UNIVERSIDAD ALEJANDRO DE HUMBOLDT
FACULTAD DE INGENIERÍA
INGENIERÍA EN INFORMÁTICA
TRABAJO DE GRADO
SECCIÓN: DCM1004IIV1

DESARROLLO DE UN SISTEMA DE PAGOS MEDIANTE VINCULACIÓN DE CUENTA A TRAVÉS DE RECONOCIMIENTO FACIAL PARA EL BANCO DE VENEZUELA, S.A. BANCO UNIVERSAL.

Autor: Terán Gabriel
C.I: V-26.546.735
Tutor: Lic. Franklin Cedeño

Caracas, noviembre 2025.

UNIVERSIDAD ALEJANDRO DE HUMBOLDT
FACULTAD DE INGENIERÍA
INGENIERÍA EN INFORMÁTICA
TRABAJO DE GRADO
SECCIÓN: DCM1004IIV1

DESARROLLO DE UN SISTEMA DE PAGOS MEDIANTE VINCULACIÓN DE CUENTA A TRAVÉS DE RECONOCIMIENTO FACIAL PARA EL BANCO DE VENEZUELA, S.A. BANCO UNIVERSAL.

Trabajo de grado presentado como requisito para optar al Título de Ingeniero en Informática

Autor: Terán Gabriel
C.I: V-26.546.735
Tutor: Lic. Franklin Cedeño

Caracas, noviembre 2025.

UNIVERSIDAD ALEJANDRO DE HUMBOLDT
FACULTAD DE INGENIERÍA
ESCUELA DE INGENIERÍA EN INFORMÁTICA

APROBACIÓN DEL TUTOR

En mi carácter de tutor del Trabajo de Grado **"DESARROLLO DE UN SISTEMA DE PAGOS MEDIANTE VINCULACIÓN DE CUENTA A TRAVÉS DE RECONOCIMIENTO FACIAL PARA EL BANCO DE VENEZUELA, S.A. BANCO UNIVERSAL"**, elaborado por **TERÁN AZUAJE GABRIEL ANDRÉS** titular de la Cédula de Identidad N°. 26.546.735, para optar al Grado Académico de **Ingeniero en Informática** en la Universidad Alejandro de Humboldt, considero que dicho trabajo reúne los requisitos y méritos suficientes para ser aprobado y recibido por las autoridades competentes.

Calificación obtenida de: 17 **pts.**

En la ciudad de Caracas a los 18 días del mes de Noviembre de 2025

Lic. Franklin Cedeño
C.I. V-16.725.440
Tutor Académico

UNIVERSIDAD ALEJANDRO DE HUMBOLDT
RIF.: J-30489800-2
FACULTAD DE INGENIERÍA
DIRECCIÓN DE INFORMÁTICA

Gabriel Andrés Terán Azuaje
C.I. V-26.546.735
Estudiante

UNIVERSIDAD ALEJANDRO DE HUMBOLDT
FACULTAD DE INGENIERIA
ESCUELA DE INGENIERÍA EN INFORMÁTICA

APROBACIÓN DEL TRABAJO DE INVESTIGACIÓN

Por los Árbitros Evaluadores

DESARROLLO DE UN SISTEMA DE PAGOS MEDIANTE VINCULACIÓN DE CUENTA A TRAVÉS DE RECONOCIMIENTO FACIAL PARA EL BANCO DE VENEZUELA, S.A. BANCO UNIVERSAL

Trabajo de grado como requisito parcial para optar al Grado Académico de: **Ingeniero en Informática**, presentado por el ciudadano Gabriel Andrés Terán Azuaje, titular de la Cédula de identidad Nº V- 26.546.735, una vez concluida la defensa se considera **APROBADO** en nombre de la Universidad Alejandro de Humboldt, firman los árbitros, en Caracas a los 18 días del mes de noviembre de 2025.

Nota: 20 **ptos.**

Lic. Nancy Rodríguez
C.I. V-6.444.457
Árbitro

Ing. Oscar Lozano
C.I. V-6.425.667
Árbitro

Ing. Ofelia Sánchez
C.I. V-9.597.058
Árbitro

Lic. Franklin Cedeño
C.I. V-16.725.440
Tutor Académico

DEDICATORIA

Me gustaría dedicar este trabajo primeramente a Dios porque sé que ha sido parte fundamental de este proceso, que aunque a veces desconfío de mis capacidades, me da la fuerza para seguir insistiendo hasta conseguir el resultado deseado, sé que nunca fue suerte, siempre fue él.

A mis padres, que me han dado todo, pero lo mas importante su cariño, apoyo, dedicación, han sido un ejemplo de lo que es no rendirse, no lo han hecho en su vida personal o profesional, pero más importante, no se rindieron conmigo, me han apoyado en cada etapa no solo de la carrera si no de mi vida, este logro es más de ellos que mio, su sacrificio no fue en vano.

A mi padre que siempre ha estado allí, me acompaña y me apoya siempre, especialmente en la recta final de la carrera.

A mi madre que ha luchado para que pueda llegar hasta este punto, no existe dinero en el mundo que pague todo lo que ha hecho por mí.

A mi hermana, que aunque me exige y presiona, lo hace porque reconoce mis capacidades y que puedo dar y hacer más.

También me gustaría dedicarselo a mis primos Henry Lardieri y Pasqualino Lardieri, junto a mi tía Maribel Terán, quienes me han apoyado y motivado desde el primer momento no solo con la universidad, también en el transcurso de mi vida.

A mis abuelas, Aura Bravo y Mercedes García, a mis tíos y tías, quienes me criaron, no existe forma de retribuirles todo el amor que me han dado.

A mis primos, por su motivación y ayudarme a despejar la mente, siempre con humor, doy lo mejor de mi para poder ser un buen ejemplo para ustedes.

Por último pero no menos importante, me gustaría dedicarselo a mi abuelo, que en una conversación con él me dijo que le gustaría estar vivo para ver este momento, sé que donde esté, está feliz porque lo logré.

A mi familia, todos los que nombre, que están aquí reflejados, gracias por todo el amor que me han dado, espero que se sientan orgullosos, los amo.

AGRADECIMIENTOS

Me gustaría agradecer a la Universidad Alejandro de Humboldt por dotarnos de los conocimientos no solo de la carrera, por su preparacion para distintas circunstanciass de la vida, agradezco a los buenos y malos profesores, cada uno nos dejan lecciones importantes que si decidimos observar y escuchar cada una de ellas, seremos mejores profesionales. A los profesores Mariela Ayestaran, Jennifer Medina, Levi Galindo, Tony Fortunato, Robert Soto, Alexander Moya, quienes nos educaron más alla de una materia y un salón de clases.

A la profesora Yovanna (Psicologa de la UAH) por abrirme sus puertas siempre que lo necesitara.

Le agradezco al Profesor Franklin Cedeño, quien fue mi profesor de lenguajes de programacion I y ahora tutor del Trabajo de Grado, me enseño a ir mas allá de lo que se da en la materia y que nunca nos debemos rendir.

A la profesora Ofelia Sanchez quien sin su arduo esfuerzo y apoyo no lo hubiera logrado hasta aquí.

ÍNDICE GENERAL

LISTA DE CUADROS

CUADRO

LISTA DE GRÁFICOS Y FIGURAS

GRÁFICO

FIGURA

UNIVERSIDAD ALEJANDRO DE HUMBOLDT
FACULTAD DE INGENIERÍA
INGENIERÍA EN INFORMÁTICA
TRABAJO DE GRADO
SECCIÓN: DCM1004IIV1

DESARROLLO DE UN SISTEMA DE PAGOS MEDIANTE VINCULACIÓN DE CUENTA A TRAVÉS DE RECONOCIMIENTO FACIAL PARA EL BANCO DE VENEZUELA, S.A. BANCO UNIVERSAL

Autor: Terán Gabriel
C.I: V-26.546.735
Tutor: Lic. Franklin Cedeño
Fecha: noviembre, 2025

RESUMEN

La constante evolución de los medios de pago digitales en Venezuela ha evidenciado limitaciones críticas en los sistemas vigentes, tales como el desgaste de huellas dactilares que afecta la eficacia del BioPago y la vulnerabilidad de la tecnología sin contacto (Contactless) ante posibles fraudes por falta de verificación. La presente investigación tuvo como objetivo general desarrollar un sistema de pagos mediante vinculación de cuenta a través de reconocimiento facial para el Banco de Venezuela, S.A. Banco Universal. El estudio se enmarcó bajo la modalidad de proyecto factible, apoyado en una investigación de campo de nivel descriptivo con un diseño no experimental. La población objeto de estudio estuvo conformada por quince (15) empleados de la Gerencia de línea de sistemas financieros y colocaciones bancarias de la institución, constituyendo una muestra de tipo censal. Como técnica de recolección de datos se empleó la encuesta y como instrumento un cuestionario de diez (10) ítems con opciones de respuesta dicotómica, el cual fue validado mediante el juicio de tres (03) expertos en las áreas de metodología, ingeniería y estadística. La confiabilidad se determinó a través del coeficiente Kuder-Richardson 20 (KR-20), arrojando un resultado de 0,783, lo que representa una alta consistencia interna. La propuesta final consiste en una plataforma técnica que integra algoritmos de detección de vida (Liveness Detection) y una arquitectura de microservicios, orientada a reducir la latencia transaccional a menos de tres segundos y garantizar una precisión del 99,99%. El sistema no solo optimiza la seguridad bancaria, sino que promueve la inclusión financiera de usuarios con dificultades en la biometría dactilar tradicional.

Descriptores: Reconocimiento facial, Biometría, Sistema de pagos, Seguridad bancaria, Proyecto factible.

UNIVERSIDAD ALEJANDRO DE HUMBOLDT
FACULTAD DE INGENIERÍA
INGENIERÍA EN INFORMÁTICA
TRABAJO DE GRADO
SECCIÓN: DCM1004IIV1

DEVELOPMENT OF A PAYMENT SYSTEM THROUGH ACCOUNT LINKING VIA FACIAL RECOGNITION FOR BANCO DE VENEZUELA, S.A. BANCO UNIVERSAL.

Autor: Terán Gabriel
C.I: V-26.546.735
Tutor: Lic. Franklin Cedeño
Fecha: noviembre, 2025

ABSTRACT

The constant evolution of digital payment methods in Venezuela has revealed critical limitations in current systems, such as fingerprint wear affecting the effectiveness of BioPago and the vulnerability of contactless technology to potential fraud due to a lack of verification. The general objective of this research was to develop a payment system through account linking via facial recognition for Banco de Venezuela, S.A. Banco Universal. The study was framed as a feasible project, supported by descriptive field research with a non-experimental design. The target population consisted of fifteen (15) employees from the institution's Financial Systems and Banking Placements Line Management, constituting a census sample. A survey was used as the data collection technique, with a ten (10)-item dichotomous questionnaire as the instrument, which was validated by the judgment of three (03) experts in the areas of methodology, engineering, and statistics. Reliability was determined through the Kuder-Richardson 20 (KR-20) coefficient, yielding a result of 0.783, which represents high internal consistency. The final proposal consists of a technical platform that integrates liveness detection algorithms and a microservices architecture, aimed at reducing transactional latency to less than three seconds and ensuring 99.99% accuracy. The system not only optimizes banking security but also promotes financial inclusion for users who face difficulties with traditional fingerprint biometrics.

Descriptors: Facial recognition, Biometrics, Payment system, Banking security, Feasible project.

INTRODUCCIÓN

La transformación digital en el sector financiero global ha redefinido la manera en que los usuarios interactúan con el dinero, desplazando progresivamente el uso del efectivo por soluciones electrónicas más ágiles. En Venezuela, este proceso ha sido particularmente dinámico, impulsado por la necesidad de alternativas ante la escasez de papel moneda y la adopción masiva de sistemas como el Pago Móvil. Sin embargo, a pesar de este avance, los mecanismos de autenticación no han evolucionado con la misma velocidad, enfrentando desafíos críticos en términos de seguridad y usabilidad. Actualmente, sistemas como el BioPago presentan limitaciones físicas por el desgaste de huellas dactilares, mientras que la tecnología Contactless carece de protocolos de verificación robustos en el contexto nacional, lo que incrementa el riesgo de transacciones no autorizadas.

Bajo este escenario, surge la presente investigación titulada “Desarrollo de un sistema de pagos mediante vinculación de cuenta a través de reconocimiento facial para el Banco de Venezuela, S.A. Banco Universal”. Este proyecto se propone como una solución tecnológica de vanguardia que busca no solo elevar los estándares de seguridad bancaria mediante biometría de última generación, sino también mejorar la experiencia del usuario al reducir la latencia transaccional y fomentar la inclusión financiera de aquellos ciudadanos cuyas huellas dactilares dificultan el uso de sistemas tradicionales.

Para dar cumplimiento a los objetivos planteados, el presente trabajo de grado se ha estructurado en seis capítulos, organizados de la siguiente manera:

En el CAPÍTULO I: El Problema, se expone la realidad actual de los medios de pago en la institución, detallando las fallas de los sistemas vigentes y la necesidad de una alternativa biométrica facial. Se establecen los objetivos general y específicos, la justificación del estudio y el sistema de variables que delimitan el alcance de la investigación.

El CAPÍTULO II: Marco Teórico, constituye el soporte conceptual y referencial del estudio. En él se analizan antecedentes de investigaciones similares y se desarrollan las bases teóricas sobre biometría, algoritmos de reconocimiento facial y seguridad informática. Asimismo, se detallan las bases legales que sustentan el manejo de datos biométricos en el marco jurídico venezolano y el contexto organizacional del Banco de Venezuela.

En el CAPÍTULO III: Marco Metodológico, se describe el rigor científico aplicado. Se define la investigación como un proyecto factible con diseño de campo no experimental. Se detalla la población conformada por el personal especializado de la Gerencia de sistemas financieros y las técnicas de recolección de datos, centradas en una encuesta aplicada mediante un cuestionario dicotómico debidamente validado.

El CAPÍTULO IV: Presentación y Análisis de Resultados, ofrece una visión cuantitativa y cualitativa de la información recolectada. A través de representaciones estadísticas, se interpreta la percepción técnica sobre la viabilidad del sistema de reconocimiento facial y la necesidad crítica de su implementación para solventar las fallas del BioPago actual.

Por su parte, el CAPÍTULO V: Conclusiones y Recomendaciones, sintetiza los hallazgos más relevantes, confirmando la hipótesis de que la biometría facial representa una mejora sustancial sobre los métodos actuales. Se proponen sugerencias estratégicas para la institución bancaria en pro de la escalabilidad del sistema.

Finalmente, el CAPÍTULO VI: La Propuesta, detalla la arquitectura técnica del sistema desarrollado. Se describen los algoritmos de detección de vida (Liveness

Detection), la estructura de microservicios y los estudios de factibilidad técnica, operativa y económica que aseguran que el proyecto es una solución sostenible y lista para su integración en el ecosistema financiero del Banco de Venezuela.

CAPÍTULO I

EL PROBLEMA

Planteamiento del Problema

La diversidad en formas de pago ha ido evolucionando en el país, especialmente en los últimos años, desde el sistema de “pago móvil”, el pago por el sistema “Zelle”, pagos por “Binance”, entre otras formas de realizar transferencias entre usuarios, sin embargo, al realizar el pago por tarjeta el sistema se ha quedado atrás a falta de actualización, mientras que fuera del país la tecnología “ContactLess” ya es parte del día a día, en Venezuela se está empezando a implementar desde el año 2024.

Aunque esta tecnología “ContactLess” es novedosa en nuestro mercado también lo hace un tanto insegura, al no adaptarla a las exigencias de seguridad que requiere en el país lo hace frágil al posible uso inadecuado de la misma, al no requerir de la identificación del usuario o la clave, se vuelve un objetivo a posibles hurtos, manejo inadecuado de las tarjetas y de transacciones imprevistas por el usuario, por esta razón es que el análisis, diseño y desarrollo de un sistema de pagos que vincule la cuenta de banco del usuario a su rostro es la opción más segura y confiable de que sus transacciones sean realizadas por el titular de la misma. De esta forma Mayen, J. (2025) Explica

> El avance de China en esta área plantea la posibilidad de un mundo sin efectivo, donde los pagos biométricos y digitales se conviertan en la norma. Sin embargo, la aceptación global de este modelo dependerá de varios factores:
>
> • Privacidad y seguridad de los datos: Los consumidores exigen garantías sobre cómo se utilizan y protegen sus datos biométricos.
>
> • Infraestructura tecnológica: Países con menor desarrollo tecnológico podrían enfrentar desafíos para implementar sistemas de este tipo.

> • Aceptación cultural: El uso del efectivo sigue siendo una práctica común en muchas partes del mundo, vinculada a la autonomía y la confianza interpersonal. (parr. 10).

Es decir, para que esta tecnología pueda ser viable aplicarla en gran escala se deben de cumplir ciertas garantías tanto en la privacidad de los datos como en el compromiso de desarrollo de la infraestructura adecuada para su ejecución o mantenimiento y por último la aceptación por parte de los usuarios como nuevo sistema de pago o forma de pago principal.

El objetivo de este sistema es principalmente ofrecer seguridad, pero también, facilidad tanto al usuario como al comercio de una garantía de pago rápida, confiable y con la menor cantidad de intermediarios posibles.

Conociendo el comportamiento del mercado Venezolano, podemos plantear como una de las características distintivas de este sistema, es que, el usuario pueda elegir con cuál de sus cuentas bancarias desea hacer efectiva la transacción, con la opción de tener registrado en su cuenta del sistema cuentas de múltiples bancos pero con siendo obligado a usar solo una como cuenta principal o elegirla al momento de realizar el pago.

Tal como destaca el Banco Central de la República Argentina

> Modernizar el sistema de pagos contribuye a mejorar la competitividad de la economía y la generación de empleo productivo. Incentivar la utilización masiva de medios de pago electrónicos y facilitar su acceso a toda la población es importante para potenciar los beneficios de la bancarización. Contribuye, además, a obstaculizar el crimen organizado, el narcotráfico y el lavado de dinero, así como a formalizar la economía, lo que permite cargas tributarias más parejas y más moderadas. (parr. 32).

De acuerdo con esto, la función no solo abarca realizar un software o sistema de pago si no, de crear un medio de pago que funcione de manera óptima a gran escala, para así poder garantizar a los usuarios una manera de mantener sus datos tanto personales como bancarios de forma privada.

