FARAUTE, Vol. 17, No. 2: 03-12, 2022 Print ISSN 1698-7418
Online ISSN 2542-3061

MICROSERVICIO DE VERIFICACIÓN BIOMÉTRICA FACIAL USANDO TÉCNICAS INTELIGENTES PARA AUMENTAR NIVELES DE SEGURIDAD. CASO DE ESTUDIO: AUTENTICACIÓN PARA APLICACIONES BANCARIAS Y PASARELAS DE PAGO.

HERRERA, M., COLMENAREZ, L., GAZCÓN, D.
Universidad de Carabobo. Facultad Experimental de Ciencias y Tecnología.
Dpto. de Computación. Bárbula, Edo. Carabobo, Venezuela.
mherrera@uc.edu.ve, luis.miguelcv2@gmail.com, daniel.gazcon27@gmail.com

Recibido: 23/09/2025, Revisado: 15/10/2025, Aceptado: 15/11/2025

Resumen

La Inteligencia Artificial (IA) ha transformado diversos aspectos de la vida diaria, desde la generación de contenido hasta la optimización de procesos. Sin embargo, su creciente aplicación en el reconocimiento y autenticación facial ha introducido desafíos de seguridad significativos, especialmente con la proliferación de imágenes sintéticas. Este trabajo presenta la implementación de un microservicio de autenticación biométrica facial que, de manera innovadora, no solo verifica identidades, sino que también identifica y descarta eficazmente imágenes generadas por IA. Esto pudiera elevar considerablemente los niveles de seguridad en aplicaciones bancarias y pasarelas de pago. En el desarrollo de la solución se empleó una metodología híbrida que combina la agilidad de *XP* con la estructura de CRISP-DM, facilitando un desarrollo iterativo y un manejo de datos optimizado. El microservicio integró técnicas avanzadas de IA como los modelos de redes neuronales convolucionales para la detección de vivacidad, asegurando la autenticidad de la fuente de la imagen. Los resultados mostraron precisión para imágenes falsas del 99.2% y para reales del 98.3% con un *recall* del 78.8% para imágenes falsas y del 97.6% para reales. Asimismo, el *F1-score* estuvo en 87.9% para imágenes falsas y un 97.9% para las reales, por lo que la precisión del microservicio al distinguir entre imágenes auténticas y falsas, cumplió con los estándares de seguridad requeridos. Esta solución no solo representa una mejora en la autenticación facial segura, sino que también establece una base para futuras investigaciones en el campo de la seguridad digital frente a los desafíos emergentes de la IA generativa.

Palabras clave: Microservicio, Autenticación, Reconocimiento facial, Suplantación de identidad, Detección de vivacidad, Redes neuronales convolucionales.

FACIAL BIOMETRIC VERIFICATION MICROSERVICE USING INTELLIGENT TECHNIQUES TO ENHANCE SECURITY LEVELS. CASE STUDY: AUTHENTICATION FOR BANKING APPLICATIONS AND PAYMENT GATEWAYS

Abstract

Artificial Intelligence (AI) has transformed various aspects of daily life, from content generation to process optimization. However, its increasing application in facial recognition and authentication has introduced significant security challenges, especially with the proliferation of synthetic images. This work presents the implementation of a facial biometric authentication microservice that, in an innovative manner, not only verifies identities but also effectively identifies and discards AI-generated images. This could significantly elevate security levels in banking applications and payment gateways. The development of the solution employed a hybrid methodology combining

the agility of XP with the structure of CRISP-DM, facilitating iterative development and optimized data management. The microservice integrated advanced AI techniques such as convolutional neural network models for liveness detection, ensuring the authenticity of the image source. Results showed an accuracy for fake images of 99.2% and for real images of 98.3%, with a recall of 78.8% for fake images and 97.6% for real images. Furthermore, the F1-score was 87.9% for fake images and 97.9% for real images, demonstrating that the microservice's precision in distinguishing between authentic and synthetic images met the required security standards. This solution not only represents an improvement in secure facial authentication but also establishes a foundation for future research in the field of digital security against the emerging challenges of generative AI.
Keywords: Microservice, Authentication, Facial recognition, Identity spoofing, Liveness detection, Convolutional neural networks.

1. Introducción

Hoy en día, el surgimiento de la Inteligencia Artificial (IA), definida por John McCarthy (2009) como "la ciencia e ingeniería de hacer máquinas inteligentes", ha traído consigo innumerables ventajas, desde la generación de contenido hasta la optimización de procesos. Estos avances han mejorado la eficiencia en el estudio y el trabajo e incluso en actividades cotidianas.

