Alta	Media
Disponibilidad De Dispositivos	Alta	Alta	Media	Baja
Accesibilidad Para Usuarios Web	Media	Alta	Baja	Media

El reconocimiento facial es una habilidad natural de los seres humanos para distinguir rostros entre multitudes, interpretando gestos, expresiones y características únicas. En informática, esta capacidad se traduce en el reconocimiento de patrones, donde se clasifican y localizan rostros independientemente de su posición, escala, edad, orientación o iluminación. Este método de autenticación biométrica utiliza medidas corporales para verificar la identidad de una persona. El reconocimiento facial identificación o verificación de la identidad de una persona utiliza sus rasgos faciales.

El funcionamiento del reconocimiento facial se podría resumir en cuatro etapas [19], mencionadas a continuación.

Con el uso de la inteligencia artificial, se realiza una primera etapa conocida como *detección*, que consiste en detectar y ubicar los rostros de un cuadro de video o imagen [8]. Este proceso implica identificar áreas que podrían contener rostros basándose en características visuales como cambios en la intensidad de los píxeles. Se utilizan algoritmos especializados, como redes neuronales convolucionales (CNN), que están entrenados para reconocer patrones específicos que indican la presencia de un rostro humano.

Una vez localizados los rostros, se procede a la etapa de *normalización*. En esa etapa, el software lee el rostro, localiza y hace mediciones de los factores claves que distinguen un rostro de otro. Entre estos factores encontramos, por ejemplo, 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 [19].

Dichos datos no están procesados y, por ende, no se pueden comparar con ninguna base de datos sin antes realizar la fase de *extracción* de características. Es transformar los datos obtenidos de la etapa de normalización en características más manejables para su procesamiento. Dicho de otra manera, es obtener un vector o código de características propias del rostro llamado huella facial. De la misma manera que las huellas dactilares son únicas, cada persona tiene su propia huella facial.

Por último, se realiza la fase de *reconocimiento*, que consiste en una etapa de comparación, donde el software compara la huella facial con la base de datos de todas las caras registradas previamente. El software utiliza algoritmos de coincidencia para determinar la similitud entre la huella facial del individuo que se está verificando y las huellas faciales registradas previamente. Esta comparación se realiza utilizando métodos estadísticos y de aprendizaje automático para garantizar una identificación precisa y confiable.

Estas cuatro fases se repiten en un ciclo cada vez que se realice un reconocimiento facial mediante visión por computadora y este ciclo se puede apreciar de mejor manera en la Fig. 1.

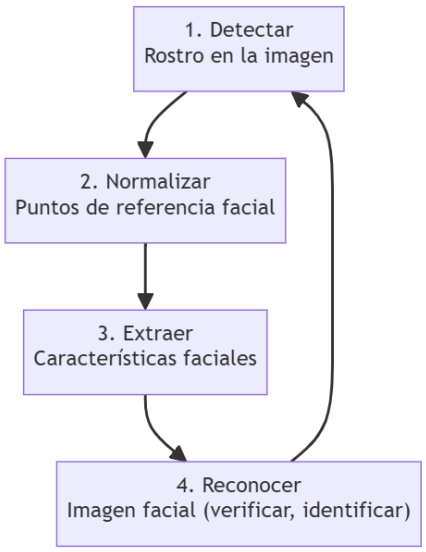

Fig. 1 Flujo del proceso de reconocimiento facial

Diferencia entre detección de rostros y reconocimiento facial

El reconocimiento facial y la detección de rostros, aunque parezcan similares, son procesos diferentes con funcionalidades y complejidades distintas.

Detección de rostros: Este es un proceso analítico sencillo que implica capturar una imagen del rostro de cualquier persona que se encuentre dentro del campo de visión de una cámara designada. El algoritmo de detección de rostros trabaja en conjunto con la cámara, que debe ser una cámara IP (Protocolo de Internet) equipada con la función de detección facial, ya que las cámaras analógicas no pueden ejecutar esta función. El sistema identifica a las personas dentro del área cubierta y automáticamente extrae y almacena una foto de su rostro en el dispositivo de grabación [20].

Reconocimiento facial*:* A diferencia de la detección de rostros, el reconocimiento facial es un proceso más avanzado y específico. Este proceso, gestionado por un algoritmo informático, realiza la identificación facial de manera automática y en tiempo real. Requiere un análisis de video más detallado para determinar si el rostro capturado coincide con alguno de los registrados en una base de datos [20].

3. Inteligencia artificial

La inteligencia artificial (IA) es un campo de la informática que se enfoca en crear sistemas capaces de realizar tareas que normalmente requieren inteligencia humana. Estas tareas incluyen el aprendizaje, la percepción, el razonamiento y la toma de decisiones. La IA se basa en algoritmos y modelos matemáticos para simular capacidades cognitivas humanas [21].

De esta forma el reconocimiento facial es una tecnología que utiliza la IA para identificar o verificar la identidad de una persona a partir de una imagen o video de su rostro [22]. Y como se menciona anteriormente, puede analizar las características faciales únicas de cada individuo.
Así, el reconocimiento facial se sustenta en dos pilares fundamentales de la IA:

a) Aprendizaje automático

El Aprendizaje Automático (AA) permite a las computadoras aprender a partir de datos sin necesidad de ser programadas explícitamente. En el contexto del reconocimiento facial, los algoritmos de AA se entrenan con grandes conjuntos de datos de imágenes faciales y sus identidades asociadas [21].

b) Visión artificial

La visión artificial es una rama de la IA que dota a las computadoras de la capacidad de "ver" y comprender el mundo que las rodea. En el reconocimiento facial, la visión artificial se utiliza para extraer las características faciales relevantes de las imágenes o videos y para representarlas en un formato que pueda ser procesado por los algoritmos de AA [21].

c) Técnicas de reconocimiento facial

Existen dos categorías principales de técnicas de reconocimiento facial: las técnicas basadas en la apariencia y las técnicas basadas en modelos [22]. Dentro de cada una de estas categorías hay diversos métodos para caracterizar la imagen.

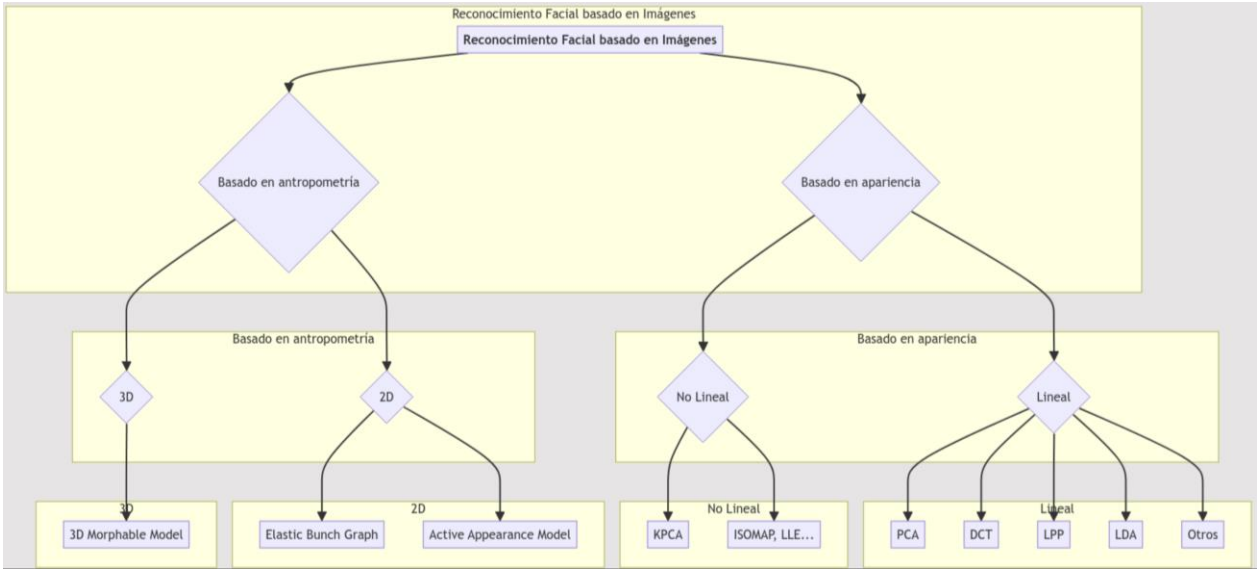

Fig. 2. Métodos de clasificación basados en reconocimiento facial.

i. Basado en antropometría

Este enfoque se basa en la medición de distancias y ángulos entre puntos clave de la cara, como los ojos, la nariz y la boca. Habitualmente estos sistemas requieren de imágenes de gran resolución [23]. Algunas de las técnicas más comunes en esta categoría son:

- **Redes neuronales convolucionales (CNNs):** Las CNNs son un tipo de red neuronal artificial que se utiliza ampliamente para el reconocimiento facial. Son capaces de aprender representaciones jerárquicas del rostro a partir de datos de entrenamiento [23].

- **Modelos de soporte vectorial (SVMs):** Los SVMs son un tipo de algoritmo de aprendizaje automático que se utiliza para clasificar datos. En el contexto del reconocimiento facial, se pueden utilizar para clasificar un rostro como perteneciente a una clase determinada o no [23].

ii. Basado en apariencia

Este enfoque analiza la textura y el patrón de la piel de la cara, utilizando técnicas como el análisis de componentes principales (PCA) o los modelos de aprendizaje profundo (deep learning) [23]. Algunas de las técnicas más comunes en esta categoría son:

- **Análisis de componentes principales (PCA):** El PCA es un algoritmo de reducción dimensional que permite encontrar los vectores que mejor representan la distribución de un grupo de imágenes. Su objetivo es representar una imagen en términos de un sistema de coordenadas óptimo reduciendo el número final de componentes que tendrá la imagen.
- **Análisis de discriminantes lineales (LDA):** Esta técnica encuentra un conjunto de proyecciones que maximizan la separación de las diferentes clases de rostros

4. Implementación del sistema de control de acceso

Este proyecto está basado en una arquitectura de microservicios, lo que permite que la aplicación se estructure en una serie de servicios pequeños, independientes y autónomos. Así, la comunicación entre estos servicios y con el usuario se realiza a través de APIs bien definidas que

garantizan una interacción eficiente y modular, la (Fig. 3) ilustra el modelo de funcionamiento de esta arquitectura, donde cada microservicio cumple un rol específico dentro del sistema general.