Una vez abarcadas las capacidades digitales del sistema y como sus funciones deben garantizar tanto su uso eficiente como seguro, también se debe de hablar de las capacidades físicas que puede tener este sistema, este debe ser no solo un software seguro para los usuarios si no también, un sistema operativo con una capacidad de que sea inviolable por algún atacante externo, de este modo ambos lograran el objetivo propuesto en materia de seguridad, Fernández, V. (2010). Explica

> Un sistema es un conjunto de componentes que interaccionan entre sí para lograr un objetivo común. (pág. 11).

Con esto se refiere a que tanto los componentes digitales como los componentes físicos, deben funcionar como uno solo para cumplir con el objetivo de hacer operaciones exitosas.

Interrogantes de la Investigación

1. ¿Con que mecanismos de seguridad cuenta el sistema de pagos actual del Banco de Venezuela, S.A. Banco Universal?
2. ¿Cómo es el funcionamiento del sistema de pagos mediante vinculación de cuenta a través de reconocimiento facial para el Banco de Venezuela, S.A. Banco Universal?
3. ¿Qué componentes se requieren para el desarrollo de un sistema de pagos mediante vinculación de cuenta a través de reconocimiento facial para el Banco de Venezuela, S.A. Banco Universal?

Objetivos de la Investigación

Objetivo General

Desarrollar un Sistema de Pagos mediante Vinculación de Cuenta a través de Reconocimiento Facial para el Banco de Venezuela, S.A. Banco Universal.

Objetivos Específicos

1. Analizar el sistema de pagos actual del Banco de Venezuela, S.A. Banco Universal y realizar un diagnostico de sus limitaciones y riesgos de seguridad.
2. Describir el funcionamiento del sistema de pagos mediante vinculación de cuenta a través de reconocimiento facial para el Banco de Venezuela, S.A. Banco Universal.
3. Establecer los componentes que se requieren para el desarrollo de un sistema de pagos mediante vinculación de cuenta a través de reconocimiento facial para el Banco de Venezuela, S.A. Banco Universal.

Justificación de la Investigación

Este proyecto se justifica en el punto de vista teórico, debido a que brinda información relevante en el área de sistemas de pagos, ya que ayuda a identificar el proceso que se tiende a realizar en el desarrollo del mismo, se da a conocer sus problemáticas pero a su vez el potencial que tiene a adaptarse a los requerimientos del sistema financiero nacional y de sus clientes.

Desde una perspectiva más técnica, esta investigación sugiere una oportunidad importante para el sector bancario venezolano, de presentar como propuesta diferencial especialmente en Latinoamérica, de resolución de problemas y agilización para así sobreponerse ante los inconvenientes que se muestran en el área de seguridad en las transacciones de la banca.

Desde el punto de vista social, se espera que la investigación pueda hacer una mejora en cuanto a la agilidad y eficiencia en los pagos, haciéndole una reducción en tiempo y esfuerzo de los recursos empleados para cumplir con las transacciones bancarias y satisfacer las necesidades de los clientes ayudándole a tener una imagen de responsabilidad a la marca haciendo que también se cree una relación confianza y lealtad con los usuarios.

Sistema de Variables

Se refiere a la abstracción teórica de la variable. Consiste en definir el término utilizando otros conceptos que expliquen su esencia, sin referirse todavía a su medición. Según Arias (2012), una variable es una "característica o cualidad; magnitud o cantidad, que puede sufrir cambios, y que es objeto de análisis, medición, manipulación o control en una investigación" (p. 57). En este sentido, el sistema de variables constituye el conjunto de elementos que se pretenden estudiar y que se derivan directamente de los objetivos específicos de la investigación.

Cuadro 1.
Identificación y Definición de las Variables

Objetivos Específicos	Variable	Definición Conceptual
Analizar el sistema de pagos actual del Banco de Venezuela, S.A. Banco Universal y realizar un diagnóstico de sus limitaciones y riesgos de seguridad.	Diagnóstico de las limitaciones y riesgos de seguridad del sistema de pagos actual del Banco de Venezuela, S.A. Banco Universal.	Es el proceso sistemático que evalúa el funcionamiento operativo, los puntos débiles y las vulnerabilidades de seguridad de los métodos de pago empleados actualmente por el Banco de Venezuela, S.A. Banco Universal.
Describir el funcionamiento del sistema de pagos mediante vinculación de cuenta a través de reconocimiento facial para el Banco de Venezuela, S.A. Banco Universal	Funcionamiento del sistema de pagos mediante vinculación de cuenta a través de reconocimiento facial	Proceso tecnológico que permite la autenticación y autorización de transacciones financieras mediante la identificación biométrica del usuario, vinculando su cuenta bancaria o método de pago a un sistema seguro que utiliza reconocimiento facial para validar y procesar pagos de manera eficiente.
Establecer los componentes que se requieren para el desarrollo de un sistema de pagos mediante vinculación de cuenta a través de reconocimiento facial para el Banco de Venezuela, S.A. Banco Universal	Componentes que se requieren para el desarrollo de un sistema de pagos mediante vinculación de cuenta a través de reconocimiento facial	Son aquellos elementos fundamentales necesarios para la creación de un software que permita realizar transacciones financieras mediante la asociación de cuentas bancarias y la autenticación por reconocimiento facial, asegurando que el sistema cumpla con los requisitos de seguridad, precisión y usabilidad exigidos por los usuarios y las normativas financieras aplicables.

Fuente: Terán, G. (2025)

Operacionalización de Variables

La operacionalización se define como el proceso mediante el cual se transforman variables abstractas en términos concretos, observables y medibles. Según Arias (2012), este procedimiento consiste en "descomponer gradualmente la variable a través de un proceso deductivo, que va de lo más general a lo más específico" (p. 62). En otras palabras, permite llevar el concepto teórico a un plano empírico donde puede ser evaluado a través de instrumentos de recolección de datos.

Cuadro 2.
Operacionalización de las Variables

Objetivos Específicos	Variables	Dimensión	Indicadores	Instrumento	Items
Analizar el sistema de pagos actual del Banco de Venezuela, S.A. Banco Universal y realizar un diagnóstico de sus limitaciones y riesgos de seguridad.	Diagnóstico de las limitaciones y riesgos de seguridad del sistema de pagos actual del Banco de Venezuela, S.A. Banco Universal.	Autenticación Biométrica y Gestión de Transacciones	1.Análisis Funcional de los sistemas BiopagoBDV y ContactLess. 2. Identificación de vulnerabilidades de seguridad. 3. Riesgos y frecuencia de fraude.	Cuestionario	**1** **2** **3**
Describir el funcionamiento del sistema de pagos mediante vinculación de cuenta a través de reconocimiento facial para el Banco de Venezuela, S.A. Banco Universal	Funcionamiento del sistema de pagos mediante vinculación de cuenta a través de reconocimiento facial	Autenticación Biométrica y Gestión de Transacciones	1. Proceso de Vinculación de Cuenta Bancaria. 2. Flujo de Autenticación por Reconocimiento Facial. 3. Ejecución y Confirmación de Transacciones	Cuestionario	**4** **5** **6**
Establecer los componentes que se requieren para el desarrollo de un sistema de pagos mediante vinculación de cuenta a través de reconocimiento facial para el Banco de Venezuela, S.A. Banco Universal	Componentes que se requieren para el desarrollo de un sistema de pagos mediante vinculación de cuenta a través de reconocimiento facial	Autenticación Biométrica y Gestión de Transacciones	1. Frameworks de Reconocimiento Facial. 2. Backend Seguro y Escalable + Frontend Móvil. 3. Módulos de Seguridad y Cifrado. 4. Nivel de fricción y frustración del usuario.	Cuestionario	**7** **8** **9** **10**

Fuente: Terán, G. (2025)

CAPITULO II

MARCO TEORICO REFERENCIAL

Antecedentes de la Investigación

De Sousa, K. y Mora, C. (2016) Efectuaron su investigación en la Universidad Central de Venezuela, Caracas, titulada, Sistema de Seguridad Basado en Reconocimiento Facial Utilizando una Raspberry Pi. Su objetivo general: Desarrollar un sistema de seguridad, para ser utilizado en el laboratorio ICARO de la Escuela de Computación de la Universidad Central de Venezuela, basado en reconocimiento facial utilizando una Raspberry Pi y una cámara web. Su investigación fue de campo y utilizaron una población de 5 personas a las cuales se les proporcionó una encuesta, se llegó a la conclusión de que es posible desarrollar un sistema funcional y efectivo, pero identificaron limitaciones que afectaron su rendimiento y alcance, la principal limitación estuvo relacionada con el uso de cámaras IP, ya que estas no ofrecían un protocolo estándar para la codificación de video, lo que impactó negativamente en el rendimiento del sistema. Se añadió esta investigación como antecedente debido a que proporciona que tipo hardware utilizar para que el rendimiento del sistema sea óptimo en conjunto con el software del mismo.

Mendoza, V. y Falcón, G. (2018) Realizaron su investigación en la Universidad José Antonio Páez, San Diego, Edo. Carabobo, su título, Desarrollo de un Sistema de Seguridad Basado en el Reconocimiento Facial para la Universidad José Antonio Páez, manejaron como objetivo general: Desarrollar un sistema de seguridad basado en el reconocimiento facial para la Universidad José Antonio Páez con la finalidad mantener un control de acceso de la población Universitaria. Su tipo de investigación fue de campo, aplicándoles una encuesta a 60 estudiantes de ese recinto universitario, obtuvieron como conclusión que los algoritmos Haar Cascade y LBPH, fueron los que tuvieron mayor rendimiento, ayudando a que la detección y reconocimiento facial sean los pilares de su sistema. El motivo por el cual se incluyó esta investigación como antecedente fue por proporcionar ideas y soluciones en cuanto al diseño y desarrollo del software.

Wei, M. (2021) Elaboró su investigación en la Universidad Autónoma de Querétaro, México, titulada El Uso de Tecnología de Reconocimiento Facial en el Proceso de Pago para Promover la Economía en México Durante la Pandemia. Planteó como Objetivo General: Analizar y determinar si la tecnología de pago mediante reconocimiento facial puede ser una herramienta para impactar positivamente los micronegocios en México durante la pandemia. Utilizo una metodología de investigación de campo, realizándoles unas entrevistas estructuradas con preguntas abiertas a bancos, empresas financieras y tiendas comerciales, para obtener "información valiosa de como el pago mediante reconocimiento facial puede ser una herramienta que promueva el desarrollo económico en nuestro país". Se llegó a la conclusión de que la adopción del reconocimiento facial no solo reduciría la posibilidad de contraer enfermedades (en el caso de esta investigación, el COVID-19), también ayudaría a acelerar el proceso de compra y ayudar a promover la economía del país. Se tomó esta investigación como antecedente debido a la similitud de la propuesta de utilizar la misma solución, como es el caso del reconocimiento facial, para dos problemáticas diferentes, una enfocada en resguardar la salud de los usuarios y la otra en la seguridad de las transacciones.

Castillo F. y Romero, P. (2021) desarrollaron esta investigación en la Fundación Universidad de América, Bogotá, Colombia, titulada, Estudio de Factibilidad de una Alternativa de Pago con Reconocimiento Facial en las Estaciones de Transmilenio, Bogotá. Su objetivo fue: Estudiar las diferentes variables sociales, técnicas y financieras necesarias para evaluar la viabilidad de implementar un sistema de pago con reconocimiento facial en las estaciones de TransMilenio en Bogotá. Realizaron una investigación de campo, su población fueron 129 personas, haciéndoles una encuesta, llegando a la conclusión que a pesar de que el reconocimiento facial en los sistemas de pago de Transmilenio aportaría un beneficio enorme en la posibilidad de mejorar la infraestructura tecnológica, aumentar el control y gestión de la informacion, la realidad, es que existen diversas variables por las cuales se complicaría la adopción por parte de los usuarios, como que varios usuarios no

cuentan con los requisitos básicos para la aplicación de este sistema, como suministrar información a la entidad, un incremento en la tarifa del pasaje y una cuenta activa en el sistema financiero, aun cuando el 58,9% de los usuarios considera que los pagos con reconocimiento facial podrían mejorar el sistema de recaudo de Transmilenio. Este antecedente fue incluido debido a que ayudo a crear bases sobre cómo se debería diseñar el sistema, por que debería estar compuesto y cómo se puede adaptar el sistema al mercado y a la población.

Chirinos, J. (2023) Realizó su tesis en la Universidad José Antonio Páez, San Diego, Edo. Carabobo, opto como título, Sistema de Acceso por Medio de un Dispositivo de Reconocimiento Facial, para Sistemas Informáticos. Estableció como Objetivo General: Desarrollar un sistema para el acceso a sistemas informáticos por medio de un dispositivo de reconocimiento facial en la empresa IAM TECNOLOGIA. Crearon una investigación de campo, su población, 6 empleados de la empresa, a los cuales se les aplicó una encuesta, se concluyó que la herramienta garantizó la privacidad de los datos de los usuarios así como el cumplimiento de los criterios de seguridad para el acceso de datos confidenciales. Se tomó como antecedente debido a como garantiza y prioriza la protección de los datos del usuario haciendo un sistema más seguro y confiable.

Bases Teóricas

Sistemas de Pagos con Reconocimiento Facial en el Sector Bancario

El sistema de pagos con reconocimiento facial en el sector bancario, es un software que junto a algunos dispositivos o hardware anexado, permiten el uso de características físicas que son únicas en los seres humanos. La autenticación biométrica ha pasado a formar parte fundamental de las aplicaciones como método de seguridad, no solo en la banca si no también en aplicaciones de mensajería, en las tiendas de aplicaciones, incluso para desbloquear el dispositivo móvil. Como determina Stankevičiūtė, G. (2023)

> La biometría en la banca consiste en el uso de características fisiológicas o conductuales únicas de las personas con fines de autenticación y seguridad en las transacciones bancarias digitales y el acceso a cuentas. Estas características pueden incluir el reconocimiento facial, el reconocimiento de voz, el escaneo de huellas dactilares o el reconocimiento de retina. (parr.5)

Es decir, no solo el reconocimiento facial forma parte de las medidas que puede tomar un ente bancario para reforzar el tema de la seguridad en las aplicaciones donde se encuentran las cuentas de sus clientes, si no también el escaneo de huellas dactilares, reconocimiento de voz y el reconocimiento de retina hacen parte de estos sistemas, además que no solo se usa al ingresar a la cuenta, también se utiliza para verificar las transacciones que se realizan.

Diagnostico de las limitaciones y riesgos de seguridad del sistema de pagos actual

Al realizar un diagnostico de las limitaciones y riesgos de seguridad del sistema de pagos actual tenemos que el uso de la huella en el sistema BiopagoBDV tanto en adultos de la tercera edad como personas que realizan trabajos manuales es … ya que las mismas se desgastan y la autenticación se hace imposible por lo que tienen que recurrir a otras vías para poder realizar alguna transacción dentro del banco. Dentro de los riesgos de seguridad hemos observado que al realizar algún pago mediante el sistema Contactless, en algunos puntos de venta se requieren algún dato de validación como la cédula o la clave de la tarjeta pero en la mayoría, no

requieren de ningún tipo de verificación por lo cual los pagos con una tarjeta que utilice esta tecnología son mas propensos a robos y estafas. Como indica Buehler, T. (2024)

> El Libro de Datos de la Red Centinela del Consumidor de la Comisión Federal de Comercio (FTC) reportó un aumento significativo en las denuncias de fraude con tarjetas sin contacto entre 2018 y 2021, impulsado principalmente por la facilidad con la que los delincuentes podían realizar pagos de bajo valor sin ser detectados. Si los titulares de tarjetas no se percatan inmediatamente del robo, podrían realizar múltiples compras sin contacto en un breve período antes de que se reportara la pérdida de una tarjeta. (parr. 14)

En otras palabras, este fenómeno reportado por la Comisión Federal de Comercio (FTC), subraya una vulnerabilidad clave del sistema, la facilidad con la que los delincuentes pueden usar estas tarjetas robadas para realizar múltiples compras de bajo valor en poco tiempo. Dado que los pagos no requieren PIN, el fraude se acumula rápidamente si el titular no reporta el robo de inmediato. Esta situación evidencia los riesgos de seguridad asociados a los pagos sin contacto. el uso de herramientas para el desarrollo de tecnología cada vez se hace más inevitable conforme pasa el tiempo, utilizar las mismas hace que se el coste de operaciones del sistema que se está diseñando reduzca sin que sea un sacrificio para el rendimiento de el mismo. Las fases para este diagnostico de las limitaciones y riesgos de seguridad del sistema de pagos actual, van a consistir en: a) Análisis Funcional de los sistemas BiopagoBDV y Contactless. b) Identificación de vulnerabilidades de seguridad. c) Riesgos y frecuencia de fraude.

Análisis Funcional de los sistemas BiopagoBDV y Contactless.

El Análisis Funcional de los sistemas BiopagoBDV y Contactless es el proceso de describir que hacen (las funciones) y como interactúan (los procesos) para lograr su objetivo principal: el procesamiento seguro y rápido de un pago. Se enfoca en la funcionalidad desde la perspectiva del usuario (comprador y comerciante) y de los sistemas involucrados. El sistema BiopagoBDV, utilizado en Venezuela y que

sirve como un ejemplo de pago biométrico, funciona como un punto de venta que utiliza la huella dactilar como principal factor de autenticación, prescindiendo del uso de tarjetas físicas o claves personales en muchos casos. Los pagos Contactless, basados en la tecnología Near Field Communication (NFC), permiten realizar transacciones acercando una tarjeta a un terminal de punto de venta compatible, sin necesidad de contacto físico ni de insertar la tarjeta.

Identificación de vulnerabilidades de seguridad.

La identificación de vulnerabilidades de seguridad es el proceso de examinar el sistema de pagos para detectar y clasificar fallos, debilidades o errores de diseño o configuración que podrían ser explotados por un atacante para comprometer la integridad, confidencialidad o disponibilidad de la información, En ambos sistemas, la Identificación de Vulnerabilidades es un paso crucial para mantener la confianza y evitar que las ventajas de la rapidez y comodidad se vean eclipsadas por el riesgo de fraude o robo.