Sin embargo, este progreso tecnológico también ha propiciado la explotación de vulnerabilidades en sistemas que no se han adaptado a este crecimiento exponencial y que carecen de la capacidad para distinguir entre una imagen legítima y una generada por IA. En el ámbito de la autenticación biométrica, la amenaza más latente es los *deepfakes*, es decir, imágenes o videos sintéticos hiperrealistas creados con IA generativa que pueden simular la apariencia y gestos de una persona con una precisión alarmante. La amplia disponibilidad de modelos generativos, como DALL-E-2 (OpenAI, 2022), junto con herramientas de código abierto como Deepfakes/Faceswap en plataformas como GitHub (2020), ha democratizado la creación de este tipo de contenido. Un ataque exitoso utilizando estas imágenes generadas por IA en aplicaciones bancarias y pasarelas de pago puede tener un impacto devastador. Esto incluye pérdidas financieras masivas para usuarios e instituciones, el compromiso de la privacidad de datos sensibles y una erosión significativa de la confianza en los sistemas de seguridad digital. Por ejemplo, en 2023, se reportaron múltiples casos de fraudes donde *deepfakes* de voz y video se utilizaron para suplantar a ejecutivos y autorizar transferencias fraudulentas de millones de dólares (Probal & Majden, S. 2025), evidenciando la creciente sofisticación de estas amenazas. La importancia de reforzar estos controles se ve reflejada en la práctica de plataformas como Binance, que requieren la verificación facial incluso para operaciones sensibles como el retiro de NFTs, demostrando la alta demanda de seguridad en transacciones digitales (Binance, 2022).

En los últimos años, según un estudio realizado por el IC3 (*Internet Crime Complaint Center*) en el año 2023, los delitos de robo de identidad y el *spoofing* han figurado consistentemente entre los 10 delitos más frecuentes en internet, causando pérdidas que superaron los $360,437,724 de dólares en un solo año (IC3, 2023). Por su parte, el *spoofing* se define como el acto deliberado de manipular información sensible y de contacto (correo electrónico, teléfono, sitios *web*, imágenes o voz) con el objetivo de suplantar una identidad. Si bien el robo de identidad ha existido por muchos años, siendo las llamadas y los mensajes los métodos más utilizados

masivamente para cometer robos o fraudes, hoy en día, gracias a la IA, se ha vuelto aún más complejo identificar este tipo de fraudes. Los sistemas actuales de autenticación biométrica facial a menudo dependen de características superficiales de la imagen o pruebas de vivacidad (*liveness detection*) que pueden ser burladas por *deepfakes* más sofisticados, poniendo en riesgo la seguridad de los mecanismos digitales (Fernando et al., 2020; Li et al., 2022). Trabajos seminales, como FaceForensics++ de Rössler et al. (2019), han destacado la complejidad de detectar imágenes faciales manipuladas y la necesidad de enfoques de aprendizaje automático para combatirlas. De hecho, la creciente sofisticación de estos ataques de suplantación, o "ataques de presentación", subraya la importancia de implementar robustos sistemas de Detección de Ataques de Presentación (PAD), un área formalmente abordada por estándares como ISO/IEC 30107-1 (2023). La limitación inherente radica en que muchos de estos sistemas no están diseñados para analizar las sutilezas y anomalías imperceptibles para el ojo humano que delatan una imagen sintética.

Este trabajo abordó la problemática planteada, mediante la implementación de un microservicio, cuya arquitectura se considera estratégica y fundamental para una solución de seguridad de esta magnitud. Específicamente, la arquitectura de microservicios ofrece ventajas cruciales como: la escalabilidad, al permitir que el componente de verificación biométrica maneje un alto volumen de solicitudes de forma independiente; la resiliencia, dado que el fallo de un microservicio no afecta la operatividad del sistema completo; y la independencia en el despliegue y desarrollo, al facilitar actualizaciones y mejora continua de los componentes de seguridad, sin interrumpir otras funcionalidades de las aplicaciones bancarias o pasarelas de pago (Richards & Ford, 2015).

