UNIVERSIDAD NACIONAL DE SAN MARTIN

RCSI
https://revistas.unsm.edu.pe/index.php/rcsi
e-ISSN: 2709-992X

Artículo original
Original article
Jul-Dic, 2024

# Aplicación móvil para el control de asistencia de docentes universitarios con autenticación biométrica y verificación de geolocalización

## Mobile application for the attendance control of university professors with biometric authentication and geolocation verification

**Montañez-Díaz, Bruno Adrián**[1*]
**García-Gutiérrez, Willy Francisco**[1]
**Prieto-Pastor, Raphael Andre**[1]
**Mendoza-De-los-Santos, Alberto**[1]

[1]Facultad de Ingeniería, Universidad Nacional de Trujillo, Trujillo, Perú

**Recibido:** 25 Dic. 2023 | **Aceptado:** 04 Mar. 2024 | **Publicado:** 10 Jul. 2024

**Autor de correspondencia*:** t453300120@unitru.edu.pe

**Cómo citar este artículo:** Montañez-Díaz, B. A., García-Gutiérrez, W. F., Prieto- Pastor, R. A. & Mendoza-De-los-Santos, A. (2024). Aplicación móvil para el control de asistencia de docentes universitarios con autenticación biométrica y verificación de geolocalización. *Revista Científica de Sistemas e Informática, 4*(2), e647. https://doi.org/10.51252/rcsi.v4i2.647

## RESUMEN

La carencia de un sistema de registro de asistencias eficiente representa un desafío tanto para los educadores como para las instituciones educativas, generando disrupciones en la planificación de clases y sus horarios, así como inquietudes acerca de la seguridad de la información del personal docente. Este estudio propone el desarrollo de una aplicación móvil para el control de asistencias docentes, integrando autenticación biométrica y verificación de geolocalización para fortalecer la seguridad en el registro. La evaluación de la aplicación, realizada con 24 participantes en la Universidad Nacional de Trujillo, revela un 95% de precisión en la autenticación biométrica y una significativa reducción en el tiempo de registro, con un tiempo promedio de 32,68 segundos. Además, los resultados de una encuesta reflejan una percepción positiva en cuanto a la seguridad por parte de los usuarios, consolidando la aceptación y confianza en la implementación de esta innovadora solución tecnológica.

**Palabras clave:** Amazon Rekognition; geoposicionamiento; huella digital; identificación inteligente; reconocimiento facial

## ABSTRACT

The absence of an effective attendance recording system presents a formidable challenge for educators and educational institutions, leading to disruptions in class schedules, timetables, and apprehensions regarding faculty information security. This study proposes the development of a mobile application for teacher attendance management, integrating biometric authentication and geolocation verification to bolster security in the registration process. Evaluation of the application, conducted with 24 participants at the National University of Trujillo, underscores a 95% accuracy rate in biometric authentication and a notable reduction in registration time, averaging at 32.68 seconds. Moreover, survey results reflect a favorable perception of security among users, consolidating acceptance and trust in the implementation of this pioneering technological solution.

**Keywords:** Amazon Rekognition; geopositioning; fingerprint; smart identification; facial recognition

## 1. INTRODUCCIÓN

La autenticación biométrica ha revolucionado la forma en que los individuos son reconocidos y verificados en el ámbito digital. La autenticación biométrica es un método de seguridad que utiliza características biológicas únicas de las personas para confirmar su identidad y asegurarse de que realmente son quienes afirman ser (Ammour et al., 2023). La función principal es obtener las características biométricas, por ejemplo, fotografiando el rostro, huella dactilar, grabar la voz y lograr identificar si el rostro, la voz o la huella dactilar de la persona coincide con los recopilados (Kausar, 2020).

Estos métodos de seguridad son potencialmente más seguros que las contraseñas convencionales, ya que verifican la identidad del usuario a través de características únicas y personales que no necesitan ser recordadas (Silvelo, 2019). Sin embargo, en un mundo cada vez más interconectado, surge la necesidad de implementar niveles adicionales de seguridad. Aquí es donde la verificación por geolocalización entra en juego. La geolocalización, definida como el proceso de determinar la ubicación geográfica y temporal específica de un dispositivo equipado con esta tecnología, tiene aplicaciones en una amplia gama de campos (Moral, 2021). Este sistema es especialmente útil en entornos laborales o educativos, donde puede reemplazar métodos tradicionales de registro de asistencia.

Es vital monitorear diariamente la asistencia para asegurar un buen rendimiento del personal en organizaciones y centros educativos, aunque puede ser desafiante hacerlo eficientemente con muchos empleados y sin sistemas de registro adecuados (Salvatierra, 2018). En el contexto de las universidades, la supervisión de la asistencia de los docentes es un componente clave de la gestión académica. Dicho proceso no solo es fundamental para asegurarse de que los educadores cumplan con sus responsabilidades académicas y administrativas, sino que también es crucial para preservar la calidad y la integridad del proceso educativo en su conjunto.

Históricamente, las instituciones educativas han empleado métodos tradicionales de control de asistencia, como la firma en listas, registros en oficinas administrativas y sistemas de fichar. A pesar de su simplicidad, estos métodos pueden ser susceptibles a errores y, en ocasiones, resultan ineficientes para gestionar un gran número de personal. Torres (2019) resalta problemas de confiabilidad en un sistema de registro de asistencia gestionado por un empleado designado, donde se manifestaron acusaciones de favoritismo hacia algunos colegas y negligencia hacia otros.

En el contexto de la Universidad Nacional de Trujillo (UNT), el sistema de control de asistencia basado en la utilización de datos biométricos, específicamente huellas dactilares, se enfrenta a una problemática de consideración en lo que respecta a la seguridad. Aunque estos sistemas ostentan un robusto mecanismo para el registro de ingreso y salida de individuos, su implementación no está exenta de planteamientos inherentes al riesgo de compromiso de información de índole altamente sensible. Asimismo, existen varias desventajas en los sistemas de asistencia actuales, como colas largas en la máquina de asistencia y dificultades en el mantenimiento y reparación de los dispositivos (Soewito et al., 2016).

Para afrontar esta problemática con la debida diligencia, se hace necesario adoptar un enfoque multifacético que armonice de manera equilibrada la eficiencia operativa con la salvaguardia de los datos sensibles. Novoa et al. (2019) proponen una solución, en forma de aplicación móvil, que facilita a los docentes la gestión del registro de asistencia a través de la ubicación geográfica del docente y los relojes biométricos. Así también, Sulla (2022) implementó un Sistema Biométrico, utilizando aplicaciones móviles, para la gestión de asistencia de los estudiantes del Instituto Superior Tecnológico Americana en Cusco.

No obstante, con el fin de garantizar la presencia de los docentes en la universidad al intentar registrar su entrada o salida, se requiere la incorporación de un nivel adicional de verificación, en este caso, basado en la geolocalización. Un ejemplo de esto se ve en el proyecto de Valverde (2018), donde se desarrolló una aplicación móvil destinada a facilitar la localización de empleados sin importar su horario de trabajo o la calidad de su conexión a internet, lo cual permite registrar su asistencia durante la jornada laboral.

En este contexto, el estudio se enfoca en desarrollar una aplicación móvil para gestionar la asistencia docente, incorporando autenticación biométrica y verificación de geolocalización para reforzar la seguridad en el registro de asistencia. Los objetivos específicos incluyen:

(i) Examinar la autenticidad del sistema biométrico durante el registro.

(ii) Medir la eficiencia de la autenticación biométrica en este proceso.

(iii) Evaluar la percepción de seguridad de los usuarios tras la implementación de la aplicación.

## 2. MATERIALES Y MÉTODOS

### 2.1. Espacio de estudio

El estudio fue llevado a cabo en la Universidad Nacional de Trujillo (UNT), ubicada en el distrito de Trujillo, Provincia de Trujillo, en el departamento de La Libertad, Perú.

La investigación se condujo siguiendo un enfoque cuantitativo y se sustentó en un diseño preexperimental. La elección de esta metodología se justifica por el hecho de que el estudio de caso implica una única medición, es decir, la evaluación se realiza después de la aplicación del tratamiento experimental o estímulo.

La población objetivo inicial de la investigación abarcó a todos los docentes de la UNT. Sin embargo, para la fase de pruebas piloto de la aplicación, se adoptó un enfoque de muestreo no probabilístico por conveniencia, eligiendo estudiantes de la UNT que estuvieran dispuestos a participar en el estudio. La muestra específica consistió en 24 estudiantes de diferentes facultades y niveles académicos, procurando así una representación diversa de la comunidad estudiantil.

La hipótesis general planteó que la implementación de una aplicación móvil de control de asistencia docente con autenticación biométrica y verificación por geolocalización contribuye significativamente al fortalecimiento de la seguridad en el proceso de registro de asistencia en la UNT.

La implementación de la aplicación móvil se definió como el estímulo central de la investigación, mientras que la seguridad en el proceso de registro de asistencia se constituyó en la variable de estudio. Para medir la variable dependiente, se consideraron tres dimensiones fundamentales.

Primero la autenticidad fue evaluada basándose en investigaciones previas que destacan la necesidad de autenticación biométrica para una identificación precisa y sostenible a lo largo del tiempo, a pesar de posibles variaciones temporales (Li et al., 2023).