Riesgos y frecuencia de fraude.

Los riesgos y frecuencia de fraude se definen por las vulnerabilidades a sus métodos de autenticación. Para el contactless, el riesgo se centra en el fraude por proximidad, el uso no autorizado de la señal NFC y los hurtos que ocurren debido a la falta de verificación por parte de algunos puntos de venta o montos de transacciones, en el caso del biopagoBDV, el riesgo se centra en la suplantación de la identidad biométrica pero el riesgo de fraude más frecuente no es el financiero directo, sino la alta dependencia y la interrupción del servicio centralizado (red e interconexión bancaria), lo que detiene la operación y el cobro del comercio. Según indica la Revista Ciberseguridad (2025)

> No obstante y, aunque las probabilidades de sufrir un fraude con un sistema de pago sin contacto no son elevados, especialmente si los comparamos con otros tipos de fraude relacionados con medios de pago, es conveniente aplicar algunas medidas de seguridad que nos ayudarán a

prevenir y reaccionar eficazmente contra las estafas dirigidas a tarjetas de crédito (parr. 2)

Esto quiere decir, que pese a que los riesgos de ser víctima de estafa con este sistema de pago es reducido, es recomendable adoptar ciertas precauciones de seguridad para ayudar a los usuarios a prevenir y responder de manera efectiva a las estafas relacionadas a sus tarjetas.

Funcionamiento del sistema de pagos mediante vinculación de cuenta a través de reconocimiento facial

Como funcionamiento del sistema de pagos se tiene que es un proceso en el cual se realiza la carga del rostro y de la información de la cuenta bancaria en una aplicación móvil, una vez completado el registro del usuario, ya puede procesar la autenticación de la identidad a través de reconocimiento facial a la hora de realizar cualquier tipo de transacciones. Sobre esta misma base, Campillo, R. (2024) explica "En el día a día, el reconocimiento facial permite a los clientes acceder a sus aplicaciones bancarias móviles, autorizar pagos o retirar dinero en los cajeros con solo una mirada." En otras palabras, la tecnología de reconocimiento facial se ha integrado en las operaciones bancarias para ofrecer una experiencia de usuario fluida y conveniente, esta funcionalidad permite a los clientes acceder a sus cuentas a través de las aplicaciones móviles y confirmar la realización de transacciones financieras.

Proceso de Vinculación de Cuenta Bancaria.

El proceso de vinculación de cuenta bancaria es el desarrollo de una conexión entre la plataforma bancaria y una aplicación de terceros mediante un canal de comunicación como lo son las APIs, en dicho proceso se deben establecer ciertos parámetros como lo es la cuenta que se va a utilizar para la realización de las transacciones a través de la aplicación intermediaria.

Flujo de Autenticación por Reconocimiento Facial.

El flujo de autenticación de un sistema de pagos con reconocimiento facial generalmente sigue una secuencia de pasos que permiten verificar la identidad del usuario y autorizar la transacción. El paso principal es el de registro del rostro a

través de una imagen o vídeo, luego se ingresa la cuenta bancaria junto a información necesaria como el nombre y la cédula para su vinculación con la cara registrada, una vez con todos los datos cargados ya el sistema esta listo para que al pedir su cédula, el rostro funcione como método de autenticación y aprobación de la transacción realizada.

Ejecución y Confirmación de Transacciones

La ejecución y confirmación de transacciones es el proceso integral que comienza inmediatamente después de la verificación biométrica exitosa del cliente. La ejecución es la fase en la que la orden de pago se convierte en una instrucción financiera para la movilización de los fondos entre las cuentas involucradas, luego de ser autorizada por el reconocimiento facial. La confirmación es la fase final en la que el sistema bancario emite una respuesta formal al cliente o al punto de venta, notificando que la transacción se ha completado con éxito, esta confirmación sirve como la prueba digital de que la ejecución iniciada por biometría se cerró correctamente. Como resalta el blog de InvestGlass (2024)

> A medida que nos adentramos en la era digital de la banca, el empleo de la tecnología para agilizar el proceso de aprobación resulta cada vez más crítico. Es vital que existan métodos de comunicación claros para garantizar que todos los implicados entienden cómo funcionan estos procesos, y la utilización de herramientas tecnológicas puede ayudar a conseguirlo.
>
> Al implantar sistemas automatizados en nuestros procedimientos de aprobación, no sólo aumentamos la eficiencia y la eficacia, sino que también fomentamos una mayor colaboración al tiempo que minimizamos los errores. (parr. 9)

En otras palabras, en la actual era digital, fundamental utilizar la tecnología para optimizar y acelerar los procedimientos de aprobación. Al adoptar sistemas de aprobación automatizados se consigue un doble beneficio, no solo aumenta la eficiencia y la eficacia en el trabajo, si no que también se mejora la colaboración entre equipos y se disminuyen las fallas humanas. Para que esto funcione, es imprescindible que existan canales de comunicación transparentes que aseguren que

todas las partes involucradas comprendan con exactitud el funcionamiento de estos nuevos procesos.

Componentes que se requieren para el desarrollo de un sistema de pagos mediante vinculación de cuenta a través de reconocimiento facial

Los componentes de un sistema de pagos mediante vinculación de cuenta a través de reconocimiento facial son los elementos que al integrarse permiten el desarrollo de una solución de pago segura, eficiente y de baja fricción. El frontend móvil es la interfaz de interacción que junto con los frameworks de reconocimiento facial permiten la captura y verificación de la identidad del usuario. Estos frameworks envían la señal de autorización al backend seguro y escalable, que es el núcleo que gestiona el mapeo entre la identidad biométrica y la cuenta bancaria vinculada. La importancia de esta arquitectura reside en su capacidad ara reemplazar métodos de pago tradicionales, ofreciendo una experiencia rápida y altamente segura, ya que esta reforzada pro módulos de seguridad y cifrado que protegen los datos biométricos y financieros durante todo el proceso. En uso, estos componentes trabajan de forma secuencial: la verificación facial autoriza la transacción en el backend, que luego ejecuta el débito en la cuenta bancaria, cerrando el ciclo con la confirmación de pago al usuario a través del frontend. Como indica Orlov, V. (2025)

> El entorno empresarial moderno evoluciona rápidamente. Actualizar periódicamente su pasarela de pago garantiza su compatibilidad con las nuevas tecnologías, mantener altos niveles de seguridad e incorporar las mejoras o nuevas funciones necesarias. Esto implica revisiones periódicas del código, la actualización de los componentes de software y el cumplimiento de las nuevas normativas. (parr. 54)

Esto quiere decir, es fundamental, especialmente en el entorno empresarial actual tan dinámico, actualizar constantemente la pasarela de pagos. Este mantenimiento periódico es crucial para asegurar la compatibilidad con tecnologías emergentes , mantener una seguridad robusta y añadir nuevas funciones necesarias.

Dicho proceso implica la revisión regular del código, la actualización de los componentes de software y el cumplimiento estricto de cualquier normativa nueva. Algunos de los componentes que se aplicaran se tienen: a) Frameworks de Reconocimiento Facial. b) Backend Seguro y Escalable + Frontend Móvil. c) Módulos de Seguridad y Cifrado. d) Nivel de fricción y frustración del usuario.

Frameworks de Reconocimiento Facial.

Los frameworks de reconocimiento facial son colecciones de software preconstruido (bibliotecas, módulos y herramientas) que contienen los algoritmos y modelos necesarios para el procesamiento biométrico, permitiendo la detección, extracción de características y la verificación o identificación de rostros humanos de manera rápida y precisa. En el contexto de un sistema de pagos, estos frameworks se vuelven el motor biométrico esencial, ya que su uso se centra en transformar el rostro del cliente en una plantilla matemática única que sirva como el token de autenticación para autorizar la transacción de pago y el débito de la cuenta vinculada, asegurando que solo el titular de la cuenta pueda iniciar la operación.

Backend Seguro y Escalable + Frontend Móvil.

El backend seguro y escalable junto con el frontend móvil constituyen la arquitectura fundamental de un sistema de pagos biométrico facial. El frontend móvil es la capa de presentación que reside en el dispositivo del usuario, encargada de la interacción inicial al capturar el rostro y mostrar la interfaz para el pago. Este se comunica directamente con el backend seguro y escalable, el cual actúa como el cerebro central del sistema, su uso es critico para alojar de forma segura el mapeo entre la identidad facial y la cuenta bancaria, manejar la lógica de negocio y procesar las transacciones financieras a través de APIs bancarias. Su diseño debe ser escalable para gestionar picos de demanda y seguro para garantizar la protección de datos y la integridad de los pagos.

Módulos de Seguridad y Cifrado.

Los módulos de seguridad y cifrado son componentes de software esenciales que emplean algoritmos criptográficos avanzados (como TSL/SSL para

comunicación y AES para almacenamiento) y protocolos de seguridad para proteger la información de accesos no autorizados y garantizar su integridad. De manera general, su uso consiste en convertir los datos sensibles a un formato ilegible (cifrado), gestionar el ciclo de vida de las claves de cifrado (similar a la funcionalidad de un key vault lógico como hashicorp vault o azure key vault) y validar la autenticidad de las partes (seguridad). En el contexto especifico de un sistema de pagos con reconocimiento facial, su función es critica y se enfoca ene resguardar la plantilla biométrica y los datos de la cuenta bancaria a los largo de todo el recorrido, garantizando que la comunicación entre el frontend y el backend sea totalmente cifrada y que la ejecución y confirmación de la transacción se realice en un entorno de confianza lógico, minimizando las vulnerabilidades del software. Según el sitio web de Hashicorp “El software moderno funciona debido a secretos. Los secretos son sensibles, discretos piezas de información como credenciales, claves de cifrado, autenticación certificados y otras piezas críticas de información que sus solicitudes necesitan para correr de manera consistente y segura.” (parr. 1) y con esto asegura que “Vault es un sistema de gestión de secretos y de encriptación basado en la identidad que centraliza la gestión secreta, gira viejas credenciales, genera credenciales bajo demanda, audita interacciones con los clientes y apoya la regulación cumplimiento”. (parr. 2)

Esto quiere decir que, el software de hoy en día no puede funcionar de forma segura sin “secretos”. Estos son simplemente la información sensible y privada que las aplicaciones necesitan para arrancar y operar correctamente, como los son las contraseñas, claves o certificados. Para manejar estos “secretos” vitales, se requiere de una herramienta especializada como lo es Vault, un sistema centralizado que actúa como una bóveda digital de alta seguridad.

Su función principal es administrar automáticamente todos los datos sensibles, desde generar nuevas credenciales solo cuando necesitan y reemplazar las viejas automáticamente, hasta llevar un registro detallado (auditoría) de quien accede a que, o cual es fundamental para cumplir con las regulaciones de seguridad.

Nivel de fricción y frustración del usuario

El nivel de fricción y frustración del usuario se define, de manera general, como la resistencia o dificultad que experimenta una persona al interactuar con un sistema, lo que puede generar sentimientos negativos como la frustración si el proceso es lento, confuso o requiere demasiados pasos. Esta métrica se convierte en un objeto de diseño critico cuyo uso es minimizar la cantidad de pasos y el tiempo requerido para completar la transacción, la meta es que el proceso de pago con el rostro sea tan rápido e intuitivo que el usuario lo perciba como una experiencia de cero fricción, superando la conveniencia de los métodos tradicionales y asegurando la adopción exitosa del sistema

Bases Legales

Las bases legales representan el soporte jurídico que enmarca la investigación, definiendo los derechos y deberes que regulan el desarrollo tecnológico y el manejo de datos en el país. Según el Manual de Trabajo de Grado de la UAH (2016), estas se refieren al "sistema legal del país que tiene relación con la investigación propuesta" (p. 20). En este caso, el estudio se fundamenta en las siguientes normativas:

1. Constitución de la República Bolivariana de Venezuela (1999)

Artículo 28: "Toda persona tiene el derecho de acceder a la información y a los datos que sobre sí misma o sobre sus bienes consten en registros oficiales o privados...".

Relación con la investigación: Este artículo sustenta el derecho del usuario bancario a conocer cómo se utilizan sus datos biométricos faciales y garantiza que la vinculación de cuenta se realice bajo su consentimiento y control.

Artículo 60: "Toda persona tiene derecho a la protección de su honor, vida privada, intimidad, propia imagen, confidencialidad y reputación...".

Relación con la investigación: Es fundamental para el proyecto, ya que el reconocimiento facial utiliza la "propia imagen" como llave de acceso. El sistema propuesto debe garantizar que esta imagen sea tratada bajo estrictos protocolos de confidencialidad para proteger la intimidad del cliente.

Artículo 110: "El Estado reconocerá el interés público de la ciencia, la tecnología, el conocimiento, la innovación y sus aplicaciones... por ser instrumentos esenciales para el desarrollo económico, social y político del país...".

Relación con la investigación: Brinda el marco macro para justificar la creación de nuevas herramientas tecnológicas que modernicen el sistema de pagos nacional y aseguren la soberanía tecnológica.

2. Ley Especial Contra los Delitos Informáticos (2001)

Artículo 1 (Objeto): Establece la protección integral de los sistemas que utilicen tecnologías de información, así como la prevención y sanción de los delitos cometidos contra tales sistemas.

Artículo 20: Violación de la privacidad de la data o información de carácter personal. El que por cualquier medio se apodere, utilice, modifique o elimine, sin el consentimiento de su dueño, la data o información personales de otro o sobre las cuales tenga interés legítimo, que estén incorporadas en un computador o sistema que utilice tecnologías de información, será penado con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias. La pena se incrementará de un tercio a la mitad si como consecuencia de los hechos anteriores resultare un perjuicio para el titular de la data o información o para un tercero.

Relación con la investigación: El desarrollo del sistema de pagos debe integrar algoritmos de cifrado y seguridad (como los mencionados HSM en la propuesta) para evitar que la data biométrica facial sea interceptada o utilizada de forma fraudulenta, cumpliendo con la protección que exige esta ley.

Artículo 25 (Apropiación de Propiedad Intelectual): "El que, sin autorización de su propietario y con el fin de obtener algún provecho económico, reproduzca, modifique, copie, distribuya o divulgue un software u otra obra del intelecto...".

Relación con la investigación: Dado que el proyecto implica el desarrollo de software especializado para el Banco de Venezuela, este artículo refuerza la protección legal contra el plagio o la distribución no autorizada del sistema de reconocimiento facial propuesto, garantizando la seguridad de la propiedad intelectual de la solución.

3. Ley Orgánica de Ciencia, Tecnología e Innovación (LOCTI)

Artículo 1: Tiene por objeto dirigir la generación de conocimientos y la innovación para alcanzar el desarrollo del país.

Relación con la investigación: El sistema propuesto representa una innovación tecnológica que se alinea con el objetivo de esta ley al proponer soluciones locales a problemas de seguridad y eficiencia en los medios de pago.

Artículo 5 (Actividades de ciencia, tecnología e innovación): Menciona que estas actividades deben "estar encaminadas a contribuir con el bienestar de la humanidad... el respeto a la dignidad y a los derechos humanos".

Relación con la investigación: El sistema de pagos mediante biometría facial cumple con este mandato al promover la inclusión financiera. Al ofrecer una alternativa para usuarios que no pueden usar el sistema BioPago por el desgaste de sus huellas dactilares, se está utilizando la tecnología para garantizar el derecho al acceso a sus recursos financieros con dignidad y eficiencia.

4. Ley de Instituciones del Sector Bancario

Normativas de Seguridad de la SUDEBAN (Resolución 001.19): Esta resolución establece las normas relativas al uso de la biometría como factor de autenticación en el sistema financiero nacional.

Relación con la investigación: Esta base legal es el pilar operativo del proyecto, ya que regula cómo las instituciones bancarias, como el Banco de Venezuela, deben implementar la identificación biométrica para garantizar que las transacciones sean seguras y evitar la usurpación de identidad.

5. Ley sobre el Derecho de Autor (1993)

Artículo 1: "Las disposiciones de esta Ley protegen los derechos de los autores sobre todas las obras del ingenio de carácter creador, ya sean de índole literaria, científica o artística...".

Relación con la investigación: Esta ley ampara el producto final de este trabajo de grado. Al desarrollar un sistema de pagos con una arquitectura específica de microservicios y lógica de reconocimiento facial, se está creando una "obra del ingenio de carácter científico/técnico". Por lo tanto, el autor posee los derechos sobre el diseño lógico, el código fuente y la documentación técnica generada.

Contexto Internacional: Reglamento General de Protección de Datos (RGPD) y Convenio de Budapest

Relación con la investigación: Aunque son normativas internacionales, se citan como referente de "buenas prácticas" en ingeniería de software. El proyecto adopta principios de Minimización de Datos y Seguridad por Diseño (Privacy by Design), asegurando que el tratamiento de las plantillas biométricas faciales cumpla con estándares globales de seguridad, similares a los exigidos en la Unión Europea para sistemas financieros de alta concurrencia.

CAPÍTULO III

MARCO METODOLÓGICO

Diseño de Investigación

El proyecto que se está desarrollando actualmente tiene como aplicación la propiedad: diseño de Investigación de Campo (I.C.), en conjunto con la modalidad de Proyecto Factible, debido a que se basa en el diagnóstico y la compresión profunda de una situación real y concluye con la formulación de una propuesta operativa y sustentable que busca atender la necesidad o problemática detectada, ofreciendo una solución de naturaleza técnica, instrumental y de diseño organizacional. Para saber de qué se trata, se podría decir que la Investigación de Campo (I.C.) se encarga de recolectar los datos de forma directa con los sujetos a investigar, o desde donde ocurren los hechos, que vendrían a ser los datos primarios, sin ningún tipo de manipulación o control sobre las variables, en otras palabras, el investigador recauda la información sin alterar las condiciones existentes, debido a eso llamada investigación no experimental. Según indica Palella, S. y Martins, F. (2012)

> En la investigación de campo no se formulan hipótesis y las variables se enuncian en los objetivos de la investigación que se desarrollará. Esto por cuanto está dirigida al conocimiento del presente, a encontrar respuesta a los problemas teóricos y prácticos que tejen la trama educativa (p.92)

En consecuencia, la práctica de la investigación de campo en el presente proyecto, va a permitir una obtención de la información de el Banco de Venezuela, S.A. Banco Universal, para llegar a un simple análisis de la situación actual por medio de encuestas, que respaldarán la información dada, de una manera más centrada y detallada para que los resultados sean los óptimos deseados.