Por consiguiente, se plantearon los siguientes objetivos:

- Diseñar e implementar un microservicio de autenticación biométrica facial, capaz de verificar la identidad de un usuario a partir de una imagen.
- Desarrollar e integrar un algoritmo basado en *Deep Learning*, específicamente *YOLO* (*You Only Look Once*), para identificar y descartar imágenes generadas por IA, como por ejemplo *DALL-E-2* OpenAI (2022), *Craiyon* o *Midjourney*) en tiempo real, garantizando la autenticidad de la fuente de la imagen.
- Evaluar la precisión y robustez del microservicio propuesto frente a diferentes tipos de ataques de *spoofing* y *deepfakes*, demostrando su capacidad para cumplir con los estándares de seguridad requeridos en entornos financieros.

La contribución principal del estudio residió en el desarrollo de un microservicio de autenticación facial que incorpora una capa de seguridad proactiva contra la IA generativa, a fin de subsanar las principales limitaciones de los sistemas biométricos tradicionales. Esta solución se enfocó en mejorar la autenticación facial, con el fin de proveer una solución para la seguridad digital en un panorama de amenazas en constante evolución, ofreciendo una defensa adaptable frente a la plantación de identidad avanzada.

2. Metodología

La investigación se fundamentó en una estrategia metodológica combinada, que integra *CRISP*-DM (*Cross-Industry Standard Process for Data Mining*) y *eXtreme Programming* (*XP*). Esta sinergia permitió un enfoque ágil y estructurado, idóneo para el desarrollo de soluciones de *Machine Learning* (*ML*) en el contexto de la seguridad biométrica.

Estrategia de Desarrollo Combinada *CRISP-DM* y *eXtreme Programming* (*XP*): Esta combinación fue seleccionada por su capacidad para manejar la complejidad de

proyectos de ciencia de datos con la agilidad necesaria para adaptarse a requisitos cambiantes. Por su parte, *CRISP-DM* (Chapman et al, 2000) proporcionó el marco estructurado para el ciclo de vida de los datos, mientras que XP aportó principios de desarrollo ágil como *pair programming*, *Test-Driven Development (TDD)* e integración continua, esenciales para el desarrollo iterativo de alta calidad. Las fases de *CRISP-DM* (Comprensión del negocio, comprensión y preparación de datos, diseño y modelado, evaluación y pruebas, despliegue y mejora continua) se gestionaron a través de *sprints* de *XP*, permitiendo una ejecución ágil y una retroalimentación constante.

Las Figuras 1 y 2 a continuación muestran las etapas y los cilclos de cada una.

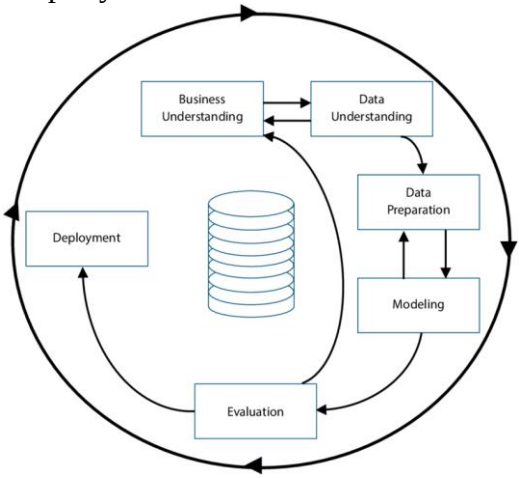

Figura 1. Etapas del modelo *CRISP-DM* 1.0
Fuente: Chapman et al., (2000)

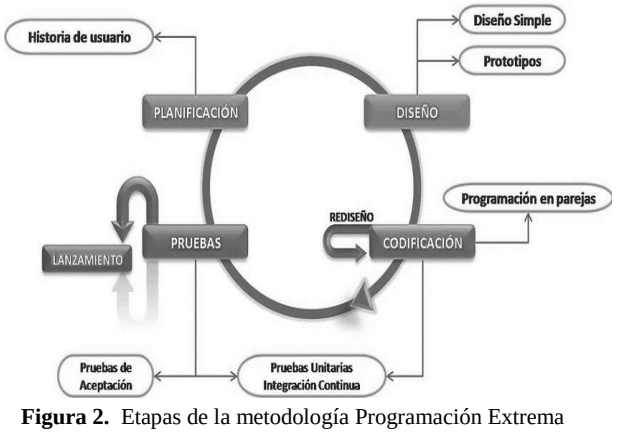

Figura 2. Etapas de la metodología Programación Extrema XP.
Fuente: Fojtik, R. (2011).