En segundo plano, se enfatizó la necesidad de que la autenticación biométrica sea efectiva. Contar con un sistema de seguimiento de asistencia eficiente en entornos corporativos y educativos es esencial (Sandhya et al., 2022). Un sistema biométrico de asistencia resulta altamente eficaz, contribuyendo a minimizar el tiempo dedicado a labores administrativas (Bhat et al., 2020).

Por último, se exploró la percepción de seguridad por parte de los usuarios, teniendo en cuenta el riesgo percibido como factor crucial que puede afectar negativamente en la aceptación de la tecnología biométrica (Balapour et al., 2020; Nakisa et al., 2023). Por lo tanto, la evaluación de la percepción de seguridad del sistema de autenticación es necesaria, ya que un sistema seguro desempeña un papel fundamental en la construcción de bases sólidas de confianza entre los usuarios.

En este contexto, se definieron indicadores específicos para cuantificar y evaluar las dimensiones mencionadas, tal como se detalla en la Tabla 1.

**Tabla 1.**
*Dimensiones evaluadas de la variable dependiente*

| Variable | Dimensión | Indicador |
|---|---|---|
| Seguridad en el proceso de registro de asistencia en la UNT | Autenticidad | Precisión en la autenticación biométrica |
| | Eficiencia | Tiempo en el proceso de registro |
| | Percepción de seguridad | Confianza en la privacidad de la información<br>Preocupación sobre acceso no autorizado<br>Confianza en la seguridad del reconocimiento facial<br>Evaluación de las políticas de seguridad |

Respecto a la recolección de datos, se hicieron uso de 2 técnicas: la encuesta y la observación no experimental. La implementación de la encuesta involucró el diseño de un cuestionario, previamente validado por expertos, que se fundamentó en la escala de Likert. Este cuestionario abordó cuatro ítems que representan los cuatro indicadores de la dimensión de percepción de seguridad. Por otro lado, la observación no experimental permitió recopilar información de los registros producidos por el uso de la aplicación, de esta forma se pudo obtener medidas respecto a la precisión y eficacia de la autenticación. Para el análisis de los datos resultantes se empleó la herramienta SPSS Statistics v27.

### 2.2. Diseño y desarrollo del software

En cuanto al desarrollo del software, se decidió emplear Scrum, una metodología ágil reconocida por su enfoque incremental e iterativo. De acuerdo con Bhavsar et al. (2020), la aplicación apropiada de Scrum en prácticas de desarrollo de software contribuye a mejorar tanto la productividad como la calidad del producto y sus características.

En la planificación del desarrollo de la aplicación, se consideró que la solución busca fortalecer la seguridad con funcionalidades de verificación biométrica, mediante un servicio web de autenticación y la local del dispositivo. Además, se consideró la geolocalización como una medida adicional de seguridad para garantizar la presencia del docente dentro del campus universitario. La Figura 1 muestra de manera representativa el flujo del registro de asistencia docente.

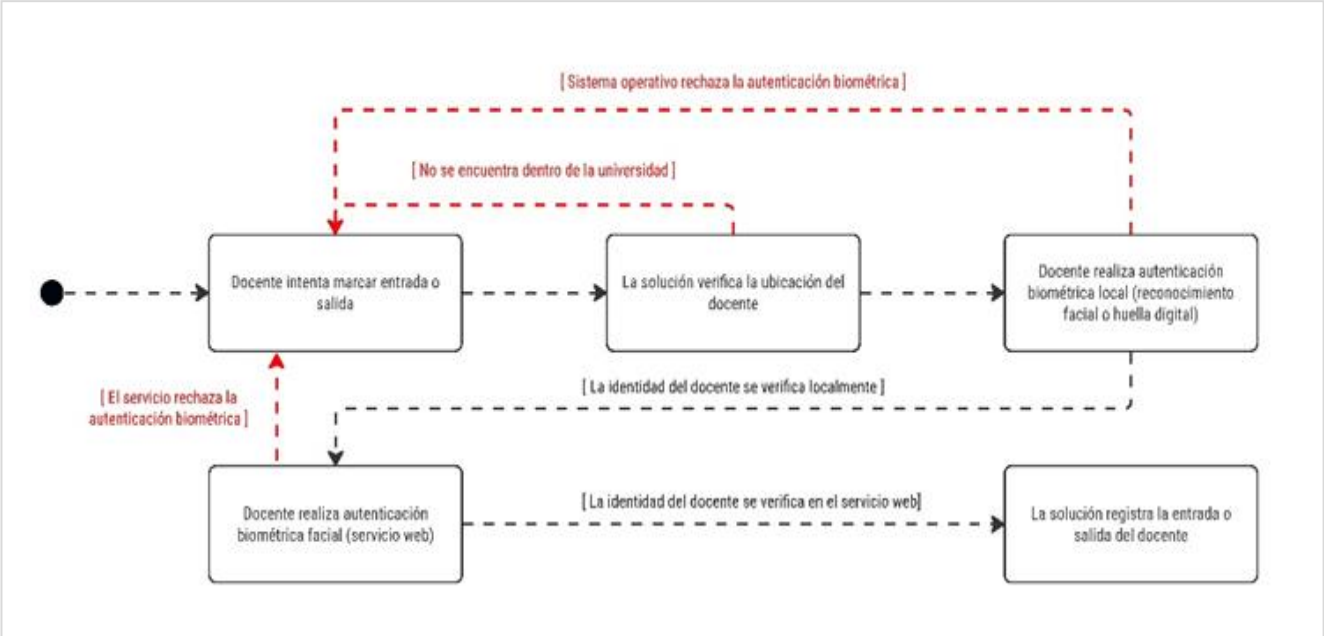


**Figura 1.** *Representación del proceso de control de asistencia en la solución propuesta*

Considerando el proceso involucrado, se procedió a realizar la estimación del product backlog, que incluyó un total de 3 sprints y 13 historias de usuario. Se proyectó una duración de 36 días para su ejecución, como se evidencia en la Tabla 2.

**Tabla 2.**

*Product Backlog estimado del proyecto*

| #Sprint | #HU | Descripción | Tamaño | Puntos | Tiempo [Días] |
|---|---|---|---|---|---|
| Primer *Sprint* | HU1 | Configurar entorno de desarrollo Flutter y Supabase | S | 2 | 1 1/2 |
| | HU2 | Diseñar la UI de la pantalla de inicio de sesión | M | 3 | 2 |
| | HU3 | Implementar la lógica de inicio de sesión con Supabase | L | 5 | 3 |
| | HU4 | Integrar paquete *local_auth* para la autenticación biométrica local en la aplicación móvil | M | 3 | 2 |
| | HU5 | Integrar Google Maps para la verificación por geolocalización | L | 5 | 3 |
| Segundo *Sprint* | HU6 | Implementar las funciones de Amazon Rekognition en el servicio web | XL | 8 | 5 |
| | HU7 | Diseñar y desarrollar la interfaz de usuario de la aplicación | XL | 8 | 5 |
| | HU8 | Diseñar y desarrollar la interfaz de usuario de la plataforma de administración web | XL | 8 | 5 |
| | HU9 | Implementar la funcionalidad de intervención manual del administrador en la plataforma de administración web | L | 5 | 2 |
| Tercer *Sprint* | HU10 | Desarrollar políticas de seguridad para evitar accesos no autorizados en Supabase | M | 3 | 2 |
| | HU11 | Realizar pruebas unitarias y de integración en la aplicación móvil y en el servicio web | L | 5 | 3 |
| | HU12 | Desplegar la aplicación móvil en las plataformas iOS y Android | S | 2 | 1 1/2 |
| | HU13 | Desplegar la plataforma de administración web en un entorno de producción | XS | 1 | 1 |
| **Puntos de historia / Tiempo estimado** | | | | **58** | **36** |

En vista de eso, la solución se centra en la construcción de una aplicación móvil implementando Flutter, un marco de trabajo de código abierto creado por Google que facilita la creación de aplicaciones multiplataforma a partir de una única base de código (Flutter, 2019). Esta elección se sustentó en su posición destacada como el marco multiplataforma más ampliamente adoptado en la actualidad (Lovrić et al., 2023). Además de su reconocida eficiencia en el tiempo de ejecución, numerosas evaluaciones han demostrado un rendimiento sobresaliente en términos de utilización de la CPU (Wasilewski & Zabierowski, 2021). Estos factores se consideraron determinantes al seleccionar la herramienta para el desarrollo de la aplicación.

Además, se desplegó una infraestructura de backend utilizando Supabase, que es una plataforma de Backend como un Servicio (BaaS). Supabase es una plataforma de código abierto que proporciona una amplia gama de servicios para el desarrollo de aplicaciones, incluyendo una base de datos, autenticación, almacenamiento, entre otros (Supabase, 2023). El enfoque de desarrollo denominado BaaS permite que los desarrolladores se concentren en las funcionalidades de la aplicación, en lugar de dedicarse al desarrollo de la compleja infraestructura de backend, al establecer conexiones con sofisticadas Interfaces de Programación de Aplicaciones (API) (Dudjak & Martinović, 2020).

Un componente crítico de esta aplicación fue la integración con Amazon Rekognition, un servicio de aprendizaje automático totalmente gestionado que proporciona las API centrales para habilitar el análisis de imágenes y videos (Amazon, 2023). Permite identificar objetos, rostros, texto, escenas y actividades, proporcionando una lista de etiquetas que describen los objetos detectados en imágenes y videos (Leotta et al., 2023). Aunque grandes plataformas como Google, Azure y Meta ofrecen tecnologías similares,

Amazon Rekognition destaca como la mejor en reconocimiento facial y la interpretación de expresiones emocionales (Saadon et al., 2023).