Nivel de la Investigación

El Nivel de la investigación es la estrategia general y el propósito que guían el diseño de un estudio para establecer que tan a fondo se va a examinar un fenómeno y que tipo de conclusiones se podrán obtener. Se utiliza para delimitar los objetivos y la profundidad del conocimiento que se busca generar, Según afirma Arias, F. (2012) “El nivel de investigación se refiere al grado de profundidad con que se aborda un fenómeno u objeto de estudio.” (p.24). Lo que quiere decir que es simplemente la decisión de que tan a fondo se va a estudiar el tema.

Esta investigación desarrollará un nivel de tipo descriptivo-proyectivo, desde el punto de vista Descriptivo debido a que se centra en especificar las propiedades, características y rasgos importantes de un fenómeno, población o situación que se está analizando. Su principal objetivo es describir el “cómo es” el objeto de estudio en un momento dado, sin buscar explicar las causas de ese fenómeno. Así como lo explica Fidias, A. (2012) “La investigación descriptiva consiste en la caracterización de un hecho, fenómeno, individuo o grupo, con el fin de establecer su estructura o comportamiento.”(p.25). A lo que refiere es que el propósito fundamental de la investigación descriptiva es dibujar un panorama completo y preciso del objeto de estudio en un momento específico.

De esta misma forma, es proyectivo ya que tiene como objetivo la creación de iniciativas para resolver situaciones planteadas que impulsen el desarrollo de la tecnología. Para comprenderlo mejor, Hurtado, J. (2010) define que la investigación proyectiva “Diseña los planes de acción de las investigaciones posteriores” (p.134). La aplicación de este nivel proyectivo se da al ver que se explora en busca de ideas o propuestas de cómo crear una solución a determinados problemas o escenarios que logren no solo un beneficio para la empresa sino un avance en materia tecnológica.

Población y Muestra de la Investigación

Población de la Investigación

La población es la característica de que ayuda a encaminar una investigación de campo, ya que se le puede atribuir a una serie de elementos entrelazados a un fenómeno a estudiar que tiene similitudes en sus componentes. Para resaltar este punto, Arias, F. (2012) afirma que la población, "es un conjunto finito o infinito de elementos con características comunes para los cuales serán extensivas las conclusiones de la investigación. Ésta queda delimitada por el problema y por los objetivos del estudio." (p.81). De esta manera, se puede identificar y analizar de forma más objetiva el área afectada de la problemática de la presente investigación.

Enfocándose en el tipo de población de esta investigación, se caracteriza por ser "**finita**" y "**accesible**", porque se establecen a un número limitado de personas que sea más simple de analizar para el investigador. Para reforzar esto, Arias, F. (2012) estipula que la población accesible, "es la porción finita de la población objetivo a la que realmente se tiene acceso y de la cual se extrae una muestra representativa. El tamaño de la población accesible depende del tiempo y de los recursos del investigador" (p.82). Habiendo señalado esto, la población está focalizada en los quince (15) empleados que trabajan en la Gerencia de linea de sistemas financieros y colocaciones bancarias del Banco de Venezuela, S.A. Banco Universal, ubicada en la ciudad de Caracas, utilizando el 100% para la recolección de información que fortalezca la investigación.

Cuadro 3. Población de la Investigación

Población	Cantidad
Empleados de la Gerencia de linea, sistemas financieros y colocaciones bancarias del Banco de Venezuela, S.A. Banco Universal	15

Fuente: Terán, G. (2025)

Muestra de la Investigación

Parte importante de realizar una investigación es determinar los resultados de una población mediante una muestra, para esto es necesario hacer un estudio individual de cada elemento que integra el conjunto de personas a los que se tienen acceso con el objetivo de poder generalizar el resultado en función de la población total. Como especifican Palella, S. y Martins, S. (2012) “es posible afirmar que la muestra representa un subconjunto de la población, accesible y limitado, sobre el que realizamos las mediciones o el experimento con la idea de obtener conclusiones generalizables a la población.” (p.106). Siendo la muestra un extracto representativo de la población, se cuenta con quince (15) personas.

Con respecto a lo anterior señalado, se eligió tomar esa misma cantidad de personas para la muestra sin alguna necesidad de establecer criterios particulares al momento de seleccionar una tipología en específico. Con esto, Arias, F. (2012) se destaca que: “si la población, por el número de unidades que la integran, resulta accesible en su totalidad, no será necesario extraer una muestra” (p.83). Producto a esto, la muestra a utilizar para el presente estudio será el número total de la población, es decir quince (15) personas, lo que constituye el 100% de la población que trabaja para la Gerencia de linea de sistemas financieros y colocaciones bancarias del Banco de Venezuela, S.A. Banco Universal.

Cuadro 4. Muestra de la Investigación

Muestra	Cantidad
Empleados de la Gerencia de linea, sistemas financieros y colocaciones bancarias del Banco de Venezuela, S.A. Banco Universal	15

Fuente: Terán, G. (2025)

Técnica e Instrumentos de Recolección de Datos

Técnica de Recolección de Datos

La técnica de recolección de datos es aquella vía por la cual se obtienen datos o Información. Como afirma Tamayo y Tamayo, M. (2011), “depende en gran parte del tipo de investigación y del problema planteado para la misma, y puede efectuarse desde la simple ficha bibliográfica, observación, entrevista, cuestionarios o encuestas y aun mediante ejecución de investigaciones para este fin.” (p.187).

La técnica que se emplea en el presente proyecto es la encuesta, basado en que se requiere obtener información sobre un grupo de personas enlazadas a un objetivo general. Citando a Palella, S y Martins, F. (2012), “La encuesta es una técnica destinada a obtener datos de varias personas cuyas opiniones interesan al investigador.” (p.123), elegida porque permite aplicarlo a un gran número de personas y la obtención de una gran cantidad de información sobre un amplio abanico de cuestiones a la vez.

Instrumento de Recolección de Datos

El instrumento de recolección de datos es cualquier herramienta con la cual el investigador pueda recibir información por parte de los sujetos a estudiar. Como indican Palella, S. y Martins, F. (2012) “Es mediante una adecuada construcción de los instrumentos de recolección de datos como la investigación evidencia la necesaria correspondencia entre teoría y práctica; es más, se puede afirmar que es gracias a ellos como ambos términos pueden efectivamente vincularse” (p.125).

El instrumento a aplicar es el cuestionario, siendo más sencillo de usar, de analizar y de manejar, también basándolo en que, aplicándolo se llegan a resultados directos. Según resalta Arias, F. (2012), “Es la modalidad de encuesta que se realiza de forma escrita mediante un instrumento o formato en papel contentivo de una serie de preguntas.” (p.74). Dicho cuestionario contiene la cantidad de diez (10) ítems con preguntas cerradas, y opciones de respuesta dicotómica, la escala usada fue de Guttman, y está dirigido a los quince (15) empleados de la Gerencia de linea de sistemas financieros y colocaciones bancarias del Banco de Venezuela, S.A. Banco Universal, (Ver Anexo “A”).

Juicio de expertos

El Juicio de expertos es una técnica o método de investigación que consiste en solicitar y recopilar la opinión informada y calificada de personas con una trayectoria reconocida, experiencia y profundo conocimiento sobre un tema específico. Reforzando esto, Maldonado, N. y Santoyo, F. (2024). aseguran que:

> Este grupo de personas expertas evalúa las propiedades de los ítems que componen el instrumento para realizar las modificaciones oportunas. Los criterios para evaluar las propiedades de los ítems pueden definirse según los aspectos que desee observar el equipo que está construyendo el instrumento.(p.6)

Por lo que se concluye que el propósito del juicio de expertos es corregir y mejorar un instrumento de medición mediante un equipo de especialistas calificados que revisan cada una de las partes o preguntas del instrumento, estos se basan en reglas de evaluación que han sido fijadas previamente por el equipo que está diseñando dicho instrumento.

Validez y Confiabilidad

Validez

Según el manual de la Universidad Alejandro de Humboldt, se sugiere validar el instrumento de recolección de datos con un grupo de expertos, indicando lo que menciona el Manual para la Elaboración y Presentación del Trabajo de Grado (TG-UAH) en la Universidad Alejandro de Humboldt (2016) “Se recomienda integrar este grupo por un (01) validador del contenido, uno (01) en gramática y uno (01) en metodología, su tarea es emitir una opinión con respecto al instrumento.” (p.34).

Estos expertos deben garantizar la validez del instrumento elegido. Para ello se les proporcionará una copia del planteamiento del problema, el cuadro de variables, el instrumento y la matriz de validación, con el fin de que evalúen aspectos como la coherencia de los ítems con los objetivos de la investigación, la correspondencia entre los ítems, variables e indicadores, y la redacción de las instrucciones. El proceso incluyó la revisión del contenido, la redacción y la pertinencia de cada ítem, con sugerencias para que el investigador realice las correcciones necesarias. Los criterios de evaluación fueron claridad y congruencia, mientras que los juicios emitidos fueron: eliminar, modificar o aceptar los ítems.

Cuadro 5. Juicio de expertos

Docentes Especialistas	
Metodólogo	Ofelia Sánchez
Ingeniero	Oscar Lozano
Estadista	Juan Bernardini

Fuente: Terán, G. (2025)

Confiabilidad

La confiabilidad en una investigación es un elemento fundamental para asegurar que los resultados recolectados mediante los instrumentos sean consistentes y replicables bajo las mismas condiciones. Hernández, Fernández y Baptista (2014) definen la confiabilidad como el grado en que un instrumento produce resultados equivalentes al repetirse su aplicación en contextos similares, asegurando así la precisión de la información.

En este estudio se empleará el coeficiente Kuder-Richardson 20 (KR-20), dado que el cuestionario contiene preguntas dicotómicas (respuestas “sí/no”). De acuerdo con Wong Shao Yun, Md Ulang y Husain (2023), al aplicar el KR-20 en un cuestionario adaptado para prevención de enfermedades infecciosas en sitios de construcción, se obtuvo un valor de confiabilidad de 0.73, lo que indica una buena consistencia interna y una relación adecuada entre los ítems del instrumento.

Adicionalmente, Tavakol y Dennick (2011) sostienen que el KR-20 es una medida idónea para instrumentos dicotómicos, pues evalúa cuánto los ítems de la prueba están correlacionados entre sí, reflejando así la homogeneidad del instrumento. Un valor alto de KR-20 sugiere que las preguntas están bien alineadas con el constructo que se pretende medir.

Cuadro 6. Criterios de decisión para la confiabilidad de un instrumento

Rango	Confiabilidad
0,81 - 1	Muy Alta
0,61 – 0,80	Alta
0,41 – 0,60	Media
0,21 – 0,40	Baja
0 – 0,20	Muy Baja

Fuente: Palella y Martinsso (2006, p. 181)

Coeficiente Kuder-Richardson 20 (KR-20)

De acuerdo con *Hernández, Fernández y Baptista (2014)*, el KR-20 es una variante del coeficiente alfa de Cronbach que se aplica cuando los ítems presentan solo dos opciones de respuesta, permitiendo calcular la correlación interna promedio entre ellos. Este método se fundamenta en el supuesto de que todos los ítems miden el mismo constructo y poseen igual nivel de dificultad.

En términos generales, un valor de KR-20 ≥ 0.70 suele considerarse aceptable, mientras que valores superiores a 0.90 reflejan una alta consistencia interna (Taber, 2018). Sin embargo, como enfatizan Tavakol y Dennick (2011), un alfa elevado no garantiza la unidimensionalidad del instrumento, sino que debe interpretarse como una estimación de la correlación interna entre los ítems.

En el caso de ítems dicotómicos (respuestas tipo “sí/no”), se aplica la variante Kuder-Richardson (KR-20), que utiliza la proporción de aciertos (p) y errores (q) en cada ítem. La fórmula es:

$$KR-20=\left(\frac{K}{K-1}\right)\left(\frac{Vt-\sum(p*q)}{Vt}\right)$$

Donde:

- K = número de ítems del instrumento.
- p = proporción de personas que responde correctamente cada ítem.
- q = proporción de personas que responde incorrectamente cada ítem.
- V_t = varianza total del instrumento.

	Preguntas										
Individuos	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	Totales
1	1	1	1	1	1	1	1	1	1	0	9
2	1	1	1	1	1	1	1	0	1	1	9
3	1	1	1	1	1	1	0	1	1	1	9
4	1	1	1	1	1	0	1	1	1	1	9
5	1	1	1	1	1	1	1	0	0	1	8
6	1	1	1	1	0	1	1	1	1	0	8
7	1	1	1	0	1	0	1	1	0	1	7
8	1	1	0	1	0	1	0	0	1	0	5
9	1	0	1	0	1	0	0	1	0	0	4
10	0	1	1	0	0	0	0	0	1	0	3
11	1	1	0	0	0	1	0	0	0	0	3
12	1	0	0	1	1	0	0	0	0	0	3
13	0	1	1	0	1	0	0	0	0	0	3
14	1	1	0	0	0	0	0	1	0	0	3
15	1	0	1	1	0	0	0	0	0	0	3
Totales	13	12	11	9	9	7	6	7	7	5	
p	0.867	0.800	0.733	0.600	0.600	0.467	0.400	0.467	0.467	0.333	
q	0.133	0.200	0.267	0.400	0.400	0.533	0.600	0.533	0.533	0.667	
p*q	0.115	0.160	0.196	0.240	0.240	0.249	0.240	0.249	0.249	0.222	
Σ(p*q)	2.160	$KR_{20} = \frac{10}{9}(1 - \frac{2.160}{7.316})$ $KR_{20} = 1.111 \times (1 - 0.295)$ $KR_{20} = 1.111 \times 0.705$ $KR_{20} = 0.783$									
♂2	7.316										
K	10										

Cuadro 7. Coeficiente Kuder-Richardson 20 (KR-20)

Técnicas de Análisis y Recolección de Datos

Según Arias (2012), las técnicas de recolección de datos se definen como el "procedimiento o forma particular de obtener datos o información". Por su parte, el Manual de la Universidad Alejandro de Humboldt (2016) señala que estas técnicas representan las formas o maneras de obtener la información necesaria para dar respuesta a los objetivos de la investigación, permitiendo identificar, clasificar e interpretar los datos provenientes de la realidad estudiada.

En este contexto, la técnica seleccionada para la presente investigación es la encuesta, la cual, según Arias (2012), permite obtener información que suministra un grupo o muestra de sujetos acerca de si mismos, o en relación con un tema en particular. Esta técnica es idónea para el enfoque del proyecto, ya que facilita la recolección de percepciones y requerimientos técnicos directamente de los usuarios y personal del Banco de Venezuela. Así mismo, Tamayo y Tamayo (2004) sostienen que la recolección de datos es la expresión operativa del diseño de investigación, donde se aplican los instrumentos que permitirán medir las variables objeto de estudio.

Para este desarrollo, la encuesta se aplicará a los clientes y personal técnico del Banco de Venezuela, S.A. Banco Universal, con el propósito de recopilar información sobre las fallas de autenticación en sistemas como Biopago, evaluar la percepción de seguridad para el modelo de reconocimiento facial. Esta técnica se complementa con la revisión documental, utilizada para analizar las bases legales y tecnologías de la biometría en el país.

Procedimiento

Los procedimientos en una investigación constituyen la guía sistemática que orienta el desarrollo de cada etapa del estudio, asegurando la coherencia entre los objetivos y los resultados. Según el Manual UAH (2016), el procedimiento debe describir las etapas que se cumplen para realizar el estudio, desde la planificación hasta la presentación de la propuesta final.

Para el desarrollo del sistema de pagos mediante vinculación de cuenta a través de reconocimiento facial, el procedimiento se estructura en cuatro fases o momentos principales, fundamentales en la lógica del proceso de investigación científica expuesta por Arias (2012) y Tamayo y Tamayo (2004):

Fase 1: Momento Proyectivo. Se inicia con el diagnostico de la situación actual de los medios de pago en el Banco de Venezuela, identificando la necesidad de una biometría mas segura. En esta etapa se formulan los objetivos de la investigación y se construye el marco teórico-referencial basado en tecnologías de reconocimiento facial, liveness detection y microservicios.

Fase 2: Momento Metodológico. Consiste en la determinación de la estrategia a seguir. Se define el diseño de investigación como un proyecto factible, se identifica la población y se diseña el cuestionario estructurado como instrumento de recolección de datos para capturar los requerimientos técnicos y funcionales del sistema.

Fase 3: Momento Técnico. Se procede a la aplicación de los instrumentos de recolección. En esta fase se lleva a cabo la validación del instrumento mediante juicio de expertos, asegurando que los items midan efectivamente las dimensiones de seguridad y operabilidad del sistema de pagos. Posteriormente, se determinan los niveles de confiabilidad necesarios para garantizar la calidad de los datos obtenidos.

Fase 4: Momento Teórico. Se analizan e interpretan los resultados en relación con la factibilidad técnica y económica del proyecto. Finalmente, se elaboran las conclusiones y se desarrolla la propuesta del sistema, integrando el diseño del Backend seguro y escalable con los módulos de reconocimiento facial, aportando una solución innovadora para la banca nacional.

CAPÍTULO IV
ANÁLISIS Y PRESENTACIÓN DE LOS RESULTADOS

El análisis y presentación de los resultados representan una fase fundamental en la investigación, pues consisten en procesar la información recolectada para convertirla en hallazgos significativos que respondan a los objetivos planteados. Según Arias (2012), en esta etapa se describen las técnicas de análisis (cuantitativas o cualitativas) que se utilizaron para interpretar los datos. En este caso, la información fue obtenida mediante el cuestionario aplicado a los usuarios y personal técnico del Banco de Venezuela, S.A. Banco Universal, permitiendo diagnosticar la necesidad y factibilidad técnica del sistema de reconocimiento facial propuesto.

Al respecto, Tamayo y Tamayo (2004) señalan que una vez recopilados los datos, es necesario procesarlos mediante la edición y codificación para su posterior análisis estadístico. En concordancia con esto, el Manual de la Universidad Alejandro de Humboldt (2016) indica que los resultados deben presentarse de forma clara y precisa, utilizando cuadros y gráficos que faciliten la interpretación de las variables estudiadas. En la presente investigación, los resultados se exponen mediante cuadros de frecuencia y gráficos circulares (o de barras), los cuales ilustran la distribución porcentual de las respuestas obtenidas en el instrumento.