3. Resultados y Análisis

El microservicio de autenticación biométrica facial desarrollado, se compone de tres módulos principales: obtención y preprocesamiento de datos, procesamiento y análisis de datos, y entrenamiento del modelo. A continuación, se presentan los resultados obtenidos en cada etapa clave del sistema.

- **Diseño del microservicio**: El microservicio de verificación biométrica facial fue diseñado utilizando los principios de la arquitectura de microservicios (Richards & Ford, 2015), con el fin de garantizar independencia de despliegue, escalabilidad (horizontalmente para los módulos críticos) y tolerancia a fallos. La comunicación entre componentes y con las aplicaciones cliente se realizó a través de *APIs RESTful* ligeras. En cuanto a la interfaz de la *API*, ésta acepta solicitudes *HTTP POST* con la imagen facial codificada en Base64. Entonces, retorna respuestas *JSON* con un veredicto de autenticación, una puntuación de confianza para la verificación, y un veredicto de detección de *deepfake* con su respectiva puntuación de confianza.
- **Tecnologías:** La arquitectura general del microservicio integra *Python* y *Flask* para la gestión de servicios web, y el modelo *YOLO* para la detección y reconocimiento facial. La selección de *YOLO* se fundamentó en su alta velocidad y precisión, así como en su naturaleza de código abierto, lo que permitió una integración eficiente y personalización según los requerimientos del sistema. Este modelo, introducido por Redmon et al. (2016), se distingue por su capacidad de realizar detección de objetos en tiempo real, procesando imágenes completas en un solo paso, lo cual es ideal para aplicaciones de autenticación biométrica que exigen baja latencia.

  En este contexto, se realizó una comparativa entre tecnologías de procesamiento de imágenes (*YOLO*, *Faster R-CNN*, *SSD*, *RetinaNet*), concluyendo que

YOLO ofrecía el mejor equilibrio entre velocidad y precisión para el contexto de autenticación biométrica en tiempo real (Tabla 1). El desarrollo se apoyó en *Python* como lenguaje principal, *PyTorch* para el *Deep Learning*, y *OpenCV* para el procesamiento de imágenes. La elección de estas herramientas se basó en características de robustez, eficiencia y amplio soporte comunitario en visión por computadora. Se utilizó *Flask* para la interfaz *API RESTful* y con *Git* se gestionó el control de versiones.

Tabla1. Comparación entre tecnologías de procesamiento de imágenes

Tecnología	Descripción	Ventajas	Calibración
YOLO (You Only Look Once)	Modelo de detección de objetos en tiempo real que utiliza una única red neuronal para predecir bounding boxes y clases simultáneamente.	• Código Abierto • Alta velocidad de inferencia. • Buena precisión en detección. • Capacidad de detectar múltiples objetos en una sola imagen.	• Ajuste de hiperparámetros como tasa de aprendizaje, tamaño del lote y número de épocas. • Evaluación mediante métricas como AP50 y puntuación F1.
Faster R-CNN	Modelo que combina un algoritmo de propuesta de región con una red neuronal para la detección de objetos	• Alta precisión en detección. • Mejor rendimiento en conjuntos de datos complejos.	Requiere ajuste fino y entrenamiento prolongado.
SSD (Single Shot MultiBox Detector)	Modelo que realiza detección en múltiples escalas utilizando una sola red para predecir bounding boxes y clases.	• Buen equilibrio entre velocidad y precisión. • Capacidad para manejar objetos en diferentes escalas	Calibración similar a YOLO, ajustando hiperparámetros y utilizando métricas como IOU (Intersección sobre Unión).
RetinaNet	Modelo que utiliza una función de pérdida focal para abordar el problema del desequilibrio entre clases en la detección.	Alta precisión en detecciones difíciles. .	Ajuste de hiperparámetros y uso de funciones de pérdida focal para mejorar la precisión