Las funcionalidades proporcionadas por Amazon Rekognition se aprovecharon a través del desarrollo de un servicio web basado en Node.js y Express. Este servicio se implementó en una Plataforma como Servicio (PaaS), en este caso, Render, para su despliegue y funcionamiento. Una PaaS es un entorno de computación en la nube que ofrece recursos y herramientas para el desarrollo, despliegue y gestión de aplicaciones sin la necesidad de preocuparse por la infraestructura subyacente (Kounev et al., 2023).

La Figura 2 esquematiza la arquitectura que se implementó para poner en funcionamiento la aplicación.

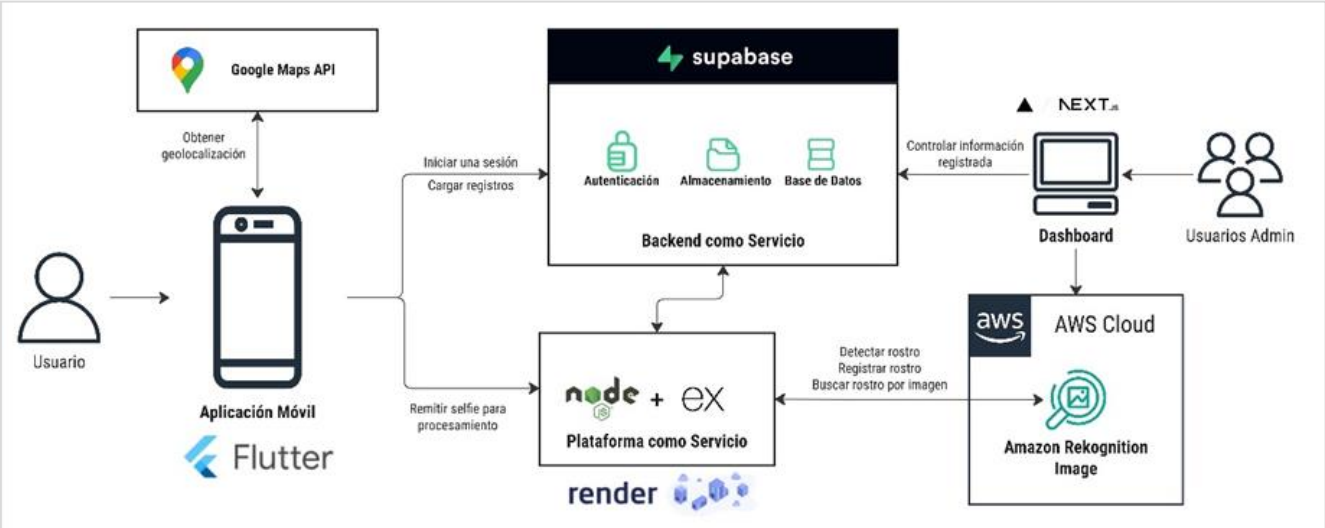


**Figura 2.** *Arquitectura de la solución propuesta*

Para la verificación por geolocalización, se incorporó la tecnología de Google Maps junto con el paquete google_maps_flutter para tener acceso a los mapas y a la ubicación precisa del docente. Esto garantizó que solo se permitiera el registro de asistencia cuando el docente se encuentre dentro del campus universitario.

Para la autenticación biométrica local, se hizo uso del paquete local_auth de Flutter. Esta característica permitió una verificación biométrica efectiva, dependiendo de los datos biométricos registrados en el dispositivo, como rostros y huellas digitales.

Para llevar a cabo la verificación biométrica en el servicio web, tanto en el registro como en la autenticación biométrica facial, se hicieron uso de tres funcionalidades proporcionadas por Amazon Rekognition (Figura 3).

En primer lugar, DetectFacesAPI se utilizó para identificar y analizar los rostros en la imagen enviada, proporcionando detalles como la ubicación y características de los rostros, así como información adicional sobre edad, género y emociones. Estos datos fueron usados para realizar ciertas validaciones de calidad que se detallarán más adelante.

En segundo lugar, SearchFacesByImageAPI se aprovechó para comparar los rostros en una imagen de referencia con la colección de rostros previamente registrados, permitiendo la verificación de la coincidencia de rostros. Haciendo uso de esta funcionalidad se evita registrar un rostro ya indexado a la colección.

Finalmente, se utilizó IndexFacesAPI para llevar a cabo la indexación de rostros en la colección. La indexación conlleva el registro del rostro en forma de un conjunto de características faciales en una colección. En este contexto, las colecciones se refieren a conjuntos organizados de vectores de características que representan rostros previamente detectados en imágenes (Amazon, 2023).

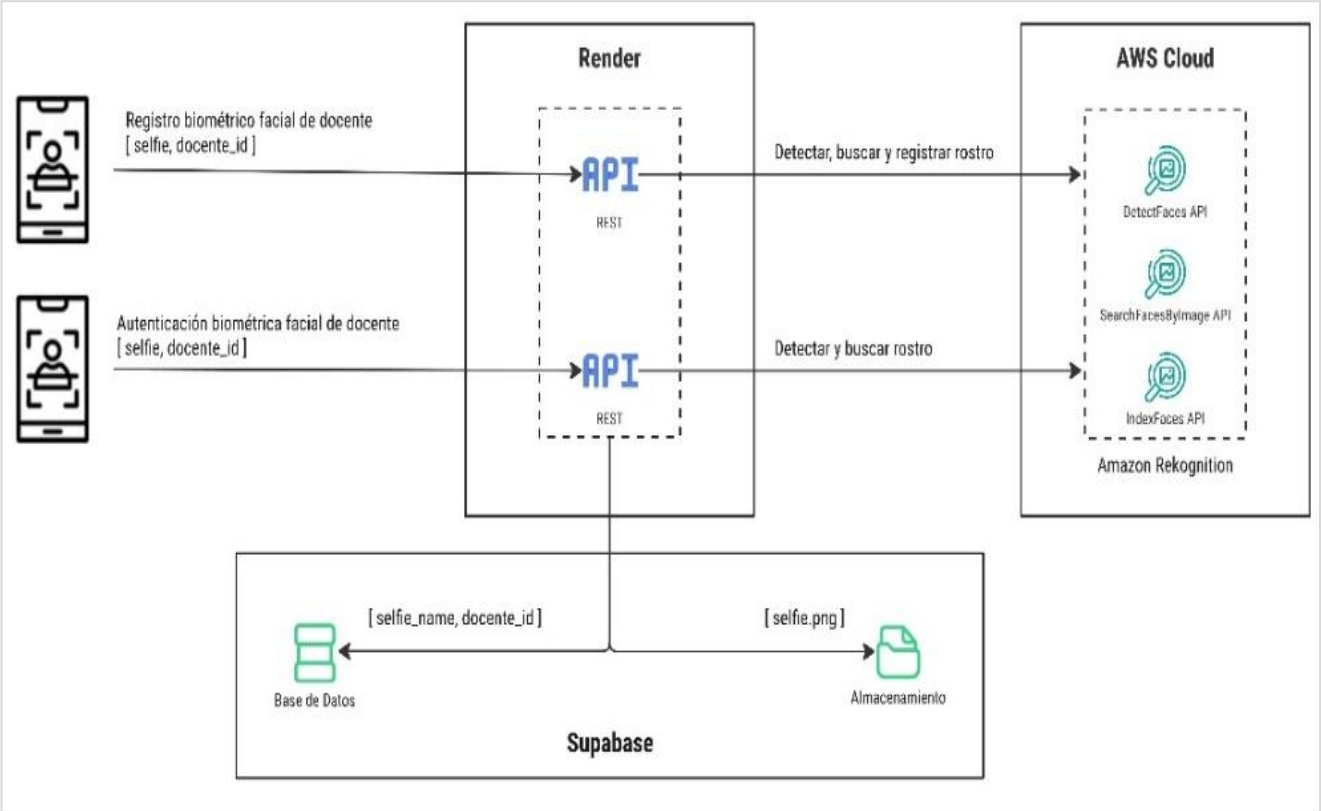


**Figura 3.** *Arquitectura referencial de verificación de identidad en el servicio web*

En el proceso de registro biométrico facial, se debe superar un umbral de calidad, como se ilustra en la Figura 4. Entre los datos proporcionados por DetectFacesAPI se encuentran el nivel de confianza, la calidad de la imagen (brillo y nitidez), la presencia de lentes o gafas de sol, la apertura de los ojos, la apertura de la boca, el tamaño relativo del rostro en relación con la imagen, la detección de emociones, la orientación (inclinación y giro) y la posición del rostro. En función de estos criterios, se definieron una serie de requisitos que determinan si la *selfie* es considerada adecuada para continuar con el proceso (Tabla 3).