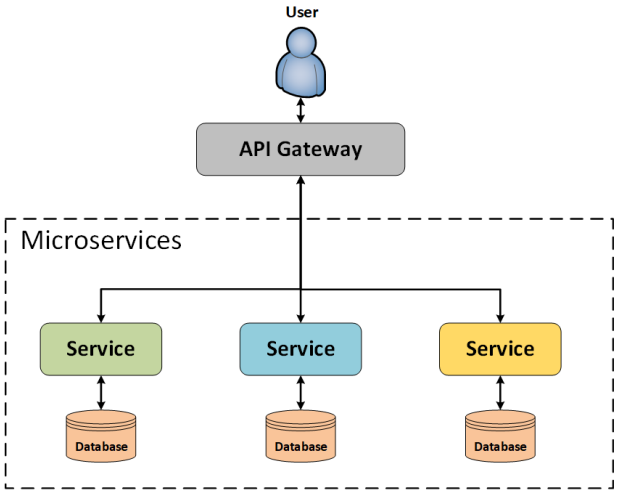

Fig. 3. Arquitectura basada en microservicios

En el contexto del sistema de control de acceso basado en biometría facial, la implementación se divide en dos componentes principales:

a) Servicio de Frontend

Este componente se encarga de la interfaz de usuario, permitiendo la interacción directa del usuario con la aplicación. El frontend está diseñado para ser intuitivo y accesible, proporcionando un entorno donde los usuarios pueden gestionar su acceso y realizar solicitudes de manera sencilla.

b) Proceso de elaboración del servicio Frontend

i. Definición del esquema de datos

La primera fase del desarrollo del servicio frontend es la definición del esquema de datos. Este paso determinó la estructura de la información que se iba a almacenar en la base de datos y que por consiguiente se iba a manejar del lado del frontend. Durante esta fase en colaboración con

el grupo de desarrolladores se determinó el conjunto de datos necesarios para el proceso de registro de los usuarios.

El diagrama de clases de la (Fig. 4) ofrece una perspectiva detallada de la clase Usuario en el contexto de la plataforma. Como aplicación que gestiona usuarios, eventos, juegos y funcionalidades de chatbot, la plataforma contempla dos tipos de usuarios: usuarios con EA y sus acompañantes. Cada uno de ellos tendrá acceso a una versión personalizada de la plataforma, acorde a su rol específico:

- *_id:* Es un identificador único para el registro de usuario, normalmente generado por la base de datos. Utiliza la notación ObjectId de MongoDB, indicando que este registro está almacenado en una base de datos MongoDB.
- *typeDocument:* Especifica el tipo de documento de identificación del usuario.
- *document*: Un identificador único relacionado con el documento de identificación del usuario.
- *firstName:* Almacena el nombre del usuario.
- *lastName:* Almacena los apellidos del usuario.
- *hashPassword:* Contiene una versión hash de la contraseña del usuario, asegurando que la contraseña real no se almacena en texto plano por razones de seguridad.
- *userType*: Un número entero que corresponde a un rol o nivel de acceso dentro de la aplicación.
- *refreshTokenExpiry*: Especifica el tiempo de expiración del token de actualización del usuario. Los tokens de actualización se utilizan en los sistemas de autenticación para permitir a los usuarios obtener un nuevo token de acceso sin tener que volver a iniciar sesión.
- *documentParticipant:* Un identificador de documento adicional que vincula al usuario con otro participante dentro de la aplicación.
- *scopes:* Una lista de cadenas que definen los permisos o niveles de acceso concedidos al usuario. Estos ámbitos permiten un control detallado de las acciones que el usuario puede realizar dentro de la aplicación.

Fig. 4 Diagrama de clase para el usuario

ii. Desarrollo del formulario de registro

Ya con el esquema establecido y con una paleta de colores y tamaños definidos por el equipo de desarrollo de Minciencias, basado en los principios de IHC para personas con EA, se asegura una experiencia visual accesible y cómoda para los usuarios. Los colores elegidos buscan evitar tonos estridentes que puedan causar confusión o incomodidad, mientras que los tamaños de fuente y elementos se han seleccionado para garantizar legibilidad y facilidad de interacción.

Como se mencionó anteriormente, la plataforma se diseñó para ofrecer diferentes versiones según el rol del usuario, lo que implica un diseño de interfaz basado en roles. En este contexto, el formulario de registro fue concebido para ser reactivo, proporcionando retroalimentación constante al usuario.

Para lograr una estructura modular y eficiente, se implementó una arquitectura basada en componentes. Se distinguen dos tipos principales de componentes:

iii. Componentes controlados

Un componente controlado es aquel cuyo estado es gestionado por React, interactúan directamente con el usuario, lo que incluye elementos como inputs o selects. Estos componentes

reaccionan a las acciones del usuario y actualizan su estado en tiempo real mediante eventos o callbacks [24].

iv. Componentes inteligentes

Además de los componentes controlados, fue necesario la creación de componentes inteligentes que son aquellos que gestionan el estado y la lógica de la aplicación. Estos componentes suelen ser responsables de obtener datos, manejar eventos y pasar datos y callbacks a los componentes presentacionales (también conocidos como componentes tontos o *dumb components*) [24]. En particular, se creó un componente inteligente encargado del proceso de captura y validación de imágenes, que se utiliza tanto en la página de registro como en la página de inicio de sesión, el cual utiliza los modelos de machine learning de la librería *face-api.js* para verificar si la imagen subida contiene un rostro. Al centralizar esta funcionalidad, se adhiere al principio DRY, evitando la duplicación de código y asegurando una implementación consistente en toda la plataforma.

De esta forma haciendo uso de una interfaz adaptativa basada en roles, haciendo uso de componentes inteligentes y controlados para manejar todas las posibles respuestas tanto del servidor como del cliente, asegurando que el sistema pueda reaccionar apropiadamente a cada escenario, como errores de autenticación, solicitudes de información adicional, o la confirmación exitosa del registro.

El flujo de trabajo completo para el registro e inicio de sesión, incluyendo cómo se gestionan las interacciones entre el cliente y la API, se detalla en el diagrama de flujo presentado en la Fig. 5.

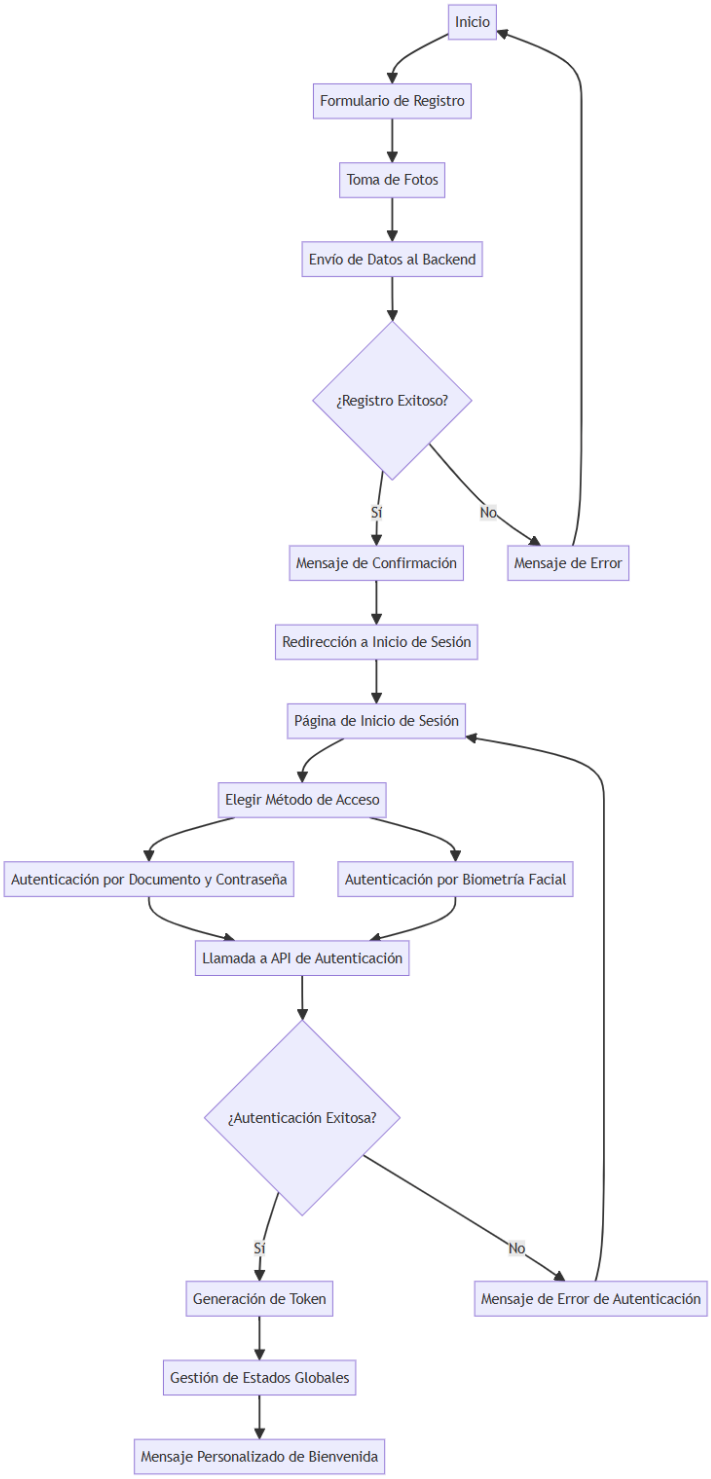

Fig. 5. Diagrama de flujo del proceso de registro e inicio de sesión

c) Servicio de Backend

Este componente maneja la lógica de negocio y la interacción con la base de datos. Su tarea principal es comparar los patrones faciales presentados con los registros almacenados en la base de datos para determinar la existencia de coincidencias.