Fuente: Elaboración propia

- **Obtención y preprocesamiento de datos:** Para el entrenamiento y validación del sistema, se construyeron dos conjuntos de datos: uno de imágenes reales, capturadas en condiciones diversas mediante una aplicación *web* que incluyó un mensaje previo de consentimiento informado conforme a normativas legales aplicables, y otro de imágenes falsas, generadas por IA o editadas digitalmente. Se recolectaron 1,439 imágenes reales y 1,146 falsas, asegurando diversidad en edad, raza y condiciones ambientales. Asimismo, el preprocesamiento incluyó validación de formato, redimensionamiento a 416x416 píxeles y normalización de los valores de píxeles. Para garantizar la seguridad y legitimidad de las muestras biométricas, el sistema consideró los lineamientos de la norma internacional ISO/IEC 30107-1 (ISO/IEC 30107-1, 2023) para la detección de ataques de presentación. Este proceso garantizó la calidad, homogeneidad y cumplimiento ético de los datos, como parte la correcta manipulación y desempeño del modelo.
- **Procesamiento y análisis de imágenes:** El módulo de análisis utiliza *YOLO v11*, cargado mediante la biblioteca *Ultralytics* basada en *PyTorch*. El flujo del sistema consistió en la detección de rostros en imágenes, extracción de las características clave y comparación de los resultados con las plantillas almacenadas; utilizando métricas como la distancia euclidiana o coseno para calcular la probabilidad de coincidencia. Específicamente, la respuesta del microservicio se estructuró a partir del formato *JSON*, indicando el estado de autenticación y el porcentaje de coincidencia, para facilitar su integración con aplicaciones externas.
- **Entorno de entrenamiento:** El modelo se desarrolló y ejecutó en un equipo con procesador *AMD Ryzen 7 5825U*, con tarjeta gráfica integrada *Radeon* y 16 GB de *RAM* bajo *Linux Ubuntu*. Se empleó *PyTorch 2.4.1* y *Ultralytics YOLO 8.3.8*, utilizando el modelo *YOLO v11*, el cual destacó por su eficiencia en precisión y velocidad para la detección en tiempo real. El procesamiento de imágenes se realizó con *OpenCV 4.10.0.84* y *NumPy 2.1.2*. El desarrollo del microservicio y las comunicaciones se gestionaron mediante *Flask 2.2.2, Flask-SQLAlchemy 3.0.2 y Flask-JWT-Extended 4.3.1*. Debido a la ausencia de *GPU* dedicada, todo el entrenamiento y la inferencia se realizaron exclusivamente en el *CPU*, garantizando la compatibilidad y estabilidad del sistema en entornos con recursos limitados.

- **Entrenamiento y evaluación del modelo:** El modelo se entrenó con una división estándar: 70% de los datos para entrenamiento, 15% para validación y 15% para prueba. Los parámetros de cada imagen (tipo, ubicación y dimensiones del rostro) se almacenaron junto a las imágenes, permitiendo un análisis detallado durante el entrenamiento (Figura 3).
- Se ajustaron hiperparámetros como la tasa de aprendizaje, número de épocas y tamaño del lote para optimizar el rendimiento. El entrenamiento se realizó durante 30 épocas, utilizando archivos de configuración específicos para *YOLO*.

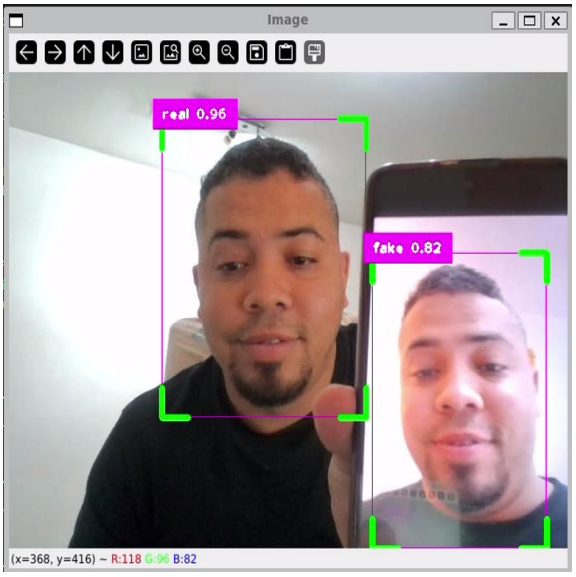

Figura 3. Prueba del modelo usando un rostro real y uno digitalizado. Fuente: Elaboración propia

La evaluación del modelo se llevó a cabo mediante validación cruzada y métricas como precisión, *recall* y *F1-score* (Figura 4).