**Tabla 3.**
*Reglas de calidad para la detección de rostro en el registro*

| Regla | Valor |
|---|---|
| Nivel de Confianza | 0,95 |
| Ancho del Rostro (%) | [50, 75] |
| Largo del Rostro (%) | [60, 90] |
| Desplazamiento del Rostro en el eje horizontal (%) | [45, 55] |
| Posición del Rostro en el eje vertical (%) | [30, 50] |
| Emoción Esperada | Calmada |
| Inclinación (°) | [-5, 5] |
| Orientación Lateral (°) | [-5, 5] |
| Inclinación Lateral (°) | [-5, 5] |
| Nitidez Mínima | 70 |
| Brillo Mínimo | 60 |
| Gafas de Sol Permitidas | No |
| Gafas de Vista Permitidas | No |
| Boca Cerrada Requerida | Sí |
| Ojos Abiertos Requeridos | Sí |

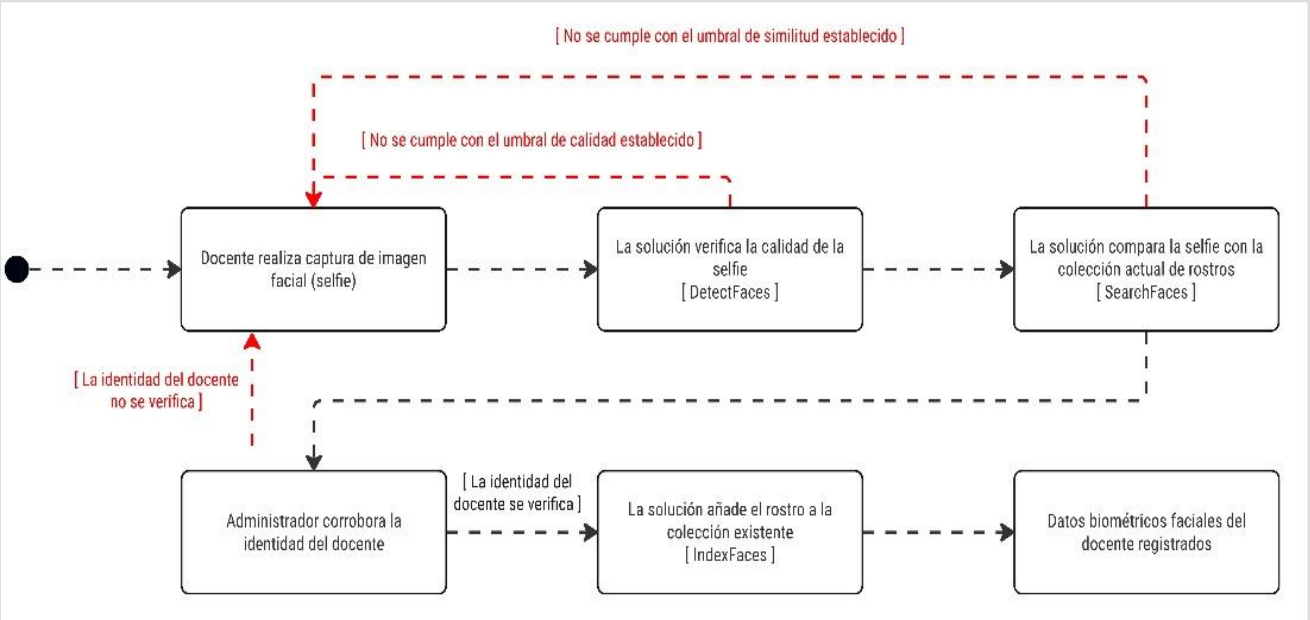


**Figura 4.** *Flujo representativo del registro biométrico facial del docente*

Estas reglas se elaboraron en cumplimiento con los requisitos de imagen facial establecidos en la norma ISO/IEC 19794-5, que se encuentran detallados en la Tabla 4. Esta norma establece pautas para la captura de imágenes faciales en aplicaciones biométricas, abordando restricciones del entorno, propiedades fotográficas, atributos digitales y prácticas recomendadas para la fotografía de rostros (ISO/IEC 19794-5:2005, 2005).

Además, se tomó la decisión de adherirse a las pautas establecidas por la Organización de Aviación Civil Internacional para la captura de retratos faciales en documentos de viaje legibles por máquina. La producción de retratos estandarizados de alta calidad al permitir inspeccionar los documentos de viaje de manera automatizada, lo que guarda una estrecha relación con la tecnología de reconocimiento facial. En la Tabla 5, se observan los requerimientos que se tomaron en cuenta para establecer las reglas de detección de rostro en esta solución. Cabe recalcar que parámetros como la distancia desde un lado hacia el centro del rostro, se usaron para establecer el porcentaje mínimo y máximo de posición que figuran en las reglas ya presentadas.

**Tabla 4.**

*Requisitos de calidad para imagen facial en la norma ISO / IEC – 19794-5*

| Cláusula | Atributo | Restricción |
|---|---|---|
| Escena | Postura | Control de desviación desde la frontal |
| | Iluminación | Iluminación uniforme sin sombras |
| | Fondo | Fondo claro y de un solo color |
| | Ojos | Abiertos y claramente visibles |
| | Boca | Cerrada y claramente visible |
| Fotográfica | Posición de la cabeza | Centrada |
| | Distancia a la cámara | Tamaño moderado de la cabeza |
| | Color | Color neutro y sin ojos rojos |
| | Exposición | Brillo apropiado |
| Digital | Enfoque | Sin desenfoque y con nitidez adecuada |
| | Resolución | Restricción de ancho de la cabeza |

*Nota:* Adaptado de Face Image Quality Evaluation (Sang et al., 2009)

**Tabla 5.**
*Requerimientos de calidad para el retrato según ICAO*

| Parámetro | Restricción |
|---|---|
| Inclinación de la cabeza respecto a la posición frontal | ≥ – 5°<br>≤ + 5° |
| Orientación lateral de la cabeza respecto a la posición frontal | ≥ – 5°<br>≤ + 5° |
| Inclinación lateral de la cabeza | ≥ – 8°<br>≤ + 8° |
| **Expresión facial** | **Neutral, sin sonrisa** |
| Ancho de la cabeza respecto a la imagen | ≥ 50%<br>≤ 75% |
| Longitud de la cabeza respecto a la imagen | ≥ 60%<br>≤ 90% |
| Distancia desde el lado izquierdo de la imagen al centro del rostro | ≥ 45%<br>≤ 55% |
| Distancia desde la parte superior de la imagen al centro del rostro | ≥ 30%<br>≤ 50% |

*Nota:* Adaptado de Reporte Técnico de Calidad de retrato (imágenes faciales de referencia para MRTD) (ISO/IEC JTC1 SC17 WG3, 2018)

Una vez que la *selfie* ha superado el umbral de calidad, se somete a un proceso de comparación con los rostros existentes en la colección, cumpliendo con un umbral de similitud predefinido. Información que se obtiene a través del resultado de *SearcFacesByImageAPI*. Se estableció que el nivel de similitud entre rostros debe ser del 95%. Por lo tanto, si la *selfie* enviada supera ese umbral de similitud, el registro se rechaza.

El siguiente paso implica la intervención manual de un administrador, quien verifica la identidad del docente, con el fin de prevenir el registro de personas no autorizadas y garantizar la autenticidad de los registros. Para ello se construyó una plataforma de administración web donde los administradores tienen acceso a la información de los registros de asistencia. Esta plataforma se ha erigido empleando tecnologías de desarrollo web de última generación, tales como NextJs, un *framework fullstack* de JavaScript; TailwindCSS, un *framework* de CSS; y Shadcn UI, un repositorio de componentes diseñados para TailwindCSS. De este modo, el administrador examina la lista de solicitudes de registro facial y procede a validar la identidad del docente.

Finalmente, realizado las tres comprobaciones, el proceso culmina con el registro del rostro en la colección. Se utiliza la función *IndexFaces* de Amazon Rekognition. Una vez que el rostro se almacena correctamente, se genera un identificador único para dicho rostro. Utilizando este identificador y el identificador del docente, se crea un registro en la tabla de solicitudes de registro de rostros en Supabase. Asimismo, la *selfie* enviada se guarda en el sistema de almacenamiento de Supabase para su futura referencia.

Por otro lado, también fue esencial desarrollar la lógica para la autenticación biométrica facial, lo que implica verificar la identidad de un docente que ya tiene su rostro registrado. Este proceso sigue un flujo que se ilustra en la Figura 5. Al igual que en el proceso de registro, la *selfie* enviada debe superar el umbral de calidad definido. En este caso, se establecieron un conjunto más reducido de reglas que el proceso de registro, lo que se justifica por la necesidad de agilizar la verificación y mantener un proceso eficiente para los docentes autorizados, sin comprometer la seguridad. Estas reglas se detallan en la Tabla 6.