Con respecto al almacenamiento de los datos, al contar con una arquitectura basada en microservicios, tal y como se menciona al inicio de esta sección, se entiende que cada servicio puede o no manejar su propia base de datos, en este caso al necesitar registrar los datos del usuario y luego utilizarlos en el reconocimiento facial se decidió manejar una base de datos no relacional Mongo la flexibilidad y escalabilidad que ofrece.

El servicio de backend procesa las solicitudes provenientes del frontend, ejecuta las búsquedas pertinentes en la base de datos y devuelve los resultados relevantes.
La conexión entre estos dos servicios se logra a través de APIs RESTful, permitiendo una comunicación eficaz y segura entre el frontend y el backend.

d) Proceso de elaboración del servicio Backend

Para desarrollar un prototipo inicial rápidamente y asegurar que el sistema sea fácilmente escalable, se ha elegido la combinación de Node.js y Express. La razón es que esta combinación es conocida por su eficiencia en el manejo de aplicaciones web de alta carga y su flexibilidad en la construcción de APIs RESTful.

Node.js es una plataforma de JavaScript que permite ejecutar código del lado del servidor, proporcionando un entorno eficiente para manejar múltiples solicitudes concurrentes sin bloquear el servidor. Por su lado, Express es un framework que ofrece un entorno minimalista para Node.js que facilita la creación de aplicaciones web y APIs.

Gracias al grupo de tecnologías elegidas, el proceso de establecer un servidor inicial no es tan complicado de realizar. Con esta base establecida, el siguiente paso es definir los endpoints necesarios para permitir la comunicación entre los distintos servicios involucrados.

Estos endpoints son puntos finales en la comunicación que sirven como acceso a los recursos de un servicio web. En términos prácticos, un endpoint es la URL a la que los clientes, como las aplicaciones frontend, envían solicitudes para interactuar con el servidor, permitiendo así la integración efectiva del sistema de reconocimiento facial con los servicios de interés.

Una petición es el acto de solicitar datos o acciones a través de estos endpoints. Las peticiones pueden variar en tipo, siendo las más comunes GET (para recuperar datos), POST (para enviar nuevos datos), PUT/PATCH (para actualizar datos existentes) y DELETE (para eliminar datos).

Inicialmente, en colaboración con el equipo de desarrollo del proyecto de Minciencias, se desarrolló un endpoint específico que permite capturar y almacenar los datos ingresados en el formulario de registro del frontend en la base de datos MongoDB. Para utilizar esta funcionalidad, el frontend debe realizar una petición POST a dicho endpoint, y adjuntar en el cuerpo de la petición la información del usuario. En la Fig. 6 se muestra a la izquierda la definición del endpoint junto con el método HTTP utilizado (POST), y a la derecha, el formato esperado del cuerpo de la petición, que contiene los datos del formulario de registro. Es importante notar que la información contenida en nuestro objeto JSON coincide con la mencionada en la Fig. 4, con la diferencia de que se añade un campo adicional destinado a contener las características faciales del usuario.

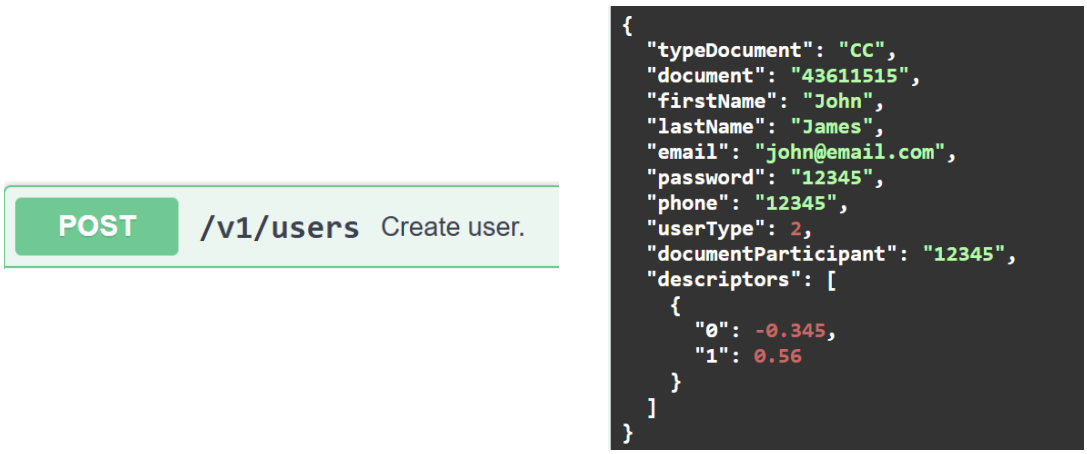

Fig. 6. Endpoint con el método POST para la creación de usuarios

Por parte del endpoint cuando una petición es procesada con éxito, el endpoint genera una respuesta en formato JSON que contiene detalles sobre cómo se ha almacenado el usuario en la base de datos. Por otro lado, en situaciones donde la petición no logra procesarse satisfactoriamente, el endpoint implementa una estructura de respuesta que incluye tanto un código de error específico como un mensaje descriptivo.

Fig. 7. Formato de respuestas del endpoint de creación de usuarios

Una vez establecida la funcionalidad de registro de usuarios a través de un endpoint específico en el backend, se procedió a integrar el componente de reconocimiento facial. Este componente, independientemente de la tecnología de machine learning subyacente (como OpenCV, TensorFlow o frameworks similares), es fundamental para capturar y procesar las características faciales del usuario durante el proceso de registro.

El flujo de registro se completa cuando el backend recibe las características faciales extraídas y las almacena de manera segura, asociándolas al perfil del usuario recién creado. De esta forma, en futuras autenticaciones, el sistema podrá comparar las características faciales proporcionadas por el usuario con las almacenadas, permitiendo así la verificación de identidad mediante reconocimiento facial.

Finalmente, el proceso de utilización de la creación de la API se condensa en la Fig. 8. Esta figura ofrece una representación visual de este proceso integral, detallando la interacción entre el usuario, la interfaz de usuario, el backend y los servicios externos involucrados. Desde la

perspectiva del usuario, el flujo comienza con el registro, donde se capturan los datos biométricos faciales. A continuación, el backend procesa esta información y la almacena de forma segura. En etapas posteriores, durante el inicio de sesión o en cualquier otra acción que requiera autenticación, el sistema vuelve a capturar las características faciales del usuario y las compara con las almacenadas, completando así el proceso de reconocimiento facial.

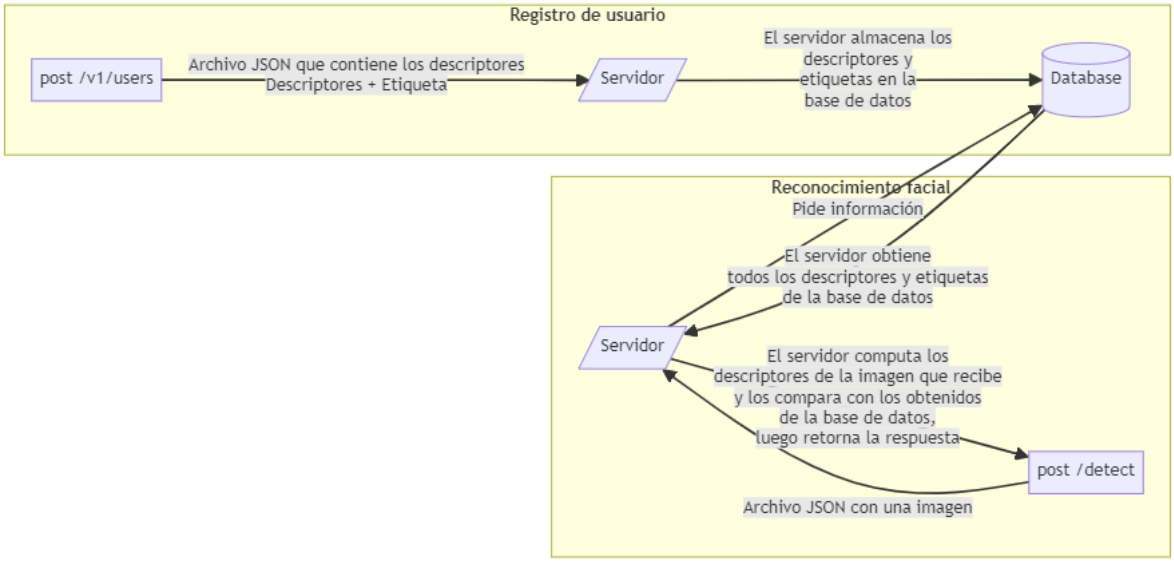

Fig. 8. Flujo de trabajo de la API

Finalmente, el procedimiento para ingresar a la plataforma ya sea para registrarse o para autenticarse haciendo uso de la biometría facial o de un método tradicional como documento y contraseña, implica una compleja interacción entre el usuario y distintos servicios. Los servicios involucrados en este proceso se pueden interpretar como capas en el diagrama de secuencia representado en la Fig. 8Fig. 9 que muestra cómo se gestionan las solicitudes desde el frontend hasta el backend y como se integran los servicios de reconocimiento y autenticación.