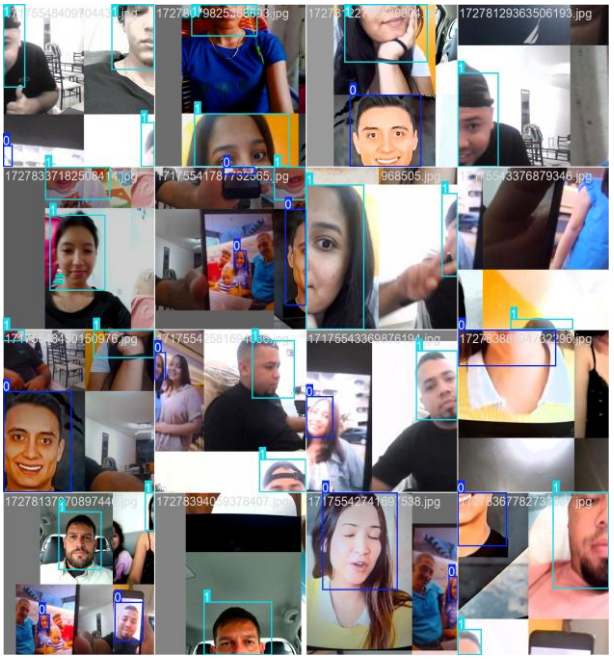

Figura 4. Conjunto de Imágenes cruzadas durante el entrenamiento por YOLO. Fuente: Elaboración propia

La matriz de confusión (Figura 5) permitió visualizar los aciertos y errores del modelo en la clasificación de imágenes reales y falsas.

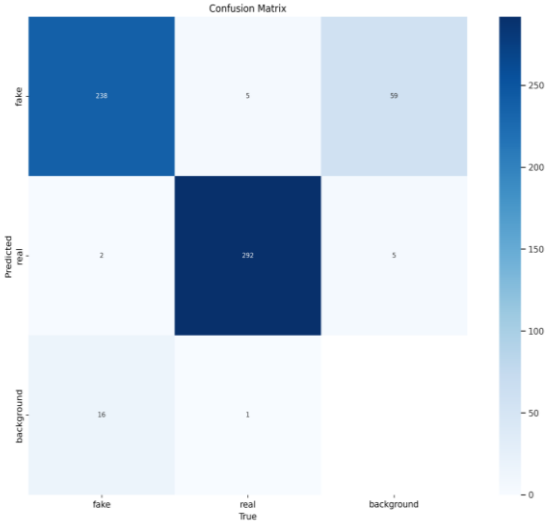

Figura 5. Matriz de Confusión generada durante el entrenamiento. Fuente: Elaboración propia

- **Principales resultados**
  - Precisión:
    Para imágenes falsas: 99.2%
    Para imágenes reales: 98.3%
  - *Recall*:

Para imágenes falsas: 78.8%
Para imágenes reales: 97.6%

- *F1-score:*
  Para imágenes falsas: 87.9%
  Para imágenes reales: 97.9%

Estos resultados reflejan un desempeño robusto en la detección de imágenes auténticas, aunque se identificó cierto margen de mejora en la sensibilidad para imágenes falsas, lo que sugiere la necesidad de realizar optimización adicional, para reducir falsos negativos.

- **Detalles de la implementación:** La implementación de esta solución como un microservicio confiere varias ventajas prácticas y estratégicas fundamentales para su aplicación en entornos bancarios y pasarelas de pago. En primer lugar, ofrece una facilidad de integración notable, ya que utiliza una *API RESTful* bien definida, que permite una conexión sin esfuerzo con sistemas existentes (móviles, *web y* escritorio) sin requerir cambios estructurales significativos en la infraestructura del cliente. Esta agilidad en la integración es clave. En segundo lugar, su arquitectura permite actualizar, mejorar o reemplazar el componente de seguridad, de forma completamente independiente al resto de la aplicación. Esto es crucial en el ámbito de la seguridad digital, donde las amenazas, como los nuevos tipos de *deepfakes*, evolucionan rápidamente, facilitando una respuesta ágil a nuevas vulnerabilidades. Además, el módulo de verificación biométrica y detección de *deepfakes* es reutilizable en diferentes aplicaciones o servicios dentro de la misma organización para optimizar recursos, y su naturaleza desacoplada permite la escalabilidad horizontal solo de este componente específico ante picos de demanda, manteniendo la eficiencia operativa y la resiliencia del sistema completo, al evitar que el fallo en el microservicio de seguridad comprometa otras funcionalidades críticas.