**Tabla 6.**
*Reglas de calidad para la detección de rostro en autenticación*

| Regla | Valor |
|---|---|
| Nivel de Confianza | 0,95 |
| Gafas de Sol Permitidas | No |
| Gafas de Vista Permitidas | No |
| Ojos Abiertos Requeridos | Sí |

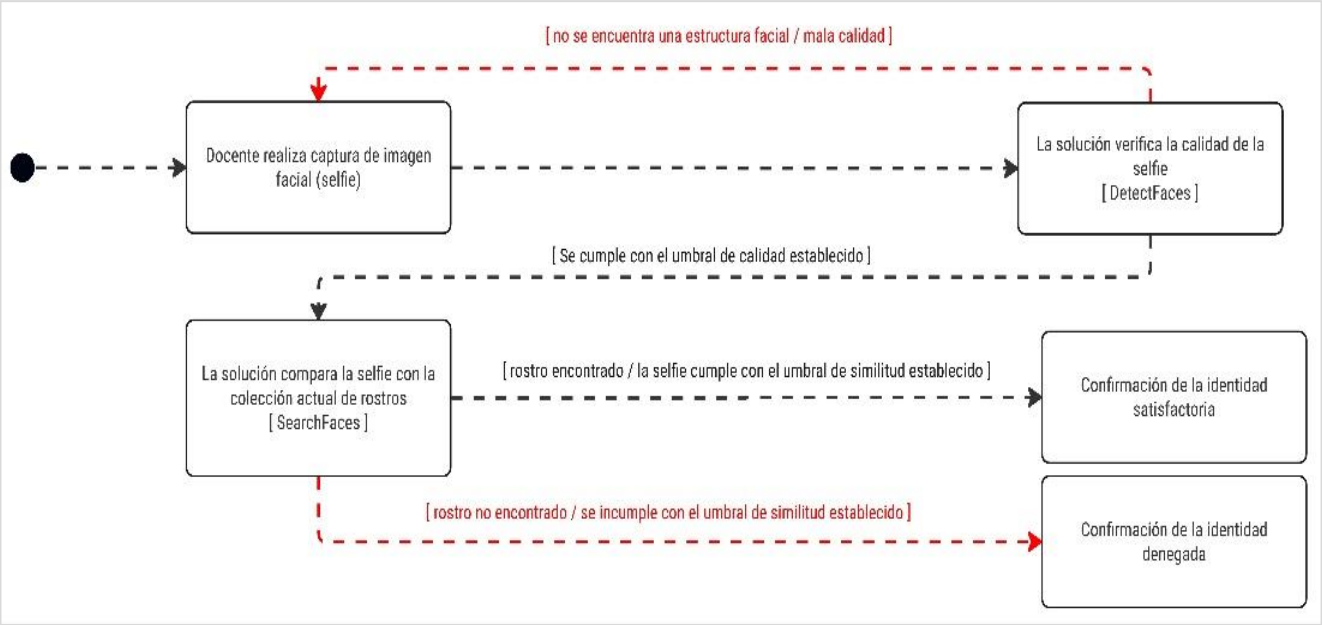


**Figura 5.** *Flujo representativo de la autenticación biométrica facial del docente*

Tras superar el umbral de calidad, el proceso continúa con la evaluación del porcentaje de similitud, que debe ser de al menos un 95%. Este criterio es esencial para garantizar una alta precisión en la verificación biométrica y evitar falsos positivos. Finalmente, se genera un registro de intento de verificación biométrica, donde la *selfie* del intento se guarda en el almacenamiento de Supabase. Esta práctica se alinea con una política de seguridad que se implementó en el *backend*, la cual establece que, si un usuario ha intentado realizar una verificación biométrica en más de tres ocasiones en los últimos cinco minutos, no se le permitirá realizar más intentos. De esta manera se evitan accesos no autorizados y se garantiza la integridad del proceso de autenticación en todo momento.

## 3. RESULTADOS Y DISCUSIÓN

Antecedida por una fase de desarrollo exhaustiva, el prototipo de la aplicación resultó con la interfaz que se visualiza en la Figura 6, donde se presentan las pantallas del flujo de registro de asistencia detallando cada uno de los elementos y funciones disponibles para el usuario. Posteriormente, se hizo una prueba piloto para evaluar el funcionamiento de la aplicación móvil con 24 estudiantes en el campus de la UNT, entre el 29 de noviembre de 2023 y el 17 de diciembre de 2023.

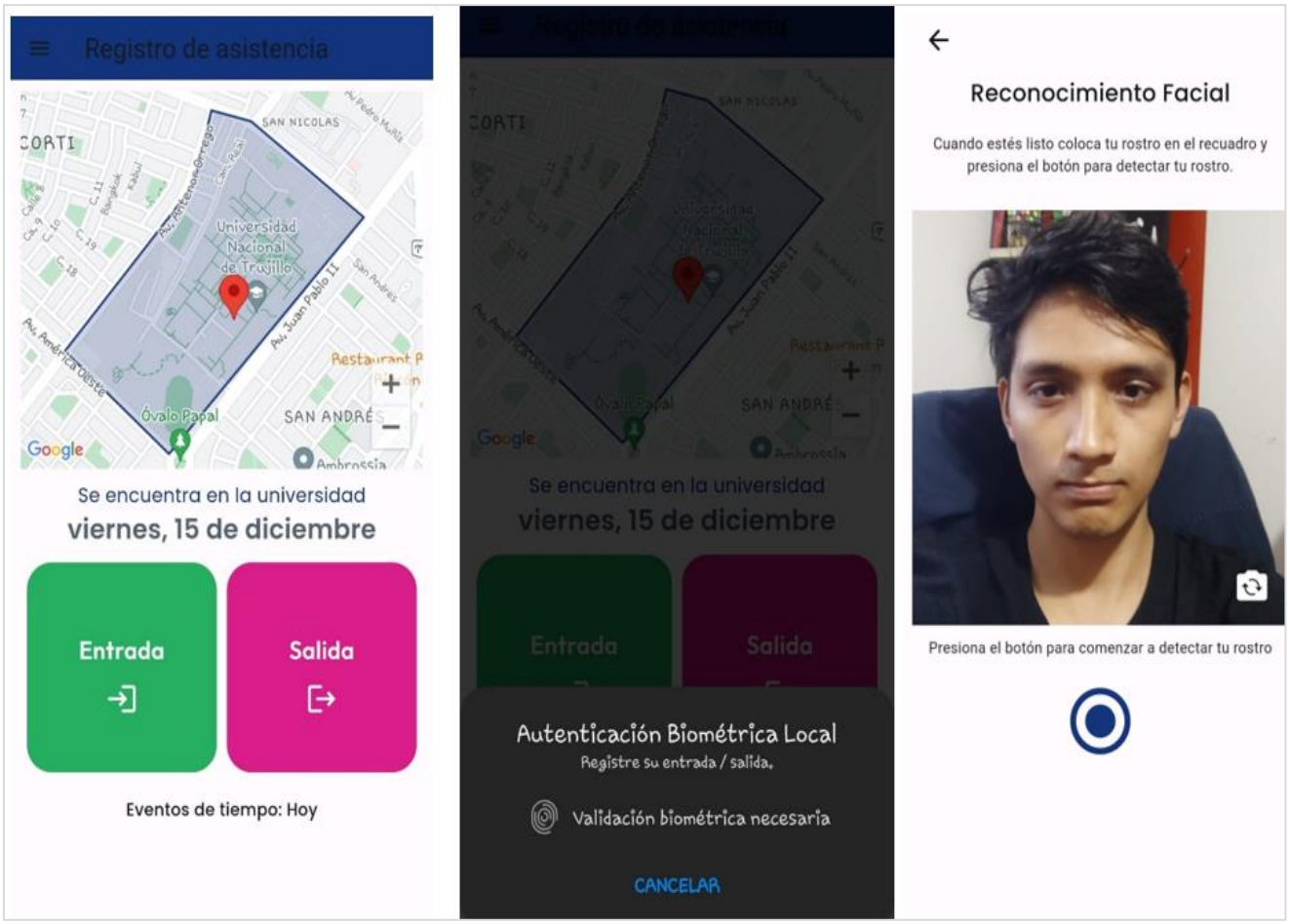


**Figura 6.** *Interfaz de verificación por geolocalización, biométrica local y por reconocimiento facial*

### 3.1. Autenticidad

En ese intervalo, se registraron 74 eventos, reflejando ocasiones en que los usuarios marcaron su entrada o salida. De estos, 70 registros corresponden a marcas de asistencia que requieren solo un intento de verificación biométrica facial, como se ilustra en la Figura 7. Esto demuestra que la precisión del aplicativo alcanza el 95%, dejando un 5% restante de intentos fallidos considerados como falsos negativos. En un experimento similar, Tee & Khoo (2020) evaluaron su sistema FaceAuth con 40 participantes, logrando una precisión del 92.5%. En comparación con el sistema propuesto, FaceAuth se enfoca en identificar a personas sin depender de internet, utilizando el algoritmo k-vecinos más cercanos (k-NN). Este algoritmo, aunque común en el reconocimiento facial, enfrenta desafíos al tratar con rostros parcialmente cubiertos y suele tener una alta tasa de falsos negativos (Guo, 2021).

En contraste, la aplicación propuesta para el registro de asistencia utiliza algoritmos de aprendizaje profundo mediante Amazon Rekognition. A diferencia del aprendizaje automático convencional, el aprendizaje profundo divide el proceso en múltiples etapas, cada una diseñada para aprender características específicas (Vardakis et al., 2022). De este modo, el empleo de algoritmos de aprendizaje profundo fundamenta la mayor precisión observada en el aplicativo propuesto en contraste con FaceAuth.