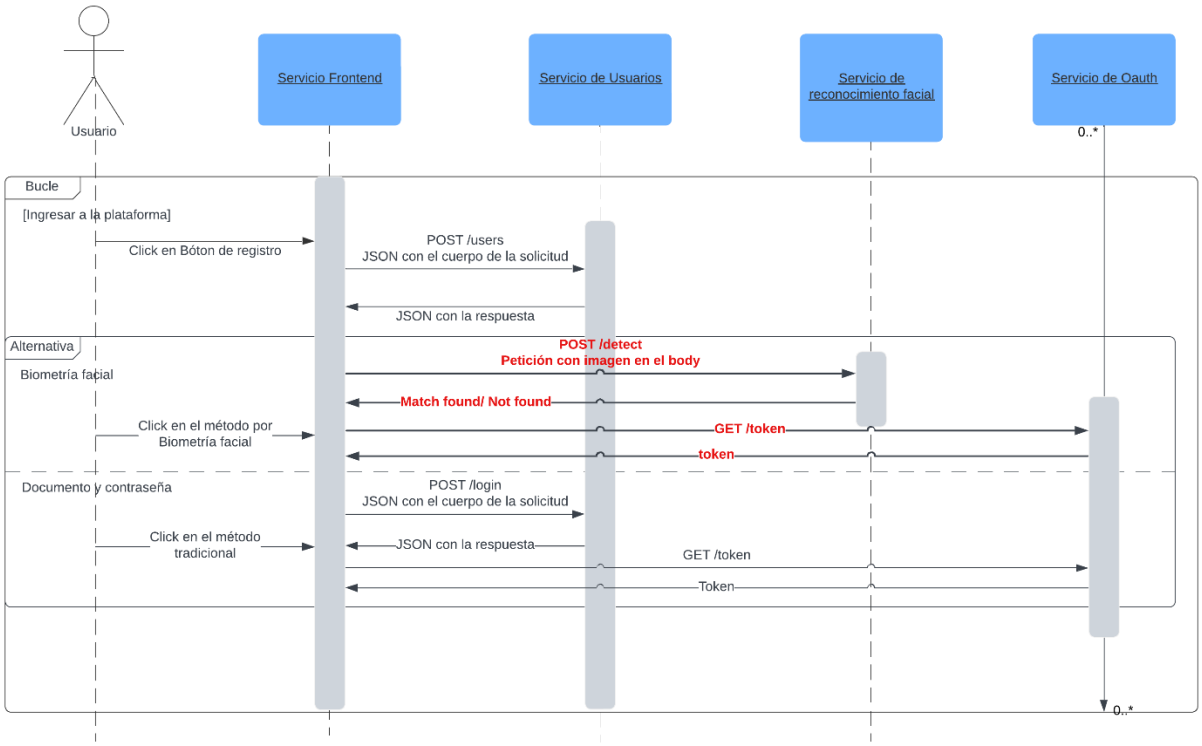

Fig. 9. Diagrama de secuencia de registro e ingreso por biometría facial y tradicional de la plataforma

5. Pruebas y validación

Durante el desarrollo del sistema de control de acceso basado en reconocimiento facial, se llevaron a cabo diversas pruebas tanto técnicas como con usuarios finales para asegurar su robustez y eficacia.

En primer lugar, en colaboración con el equipo de desarrolladores se realizaron pruebas para garantizar la solidez técnica del sistema. Estas pruebas incluyeron la verificación de la integración entre el frontend y el backend, la evaluación del rendimiento del sistema en diversas condiciones, y la implementación de medidas de seguridad para proteger los datos biométricos.

Además de las pruebas técnicas, se realizaron pruebas de usabilidad con sujetos de prueba que padecen la enfermedad de Alzheimer y con sus acompañantes. Estas pruebas no solo evaluaron la efectividad del sistema de reconocimiento facial, sino que también compararon este método con el método tradicional de autenticación basado en documento y contraseña. Estas pruebas sirvieron

para identificar y abordar posibles aspectos de mejora en términos de Interacción Humano-Computadora (IHC).

6. Iteración y ajustes

A partir de las pruebas técnicas y de usabilidad se pudo ajustar y refinar la interfaz del sistema, asegurando que fuera intuitiva y fácil de usar para los pacientes con Alzheimer. A través de la retroalimentación obtenida, se hicieron modificaciones que mejoraron significativamente la experiencia del usuario.

VI. RESULTADOS Y ANÁLISIS

En el contexto de los objetivos de este proyecto de investigación, se analizaron los diferentes framework de reconocimiento facial disponibles en la actualidad y que cuentan con la capacidad de ejecutarse en el navegador web, esto debido a las ventajas que presenta esta modalidad frente a los framework que requieren de un procesamiento remoto.

Con esta investigación se encontró que una de las ventajas de esta modalidad en el reconocimiento facial fue que todos los datos faciales se procesan localmente en el dispositivo del usuario, lo cual contribuye a reducir el riesgo de exposición de datos personales, esto disminuye la transmisión de datos sensibles a través de la red y disminuye el riesgo de intercepciones y ataques de seguridad. Además de la seguridad que ofrecen, también permiten una respuesta más rápida ya que se elimina la dependencia de la latencia de la red, lo que se traduce en una respuesta más rápida y fluida para el usuario. Finalmente, al procesarse los datos localmente se reduce la carga computacional sobre los servidores, mejorando la escalabilidad de la plataforma y optimizando el uso de recursos.

A continuación, se presentan los diferentes frameworks investigados, junto con una breve descripción de cada uno. Los resultados de esta comparación se detallan al final en la (TABLA II).

OpenCV.js

Esta librería es una adaptación del popular framework de visión artificial OpenCV para ejecutarse en el navegador web. Utiliza Emscripten y WebAssembly para compilar el código C++ de OpenCV a JavaScript, lo que permite aprovechar las potentes funciones de procesamiento de imágenes y reconocimiento facial de OpenCV en aplicaciones web [25].

Debido a la inclusión de casi todas las características de OpenCV, el tamaño de OpenCV.js es considerablemente mayor que el de otras librerías. Esto puede afectar negativamente el tiempo de carga de las páginas web y el consumo de ancho de banda.

TensorFlow.js

TensorFlow.js es una librería JavaScript creada por Google que permite ejecutar modelos de aprendizaje automático en el navegador web. Esto permite una gran variedad de posibilidades para el desarrollo de aplicaciones web inteligentes, incluyendo el reconocimiento facial [25].

TensorFlow.js permite utilizar una amplia gama de modelos de aprendizaje automático, incluyendo modelos pre-entrenados y personalizados, además de que puede aprovechar los recursos de hardware del navegador, como la GPU, para lograr un rendimiento acelerado. No obstante, cuenta con una curva de aprendizaje moderada, lo que implica que la comprensión de algunos conceptos de aprendizaje automático pueden ser un desafío para los desarrolladores.

ConvNet.js

ConvNet.js es una librería JavaScript ligera y fácil de usar diseñada específicamente para el reconocimiento facial en el navegador web. Se basa en redes convolucionales neuronales (CNNs) para detectar y reconocer rostros en imágenes y videos [25].

ConvNet.js ofrece una API simple y fácil de entender además de que su tamaño es considerablemente menor que el de otras librerías. A pesar de esto con el crecimiento de TensorFlow.js, y por no ofrecer las funcionalidades de su competencia, esta librería se descontinuó [26].

Face-api.js

El módulo Face-api.js V0.20 utiliza redes neuronales convolucionales para abordar la detección y reconocimiento de rostros, así como la identificación de puntos de referencia faciales. Este módulo se basa en el núcleo de TensorFlow.js para proporcionar capacidades eficientes de detección de rostros y reconocimiento de expresiones faciales y está optimizado para funcionar en aplicaciones web y móviles [27].

TABLA II COMPARATIVA DE FRAMEWORKS PARA EL RECONOCIMIENTO FACIAL EN EL NAVEGADOR

CARACTERÍSTICA	OPENCV.JS	TENSORFLOW.JS	CONVNET.JS	FACE-API.JS
FUNCIONALIDADES	Amplia gama de funciones de procesamiento de imágenes y reconocimiento facial	Ejecución de modelos de aprendizaje automático para reconocimiento facial	Reconocimiento facial básico con redes convolucionales neuronales	Detección y reconocimiento de rostros, estimación de emociones, seguimiento facial
RENDIMIENTO	Alto rendimiento gracias a WebAssembly	Rendimiento acelerado con la GPU del navegador	Eficiencia en tareas de reconocimiento facial	Rendimiento adecuado para diversas tareas de reconocimiento facial
TAMAÑO	Tamaño considerablemente grande	Tamaño moderado	Tamaño ligero	Tamaño moderado
CURVA DE APRENDIZAJE	Pronunciada debido a la gran cantidad de funciones	Moderada, requiere conocimientos de aprendizaje automático	Simple y fácil de usar	Moderada, requiere conocimientos de JavaScript y conceptos básicos de aprendizaje automático
FLEXIBILIDAD	Permite la utilización de modelos pre-entrenados y personalizados	Alta flexibilidad para personalizar modelos y realizar tareas complejas	Menos flexible, no permite la personalización de modelos	Permite la personalización de modelos y la creación de nuevas funcionalidades
CASOS DE USO	Aplicaciones web que requieren procesamiento de imágenes complejo y de alto rendimiento	Aplicaciones web que necesitan realizar tareas de reconocimiento facial complejas	Aplicaciones web con recursos limitados que buscan una librería ligera y fácil de integrar	Aplicaciones web que requieren una amplia gama de funcionalidades de reconocimiento facial
USABILIDAD	Intermedio	Intermedio	Principiante	Principiante
DISCONTINUADA	No	No	Sí	No

A partir de la tabla comparativa, se seleccionó el módulo de Face-api.js porque sus características ofrecen mejores beneficios para ejecutarse en el navegador web. A continuación, se presenta una explicación más detallada de su funcionamiento y de las ventajas que ofrece en el reconocimiento facial.

La función de detección de rostros de este módulo utiliza un detector de multicaja de disparo único (SSD) basado en la arquitectura MobileNetV1. Este detector puede calcular la ubicación precisa de cada rostro en una imagen, devolviendo los recuadros delimitadores junto con las probabilidades correspondientes. A pesar de que el modelo prioriza la precisión en la detección de rostros, no está diseñado para optimizar el tiempo de inferencia [26].

Así, el reconocimiento facial en Face-api.js se basa en una arquitectura similar a ResNet-34, capaz de calcular un vector descriptor de características de 128 dimensiones a partir de cualquier imagen facial. Este vector describe las características faciales de una persona y no se limita al conjunto de rostros utilizados durante el entrenamiento, permitiendo el reconocimiento de cualquier individuo [26].

Face-api.js es un proyecto de software de código abierto, lo que significa que cualquiera puede usarlo, modificarlo y distribuirlo bajo la licencia MIT. Además, aceptan contribuciones de la comunidad a través del repositorio de GitHub del proyecto.