  A pesar de las ventajas, se identificaron ciertas limitaciones y desafíos durante el desarrollo e implementación del microservicio. Uno de los principales es la necesidad continua de grandes conjuntos de datos de *deepfakes*; el rendimiento del modelo en su detección está directamente correlacionado con la diversidad y el volumen de imágenes sintéticas usadas para su entrenamiento, y obtener datos que representen la evolución constante de las técnicas de IA generativa, sigue siendo un desafío considerable. Asimismo, la privacidad y la ética en la recolección de datos biométricos, incluso con el debido consentimiento aplicado en la fase experimental, plantean importantes consideraciones, exigiendo un manejo seguro y la anonimización de la información recolectada de voluntarios, así como una estricta adherencia a las regulaciones de protección de datos. Otro desafío, es la complejidad de detectar ataques de *liveness* más sofisticados como, por ejemplo, las máscaras *3D* de alta fidelidad, entre otras técnicas, lo cual configura a esta área de investigación como activa y se pudiera considerar como un desafío permanente para cualquier sistema. Finalmente, el consumo de recursos computacionales para el entrenamiento de modelos de *Deep Learning* como *YOLOv11* y su posterior inferencia, aunque optimizada, puede implicar costos de infraestructura y consideraciones de latencia en despliegues a gran escala.

- **Pruebas de integración y validación en aplicaciones:** El microservicio fue integrado exitosamente en un entorno de prueba de banca electrónica, *Bárbula Bank*, que permitió evaluar su desempeño en un escenario real de autenticación facial (Figura 6). La integración presentó dos aspectos novedosos que facilitaron su adopción y robustez para la seguridad del sistema.

Figura 6. Aplicación Bancaria Bárbula Bank, Pantalla de Inicio de sesión. Fuente: Elaboración propia

En primer lugar, la captura de la imagen facial y su análisis se realizaron directamente en el servidor propio del microservicio, mediante una *URL* proporcionada por la aplicación bancaria (Figura 7 y Figura 8). Esto implicó que la banca no necesitó implementar localmente la captura ni el procesamiento de imágenes, sino que consumía un servicio *web* centralizado que gestionaba todo el flujo de verificación biométrica. En consecuencia, la arquitectura basada en microservicios redujo la complejidad técnica en el cliente, agilizando la integración y permitiendo mantener un control centralizado sobre la calidad y actualización del modelo de autenticación.

```json
{
    "reference": "tracking_id_12345",
    "redirect_url": "https://miaplicacion.com/resultado",
    "notification_url": "https://miaplicacion.com/webhook",
    "reference_image": {
        "id": "reference_image_id",
        "base64": "iVBORw0KGgoAAAANSUhEUgAAAAUA..."
    }
}
```

Figura 7. Ejemplo de estructura *JSON* de solicitud al servicio que genera la verificación. Fuente: Elaboración propia

```json
{
    "verification_url": "http://sure.app/verification/MzEx"
}
```

Figura 8. Ejemplo de *JSON* de respuesta con *URL* que inicia la verificación con captura de rostros. Fuente: Elaboración Propia

En segundo lugar, para la comunicación de resultados, se implementó un *webhook* de notificaciones que enviaba en tiempo real la respuesta del análisis biométrico a la aplicación bancaria (Figura 9). A través de este mecanismo, *Bárbula Bank* recibía automáticamente el estado de autenticación y el porcentaje de coincidencia, facilitando la toma de decisiones en los procesos de acceso y mitigando riesgos de fraude.

Durante las pruebas, el sistema demostró identificar correctamente imágenes reales y detectar intentos de suplantación mediante imágenes generadas artificialmente, proporcionando resultados confiables y tiempos de respuesta adecuados para aplicaciones críticas. Esta solución integrada evidenció un avance significativo en la autenticación biométrica para entornos bancarios, combinando innovación tecnológica con facilidad de despliegue y operación.

```json
{
    "reference": "tracking_id_12345",
    "real_match_probability": 90,
    "real_images": 2,
    "fake_images": 0
}
```

Figura 9. Ejemplo de Json recibido en el *webhook* de notificaciones tras análisis de autenticación biométrica. Fuente: Elaboración propia

4. Conclusiones

El microservicio de verificación biométrica facial desarrollado, ha demostrado ser una solución eficiente y segura para la autenticación de identidades en entornos digitales críticos. Su arquitectura basada en microservicios facilitó una integración flexible y escalable, mientras que la aplicación de técnicas avanzadas de *Machine Learning*, específicamente el modelo *YOLOv11* para la detección de *deepfakes*, permitió

alcanzar altos niveles de precisión en la clasificación de imágenes auténticas y sintéticas, elevando significativamente el estándar de seguridad.