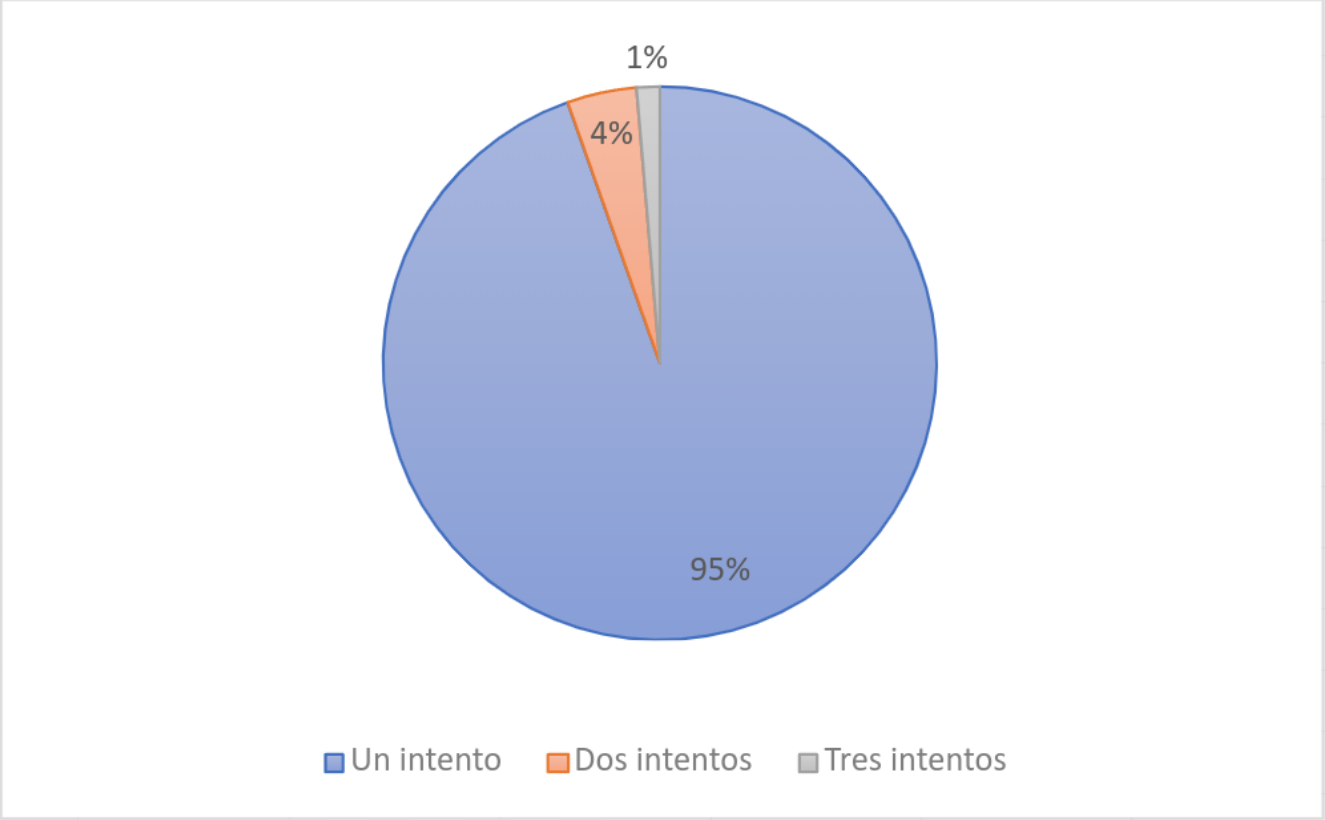


**Figura 7.** *Intentos por registro para lograr una autenticación exitosa*

### 3.2. Eficiencia

En cada registro de asistencia se incluye un campo que refleja el tiempo en segundos empleado para completar el proceso. Para garantizar una comparación más precisa, se optó por analizar únicamente la autenticación exitosa en el primer intento, ya que los intentos múltiples tienden a requerir más tiempo, como se observa en la Figura 8. Con 70 registros en un intento, se aplicó la prueba de normalidad de Kolmogorov-Smirnov, una elección apropiada para muestras superiores a 50. La hipótesis nula (Ho) plantea que los registros tienen una distribución normal, mientras que la hipótesis alternativa (Ha) sostiene que los registros no tienen una distribución normal.

**Tabla 7.**

*Prueba de normalidad - Kolmogorov-Smirnov*

| | Estadístico | gl | p |
|---|---|---|---|
| **Tiempo del proceso** | 0,081 | 70 | 0,2 |

Como se contempla en la Tabla 7, con un valor p de 0,2 en la prueba de Kolmogorov-Smirnov, no hay evidencia suficiente para rechazar Ho. Por lo tanto, se puede asumir la normalidad para el análisis correspondiente.

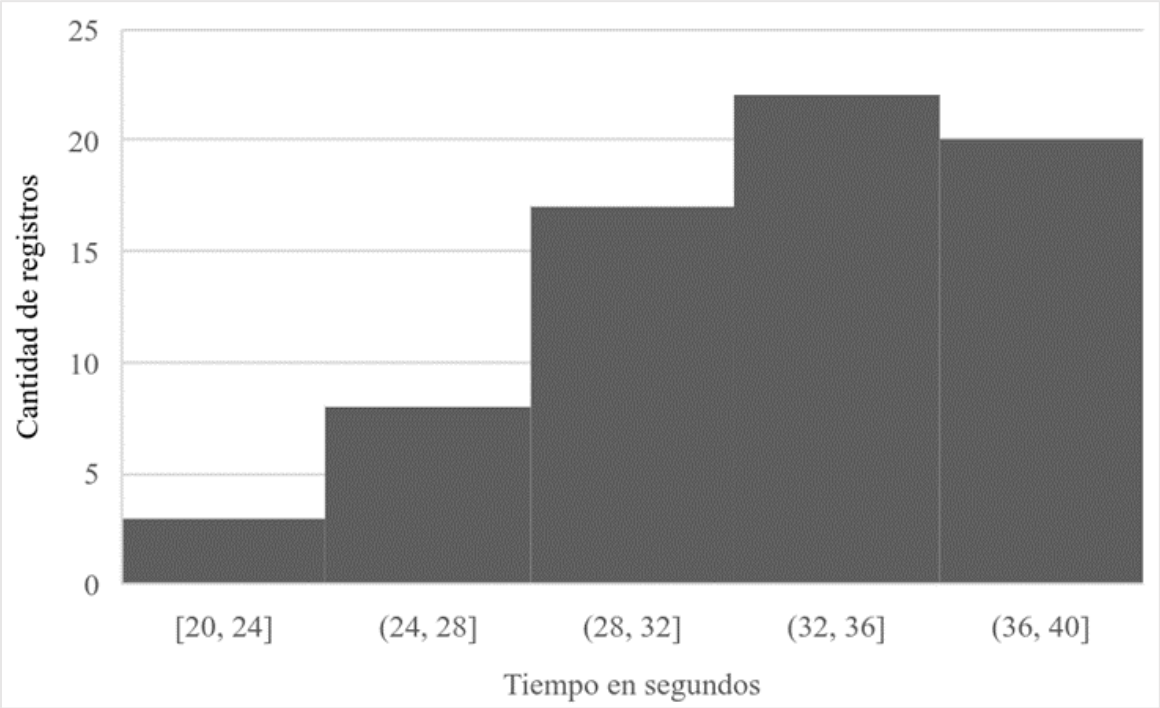


**Figura 8.** *Tiempo empleado en el proceso de marcado de asistencia durante la autenticación al primer intento*

Se inicia el análisis de los resultados introduciendo al estándar ISO/IEC 25010, el cual proporciona una definición clara de características y subcaracterísticas, estableciendo un lenguaje coherente para la descripción y evaluación de la calidad de un software (ISO/IEC 25010, 2011). La utilidad de este modelo reside en su capacidad para abordar aspectos específicos, centrándose en la eficiencia para medir el tiempo.

Una vez cuantificadas las métricas, se procede a evaluar los resultados. En este contexto, la norma ISO/IEC 25040:2011 proporciona un marco que establece requisitos y recomendaciones para la evaluación del software. Este estándar facilita la definición de criterios de satisfacción, alineados con los objetivos de calidad deseados (ISO/IEC 25040, 2011). Como se detalla en la Tabla 8, se presentan cuatro rangos de medición, con valores del 0 al 10, cada uno con sus respectivos niveles de puntuación asignados a tres grados de satisfacción.

**Tabla 8.**
*Rangos de medición para las métricas*

| Valor de medición | Nivel de puntuación | Grado de satisfacción |
|---|---|---|
| 7,50 - 10 | Cumple con los requerimientos | Muy satisfactorio |
| 5 – 7,49 | Aceptable | Satisfactorio |
| 2,51 – 4,99 | Mínimamente aceptable | Insatisfactorio |
| 0 – 2,50 | No aceptable | Insatisfactorio |

Adheridos al formato de ambos estándares, es esencial establecer un valor esperado para cada métrica. El estudio de Zambrano-Vega et al. (2020) presentó bioFace, una aplicación de registro de asistencia para docentes con verificación por geolocalización y reconocimiento facial. Durante una prueba de cuatro días, los tiempos promedio del proceso fueron 1,74; 2; 1,56 y 1,75 minutos, siendo 1,56 minutos (equivalente a 93,6 segundos) la marca más baja y tomada como referencia. En el proceso de medición, se establece la comparación de la siguiente manera: si el tiempo planificado (A) es mayor que el tiempo obtenido (B), se asigna un valor de 10 (X); en caso contrario, si B supera a A, se asigna un valor de 0.