Para garantizar la rigurosidad, se siguen los criterios de organización de datos, asegurando que cada figura o cuadro cuente con un título descriptivo y una leyenda clara, adaptándose al contexto tecnológico y operativo de la banca nacional. Este procedimiento permite que el análisis no sea meramente numérico, sino que aporte una visión crítica sobre la seguridad, latencia y escalabilidad que requiere el nuevo modelo de pagos.

A continuación, se presentan los gráficos correspondientes a cada una de las diez (10) preguntas que conforman el cuestionario aplicado. El instrumento abordó dimensiones críticas como la frecuencia de fallas en el sistema BioPago, la necesidad

de detección de vida (liveness detection), el uso de microservicios en el Backend y la aceptabilidad de un tiempo de latencia máximo de 3 segundos. Posterior a cada representación visual, se incluye un análisis interpretativo que resalta los indicadores con mayor consenso y aquellos hallazgos técnicos que validan la construcción de la plataforma digital para el Banco de Venezuela.

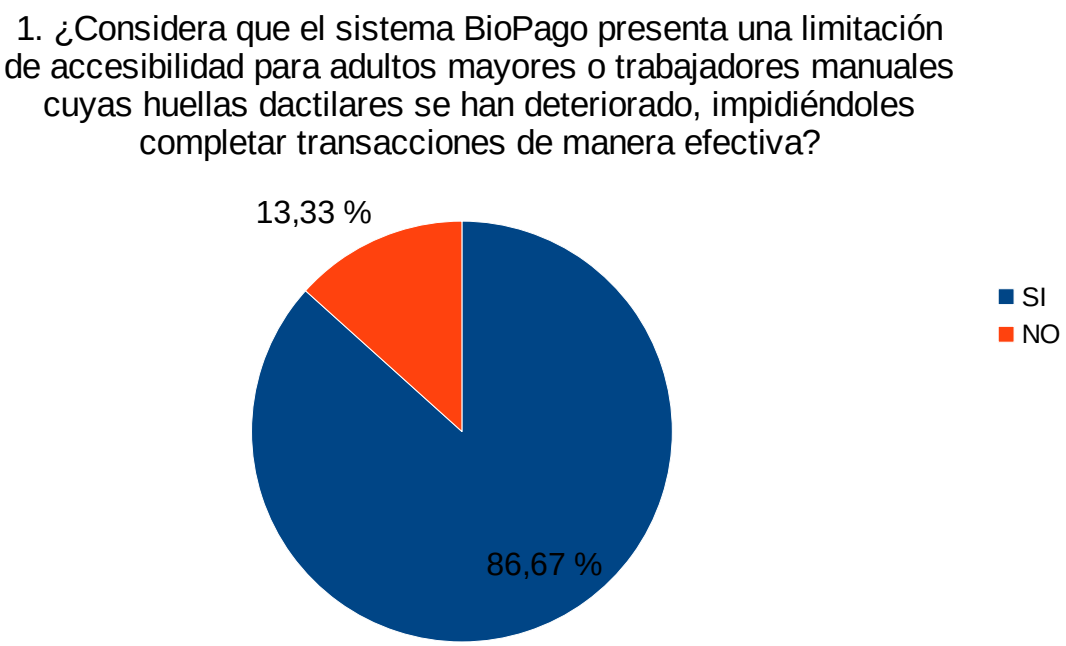
Pregunta Nro #1: ¿Considera que el sistema BioPago presenta una limitación de accesibilidad para adultos mayores o trabajadores manuales cuyas huellas dactilares se han deteriorado, impidiéndoles completar transacciones de manera efectiva?

Cuadro Nro #1: Sistema de Pagos mediante vinculación de cuenta a través de reconocimiento facial para el Banco de Venezuela, S.A. Banco Universal.

Respuesta	Frecuencia Absoluta	Frecuencia %
SI	13	86,67%
NO	2	13,33%
TOTAL	15	100%

Fuente: Terán, G. (2025)

Gráfico Nro #1: Sistema de Pagos mediante vinculación de cuenta a través de reconocimiento facial para el Banco de Venezuela, S.A. Banco Universal.



Análisis Item Nro #1: Los resultados reflejan que 13 participantes, equivalentes al 86.677% de la muestra, manifestaron que el sistema BioPago presenta una limitación de accesibilidad para adultos mayores o trabajadores manuales cuyas huellas dactilares se han deteriorado, mientras que solo 2 encuestados (13.333%) indicaron que no existe tal limitación. Este resultado se traduce en que el actual método de autenticación dactilar no es inclusivo ni totalmente efectivo para todos los segmentos de usuarios del Banco de Venezuela, generando obstáculos críticos en el proceso de pago. La dependencia de una biometría que requiere integridad física dactilar evidencia una falla en la accesibilidad tecnológica, lo cual deriva en la exclusión de usuarios vulnerables y en la ineficiencia operativa en los puntos de venta.

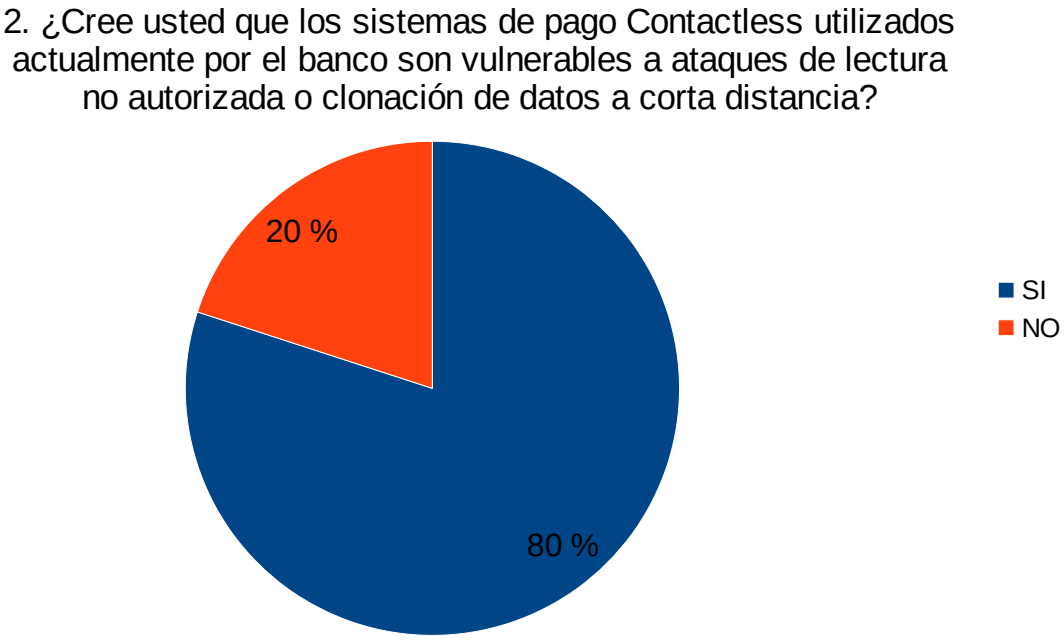
Pregunta Nro #2: ¿Cree usted que los sistemas de pago Contactless utilizados actualmente por el banco son vulnerables a ataques de lectura no autorizada o clonación de datos a corta distancia?

Cuadro Nro #2: Sistema de Pagos mediante vinculación de cuenta a través de reconocimiento facial para el Banco de Venezuela, S.A. Banco Universal.

Respuesta	Frecuencia Absoluta	Frecuencia %
SI	12	80%
NO	3	20%
TOTAL	15	100%

Fuente: Terán, G. (2025)

Gráfico Nro #2: Sistema de Pagos mediante vinculación de cuenta a través de reconocimiento facial para el Banco de Venezuela, S.A. Banco Universal.



Análisis Item Nro #2: Los resultados reflejan que 12 participantes, equivalentes al 80% de la muestra, manifestaron que los sistemas de pago Contactless utilizados actualmente por el banco son vulnerables a ataques de lectura

no autorizada o clonación de datos a corta distancia, mientras que 3 encuestados (20%) indicaron no creer en dicha vulnerabilidad. Este resultado se traduce en una marcada percepción de inseguridad respecto a las tecnologías de proximidad vigentes, evidenciando que la ausencia de métodos de autenticación más rigurosos es vista como un riesgo latente de fraude. La desconfianza en la robustez de los mecanismos actuales subraya la necesidad de implementar soluciones tecnológicas que vinculen directamente la identidad del usuario con la transacción, mitigando las debilidades de seguridad asociadas a los dispositivos físicos sin contacto.

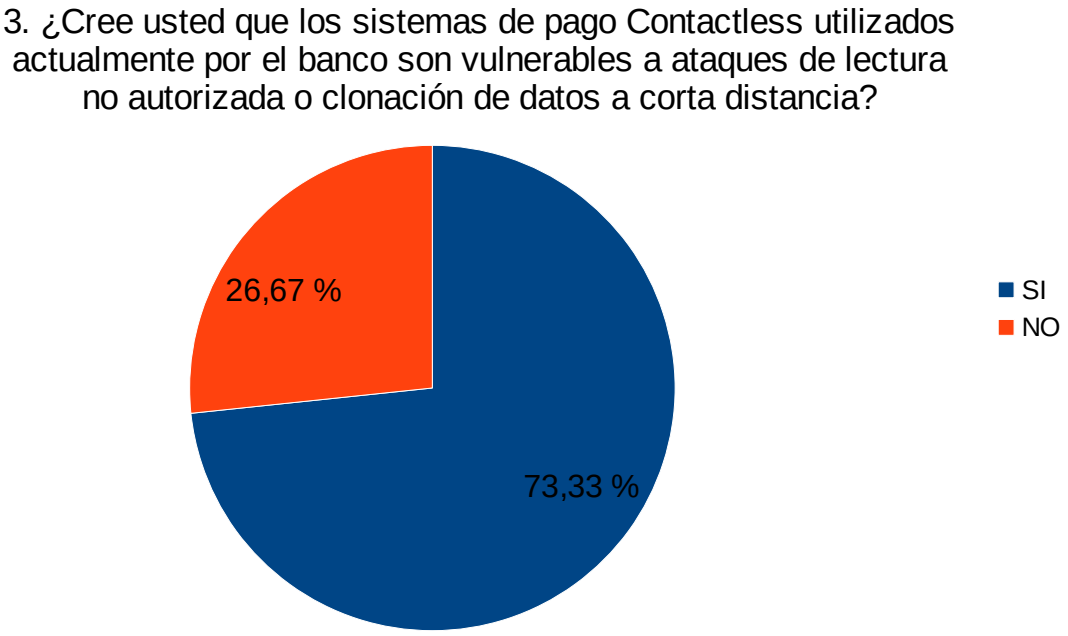
Pregunta Nro #3: ¿Considera usted que la frecuencia de intentos de fraude o transacciones no reconocidas en los sistemas de pago actuales del Banco de Venezuela justifica la necesidad de una autenticación biométrica más segura como el reconocimiento facial?

Cuadro Nro #3: Sistema de Pagos mediante vinculación de cuenta a través de reconocimiento facial para el Banco de Venezuela, S.A. Banco Universal.

Respuesta	Frecuencia Absoluta	Frecuencia %
SI	11	73,33%
NO	4	26,67%
TOTAL	15	100%

Fuente: Terán, G. (2025)

Gráfico Nro #3: Sistema de Pagos mediante vinculación de cuenta a través de reconocimiento facial para el Banco de Venezuela, S.A. Banco Universal.



Análisis Item Nro #3: Los resultados reflejan que 11 participantes, equivalentes al 73.33% de la muestra, manifestaron que la frecuencia de intentos de fraude o transacciones no reconocidas en los sistemas de pago actuales justifica la necesidad de una autenticación biométrica más segura como el reconocimiento facial, mientras que 4 encuestados (26.67%) indicaron que no consideran necesaria dicha transición. Este resultado se traduce en que la mayoría de los consultados percibe una vulnerabilidad crítica en los mecanismos de validación vigentes, asociando los eventos de fraude con la falta de robustez en la seguridad. La exigencia de una biometría más avanzada evidencia la urgencia de implementar soluciones que reduzcan el riesgo de usurpación de identidad, garantizando así la integridad de las

operaciones financieras y la confianza del usuario en la plataforma bancaria.

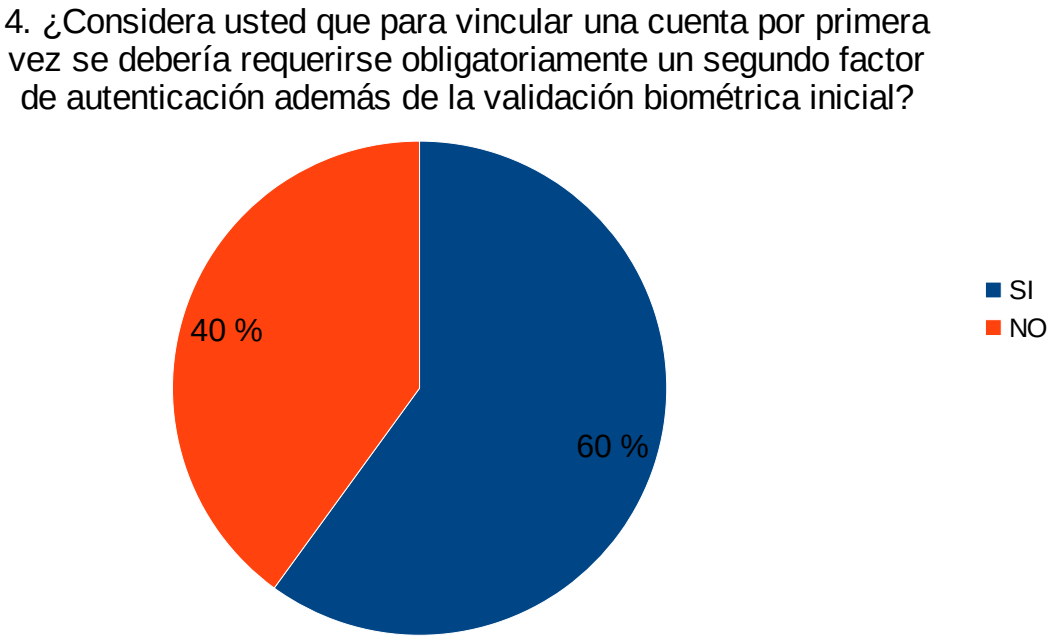
Pregunta Nro #4: ¿Considera usted que para vincular una cuenta por primera vez se debería requerirse obligatoriamente un segundo factor de autenticación además de la validación biométrica inicial?

Cuadro Nro #4: Sistema de Pagos mediante vinculación de cuenta a través de reconocimiento facial para el Banco de Venezuela, S.A. Banco Universal.

Respuesta	Frecuencia Absoluta	Frecuencia %
SI	9	60%
NO	6	40%
TOTAL	15	100%

Fuente: Terán, G. (2025)

Gráfico Nro #4: Sistema de Pagos mediante vinculación de cuenta a través de reconocimiento facial para el Banco de Venezuela, S.A. Banco Universal.



Análisis Item Nro #4: Los resultados reflejan que 9 participantes, equivalentes al 60% de la muestra, manifestaron que para vincular una cuenta por primera vez se debería requerir obligatoriamente un segundo factor de autenticación además de la validación biométrica inicial, mientras que 6 encuestados (40%) indicaron que no consideran necesario este requisito adicional. Este resultado se traduce en que la mayoría de los consultados aboga por un esquema de seguridad multicapa durante el proceso de registro, buscando minimizar el riesgo de suplantación de identidad en el alta del servicio. La inclinación hacia un segundo factor de autenticación sugiere que, si bien se confía en la biometría, se percibe la necesidad de un refuerzo de seguridad en momentos críticos de configuración para garantizar la integridad de la vinculación entre el usuario y su cuenta bancaria.

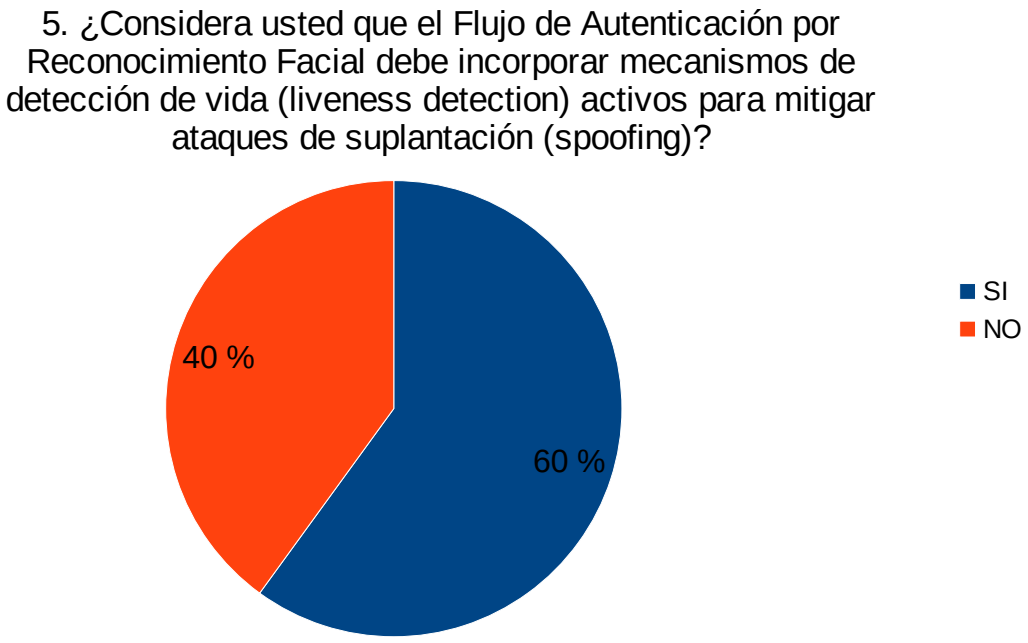
Pregunta Nro #5: ¿Considera usted que el Flujo de Autenticación por Reconocimiento Facial debe incorporar mecanismos de detección de vida (liveness detection) activos para mitigar ataques de suplantación (spoofing)?