La combinación de las metodologías *CRISP-DM* y *eXtreme Programming* (*XP*) garantizó un desarrollo organizado, iterativo y de alta calidad, cumpliendo con los objetivos planteados. Las pruebas funcionales y de rendimiento confirmaron la capacidad del sistema para procesar imágenes en tiempo real y mitigar eficazmente los riesgos de fraude. La integración innovadora, que centraliza la captura y el análisis de la imagen en el servidor del microservicio (mediante una *URL*), comunica los resultados vía *webhook*, simplificando drásticamente la adopción por parte de las aplicaciones bancarias y reduciendo la complejidad técnica en el cliente para hacer más robusto el control centralizado sobre la calidad y actualización del modelo. Este trabajo establece una base de partida y un hallazgo que contribuye tangiblemente al aumento de la seguridad en la autenticación biométrica.

A pesar del robusto desempeño alcanzado, se identificaron áreas y oportunidades de mejora para futuras investigaciones que podrían potenciar aún más la solución y abrir nuevas vías en el campo de investigación. En este sentido, se recomienda explorar técnicas más avanzadas para la detección de *liveness* multimodal, combinando, por ejemplo, datos de voz, movimiento o profundidad junto con el video facial. Asimismo, será crucial realizar una evaluación exhaustiva del rendimiento del microservicio con datos en producción y bajo un rango más amplio de condiciones ambientales no controladas, como variaciones extremas de iluminación, resolución de cámara y calidad de imagen. Otro aspecto relevante, es el análisis de la robustez del sistema frente a ataques adversarios diseñados para engañar intencionadamente al modelo de IA, y el desarrollo de contramedidas específicas. Finalmente, es fundamental continuar profundizando en las consideraciones éticas y de privacidad del uso generalizado de la biometría facial y la IA en la autenticación, con el fin de proponer directrices y mejores prácticas para asegurar un despliegue responsable y beneficioso para la sociedad.

5. Bibliografía

Binance (2022) Why Do I Need to Complete Facial Verification Again When Withdrawing NFT. https://www.binance.com/en/support/faq/why-do-i-need-to-complete-facial-verification-again-when-withdrawing-nft-b3ecf2f5cefd4435bb7e12f043e88679 (Última visita, 25 de septiembre 2023)

Chapman, P., Clinton, J., Kerber, R., Khabaza, T., Reinartz, T., Shearer, C. and Wirth, R., (2000). CRISP-DM 1.0 Step-by-step data mining guide.

Fernando, T., Priyasad, D., Sridharan, S., Ross, A., & Fookes, C. (2020). Face Deepfakes - A Comprehensive Review. *arXiv preprint arXiv:2005.09812*.

Github (2020) deepfakes/faceswap: Deepfakes Software for All. Retrieved obtenido de https://github.com/deepfakes/faceswap

IC3 (2023). Internet Crime Reporte by Federal Bureau of Investigation. https://www.ic3.gov/AnnualReport/Reports/2023_IC3Report.pdf

ISO/IEC 30107-1(2023). Information technology — Biometric presentation attack detection — Part 1: Framework ISO/IEC 30107-1:2023 - ISO/IEC 30107-1:2023 (Última visita 21 de julio de 2025)

Li, C., Dhillon, G., & Han, R. (2022). A deepfake-powered attack framework for automated security evaluation of facial liveness verification. *Penn State College of Information Sciences and Technology*.

McCarthy, J (2009) What is Artificial Intelligence. https://www-formal.stanford.edu/jmc/whatisai.pdf

(Última visita 29 de septiembre de 2023)
OpenAI (2022, 28 de septiembre). DALL·E now available without waitlist https://openai.com/blog/dall-e-now-available-without-waitlist (Última visita, 29 de septiembre de 2023)
Probal, & Majden, S. (2025). Deepfake fraud prevention: A strategic defense framework describing un aumento en fraudes con IA [Post]. LinkedIn. https://www.linkedin.com/pulse/deepfake-fraud-prevention-strategic-defense-framework-probal-tkc9c/
Redmon, J., Divvala, S., Girshick, R., & Farhadi, A. (2016). You Only Look Once: Unified Real-Time Object Detection. Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 779-788. https://doi.org/10.1109/CVPR.2016.91
Rössler, A., Cozzolino, D., Verdoliva, L., Riess, C., Thies, J., & Nießner, M. (2019). *FaceForensics++: Learning to detect manipulated facial images*. Proceedings of the IEEE International Conference on Computer Vision (ICCV), 1–11. https://doi.org/10.48550/arXiv.1901.08971