Capacidades

Face-api.js ofrece varios modelos con capacidades específicas, entre las cuales se incluyen:

- Detección de Rostros: Identifica la presencia y ubicación de rostros en una imagen o video.
- Detección de Puntos de Referencia de Rostros: Reconoce y marca características faciales clave, como ojos, nariz y boca.
- Reconocimiento de Rostros: Permite identificar y verificar identidades faciales comparando rostros en diferentes imágenes.
- Reconocimiento de Expresiones Faciales: Detecta y clasifica diversas expresiones faciales, como alegría, tristeza, enojo, entre otras.
- Estimación de Edad: Predice la edad aproximada de una persona basándose en sus rasgos faciales.

Optimización y Uso

Al estar optimizado para la web y dispositivos móviles, Face-api.js es versátil y puede ser utilizado en una amplia variedad de aplicaciones, desde simples páginas web hasta complejas aplicaciones móviles. Esto hace que sea una herramienta poderosa para desarrolladores que buscan incorporar capacidades avanzadas de visión por computadora en sus proyectos.

Resultados del frontend

Para el desarrollo del formulario de registro e ingreso, se optó por la combinación de React y Tailwind CSS. React, una biblioteca de JavaScript para la construcción de interfaces de usuario se encargó de la gestión eficiente de los componentes, permitiendo una actualización dinámica y eficiente del DOM. Por su parte, Tailwind CSS aportó con su flexibilidad en el diseño personalizado, permitiendo aplicar estilos de manera rápida y coherente sin necesidad de escribir CSS desde cero.

La librería de React-hook-form se incorporó como herramienta clave para el maquetado y gestión del formulario. Esta librería permitió la validación y gestión de errores en tiempo real, y también mejoró la experiencia de usuario al proporcionar retroalimentación constante, reduciendo la frustración y aumentando la facilidad de uso. Además, se implementó Redux para el manejo global de estados de la aplicación. Redux es una librería de JavaScript que permite gestionar el estado de manera predecible y centralizada [28]. En este proyecto, se utiliza específicamente para gestionar el estado de autenticación del usuario, es decir, determinar si el usuario está autenticado o no. Este aspecto presenta importancia en una interfaz que renderiza contenido basado en roles, ya que facilita la comunicación entre componentes y garantiza la correcta renderización de la interfaz según el estado del usuario.

Gracias a Redux, el estado del usuario se encuentra centralizado y accesible para todos los componentes que lo requieran, lo que permite una funcionalidad dinámica y consistente. La centralización del estado ayuda a evitar problemas comunes en aplicaciones más grandes, como la inconsistencia de datos y la dificultad de mantener sincronizados diferentes componentes.

En la Fig. 10 se muestra como la combinación entre React y Tailwind CSS permitió realizar una maquetación acorde a los estándares establecidos y en la Fig. 11 se muestra como existe una retroalimentación constante en el manejo de errores y campos faltantes.

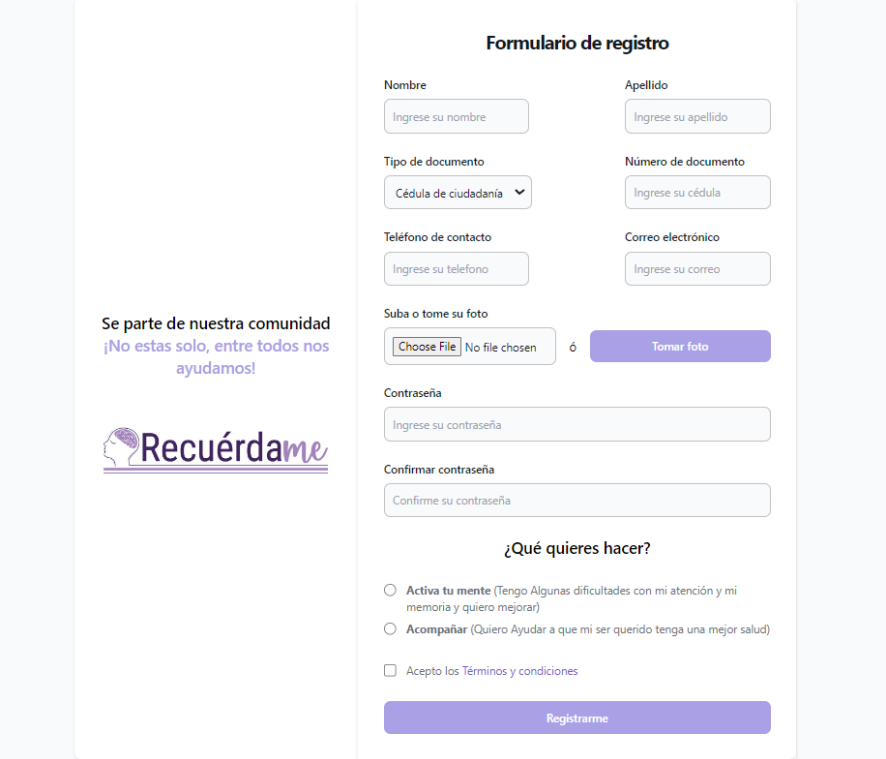

Fig. 10. Formulario de registro de la plataforma

Fig. 11. Manejo de errores y retroalimentación constante

Por ejemplo, en el formulario de registro, existe un campo de input radio que, al seleccionar una de las opciones, cambia dinámicamente el contenido del formulario. Específicamente, si se escoge el rol de acompañante, aparece un nuevo campo para ingresar el documento del participante, estableciendo así una relación entre ambos roles. En la Fig. 12 se muestra el funcionamiento de este componente controlado.

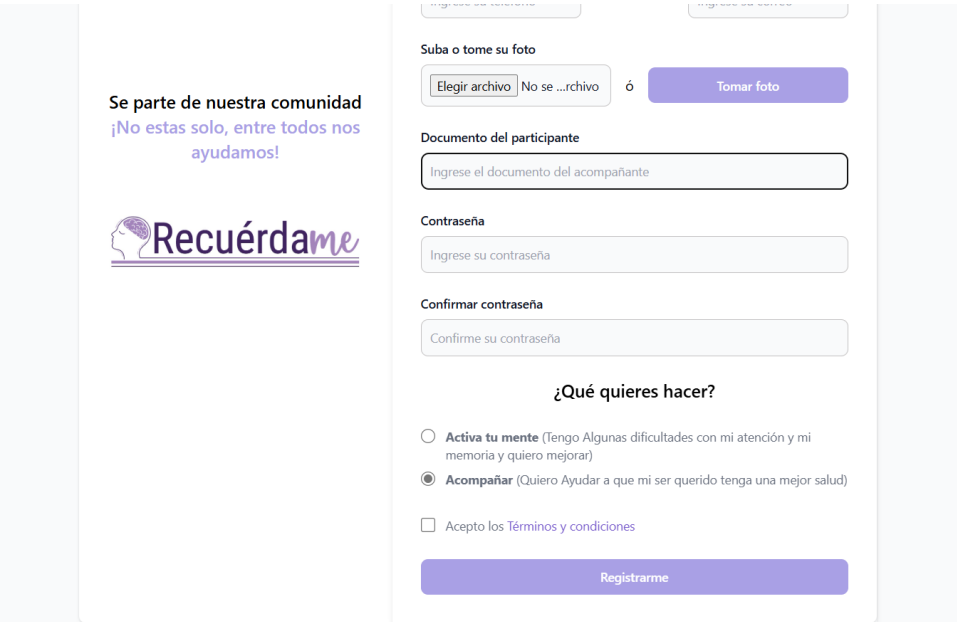

Fig. 12. Componente controlado input radio

Para facilitar el proceso de registro y garantizar la seguridad de los usuarios, se desarrolló un componente inteligente encargado de capturar imágenes faciales. Este componente, que integra la librería face-api.js, permite extraer las características faciales distintivas de cada usuario a partir de una fotografía tomada con la cámara del dispositivo. Las figuras (Fig. 13 y Fig. 14) ilustran el funcionamiento de este componente en la interfaz de registro, donde el usuario puede capturar y revisar su imagen de registro. Las instrucciones que acompañan al proceso de captura, diseñadas de acuerdo con los principios de interacción humano-computadora, garantizan una experiencia de usuario intuitiva y accesible.

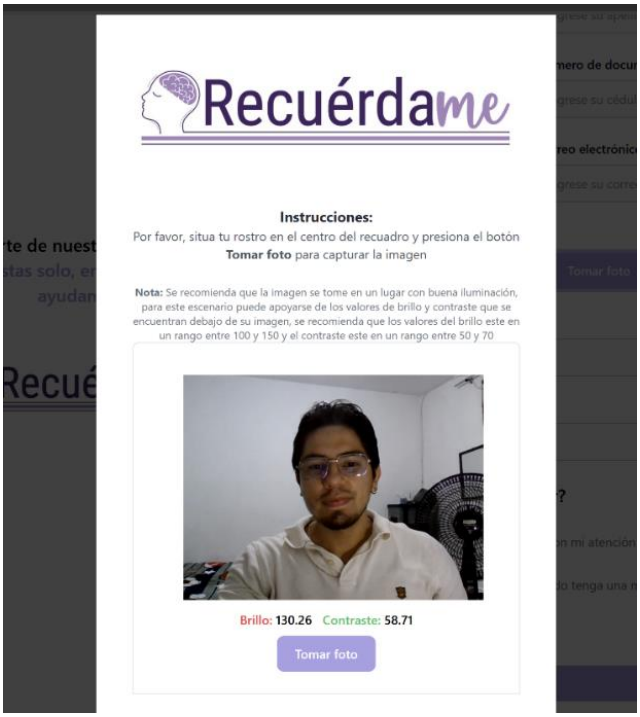

Fig. 13. Módulo para tomar fotografías utilizando la API Canvas.

Fig. 14. Visualización de la imagen capturada y opciones de imagen.

El componente de captura facial, además de extraer las características faciales del usuario, incorpora un sistema de validación de imágenes. Este sistema analiza cada imagen capturada para determinar si contiene al menos un rostro humano. En caso de que se detecte un rostro, el componente proporciona una confirmación visual al usuario y procede a extraer las características faciales necesarias para el proceso de registro. Por el contrario, si no se detecta ningún rostro, el componente muestra un mensaje de error amigable, indicando al usuario que debe intentar capturar una imagen más clara y frontal.