**Tabla 9.**

*Evaluación de la eficiencia del aplicativo en el proceso de registro de asistencia*

| Característica | | | Métrica | | | Meta | Fórmula A / B | |
|---|---|---|---|---|---|---|---|---|
| Eficiencia de Desempeño | | | Tiempo de la tarea | | | <93,6 | A = t. planeado<br>B = t. obtenido<br>A > B; 0 ; 10 | |
| **Datos obtenidos** | | | | | | | | |
| **A** | **B** | **X** | **A** | **B** | **X** | **A** | **B** | **X** |
| 31,997 | 93,6 | 10 | 29,841 | 93,6 | 10 | 30,726 | 93,6 | 10 |
| 35,009 | 93,6 | 10 | 34,653 | 93,6 | 10 | 31 | 93,6 | 10 |
| 33,874 | 93,6 | 10 | 38,326 | 93,6 | 10 | 36,333 | 93,6 | 10 |
| 35,982 | 93,6 | 10 | 39,735 | 93,6 | 10 | 33,348 | 93,6 | 10 |
| 34,587 | 93,6 | 10 | 26,899 | 93,6 | 10 | 30 | 93,6 | 10 |
| 39,090 | 93,6 | 10 | 37,374 | 93,6 | 10 | 33,1 | 93,6 | 10 |
| 32,853 | 93,6 | 10 | 39,243 | 93,6 | 10 | 38,665 | 93,6 | 10 |
| 30,873 | 93,6 | 10 | 33,014 | 93,6 | 10 | 36,771 | 93,6 | 10 |
| 33,354 | 93,6 | 10 | 31,1 | 93,6 | 10 | 34,099 | 93,6 | 10 |
| 32,857 | 93,6 | 10 | 33,906 | 93,6 | 10 | 36,862 | 93,6 | 10 |
| 38,030 | 93,6 | 10 | 33,232 | 93,6 | 10 | 31,489 | 93,6 | 10 |
| 24,201 | 93,6 | 10 | 31,222 | 93,6 | 10 | 35,449 | 93,6 | 10 |
| 23,010 | 93,6 | 10 | 32,484 | 93,6 | 10 | 26,482 | 93,6 | 10 |
| 20,235 | 93,6 | 10 | 38,892 | 93,6 | 10 | 31,015 | 93,6 | 10 |
| 36,457 | 93,6 | 10 | 30,598 | 93,6 | 10 | 28,126 | 93,6 | 10 |
| 26,317 | 93,6 | 10 | 36,354 | 93,6 | 10 | 20,283 | 93,6 | 10 |
| 38,739 | 93,6 | 10 | 37,951 | 93,6 | 10 | 26,284 | 93,6 | 10 |
| 30,690 | 93,6 | 10 | 33,828 | 93,6 | 10 | 38,524 | 93,6 | 10 |
| 26,089 | 93,6 | 10 | 28,239 | 93,6 | 10 | 39,086 | 93,6 | 10 |
| 34,537 | 93,6 | 10 | 27,035 | 93,6 | 10 | 30,915 | 93,6 | 10 |
| 34,125 | 93,6 | 10 | 34,228 | 93,6 | 10 | 37,856 | 93,6 | 10 |
| 32,396 | 93,6 | 10 | 30,019 | 93,6 | 10 | 27,7 | 93,6 | 10 |
| 31,826 | 93,6 | 10 | 36,52 | 93,6 | 10 | | | |
| 28,891 | 93,6 | 10 | 32,496 | 93,6 | 10 | | | |
| **Puntaje promedio** | | | | | | | 10 | |
| **Grado de satisfacción** | | | | | | | Muy satisfactorio | |

Como se observa en la Tabla 9, los resultados son consistentemente positivos, ya que ninguna marca de tiempo registrada excede el tiempo esperado. El tiempo promedio requerido para registrar la asistencia se sitúa en 32,68 segundos. Esto indica que, en términos de eficiencia, se han cumplido satisfactoriamente los requisitos establecidos. Excluyendo consideraciones de conectividad y velocidad de internet, este resultado se atribuye principalmente al servicio de reconocimiento facial utilizado. Mientras que bioFace emplea Microsoft Face API, la aplicación propuesta utiliza Amazon Rekognition.

### 3.3. Percepción de Seguridad

Se ha realizado un análisis de confiabilidad de los resultados obtenidos en la encuesta, revelando un coeficiente Alfa de Cronbach de 0,829. Este valor denota una sólida consistencia interna en la evaluación de la percepción de seguridad en la aplicación de registro de asistencia. Aunque el coeficiente se sitúa ligeramente por debajo del umbral de 0,80 registrado en una investigación previa sobre la percepción de seguridad en aplicativos móviles, llevada a cabo por Balapour et al. (2020), continúa siendo un indicador destacado de consistencia interna en la presente investigación.

**Tabla 10.**
*Estadísticas de los ítems del cuestionario sobre percepción de seguridad*

| Items | Media | Des. Est. |
|---|---|---|
| Estoy seguro de que la información privada (biometría facial y geolocalización) que proporcioné durante mi proceso de registro con la aplicación solo se almacenará en su sistema | 4,71 | 0,464 |
| Me preocupa que personas inapropiadas puedan acceder a la información privada que proporcioné durante mi interacción con la aplicación de registro de asistencia. | 3,71 | 0,464 |
| Confío en la seguridad de las operaciones de reconocimiento facial en el registro de asistencia. | 4,71 | 0,550 |
| Las políticas de seguridad en la aplicación de registro de asistencia son las adecuadas | 4,67 | 0,565 |

Como se evidencia en la Tabla 10, las estadísticas de las respuestas para cada ítem revelan una tendencia positiva, siendo el ítem relacionado con la preocupación sobre el acceso no autorizado aquel que presenta la menor media. Esta percepción es comprensible, ya que el encuestado tiene conocimiento de que, en el proceso de registro, la validación de identidad es llevada a cabo por un administrador en la plataforma de administración. Para aclarar este aspecto, es crucial destacar en primer lugar que el acceso a la plataforma está restringido, requiriendo credenciales para la entrada.

En segundo lugar, la información a la que el administrador tiene acceso se limita exclusivamente a la *selfie* enviada, la cual ni siquiera se considera confidencial. Esta práctica contrasta con el enfoque de Aza Poveda & Rodriguez Vanegas (2020), cuyo panel de administración muestra imágenes de huellas dactilares escaneadas, generando una mayor preocupación en caso de acceso no autorizado a dicha información. En una situación análoga, la UNT enfrentaría riesgos similares, ya que las huellas digitales de los docentes quedarían vulnerables si su sistema biométrico fuera comprometido por atacantes.

En líneas generales, la aplicación destaca por su impecable robustez en materia de seguridad, aunque se ve afectada por una limitación significativa que podría afectar dicha característica distintiva. Esta restricción está vinculada a la condición de que los usuarios cuenten con un dispositivo móvil dotado de capacidades de reconocimiento facial o dactilar. A pesar de que los dispositivos móviles son cada vez más accesibles y ubicuos, la integración de sistemas de autenticación facial sigue siendo un proceso en constante evolución. Es crucial tener en cuenta que, a pesar de los avances tecnológicos, algunos dispositivos aún presentan limitaciones (Padilha et al., 2020). Los educadores que carezcan de dispositivos actualizados o que no dispongan de estas capacidades específicas se encontrarán con una capa de autenticación menos, aumentando así el riesgo de falta de autenticidad en el registro.

Indudablemente, la conexión intrínseca de una capa de autenticación con la tecnología nativa del dispositivo es un hecho innegable. No obstante, la otra capa de verificación de identidad mantiene la mayor seguridad, incluso en dispositivos que carecen de esta función, gracias a la implementación de Amazon Rekognition. Esta plataforma, ya consolidada como un referente en seguridad, demuestra su valía al ofrecer beneficios sustanciales en el proceso de registro de asistencia. Aspectos como una seguridad ampliada y una transparencia mejorada se han evidenciado, respaldados por investigaciones recientes que destacan sus potenciales ventajas en este contexto (Kodali et al., 2023).

## CONCLUSIONES

Los resultados de este estudio indican que la aplicación móvil para el control de asistencia docente, que incorpora autenticación biométrica y verificación por geolocalización en la Universidad Nacional de Trujillo es una herramienta que fortalece la seguridad en el proceso de registro de asistencia. Se ha observado una tasa de precisión del 95% en la autenticación biométrica, se evidenció una significativa reducción en el tiempo necesario para completar el proceso de registro, con un promedio de tan solo 32,68 segundos, y los

resultados de la encuesta aplicada revelan una percepción positiva en cuanto a la seguridad por parte de los usuarios, consolidando la aceptación y confianza en la implementación de esta solución tecnológica.

A pesar de la limitación asociada a la dependencia de las capacidades de reconocimiento facial o dactilar en los dispositivos, es innegable que la autenticación facial proporcionada por un servicio, en este caso, el Amazon Rekognition, demuestra ser más que adecuada para llevar a cabo una gestión segura y transparente de la asistencia. En perspectiva de futuras investigaciones, se contempla la replicación del experimento con docentes y personal administrativo, dado que, por restricciones de tiempo, no fue posible incluirlos en esta ocasión. También se sugiere investigar la adopción de esta tecnología en el registro de asistencia de los estudiantes, evaluando su impacto en la calidad y dinamismo de las clases.

## FINANCIAMIENTO

Ninguno.

## CONFLICTO DE INTERESES

No existe ningún tipo de conflicto de interés relacionado con la materia del trabajo.

## CONTRIBUCIÓN DE LOS AUTORES

Conceptualización, curación de datos, análisis formal, adquisición de fondos, investigación, administración del proyecto, software, supervisión, validación, visualización, redacción - borrador original, redacción - revisión y edición: Montañez-Díaz, B. A., García-Gutiérrez, W. F., Prieto-Pastor, R. A. y Mendoza-De-los-Santos, A.