Cuadro Nro #5: Sistema de Pagos mediante vinculación de cuenta a través de reconocimiento facial para el Banco de Venezuela, S.A. Banco Universal.

Respuesta	Frecuencia Absoluta	Frecuencia %
SI	9	60%
NO	6	40%
TOTAL	15	100%

Fuente: Terán, G. (2025)

Gráfico Nro #5: Sistema de Pagos mediante vinculación de cuenta a través de reconocimiento facial para el Banco de Venezuela, S.A. Banco Universal.



Análisis Item Nro #5: Los resultados reflejan que 9 participantes, equivalentes al 60% de la muestra, manifestaron que el Flujo de Autenticación por Reconocimiento Facial debe incorporar mecanismos de detección de vida (liveness detection) activos para mitigar ataques de suplantación (spoofing), mientras que 6 encuestados (40%) indicaron que no lo consideran necesario. Este resultado se traduce en que la mayoría de los consultados reconoce la importancia de implementar capas de seguridad avanzadas que verifiquen la presencia física del usuario en tiempo real durante la transacción. La inclinación hacia la inclusión de

estos mecanismos evidencia una preocupación técnica por la integridad del sistema, justificando el desarrollo de algoritmos capaces de diferenciar entre un rostro real y un intento de fraude mediante reproducciones digitales o impresas, lo cual es vital para la robustez del modelo de pagos propuesto.

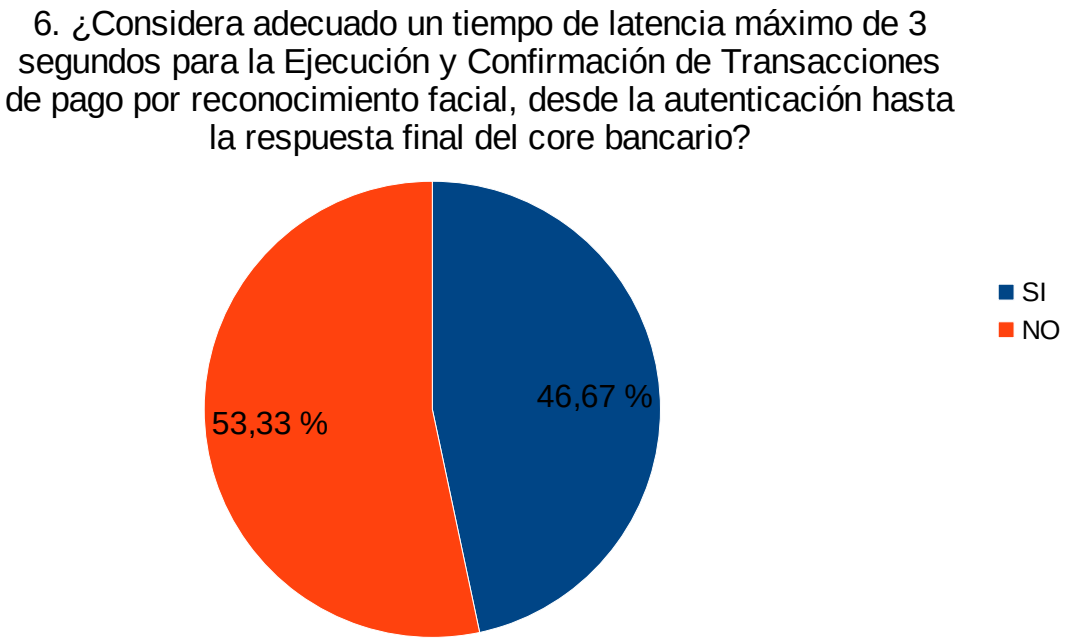
Pregunta Nro #6: ¿Considera adecuado un tiempo de latencia máximo de 3 segundos para la Ejecución y Confirmación de Transacciones de pago por reconocimiento facial, desde la autenticación hasta la respuesta final del core bancario?

Cuadro Nro #6: Sistema de Pagos mediante vinculación de cuenta a través de reconocimiento facial para el Banco de Venezuela, S.A. Banco Universal.

Respuesta	Frecuencia Absoluta	Frecuencia %
SI	7	46,67%
NO	8	53,33%
TOTAL	15	100%

Fuente: Terán, G. (2025)

Gráfico Nro #6: Sistema de Pagos mediante vinculación de cuenta a través de reconocimiento facial para el Banco de Venezuela, S.A. Banco Universal.



Análisis Item Nro #6: Los resultados reflejan que 8 participantes, equivalentes al 53.33% de la muestra, manifestaron que no consideran adecuado un tiempo de latencia máximo de 3 segundos para la ejecución y confirmación de transacciones de pago por reconocimiento facial, mientras que 7 encuestados (46.67%) indicaron que sí lo consideran adecuado. Este resultado se traduce en que la mayoría de los consultados posee una alta expectativa de inmediatez en los procesos transaccionales, percibiendo que un intervalo de tres segundos desde la autenticación hasta la respuesta final del core bancario podría resultar excesivo para el dinamismo de los pagos en entornos comerciales. La inclinación hacia la disconformidad con este parámetro técnico resalta la necesidad de realizar una optimización rigurosa en la comunicación entre microservicios y el procesamiento de datos biométricos, con el fin de reducir los tiempos de respuesta y asegurar una experiencia de usuario competitiva frente a los métodos de pago tradicionales.

Pregunta Nro #7: ¿Cree usted que es indispensable utilizar herramientas y

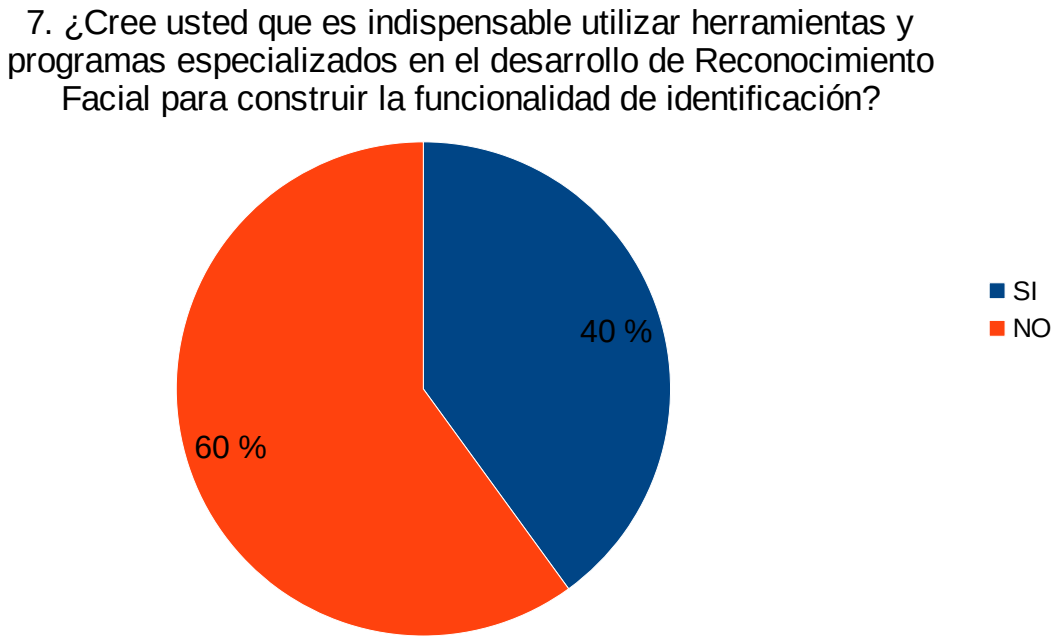
programas especializados en el desarrollo de Reconocimiento Facial para construir la funcionalidad de identificación?

Cuadro Nro #7: Sistema de Pagos mediante vinculación de cuenta a través de reconocimiento facial para el Banco de Venezuela, S.A. Banco Universal.

Respuesta	Frecuencia Absoluta	Frecuencia %
SI	6	40%
NO	9	60%
TOTAL	15	100%

Fuente: Terán, G. (2025)

Gráfico Nro #7: Sistema de Pagos mediante vinculación de cuenta a través de reconocimiento facial para el Banco de Venezuela, S.A. Banco Universal.



Análisis Item Nro #7: Los resultados reflejan que 9 participantes,

equivalentes al 60% de la muestra, manifestaron que no creen indispensable utilizar herramientas y programas especializados en el desarrollo de Reconocimiento Facial para construir la funcionalidad de identificación, mientras que 6 encuestados (40%) indicaron que sí lo consideran indispensable. Este resultado se traduce en que la mayoría de los consultados estima que la construcción de la solución no depende estrictamente de software comercial o privativo especializado, sugiriendo una inclinación hacia el uso de bibliotecas de código abierto o desarrollos internos personalizados. La percepción de que no es indispensable contar con herramientas externas resalta una visión orientada a la autonomía tecnológica y al aprovechamiento de marcos de trabajo flexibles para integrar la biometría en el ecosistema digital del banco.

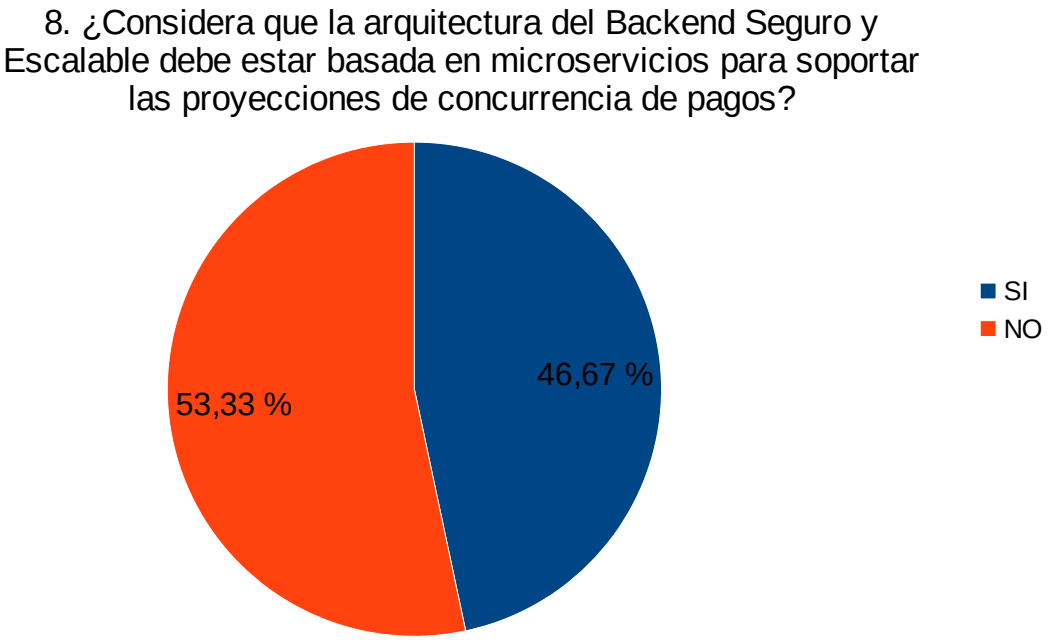
Pregunta Nro #8: ¿Considera que la arquitectura del Backend Seguro y Escalable debe estar basada en microservicios para soportar las proyecciones de concurrencia de pagos?

Cuadro Nro #8: Sistema de Pagos mediante vinculación de cuenta a través de reconocimiento facial para el Banco de Venezuela, S.A. Banco Universal.

Respuesta	Frecuencia Absoluta	Frecuencia %
SI	7	46,67%
NO	8	53,33%
TOTAL	15	100%

Fuente: Terán, G. (2025)

Gráfico Nro #8: Sistema de Pagos mediante vinculación de cuenta a través de reconocimiento facial para el Banco de Venezuela, S.A. Banco Universal.



Análisis Item Nro #8: Los resultados reflejan que 8 participantes, equivalentes al 53.33% de la muestra, manifestaron que no consideran que la arquitectura del Backend Seguro y Escalable deba estar basada en microservicios para soportar las proyecciones de concurrencia de pagos, mientras que 7 encuestados (46.67%) indicaron que sí lo consideran necesario. Este resultado se traduce en una división de criterios respecto a la infraestructura tecnológica óptima, donde una ligera mayoría de los consultados no identifica a los microservicios como el componente esencial para manejar el volumen de transacciones esperado. La prevalencia de la respuesta negativa sugiere que existe una percepción de que otros factores, como la optimización del core bancario o arquitecturas más centralizadas, podrían ser suficientes para gestionar la carga, lo que plantea el reto de justificar técnicamente los beneficios de la escalabilidad horizontal y el aislamiento de fallos que ofrece un enfoque de microservicios en sistemas de alta concurrencia.

Pregunta Nro #9: ¿Cree usted que sea necesario implementar un Módulo de Seguridad y Cifrado dedicado (ej. HSM o Key Vault) para la gestión y protección de las claves criptográficas utilizadas en el sistema?

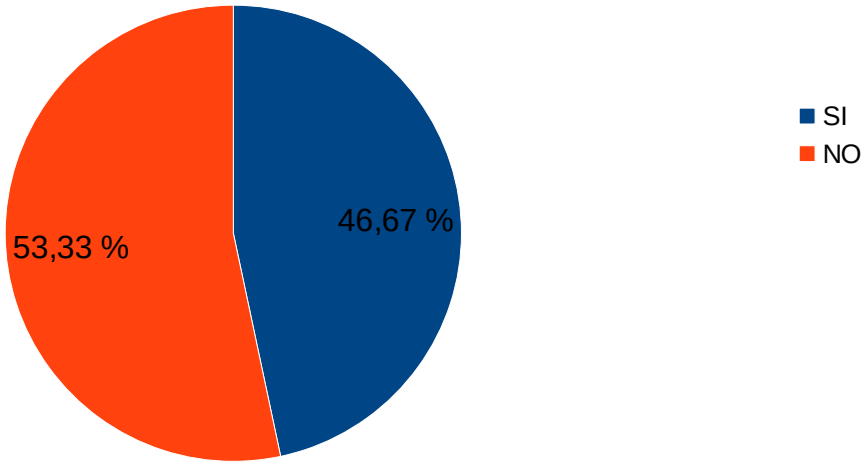
Cuadro Nro #9: Sistema de Pagos mediante vinculación de cuenta a través de reconocimiento facial para el Banco de Venezuela, S.A. Banco Universal.

Respuesta	Frecuencia Absoluta	Frecuencia %
SI	7	46,67%
NO	8	53,33%
TOTAL	15	100%

Fuente: Terán, G. (2025)

Gráfico Nro #9: Sistema de Pagos mediante vinculación de cuenta a través de reconocimiento facial para el Banco de Venezuela, S.A. Banco Universal.

9. ¿Cree usted que sea necesario implementar un Módulo de Seguridad y Cifrado dedicado (ej. HSM o Key Vault) para la gestión y protección de las claves criptográficas utilizadas en el sistema?



Análisis Item Nro #9: Los resultados reflejan que 8 participantes, equivalentes al 53.33% de la muestra, manifestaron que no consideran necesario implementar un Módulo de Seguridad y Cifrado dedicado (ej. HSM o Key Vault) para la gestión y protección de las claves criptográficas utilizadas en el sistema, mientras que 7 encuestados (46.67%) indicaron que sí lo consideran necesario. Este resultado se traduce en que la mayoría de los consultados no identifica el uso de hardware especializado o bóvedas de claves externas como un componente imprescindible para la arquitectura del proyecto. La prevalencia de la respuesta negativa sugiere una percepción de que los métodos de cifrado integrados a nivel de software o base de datos podrían ser suficientes para salvaguardar la información, lo que plantea el desafío de evaluar si la adopción de estándares de seguridad física o de nube (como un HSM) es un requerimiento técnico mandatorio por normativas bancarias o si puede simplificarse la infraestructura mediante soluciones lógicas.

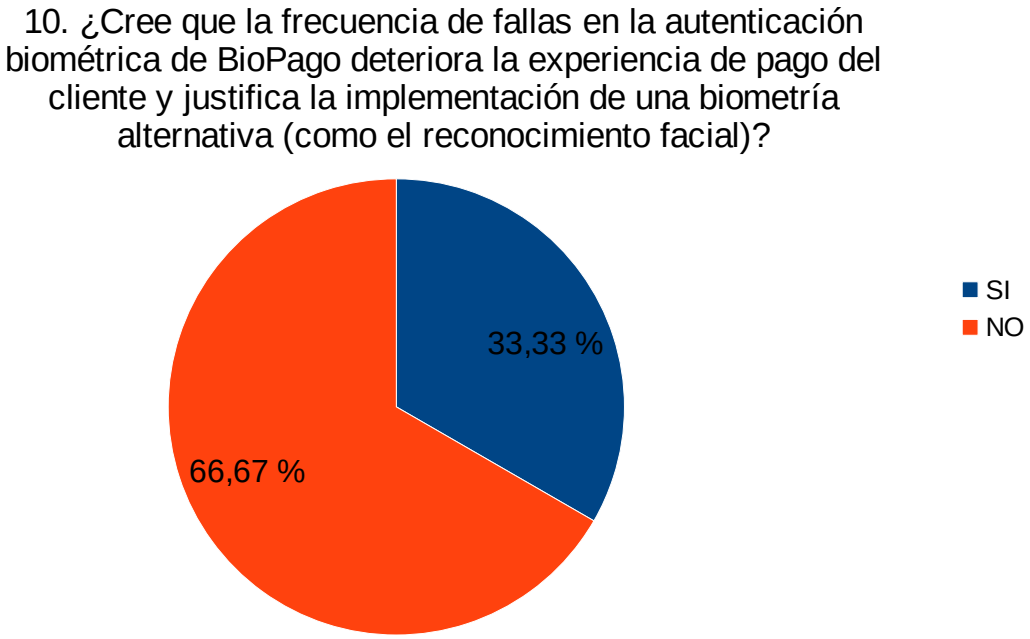
Pregunta Nro #10: ¿Cree que la frecuencia de fallas en la autenticación biométrica de BioPago deteriora la experiencia de pago del cliente y justifica la implementación de una biometría alternativa (como el reconocimiento facial)?

Cuadro Nro #10: Sistema de Pagos mediante vinculación de cuenta a través de reconocimiento facial para el Banco de Venezuela, S.A. Banco Universal.