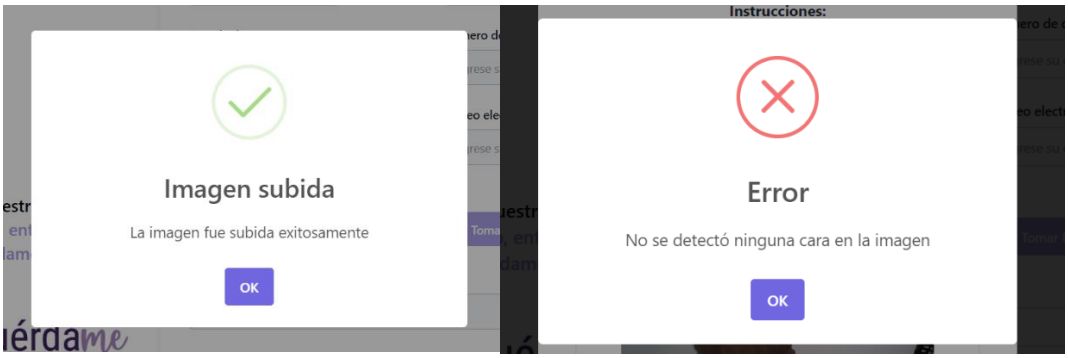

Fig. 15. Notificaciones de carga de imagen

Una vez que el usuario completa el proceso de registro y envía los datos al servidor, se inicia una petición al backend para crear una nueva cuenta. Si el servidor procesa la solicitud de manera exitosa, se muestra un mensaje de confirmación al usuario, como el que se presenta en la Fig. 16 Este mensaje generalmente indica que el registro se ha completado con éxito y que ya puede iniciar sesión. A continuación, el sistema redirecciona automáticamente al usuario a la página de inicio de sesión, donde podrá utilizar sus nuevas credenciales para acceder a la plataforma.

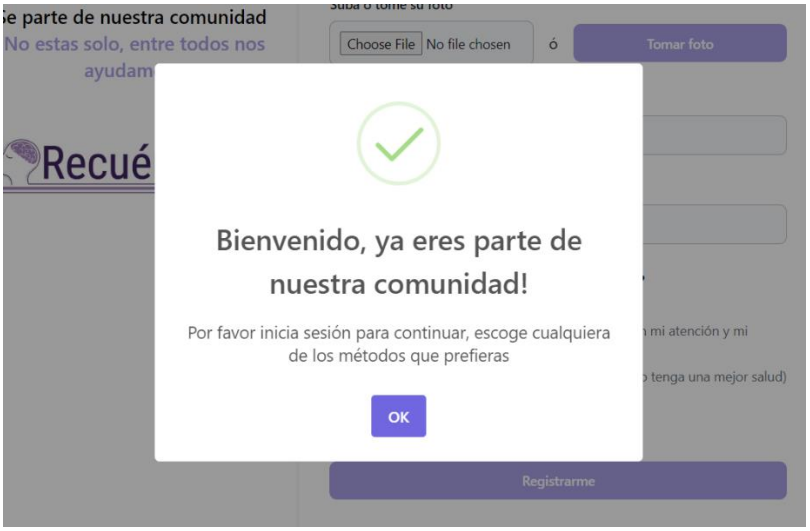

Fig. 16. Mensaje de Bienvenida.

Para ofrecer una mayor flexibilidad a los usuarios, se ha implementado un sistema de autenticación que permite elegir entre diferentes métodos de acceso. Al ingresar a la página de inicio de sesión, los usuarios se encontrarán con una interfaz intuitiva Fig. 17 que presenta claramente las opciones disponibles. Al pasar el cursor sobre cada método, se despliega una breve descripción que detalla los requisitos y beneficios de cada uno Fig. 18 y Fig. 19. Esta personalización de la experiencia de inicio de sesión brinda a los usuarios la libertad de seleccionar el método que mejor se adapte a sus preferencias y necesidades.

Fig. 17. Página para seleccionar el método de acceso

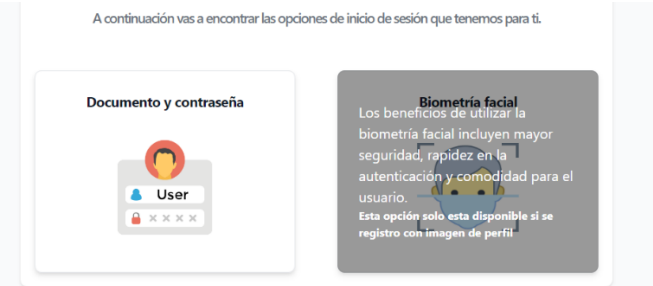

Fig. 18. Información del método de biometría facial para acceder a la plataforma

Fig. 19. Información del método por Documento y contraseña para acceder a la plataforma

Al seleccionar la opción de inicio de sesión por biometría facial, el sistema presenta al componente inteligente mostrado en las figuras Fig. 13 y Fig. 14 que le permite capturar una imagen de su rostro. Durante este proceso, se activa un indicador de carga (Fig. 20) para mantener al usuario informado sobre el estado de la operación.

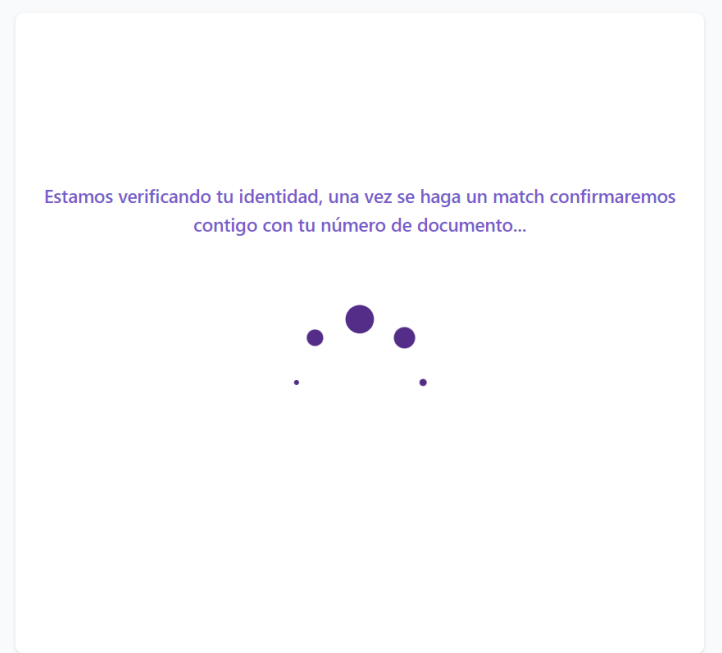

Fig. 20. Retroalimentación del proceso mientras se encuentra una coincidencia

Finalmente, si se encuentra una coincidencia en la base de datos, se presenta al usuario la información para que verifique si corresponden a los últimos cuatro dígitos de su número de documento. Como se ilustra en la Fig. 21, esta validación adicional del usuario es necesaria para acceder al servicio OAuth de la plataforma, lo que permite mantener la sesión activa durante 6 horas.

Este proceso asegura una capa extra de seguridad, permitiendo que los usuarios verifiquen su identidad mediante reconocimiento facial antes de acceder a sus cuentas. Con el servicio de OAuth, se facilitará una experiencia de autenticación fluida y segura con la que los consumidores disfrutarán de un largo tiempo de sesión sin que se vuelva a autenticarse continuamente.

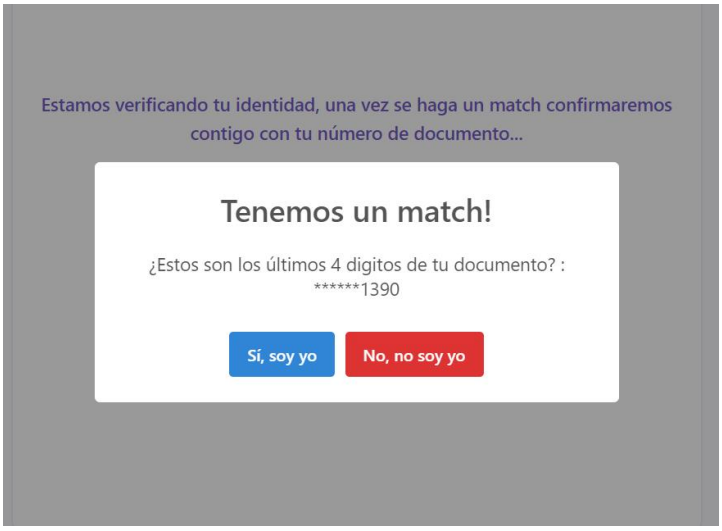

Fig. 21. Confirmación de identidad

Si la verificación es positiva, se realiza una llamada a la API para generar un token de autenticación personalizado para el usuario. Este token permite gestionar los estados globales de la aplicación y garantiza que el usuario esté correctamente autenticado durante su sesión. Una vez autenticado, el usuario es recibido con un mensaje personalizado que incluye su nombre, como se muestra claramente en la Fig. 22.

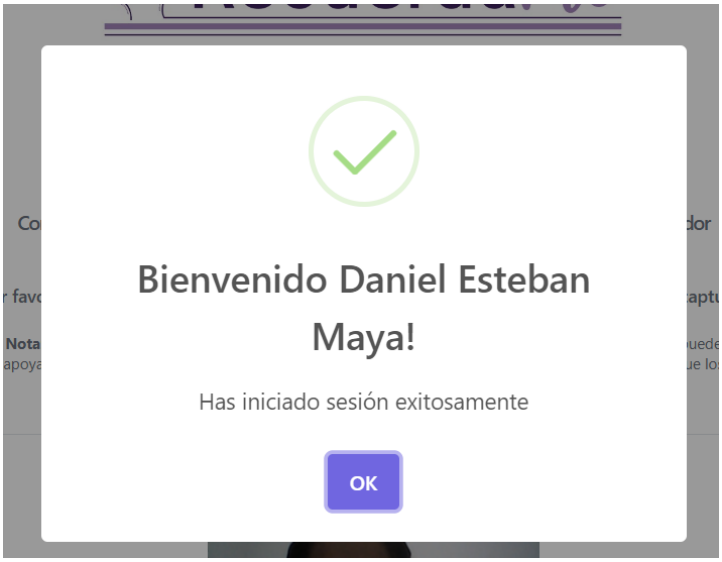

Fig. 22. Bienvenida a la plataforma

Resultados del backend

La integración de face-api.js presentó desafíos técnicos interesantes. Uno de los principales retos fue optimizar el proceso de extracción de características faciales para garantizar un rendimiento adecuado en tiempo real. Fig. 23 presenta una visión general simplificada del proceso de extracción de características faciales utilizando face-api.js.