## REFERENCIAS BIBLIOGRÁFICAS

Amazon. (2023). *Amazon Rekognition Image*. AWS. https://aws.amazon.com/es/rekognition/image-features/

Ammour, N., Bazi, Y., & Alajlan, N. (2023). Multimodal Approach for Enhancing Biometric Authentication. *Journal of Imaging*, *9*(9), 168. https://doi.org/10.3390/jimaging9090168

Aza Poveda, S., & Rodriguez Vanegas, J. S. (2020). *Sistema de control biométrico de asistencia docente* [Universidad Distrital Francisco José de Caldas]. http://hdl.handle.net/11349/28315

Balapour, A., Nikkhah, H. R., & Sabherwal, R. (2020). Mobile application security: Role of perceived privacy as the predictor of security perceptions. *International Journal of Information Management*, *52*, 102063. https://doi.org/10.1016/j.ijinfomgt.2019.102063

Bhat, A., Rustagi, S., Purwaha, S. R., & Singhal, S. (2020). Deep-learning based group-photo Attendance System using One Shot Learning. *2020 International Conference on Electronics and Sustainable Communication Systems (ICESC)*, 546–551. https://doi.org/10.1109/ICESC48915.2020.9155755

Bhavsar, K., Shah, D. V., & Gopalan, D. S. (2020). Scrum: An Agile Process Reengineering In Software Engineering. *International Journal of Innovative Technology and Exploring Engineering*, *9*(3), 840–848. https://doi.org/10.35940/ijitee.C8545.019320

Dudjak, M., & Martinović, G. (2020). An API-first methodology for designing a microservice-based Backend as a Service platform. *Information Technology And Control*, *49*(2), 206–223. https://doi.org/10.5755/j01.itc.49.2.23757

Flutter. (2019). *Build beautiful native apps in record time*. Flutter. https://flutter-website-staging.firebaseapp.com/

Guo, X. (2021). A KNN Classifier for Face Recognition. *2021 International Conference on Communications, Information System and Computer Engineering (CISCE)*, 292–297. https://doi.org/10.1109/CISCE52179.2021.9445908

ISO/IEC 19794-5:2005. (2005). *Information technology — Biometric data interchange formats*. International Organization for Standardization. https://www.iso.org/standard/38749.html

ISO/IEC 25010. (2011). *Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — System and software quality models*. Organization for Standardization, Technical Committee ISO/IEC JTC 1/SC 7. https://www.iso.org/obp/ui/#iso:std:iso-iec:25010:ed-1:v1:en

ISO/IEC 25040. (2011). *Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — Evaluation process*. The International Organization for Standardization, Technical Committee ISO/IEC JTC1/SC7. https://www.iso.org/obp/ui/#iso:std:iso-iec:25040:ed-1:v1:en

ISO/IEC JTC1 SC17 WG3. (2018). *Portrait Quality: Reference Facial Images for MRTD (Technical Report)*. International Civil Aviation Organization. https://www.icao.int/Security/FAL/TRIP/Documents/TR - Portrait Quality v1.0.pdf

Kausar, F. (2020). Cancelable Face Template Protection using Transform Features for Cyberworld Security. *International Journal of Advanced Computer Science and Applications*, *11*(1). https://doi.org/10.14569/IJACSA.2020.0110142

Kodali, R. K., Panda, A., & Boppana, L. (2023). Attendance System using Amazon Rekognition. *TENCON 2023 - 2023 IEEE Region 10 Conference (TENCON)*, 65–70. https://doi.org/10.1109/TENCON58879.2023.10322521

Kounev, S., Herbst, N., Abad, C. L., Iosup, A., Foster, I., Shenoy, P., Rana, O., & Chien, A. A. (2023). Serverless Computing: What It Is, and What It Is Not? *Communications of the ACM*, *66*(9), 80–92. https://doi.org/10.1145/3587249

Leotta, M., Mori, F., & Ribaudo, M. (2023). Evaluating the effectiveness of automatic image captioning for web accessibility. *Universal Access in the Information Society*, *22*(4), 1293–1313. https://doi.org/10.1007/s10209-022-00906-7

Li, L., Chen, C., Pan, L., Zhang, L. Y., Wang, Z., Zhang, J., & Xiang, Y. (2023). A Survey of PPG's Application in Authentication. *Computers & Security*, *135*, 103488. https://doi.org/10.1016/j.cose.2023.103488

Lovrić, L., Fischer, M., Röderer, N., & Wünsch, A. (2023). Evaluation of the Cross-Platform Framework Flutter Using the Example of a Cancer Counselling App. *Proceedings of the 9th International Conference on Information and Communication Technologies for Ageing Well and E-Health*, 135–142. https://doi.org/10.5220/0011824500003476

Moral, P. (2021). *Sistemas de geolocalización, control del trabajador y facultad disciplinaria empresarial* [Universidad de Valladolid]. https://uvadoc.uva.es/handle/10324/50965

Nakisa, B., Ansarizadeh, F., Oommen, P., & Kumar, R. (2023). Using an extended technology acceptance model to investigate facial authentication. *Telematics and Informatics Reports*, *12*, 100099. https://doi.org/10.1016/j.teler.2023.100099

Novoa, P., Reyes, J., & Cedeño, J. (2019). Aplicación móvil inteligente para asistir el registro de actividades académicas en sistemas biométricos: una experiencia universitaria en el Ecuador. *Revista Científica de La Universidad de Cienfuegos*, *11*(2), 55–60. https://rus.ucf.edu.cu/index.php/rus/article/view/1150

Padilha, R., Andaló, F. A., Bertocco, G., Almeida, W. R., Dias, W., Resek, T., Torres, R. da S., Wainer, J., & Rocha, A. (2020). Two-tiered face verification with low-memory footprint for mobile devices. *IET Biometrics*, *9*(5), 205–215. https://doi.org/10.1049/iet-bmt.2020.0031

Saadon, J. R., Yang, F., Burgert, R., Mohammad, S., Gammel, T., Sepe, M., Rafailovich, M., Mikell, C. B., Polak, P., & Mofakham, S. (2023). Real-time emotion detection by quantitative facial motion analysis. *PLOS ONE*, *18*(3), e0282730. https://doi.org/10.1371/journal.pone.0282730

Salvatierra, G. (2018). *Desarrollo de un sistema de control de asistencia estudiantil mediante reconocimiento facial* [Universidad Internacional de la Rioja]. https://reunir.unir.net/handle/123456789/7425

Sandhya, N., Vijaya Saraswathi, R., Preethi, P., Aarti Chowdary, K., Rishitha, M., & Sai Vaishnavi, V. (2022). Smart Attendance System Using Speech Recognition. *2022 4th International Conference on Smart Systems and Inventive Technology (ICSSIT)*, 144–149. https://doi.org/10.1109/ICSSIT53264.2022.9716261

Sang, J., Lei, Z., & Li, S. Z. (2009). *Face Image Quality Evaluation for ISO/IEC Standards 19794-5 and 29794-5* (pp. 229–238). https://doi.org/10.1007/978-3-642-01793-3_24

Silvelo, A. (2019). *Sistema de autenticación biométrica basado en el análisis del comportamiento mediante interacción por pantalla táctil y sensores de movimiento* [Universidad de La Coruña]. http://hdl.handle.net/2183/24560

Soewito, B., Gaol, F. L., Simanjuntak, E., & Gunawan, F. E. (2016). Smart mobile attendance system using voice recognition and fingerprint on smartphone. *2016 International Seminar on Intelligent Technology and Its Applications (ISITIA)*, 175–180. https://doi.org/10.1109/ISITIA.2016.7828654

Sulla, T. (2022). *Sistema biométrico basado en aplicaciones móviles para el control de asistencia de estudiantes del Instituto Superior Tecnológico Americana del Cusco* [Universidad de Guayaquil]. http://repositorio.ug.edu.ec/handle/redug/30756

Supabase. (2023). *The Open Source Firebase Alternative*. Supabase. https://supabase.com/

Tee, T. X., & Khoo, H. K. (2020). Facial Recognition using Enhanced Facial Features k-Nearest Neighbor (k-NN) for Attendance System. *Proceedings of the 2020 2nd International Conference on Information Technology and Computer Communications*, 14–18. https://doi.org/10.1145/3417473.3417475

Torres, E. (2019). *Implementación De Un Sistema De Control De Asistencia Con Código Qr Para La Institución Educativa Ricardo Palma – Carhuaz; 2019* [Universidad Católica Los Ángeles Chimbote]. http://repositorio.uladech.edu.pe/handle/20.500.13032/13800

Valverde, M. (2018). *Desarrollo de una aplicación móvil android para la Empresa Righttek S.A. como aporte a los controles de localización y registro de ubicación del personal de soporte a usuarios* [Universidad César Vallejo]. https://hdl.handle.net/20.500.12692/87748

Vardakis, G., Tsamis, G., Koutsaki, E., Haridimos, K., & Papadakis, N. (2022). Smart Home: Deep Learning as a Method for Machine Learning in Recognition of Face, Silhouette and Human Activity in the Service of a Safe Home. *Electronics*, *11*(10), 1622. https://doi.org/10.3390/electronics11101622

Wasilewski, K., & Zabierowski, W. (2021). A Comparison of Java, Flutter and Kotlin/Native Technologies for Sensor Data-Driven Applications. *Sensors*, *21*(10), 3324. https://doi.org/10.3390/s21103324

Zambrano-Vega, C., Oviedo, B., & Moncayo Carreño, O. (2020). *Assessing the Performance of a Biometric Mobile Application for Workdays Registration* (pp. 1004–1015). https://doi.org/10.1007/978-3-030-12385-7_68