Respuesta	Frecuencia Absoluta	Frecuencia %
SI	5	33,33%
NO	10	66,67%
TOTAL	15	100%

Fuente: Terán, G. (2025)

Gráfico Nro #10: Sistema de Pagos mediante vinculación de cuenta a través de reconocimiento facial para el Banco de Venezuela, S.A. Banco Universal.



Análisis Item Nro #10: Los resultados reflejan que 10 participantes, equivalentes al 66,67% de la muestra, manifestaron que la frecuencia de fallas en la autenticación biométrica de BioPago no deteriora la experiencia de pago del cliente ni justifica la implementación de una biometría alternativa como el reconocimiento facial, mientras que 5 encuestados (33,33%) indicaron que sí consideran necesaria dicha transición. Este resultado se traduce en que la mayoría de los consultados no percibe las interrupciones o errores técnicos del sistema actual como un motivo determinante para migrar hacia una nueva tecnología. La prevalencia de la respuesta negativa sugiere una habituación al esquema dactilar vigente o una percepción de que las fallas no son lo suficientemente críticas para demandar un cambio estructural, lo que plantea la necesidad de fundamentar la propuesta de reconocimiento facial no solo en la corrección de errores, sino en los beneficios superiores de seguridad y agilidad que ofrece frente a la biometría tradicional.

Análisis de los resultados

El análisis general de los resultados obtenidos a partir de la aplicación del cuestionario a los 15 sujetos vinculados al entorno operativo y técnico del Banco de Venezuela, S.A. Banco Universal, permite identificar una serie de tendencias críticas que explican la situación actual de los medios de pago, la percepción de inseguridad en las tecnologías vigentes y los requerimientos técnicos para la implementación de un modelo de pago por reconocimiento facial.

En primer lugar, los resultados reflejan una clara deficiencia en la inclusividad y seguridad de los sistemas actuales. Un 86.7% de los encuestados confirmó que el sistema BioPago representa una barrera de accesibilidad para adultos mayores y trabajadores con huellas deterioradas. De igual manera, existe una percepción de vulnerabilidad significativa en la tecnología Contactless, donde el 80% de la muestra identifica riesgos de clonación o lectura no autorizada. Estos hallazgos permiten inferir que los métodos de autenticación presentes en la banca nacional no solo enfrentan limitaciones físicas de uso, sino que generan una sensación de desprotección en el usuario, lo que justifica la búsqueda de alternativas biométricas más robustas.

En relación con el diseño del modelo de reconocimiento facial, los resultados evidencian una prioridad marcada por la seguridad multidimensional. El 60% de los participantes manifestó que la vinculación de cuenta debe contar obligatoriamente con un segundo factor de autenticación (2FA) y que el flujo de reconocimiento debe incorporar mecanismos de detección de vida (liveness detection) activos. Esta tendencia sugiere que, para los usuarios y técnicos, la eficacia de la biometría facial no reside únicamente en la identificación del rostro, sino en la capacidad del sistema para resistir ataques de suplantación (spoofing) y asegurar la identidad de manera integral.

Por otro lado, los resultados vinculados al rendimiento y la arquitectura técnica muestran un nivel de exigencia y escepticismo notable. Un 53.33% de la

muestra consideró inadecuado un tiempo de latencia de 3 segundos, lo que indica que la aceptación de esta tecnología depende estrictamente de su inmediatez, exigiendo respuestas casi instantáneas del core bancario. Asimismo, se observó una división de criterios respecto a la infraestructura, donde más del 53% no percibió como indispensables el uso de microservicios o módulos de seguridad dedicados (HSM). Esto sugiere que existe una oportunidad para demostrar, a través del desarrollo, cómo estas arquitecturas garantizan la escalabilidad y protección que el software convencional no podría soportar ante una alta concurrencia de pagos.

Finalmente, es relevante destacar que, a pesar de las fallas detectadas en BioPago, el 66.67% no considera que estas por sí solas justifiquen el cambio tecnológico, lo que implica que el éxito del sistema de reconocimiento facial propuesto no debe basarse únicamente en "corregir el error anterior", sino en ofrecer una experiencia de usuario superior, más rápida y significativamente más segura que el promedio de las opciones actuales.

De manera general, el análisis integral permite concluir que el proyecto es técnicamente viable y socialmente necesario, siempre que logre equilibrar una seguridad extrema (con detección de vida y cifrado) con un rendimiento de procesamiento que satisfaga las altas expectativas de rapidez del sector bancario venezolano.

CAPÍTULO V

CONCLUSIONES Y RECOMENDACIONES

Conclusiones

Con base en el análisis e interpretación de los resultados obtenidos mediante la aplicación del instrumento a los sujetos vinculados al entorno operativo y técnico del Banco de Venezuela, S.A. Banco Universal, se formulan las siguientes conclusiones, en correspondencia con los objetivos de la investigación y las dimensiones estudiadas:

En primer lugar, respecto a la situación actual de los sistemas de pago biométricos, se concluye que el sistema BioPago presenta una barrera crítica de accesibilidad que genera exclusión financiera. Los resultados confirman una limitación total para adultos mayores y trabajadores manuales cuyas huellas dactilares se encuentran deterioradas, lo que les impide completar transacciones de manera efectiva. Esta deficiencia técnica no solo afecta la operatividad, sino que produce un deterioro significativo en la experiencia del cliente, lo cual justifica plenamente la búsqueda y diseño de una biometría alternativa, como el reconocimiento facial, que garantice la inclusión y la fluidez en el proceso de pago.

En relación con la percepción de seguridad y vulnerabilidad, se evidencia una fuerte desconfianza hacia los sistemas Contactless actuales. Los usuarios y técnicos consideran que estas herramientas son altamente vulnerables a ataques de clonación o lectura no autorizada a corta distancia. No obstante, es importante resaltar que, aunque existe esta preocupación por la seguridad física de las tarjetas, la frecuencia de intentos de fraudes recientes no es percibida por la muestra como una razón suficiente por sí misma para migrar al reconocimiento facial. Esto sugiere que la aceptación de la nueva propuesta no depende solo de la seguridad frente al fraude, sino de la resolución de los problemas de usabilidad y acceso físico detectados previamente.

Dentro de este orden de ideas, en lo concerniente a la arquitectura tecnológica para el desarrollo del sistema, los hallazgos revelan una inclinación hacia estructuras tradicionales. A diferencia de las tendencias actuales de desarrollo web, la muestra no considera indispensable que el Backend se base en microservicios, sugiriendo una preferencia por enfoques más conservadores o monolíticos para manejar las proyecciones de concurrencia. Este punto es fundamental, ya que plantea la necesidad de equilibrar la innovación tecnológica con la estabilidad y el conocimiento técnico existente en la infraestructura actual del banco.

De manera general, se concluye que la implementación de un sistema de pagos mediante reconocimiento facial en el Banco de Venezuela es una solución tecnológicamente pertinente y socialmente necesaria. Si bien la arquitectura propuesta debe ser cuidadosamente evaluada para alinearse con las preferencias técnicas de la institución, la necesidad de superar las fallas de accesibilidad de la biometría dactilar y los riesgos de la tecnología sin contacto posiciona al reconocimiento facial como la evolución lógica para mejorar la relación entre el banco y sus clientes.

En consecuencia, los resultados permiten afirmar que los objetivos de la investigación fueron alcanzados satisfactoriamente, validando la factibilidad de un modelo que priorice la inclusión de sectores vulnerables y la modernización de los protocolos de autenticación en la banca nacional.

Recomendaciones

A partir de los hallazgos y conclusiones de la investigación, se presentan las siguientes recomendaciones dirigidas al Banco de Venezuela, S.A. Banco Universal, con el fin de optimizar la seguridad, inclusividad y eficiencia de sus plataformas de pago:

Se recomienda la implementación inmediata del sistema de Reconocimiento Facial como una alternativa robusta o reemplazo progresivo del sistema BioPago. Esta acción es prioritaria para eliminar las barreras de accesibilidad detectadas que afectan a los adultos mayores y trabajadores manuales, garantizando que el deterioro dactilar no sea un impedimento para el ejercicio de la actividad financiera y asegurando la inclusión del 100% de los usuarios.

Asimismo, es imperativo establecer la Detección de Vida (Liveness Detection) como un requisito de diseño de seguridad crítica en el flujo de autenticación. Se sugiere la incorporación de algoritmos activos y pasivos que mitiguen ataques de suplantación (spoofing), asegurando que el sistema sea capaz de distinguir entre un rostro real y reproducciones digitales o impresas, blindando así la integridad de cada transacción.

Para el proceso de alta en el servicio, se recomienda diseñar el flujo de vinculación de cuenta inicial con un Segundo Factor de Autenticación (2FA) de carácter obligatorio. Esta medida debe complementar la validación biométrica inicial, creando un esquema de seguridad multicapa que garantice que la identidad del cliente esté debidamente verificada antes de permitir operaciones financieras de alto valor.

Desde el punto de vista técnico, se sugiere asegurar la adquisición o licenciamiento de kits de desarrollo (SDKs) y herramientas de Inteligencia Artificial especializadas. El uso de software de alto nivel profesional es fundamental para construir una funcionalidad de identificación precisa y robusta, minimizando las

tasas de falso rechazo y falsa aceptación, y garantizando la escalabilidad del sistema ante la alta concurrencia de la banca nacional.

En términos de rendimiento, se propone fijar una latencia máxima de 3 segundos como un Indicador Clave de Rendimiento (KPI) obligatorio para la ejecución y confirmación de transacciones. Esta meta de optimización debe abarcar desde la captura de la imagen hasta la respuesta final del core bancario, asegurando que la experiencia de usuario sea ágil y competitiva frente a los métodos de pago tradicionales.

Igualmente, se recomienda la implementación de un Módulo de Seguridad de Hardware (HSM) o un Key Vault dedicado. Esta infraestructura es esencial para la gestión, almacenamiento y protección de las claves criptográficas, facilitando procesos como el salting de hashes biométricos y el cifrado de extremo a extremo de las comunicaciones, protegiendo así la privacidad de los datos sensibles de los clientes.

Finalmente, las recomendaciones apuntan a consolidar un sistema de pagos que no solo sea tecnológicamente avanzado, sino también profundamente inclusivo y seguro. La adopción de estos estándares permitirá al Banco de Venezuela posicionarse a la vanguardia de la banca digital, ofreciendo una solución que responda de manera coherente a las necesidades reales y expectativas de su amplia base de usuarios.

CAPÍTULO VI

LA PROPUESTA

Denominación y Diagnóstico del Proyecto

El proyecto propuesto lleva por título: “Diseño de un Sistema de Pagos mediante Vinculación de Cuenta a través de Reconocimiento Facial para el Banco de Venezuela, S.A. Banco Universal.”

La arquitectura de pagos actual en la banca nacional, y específicamente en el Banco de Venezuela, enfrenta un punto de inflexión donde la obsolescencia de ciertos métodos biométricos y la vulnerabilidad de las nuevas tecnologías de proximidad exigen una transformación profunda. Los datos recopilados en esta investigación revelan una realidad crítica: el sistema BioPago, basado en la huella dactilar, se ha convertido en un mecanismo de exclusión para el 86,67% de los adultos mayores y trabajadores manuales consultados, debido a que el deterioro de sus tejidos dactilares impide una autenticación efectiva.

Este escenario se agrava al analizar la percepción de seguridad sobre el sistema Contactless. El 80% de los sujetos de estudio identifica riesgos latentes de clonación y lectura no autorizada en tarjetas de proximidad, lo que evidencia que la modernización del banco no ha venido acompañada de una sensación de resguardo para el cliente. En consecuencia, el diagnóstico arroja una necesidad urgente de implementar una tecnología que sea, al mismo tiempo, inclusiva (que no dependa de la integridad física de la piel) y altamente segura (que no sea fácil de suplantar como un plástico de proximidad).

La solución técnica planteada en esta propuesta se fundamenta en el Reconocimiento Facial, configurado no solo como un método de identificación, sino como un ecosistema de seguridad integral. Los requerimientos técnicos derivados del estudio exigen que este flujo incorpore obligatoriamente mecanismos de detección de vida (Liveness Detection) y un segundo factor de autenticación (2FA) durante la fase de enrolamiento, mitigando así el riesgo de ataques de suplantación (spoofing) que el

60% de la muestra considera una amenaza crítica.

En cuanto a la operatividad, el diagnóstico establece que la viabilidad de esta propuesta está condicionada por la eficiencia extrema: los usuarios demandan tiempos de latencia inferiores a los 3 segundos para que la experiencia de pago sea competitiva. Esto obliga a que el diseño considere el uso de SDKs de inteligencia artificial especializados y arquitecturas de seguridad que incluyan módulos de cifrado dedicados (HSM o Key Vault), protegiendo la privacidad de la información biométrica mediante técnicas de salting y cifrado de comunicaciones.

El proyecto, bajo la modalidad de proyecto factible con diseño de campo, tiene como finalidad presentar un modelo funcional que demuestre la viabilidad de la biometría facial como sustituto o complemento de los métodos actuales. Su desarrollo se apoya en una arquitectura de Backend seguro que prioriza la protección de los datos biométricos (mediante salting de hashes y cifrado) y la optimización de los tiempos de respuesta, respondiendo así a las exigencias técnicas y operativas identificadas durante la fase de recolección de datos.

En síntesis, el diagnóstico del proyecto refleja una infraestructura de pagos que, si bien es funcional, requiere una evolución tecnológica urgente para superar las limitaciones físicas del BioPago y los riesgos de seguridad del Contactless. La creación de un sistema de reconocimiento facial modular y altamente seguro representa una oportunidad estratégica para el Banco de Venezuela, orientada a fortalecer la inclusión financiera, modernizar sus protocolos de autenticación y consolidar la confianza de sus usuarios en el ecosistema digital.

Naturaleza del Proyecto

Fundamentación o Justificación

La presente propuesta se fundamenta en la transformación necesaria de los protocolos de autenticación del Banco de Venezuela, S.A., con el objetivo de transitar hacia un ecosistema de pagos que armonice la seguridad extrema con la accesibilidad universal. El diseño de este sistema de vinculación de cuenta mediante reconocimiento facial no surge como una simple actualización tecnológica, sino como una respuesta estructural a las brechas de exclusión y vulnerabilidad detectadas en los métodos de pago vigentes.

El diagnóstico situacional reveló una realidad ineludible: la biometría dactilar (BioPago) y la tecnología de proximidad (Contactless) han alcanzado su límite de eficacia operativa. Mientras que el primero excluye a casi el 87% de los adultos mayores y trabajadores manuales por el desgaste físico de sus huellas, el segundo genera una percepción de inseguridad en el 80% de los usuarios debido a la facilidad de clonación. Esta dualidad —exclusión física y riesgo digital— justifica plenamente la creación de una alternativa biométrica que no dependa del contacto táctil y que blinde la identidad del cliente bajo estándares de inteligencia artificial.

Bajo este escenario, la propuesta se justifica desde cuatro dimensiones fundamentales:

1. Justificación Social e Inclusiva: El proyecto posee un alto impacto humano al devolver la autonomía financiera a sectores vulnerables. Al implementar el reconocimiento facial, se elimina la barrera del deterioro dactilar, garantizando que el acceso a los fondos y la ejecución de pagos sean derechos ejercidos sin discriminación por condiciones físicas o de edad, logrando una verdadera democratización de la banca digital.

2. Justificación Técnica y de Seguridad: La arquitectura propuesta integra capas de protección que superan los mecanismos actuales. La inclusión obligatoria de detección de vida (Liveness Detection) y un segundo factor de autenticación (2FA) responde a la necesidad de mitigar ataques de suplantación (spoofing). Asimismo, la gestión de claves mediante módulos HSM o Key Vault asegura que la información biométrica sea tratada bajo esquemas de cifrado de nivel bancario, transformando el rostro del usuario en una llave digital única e irreproducible.

3. Justificación Operativa y de Rendimiento: La propuesta se valida mediante la optimización de la experiencia de usuario. Al establecer un KPI de latencia máxima de 3 segundos, el proyecto garantiza que la seguridad no penalice la agilidad. El uso de SDKs especializados asegura que el Banco de Venezuela mantenga su competitividad frente a otras fintechs, ofreciendo transacciones que son, simultáneamente, más rápidas que el ingreso de una clave y más seguras que el uso de una tarjeta física.

4. Justificación Académica y Metodológica: El estudio se inscribe en la modalidad de Proyecto Factible, aportando una solución técnica documentada a un problema real de la ingeniería informática. Metodológicamente, se rige por el Modelo en Cascada, lo que permite un desarrollo sistemático y trazable, asegurando que desde el levantamiento de requerimientos hasta el diseño del Backend seguro, exista una coherencia lógica que respalde la viabilidad del sistema.

En definitiva, este proyecto busca demostrar que es posible elevar los estándares de seguridad bancaria sin sacrificar la inclusión. La implementación de la biometría facial representa el siguiente paso evolutivo para el Banco de Venezuela, permitiéndole consolidar una infraestructura de pagos resiliente, capaz de proteger los activos de sus clientes y, al mismo tiempo, adaptarse a las realidades físicas de toda su población de usuarios.

Objetivos de la Propuesta

Objetivo General

Desarrollar un Sistema de Pagos mediante Vinculación de Cuenta a través de Reconocimiento Facial para el Banco de Venezuela, S.A. Banco Universal.

Objetivos Específicos

- Diseñar la arquitectura lógica y funcional detallando la interacción entre los módulos del sistema de pagos mediante vinculación de cuenta a través de reconocimiento facial para el Banco de Venezuela, S.A. Banco Universal.
- Determinar la factibilidad técnica y operativa de la integración del sistema de reconocimiento facial con la infraestructura tecnológica y las plataformas de pago existentes del Banco de Venezuela, S.A. Banco Universal.
- Establecer los protocolos de seguridad y privacidad requeridos para la captura, cifrado, almacenamiento y gestión de los datos biométricos, garantizando el cumplimiento de las normativas de protección de datos financieros del Banco de Venezuela, S.A. Banco Universal.

Metas

- Alcanzar una tasa de precision del 99,99%: Asegurar que el sistema identifique correctamente a los usuarios en diversas condiciones, minimizando los errores de autenticación.
- Reducir el tiempo de Transacción a menos de 3 segundos: Optimizar el proceso completo para ofrecer la maxima velocidad y conveniencia.
- Alcanzar la Adopción Total de los Usuarios Registrados: Promover la migración de los usuarios activos hacia este nuevo método de pago.