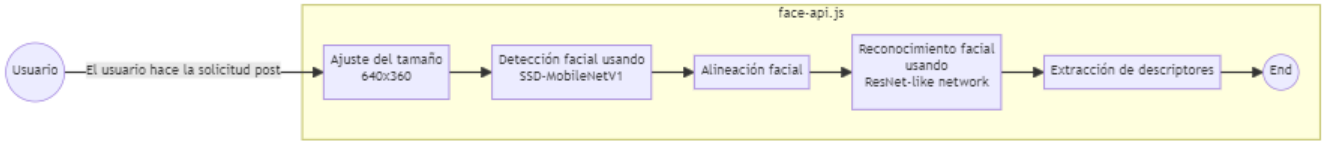

Fig. 23. Modelo conceptual del funcionamiento del sistema

Así, en la práctica se determinó como era posible realizar un procesamiento y comparación con los registros almacenados en la base de datos, para este proceso se diseñó una función que lo haga automáticamente cuando el usuario haga una solicitud por medio del frontend.

Para entender la función *getDescriptorsAndReturnBestMatch()* es necesario desglosarla en sus componente principales y describir su funcionalidad paso a paso. Este código se centra en dos aspectos clave: la carga de modelos preentrenados para detección facial, y la implementación del sistema de reconocimiento facial.

Dentro de la función existe una función asíncrona que carga los modelos preentrenados desde el servidor, ya que son necesarios para realizar las tareas relacionadas con el procesamiento de imágenes faciales.

En el otro aspecto, primero recupera todos los usuarios de la base de datos y filtra aquellos que tienen descriptores faciales almacenados y luego crea un array *LabeledFaceDescriptors* usando estos descriptores. Los descriptores son convertidos a *Float32Array* para ser compatibles con la biblioteca *face-api.js*.

A continuación, la creación del *FaceMatcher* se realizó estableciendo un umbral de coincidencia del 60% con los descriptores etiquetados. Esta elección se basó en las recomendaciones de la documentación oficial de face-api.js, que sugiere este valor como un punto de partida para lograr un equilibrio adecuado entre la tasa de aciertos y la tasa de falsos positivos. Al recibir una imagen, esta se ajusta a un tamaño estándar para optimizar el proceso de detección. A continuación, se localizan los puntos de referencia faciales clave, que sirven como base para calcular un descriptor numérico que representa las características únicas del rostro. Este descriptor se compara con los descriptores almacenados en la base de datos, utilizando una distancia euclidiana para determinar la similitud. Si la distancia es menor que el umbral establecido, se considera que se ha encontrado una coincidencia. Si no se encuentra ninguna coincidencia o si ocurre un error durante el proceso, se devuelve un mensaje apropiado. La Fig. 24 ilustra este proceso de forma esquemática. Es importante destacar que la elección del umbral de coincidencia es un compromiso entre la seguridad y la usabilidad del sistema. Un umbral más bajo aumentaría la tasa de falsos positivos, mientras que un umbral más alto podría ocasionar un mayor número de falsos negativos. En nuestro caso, el valor de 60% se considera óptimo para las necesidades de nuestra aplicación.

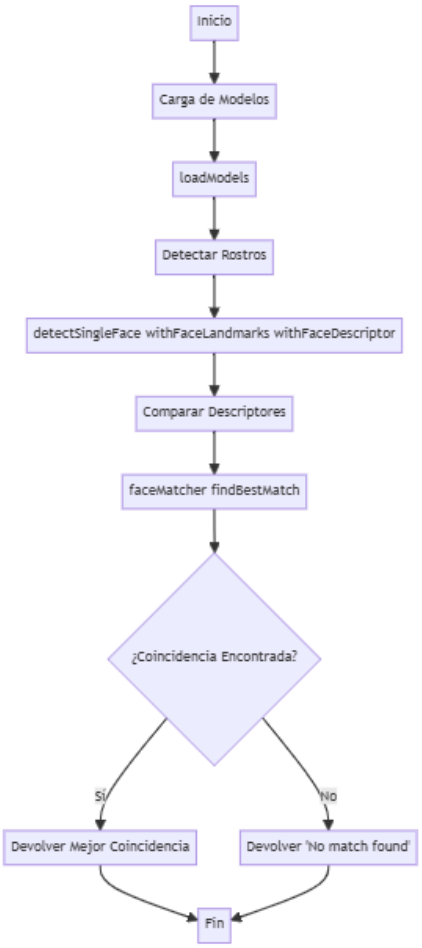

Fig. 24. Flujo de trabajo del reconocimiento facial

El endpoint ilustrado en la Fig. 25 encapsula la lógica completa del proceso de reconocimiento facial descrito anteriormente. Al recibir una imagen como entrada, este endpoint se encarga de preprocesar la imagen, detectar los rostros, extraer los descriptores faciales y compararlos con la base de datos, devolviendo un resultado de autenticación.

```
// GET Best Match
app.post('/detect', async (req, res) => {
    if (!req.files || Object.keys(req.files).length === 0) {
        return res.status(400).send('No files were uploaded.');
    }
    const image = req.files.image.tempFilePath;
    const bestMatch = await getDescriptorsAndReturnBestMatch(image);
    if (bestMatch.message === 'No match found') {
        return res.status(404).json(bestMatch);
    }
    res.json(bestMatch);
    cleanTemporaryFiles();
});
```

Fig. 25. Definición del endpoint /detect que permite el reconocimiento facial

Resultados de pruebas y validación

Para evaluar la usabilidad y efectividad de los métodos de registro, tanto por reconocimiento facial como por formulario tradicional, se implementó una estrategia combinada. En primer lugar, se empleó la técnica de "piensa en voz alta" para obtener una visión cualitativa de la experiencia del usuario. Esta técnica consistió en solicitar a los participantes que verbalizaran sus pensamientos y acciones mientras interactuaban con el sistema, lo que permitió identificar dificultades, confusiones y oportunidades de mejora de manera detallada.

Adicionalmente, se cuantificó la percepción de facilidad de uso mediante la escala de Likert de 7 puntos de la herramienta Single Ease Question (SEQ). Los usuarios calificaron en esta escala tanto el proceso de registro por biometría facial como el convencional, lo que permitió obtener una medida numérica de la experiencia percibida. Se consideró que una puntuación igual o superior a 5 indicaba una percepción de facilidad de uso, mientras que una puntuación inferior a 5 señalaba la presencia de dificultades.

El grupo de usuarios utilizados en las pruebas de validación estuvo conformado por 4 voluntarios: dos personas con EA y sus respectivos acompañantes. La TABLA III presenta un perfil detallado de cada participante con EA, incluyendo fecha de la prueba, género, edad, nivel

educativo, tipo de Alzheimer y puntuación en la escala de evaluación de la demencia de Clinical Dementia Rating (CDR).

TABLA III
PERSONAS CON TRANSTORNO NEUROCOGNITIVO MAYOR POR ENFERMEDAD DE ALZHEIMER

Paciente con EA	Fecha	Genero	Edad (años)	Escolaridad (años)	Tipo de Alzheimer	CDR*
1	11/07/2024	Masculino	74	19	Tardío	1
2	11/07/2024	Masculino	46	14	Temprano	1

***** CDR significa Clinical Dementia Rating Scale.

La TABLA IV presenta los datos demográficos de los acompañantes, así como su relación con los participantes con EA

TABLA IV
CUIDADORES Y FAMILIARES

Acompañante	Fecha	Genero	Edad (años)	Escolaridad (años)	Relación con el paciente
1	11/07/2024	Femenino	75	16	Esposa
2	11/07/2024	Femenino	51	14	Esposa

En la TABLA V se consolidan los resultados obtenidos a través de la escala SEQ, donde los participantes evaluaron la facilidad de uso de la plataforma. Además de las puntuaciones numéricas, se han incluido los comentarios cualitativos expresados por cada usuario.

TABLA V
PUNTUACIONES DE LA ESCALA SEQ Y COMENTARIOS

Grupo (Paciente / Acompañante)	Número	Puntuación SEQ	Comentarios
Paciente	1	7	Se sintió muy cómodo con la autenticación por biometría facial
Acompañante	1	7	El proceso de registro es complicado, pero una vez se registra el inicio de sesión es rápido e intuitivo
Paciente	2	4	Comenta que la interfaz no solo puede ser para personas con EA sino que también para personas de avanzada edad
Acompañante	2	6	Recomienda poner instrucciones para la captura de la imagen

Finalmente, uno de los principales objetivos de este estudio fue comparar la aceptación de diferentes métodos de autenticación. Los resultados obtenidos al respecto son claros: la autenticación biométrica facial resultó ser la opción preferida por todos los participantes.

Si bien uno de los participantes obtuvo una puntuación baja en la escala SEQ debido a una confusión en la comprensión de la pregunta, los resultados generales de la evaluación mostraron una clara preferencia por la autenticación biométrica facial. Este hallazgo se vio respaldado por las observaciones realizadas durante las pruebas, donde los usuarios destacaron la facilidad y rapidez de este método.

Un caso particularmente ilustrativo fue el de un paciente con EA que, a pesar de su condición, demostró un fuerte deseo de autonomía al intentar crear su propia contraseña. Sin embargo, al utilizar el método tradicional de usuario y contraseña, experimentó dificultades para recordar sus credenciales, lo que resalta la complejidad que puede representar este método para personas con esta enfermedad.

Las entrevistas complementarias realizadas a los participantes que obtuvieron puntuaciones más bajas en la SEQ permitieron identificar factores adicionales que influyeron en la percepción de usabilidad, como problemas relacionados con la calidad de la imagen y la complejidad de los formularios. Estos hallazgos, junto con las observaciones cualitativas obtenidas a través de la

técnica de "piensa en voz alta", sugieren que la autenticación biométrica facial ofrece una experiencia de usuario más intuitiva y menos frustrante para personas con EA.

Es importante señalar que, durante las pruebas, se identificaron pequeñas áreas de mejora que podrían optimizar aún más la experiencia del usuario. En particular, se observó la necesidad de prestar atención a factores como el brillo y la iluminación del entorno, la calidad de la imagen capturada, y la correcta posición del paciente frente a la cámara.

VII. CONCLUSIONES

En conclusión, esta investigación ha demostrado que la autenticación biométrica facial ofrece una alternativa prometedora para mejorar la accesibilidad y usabilidad de las tecnologías digitales para personas con Enfermedad de Alzheimer. Si bien la presencia de un acompañante resultó esencial durante el proceso de registro inicial, la autenticación biométrica posterior brinda a los usuarios una mayor autonomía y facilita su interacción con dispositivos digitales, lo que podría aliviar algunas dificultades que presentan los métodos tradicionales, como la dificultad para recordar contraseñas.

Sin embargo, es importante abordar las preocupaciones relacionadas con la seguridad y la privacidad de los datos biométricos. Al garantizar la seguridad de los datos, obtener el consentimiento informado de los usuarios y ofrecer opciones de autenticación alternativas, se puede maximizar los beneficios de la biometría y minimizar los riesgos.

Dada la importancia de la privacidad y la autonomía de los usuarios, es importante que la autenticación biométrica sea una opción no obligatoria. Los usuarios deben tener la libertad de elegir el método de autenticación que consideren más adecuado, ya sea biométrico o tradicional.

Es importante continuar investigando y desarrollando soluciones tecnológicas que se adapten a las necesidades específicas de las personas con Alzheimer. Al centrarnos en el diseño centrado en el usuario y en la colaboración interdisciplinaria, podemos crear herramientas que empoderen a las personas con EA y mejoren significativamente su calidad de vida.

VIII. RECOMENDACIONES

El método de búsqueda actual presenta una complejidad lineal, lo que significa que el tiempo necesario para encontrar una coincidencia aumenta proporcionalmente al número de usuarios. A medida que la base de datos crece, el sistema se vuelve más lento y menos eficiente. Para abordar este problema, se recomienda la implementación de algoritmos de búsqueda más eficientes, como búsquedas binarias o estructuras de datos más optimizadas (por ejemplo, tablas hash o árboles balanceados), que permitan reducir significativamente el tiempo de respuesta y mejorar la experiencia del usuario.

En cuanto al proceso de registro, se sugiere simplificarlo solicitando únicamente la información esencial en la fase inicial. Esto permitirá que el usuario cree su cuenta y comience a utilizar la plataforma rápidamente. Posteriormente, se podrá invitar al usuario a completar su perfil con mayor detalle, según lo desee, ofreciendo una experiencia más fluida y menos intimidante en la primera interacción con la plataforma.

Además, es recomendable implementar mejoras en el sistema de autenticación biométrica para asegurar la calidad y precisión de las imágenes capturadas. Se debe prestar atención a factores como el brillo y la iluminación del entorno en el que se realiza la autenticación, ya que una iluminación deficiente puede afectar negativamente la precisión del reconocimiento facial. Para ello, se podrían ofrecer sugerencias al usuario sobre cómo optimizar la iluminación del lugar y la posición frente a la cámara, garantizando que las condiciones sean óptimas para un escaneo preciso.

Por otro lado, para prevenir posibles casos de suplantación de identidad, es necesario implementar métodos adicionales de verificación. Se sugiere el uso de técnicas que analicen la profundidad de la imagen, como la tecnología de detección en 3D, lo que permitiría identificar si la imagen es real o una reproducción plana (como una fotografía o un video). También se podría integrar un protocolo para la toma de fotos, en el cual el usuario reciba instrucciones específicas para asegurar que se trata de su identidad. Por ejemplo, pedirle que realice ciertos movimientos faciales o que ajuste su posición de manera que el sistema pueda confirmar su autenticidad de manera más rigurosa.

REFERENCIAS

[1] D. J. Selkoe, "Alzheimer's disease: a central role for amyloid," Journal of Neuropathology and Experimental Neurology, vol. 53, no. 5, pp. 438–447, Sep. 1994, doi: 10.1097/00005072-199409000-0000 de 3.

[2] A. Camacho, A. G. M. José, and R. Oliveira, "Las TIC orientadas a las personas mayores con demencia temprana de Alzheimer," 2024. https://sedici.unlp.edu.ar/handle/10915/162901

[3] "Diagnostic and Statistical Manual of Mental Disorders | Psychiatry Online," *DSM Library*. https://psychiatryonline.org/doi/book/10.1176/appi.books.9780890425596

[4] B. Allen, "Multimodal behavior management for people with dementia," *American Journal of Alzheimer's Disease and Other Dementias*, vol. 17, no. 2, pp. 89–91, Mar. 2002, doi: 10.1177/153331750201700203.

[5] "Hoja informativa sobre la enfermedad de Alzheimer | NIA," National Institute on Aging. https://www.nia.nih.gov/espanol/enfermedad-alzheimer/enfermedad-alzheimer

[6] Homini Biometrics, "Biometría - soluciones biométricas," *Homini Biometrics*, Jun. 06, 2023. https://www.homini.com.co/

[7] C. M. Travieso González, Sistemas Biométricos, Las Palmas de Gran Canaria - España: Universidad de las Palmas de Gran Canaria, 2012

[8] G. Etchart, L. Luna, C. Leal, M. G. Benedetto, and C. E. Alvez, "Sistemas de reconocimiento biométricos, importancia del uso de estándares en entes estatales," 2011. https://sedici.unlp.edu.ar/handle/10915/20052

[9] O. Lizama, G. Kindley, y J. I. Jeria Morales, "Redes de computadores: Arquitectura Cliente - Servidor," Profesor: A. Gonzales, Universidad de Chile, Santiago, Chile, Informe Técnico, 1 de Julio del 2016.

[10] "HTML: Lenguaje de etiquetas de hipertexto | MDN," MDN Web Docs, Jul. 28, 2024. https://developer.mozilla.org/es/docs/Web/HTML

[11] "CSS básico - Aprende desarrollo web | MDN," *MDN Web Docs*, Jul. 28, 2024. https://developer.mozilla.org/es/docs/Learn/Getting_started_with_the_web/CSS_basics

[12] "JavaScript | MDN," *MDN Web Docs*, Mar. 05, 2024. https://developer.mozilla.org/en-US/docs/Web/JavaScript

[13] "Amexcomp | Academia Mexicana de Computación." https://amexcomp.mx/sections/section/interaccion-humano-computadora/

[14] C. A. Díaz, "Consideraciones teóricas y éticas del reconocimiento facial de las emociones en contexto de pandemia," *Veritas*, no. 46, pp. 55–75, Aug. 2020, doi: 10.4067/s0718-92732020000200055.

[15] A. Banbury, S. Pedell, L. Parkinson, and L. Byrne, "Using the Double Diamond model to co-design a dementia caregivers telehealth peer support program," *Journal of Telemedicine and Telecare*, vol. 27, no. 10, pp. 667–673, Nov. 2021, doi: 10.1177/1357633x211048980.

[16] "Mural," *GetApp*, Jul. 22, 2021. https://www.getapp.es/software/123863/mural

[17] Slack, "¿Qué es Slack?," *Slack Help Center*. https://slack.com/intl/es-es/help/articles/115004071768-%C2%BFQu%C3%A9-es-Slack-

[18] "Acerca de Projects - Documentación de GitHub," *GitHub Docs*. https://docs.github.com/es/issues/planning-and-tracking-with-projects/learning-about-projects/about-projects

[19] J. Brownlee, "A gentle introduction to deep learning for face recognition," MachineLearningMastery.com, Jul. 05, 2019. https://machinelearningmastery.com/introduction-to-deep-learning-for-face-recognition/

[20] T. Agagu and B. Akinnuwesi, "Automated students' attendance taking in tertiary institution using hybridized facial recognition algorithm," Journal of Computer Science and Its Application, vol. 19, no. 2, May 2013, doi: 10.4314/jcsia.v19i2.1.

[21] Rouhiainen, L. (2018). Inteligencia artificial. Madrid: Alienta Editorial, 20-21.

[22] Espinoza Olguín, David Eduardo. "Reconocimiento facial." (2015).

[23] R. Gimeno Hernández, "Estudio de técnicas de reconocimiento facial," Bachelor's thesis, Dept. of Signal Processing and Communications, Universitat Politècnica de Catalunya, Barcelona, Spain, May 2010.

[24] E. Frontend, "Las diferencias entre Componentes Controlados y No-Controlados en React," *Escuela Frontend*, Sep. 19, 2022. https://www.escuelafrontend.com/componentes-controlados-y-no-controlados-en-react

[25] Li, C., & Li, C. (2019). Web Front-End Realtime Face Recognition Based on TFJS. 2019 12th International Congress on Image and Signal Processing, BioMedical Engineering and Informatics (CISP-BMEI). doi:10.1109/cisp-bmei48845.2019.8965963

[26] "View of IMPLEMENTATION OF FACE RECOGNITION AND LIVENESS DETECTION SYSTEM USING TENSORFLOW.JS." https://jurnal.polinema.ac.id/index.php/jip/article/view/3977/2759

[27] "justadudewhohacks/face-api.js: JavaScript API for face detection and face recognition in the browser and nodejs with tensorflow.js," *GitHub*. https://github.com/justadudewhohacks/face-api.js/

[28] "Redux - A JS library for predictable and maintainable global state management | Redux." https://redux.js.org/