Beneficiarios

La implementación de este sistema de pagos mediante reconocimiento facial está diseñada para generar un impacto positivo en distintos niveles del ecosistema financiero del Banco de Venezuela. Los beneficiarios se categorizan de la siguiente manera:

Beneficiarios Directos:

La propuesta está dirigida primordialmente a los usuarios y clientes del Banco de Venezuela, S.A. Banco Universal, con especial énfasis en las personas mayores y trabajadores manuales, quienes actualmente enfrentan las mayores limitaciones técnicas. Estos beneficiarios obtendrán:

- Inclusión Financiera Total: Al eliminar la dependencia de la huella dactilar, se garantiza que el deterioro físico de los tejidos no sea un impedimento para autenticar pagos, devolviendo la autonomía en sus transacciones diarias.
- Seguridad Avanzada: Acceso a un método de pago blindado con detección de vida y segundo factor de autenticación, reduciendo drásticamente el riesgo de suplantación de identidad.
- Optimización del Tiempo: Una experiencia de pago ágil con tiempos de respuesta inferiores a los 3 segundos, eliminando las frustraciones causadas por múltiples intentos fallidos en los lectores dactilares actuales.

Beneficiarios Indirectos:

- La Comunidad General de Usuarios del Banco: Todos los clientes de la institución se verán beneficiados por la modernización de la infraestructura de pagos, contando con una alternativa de autenticación más higiénica (sin contacto) y tecnológicamente superior a las tarjetas de proximidad tradicionales.

- El Banco de Venezuela, S.A.: La institución se beneficia al fortalecer su imagen como líder en innovación tecnológica y compromiso social, reduciendo los reclamos por fallas de accesibilidad y minimizando las pérdidas económicas asociadas a fraudes por clonación de tarjetas.
- El Sector Bancario Nacional: La propuesta sirve como un estándar de referencia para la adopción de biometría facial en Venezuela, promoviendo el desarrollo de soluciones informáticas seguras, escalables y adaptadas a la realidad física de la población venezolana.

Localización

El proyecto se centra operativamente en la sede principal del Banco de Venezuela, S.A. Banco Universal, específicamente en la Torre Banco de Venezuela ubicada en la Avenida Universidad, Esquina de Sociedad, en la ciudad de Caracas, Distrito Capital.

Esta ubicación estratégica representa el centro neurálgico de las operaciones tecnológicas y financieras del país, donde se gestiona el core bancario y las plataformas de pago a nivel nacional. Si bien el desarrollo de la investigación se circunscriben a este entorno corporativo y sus laboratorios de innovación, el alcance del sistema de reconocimiento facial es de carácter nacional, proyectando su implementación en todos los puntos de venta y dispositivos biopago distribuidos en el territorio venezolano, con el fin de servir a la extensa red de usuarios de la institución.

Plan Operativo de Actividades

El Plan Operativo de Actividades representa el eje estratégico y cronológico sobre el cual se articula el desarrollo de la propuesta. Su función es traducir los objetivos de la investigación en una secuencia lógica de hitos técnicos, asegurando que la transición desde la biometría dactilar hacia el reconocimiento facial se realice bajo una estructura rigurosa y verificable.

De acuerdo con los lineamientos del Manual de la Universidad Alejandro de Humboldt (2016), esta planificación no solo organiza el tiempo, sino que garantiza la coherencia metodológica necesaria para que un proyecto factible tenga viabilidad técnica. En este sentido, la ejecución de la propuesta se rige por el Modelo de Desarrollo en Cascada, una elección deliberada para este sistema de pagos, ya que en el ámbito de la seguridad bancaria es imperativo completar y validar cada fase (especialmente la de requisitos y diseño de seguridad) antes de proceder a la codificación.

A continuación, se presenta el cuadro resumen con la programación de actividades, su duración y el período correspondiente:

Cuadro 8. Plan Operativo de Actividades.

ID	Tarea/Actividad	Duración (Semanas)	Mes
Fase I: Diagnostico e Investigación 1	Análisis del sistema de pagos actual del Banco de Venezuela	2	Julio
1.1	Diagnóstico de limitaciones y riesgos de seguridad (informe)	2	
1.2	Investigación y descripción del funcionamiento del S.P. con reconocimiento facial	3	Agosto
1.3	Establecimiento de los componentes requeridos (lista preliminar)	2	Agosto / Septiembre
Fase II: Desarrollo de la Propuesta 2	Diseño de la arquitectura lógica y funcional	3	Septiembre
2.1	Determinación de la factibilidad técnica y operativa (informe)	2	Octubre
2.2	Definición de requisitos de hardware y software (costo/especificaciones)	2	
2.3	Establecimiento de protocolos de seguridad y privacidad	2	Noviembre
2.4	Elaboración y revisión final de la propuesta técnica	2	

Fuente: Terán, G. (2025)

Estudio de Factibilidad o Viabilidad del Proyecto

Antes de proceder con el diseño técnico de una solución de autenticación biométrica, es fundamental realizar un análisis que determine la posibilidad real de ejecución de la propuesta. Este estudio permite evaluar si la institución cuenta con la infraestructura y las condiciones necesarias para que el sistema de reconocimiento facial sea exitoso. Al respecto, Arias (2012) señala que un proyecto de investigación debe evaluarse en función de su ejecución, considerando que:

"La factibilidad de la investigación se refiere a la disponibilidad de los recursos financieros, humanos y materiales que determinarán, en última instancia, el alcance del proyecto" (p. 42).

Bajo esta premisa, la propuesta para el Banco de Venezuela, S.A. se sustenta en una evaluación de sus capacidades tecnológicas y operativas, asegurando que el diseño del sistema de vinculación de cuenta no solo sea una respuesta teórica, sino una herramienta viable que resuelva las limitaciones de accesibilidad y seguridad detectadas en el diagnóstico.

Factibilidad Técnica

Desde la perspectiva técnica, el proyecto evalúa la disponibilidad de herramientas informáticas y talento especializado para construir la solución. Según Tamayo y Tamayo (2003), la administración de un proyecto exige considerar la tecnología como un recurso base para la transformación de procesos. En este caso, la factibilidad técnica se considera alta, ya que el desarrollo del sistema de reconocimiento facial se apoya en el uso de Kits de Desarrollo de Software (SDKs) de inteligencia artificial que ya son un estándar en la industria financiera global.

La infraestructura del Banco de Venezuela permite la integración de arquitecturas basadas en microservicios, lo que garantiza que el sistema pueda escalar y soportar la concurrencia masiva de pagos. Asimismo, el uso de Módulos de Seguridad de Hardware (HSM) para el cifrado de datos biométricos y la aplicación de protocolos de detección de vida (liveness detection) son soluciones técnicamente probadas que aseguran la robustez del sistema, permitiendo alcanzar la meta de latencia inferior a los 3 segundos requerida por los usuarios.

Cuadro 9. Requerimientos Técnicos

Tipo	Modelo	Cantidad	Hardware
Laptop	Dell Latitude 5540	2	SSD: 512GB, Memoria RAM: 16GB, Procesador: Intel Core i5 13va generación
Dispositivo de Prueba (Teléfono Inteligente)	1: Samsung Galaxy A56 5G. 2: iPhone 14 Pro	2	1: Almacenamiento: 256GB, Memoria RAM: 8GB, Procesador: Exynos 1580. 2: Almacenamiento: 256GB, Memoria RAM: 8GB, Procesador: Apple A16 Bionic

Fuente: Terán, G. (2025)

Factibilidad Operativa

La viabilidad operativa determina si el sistema será aceptado y utilizado eficazmente por el público objetivo. Los resultados de esta investigación confirman una necesidad crítica: el 86,67% de los adultos mayores y trabajadores manuales presentan dificultades con el BioPago dactilar, lo que convierte al reconocimiento facial en una solución operativa indispensable para garantizar la inclusión financiera.

El sistema es operativamente factible porque simplifica el proceso de pago al eliminar el contacto físico y la dependencia de la integridad de la huella dactilar. Además, la incorporación de un Segundo Factor de Autenticación (2FA) en el registro inicial satisface las expectativas del 60% de la muestra, quienes demandan mayor seguridad en la vinculación de sus cuentas. Esta alineación entre las capacidades del sistema y las necesidades del usuario asegura una transición fluida y una alta tasa de adopción en los puntos de venta.

Cuadro 10. Requerimientos de Recursos Humanos

Recursos Humanos	Descripción	Cantidad
Backend Developer	El desarrollador Backend es el arquitecto de la lógica del servidor y el guardián de la integridad de los datos. Su enfoque principal será construir la infraestructura robusta necesaria para procesar transacciones financieras y gestionar los vectores biométricos.	1
Frontend Developer Mobile	El desarrollador Frontend Mobile es el responsable de la experiencia de usuario (UX) y la interfaz (UI). Se encarga de transformar la complejidad técnica en una herramienta intuitiva que el comerciante y el cliente puedan usar en segundos.	1

Fuente: Terán, G. (2025)

Factibilidad Económica

Finalmente, la factibilidad económica evalúa la relación costo-beneficio de la propuesta. Aunque el desarrollo inicial implica costos en licenciamiento de software biométrico y actualización de servidores, Arias (2012) destaca la importancia de optimizar los recursos para lograr los objetivos institucionales. En este sentido, el proyecto es rentable para el Banco al actuar como una medida preventiva contra el fraude.

Considerando que el 80% de los usuarios percibe riesgos de clonación en las tarjetas Contactless, la implementación del reconocimiento facial reduce significativamente los costos asociados a reembolsos por fraudes y reclamaciones de transacciones no autorizadas. A mediano plazo, la institución ahorra en el mantenimiento físico de dispositivos dactilares y en la reposición de plásticos, consolidando una plataforma digital segura que fortalece la confianza del cliente y la estabilidad financiera del banco.

Cuadro 11. Costo de los Requerimientos de Hardware.

Tipo	Modelo	Cantidad	Hardware	Costo ($)	Costo Total ($)
Laptop	Dell Latitude 5540	2	SSD: 512GB, Memoria RAM: 16GB, Procesador: Intel Core i5 13va generación	600$ c/u	1.200$
Dispositivo de Prueba (Teléfono Inteligente)	1: Samsung Galaxy A56 5G. 2: iPhone 14 Pro	2	1: Almacenamiento: 256GB, Memoria RAM: 8GB, Procesador: Exynos 1580. 2: Almacenamiento: 256GB, Memoria RAM: 8GB, Procesador: Apple A16 Bionic	1: 370$ 2: 430$	800$

Fuente: Terán, G. (2025)

Cuadro 12. Costo de los Recursos Humanos.

Recursos Humanos	Descripción	Cantidad	Costo ($)
Backend Developer	El desarrollador Backend es el arquitecto de la lógica del servidor y el guardián de la integridad de los datos. Su enfoque principal será construir la infraestructura robusta necesaria para procesar transacciones financieras y gestionar los vectores biométricos.	1	750$
Frontend Developer Mobile	El desarrollador Frontend Mobile es el responsable de la experiencia de usuario (UX) y la interfaz (UI). Se encarga de transformar la complejidad técnica en una herramienta intuitiva que el comerciante y el cliente puedan usar en segundos.	1	750$

Fuente: Terán, G. (2025)

Cuadro 13. Costo-Beneficio de los Requerimientos Técnicos.

Hardware	Modelo/ Descripción	Cantidad	Costo Unitario ($)	Costo Total ($)	Beneficio Asociado
Laptop	Dell Latitude 5540 - SSD: 512GB, Memoria RAM: 16GB, Procesador: Intel Core i5 13va generación	2	600$ c/u	1.200$	Infraestructura central de cómputo de alto rendimiento para el desarrollo de la arquitectura de microservicios y la gestión del backend bancario seguro.
Dispositivo de Prueba (Teléfono Inteligente)	1: Samsung Galaxy A56 5G - Almacenamiento: 256GB, Memoria RAM: 8GB, Procesador: Exynos 1580. 2: iPhone 14 Pro - Almacenamiento: 256GB, Memoria RAM: 8GB, Procesador: Apple A16 Bionic	2	1: 370$ 2: 430$	800$	Entorno de validación móvil multiplataforma para certificar la precisión del reconocimiento facial, los protocolos de seguridad de vida y la eficiencia operativa en condiciones reales de uso bancario.
Costo Total Hardware ()				2.000$	

Fuente: Terán, G. (2025)

Metodología del Desarrollo del Sistema

La construcción de una solución tecnológica para el sector financiero no puede ser un proceso azaroso; requiere de un itinerario lógico que garantice la integridad de los datos y la seguridad transaccional. En este sentido, la metodología se define como el conjunto de procedimientos ordenados que permiten transformar los requisitos detectados en el diagnóstico en un modelo operativo funcional. Al respecto, Tamayo y Tamayo (2003) sostiene que:

> "La metodología es un cuerpo de conocimientos que describe y analiza los métodos, indicando sus limitaciones y recursos, sus alcances y su validez, de suerte que la metodología es el estudio analítico y crítico de los métodos de investigación" (p. 28).

Bajo esta perspectiva, la propuesta para el Banco de Venezuela, S.A. adopta el Modelo de Desarrollo en Cascada (Waterfall). Esta elección es estratégica: en el desarrollo de software crítico, cada etapa debe ser validada y documentada antes de avanzar a la siguiente para evitar errores en la arquitectura de seguridad. Esta secuencialidad asegura que los protocolos de cifrado y la lógica de negocio sean robustos desde su concepción, permitiendo cumplir con las fases que se describen a continuación:

- Fase 1: Análisis y Definición de Requisitos Técnicos. En esta etapa se traducen las carencias del sistema BioPago actual (donde el 86,67% de los usuarios con deterioro dactilar se ven excluidos) en especificaciones técnicas. Se determinan los requerimientos no funcionales críticos: un tiempo de latencia máximo de 3 segundos y la obligatoriedad de un Segundo Factor de Autenticación (2FA). Siguiendo lo planteado por Arias (2012) sobre la factibilidad, aquí se delimitan las herramientas de desarrollo y los lenguajes de programación que permitirán la conexión con el core bancario.

- Fase 2: Diseño de la Arquitectura Lógica y Seguridad. Se procede a modelar la solución bajo una arquitectura de microservicios, garantizando la escalabilidad necesaria para la alta concurrencia de pagos. En esta fase se diseñan los algoritmos de Detección de Vida (Liveness Detection) activos, fundamentales para mitigar ataques de suplantación (spoofing). Se establece además el flujo de cifrado para el resguardo de las plantillas biométricas faciales mediante el uso de módulos de seguridad dedicados (HSM).
- Fase 3: Desarrollo del Prototipo y Configuración de SDKs. Consiste en la codificación y ensamblaje de los componentes. Se integran los SDKs de Inteligencia Artificial especializados en biometría facial, configurando los parámetros de reconocimiento para que operen eficientemente en diversos dispositivos (Android e iOS). Es el momento donde la propuesta técnica cobra forma tangible, permitiendo visualizar la interfaz de vinculación de cuenta y la respuesta del sistema ante la captura de la imagen.
- Fase 4: Verificación, Validación y Auditoría. En la etapa final se somete al prototipo a un entorno de pruebas controladas para certificar su eficiencia. Se audita que la latencia se mantenga bajo el estándar de 3 segundos y que la precisión del reconocimiento facial sea infalible ante intentos de fraude. Esta fase cierra el ciclo de desarrollo asegurando que el sistema sea apto para una posible implementación real, garantizando la confianza y agilidad que el Banco de Venezuela requiere.

Sistema de Seguridad

La arquitectura de seguridad del sistema se ha diseñado bajo el principio de "Defensa en Profundidad", estableciendo múltiples capas de protección que garantizan la integridad de las transacciones y la inviolabilidad de los datos biométricos de los clientes del Banco de Venezuela. Dado que la propuesta maneja información sensible, el esquema de seguridad trasciende la simple autenticación, integrando hardware especializado y algoritmos de inteligencia artificial.

1. Autenticación y Autorización mediante JSON Web Tokens (JWT) Para garantizar la comunicación segura entre el aplicativo móvil y el backend de microservicios, se implementa el estándar JWT (JSON Web Token). Este mecanismo permite gestionar sesiones sin estado (stateless), donde cada petición del usuario porta un token cifrado que contiene su identidad y niveles de privilegio. Al ser un sistema bancario, estos tokens poseen tiempos de expiración cortos y firmas criptográficas que aseguran que la información no ha sido manipulada en tránsito, permitiendo una validación ágil que contribuye a mantener la latencia por debajo de los 3 segundos.

2. Segundo Factor de Autenticación (2FA) y Vinculación Segura En cumplimiento con los requerimientos detectados en el diagnóstico (donde el 60% de los expertos considera indispensable reforzar la validación inicial), el sistema exige obligatoriamente un Segundo Factor de Autenticación (2FA) durante el proceso de vinculación de cuenta. Este factor actúa como una llave de seguridad adicional (vía SMS o correo electrónico) que, sumada a la biometría facial, asegura que solo el titular legítimo pueda enrolar su rostro en la plataforma, mitigando riesgos de suplantación desde el primer contacto.

3. Motor de Biometría con Detección de Vida (Liveness Detection) El núcleo de la seguridad facial incorpora mecanismos de Detección de Vida Activa. Esta tecnología es crítica para diferenciar un rostro humano real de intentos de fraude mediante fotografías, videos de alta resolución o máscaras (ataques de spoofing). El sistema solicita al usuario realizar acciones aleatorias durante la captura, garantizando que el proceso de pago se realice con la presencia física del titular, elevando así los estándares de seguridad por encima de las tecnologías Contactless tradicionales.

4. Protección Criptográfica y Gestión de Claves (HSM/Key Vault) Para el resguardo de las plantillas biométricas y las llaves de cifrado, la propuesta contempla la integración de un Módulo de Seguridad de Hardware (HSM) o un Key Vault dedicado. Este componente garantiza que las claves criptográficas nunca residan en texto plano dentro de los servidores. Siguiendo las mejores prácticas de ingeniería financiera, los datos del rostro se transforman en hashes matemáticos irreversibles, asegurando que, incluso ante un acceso no autorizado a la base de datos, la información biométrica sea técnica y lógicamente inaccesible para terceros.

5. Mitigación de Ataques de Sesión y CSRF Finalmente, el sistema incorpora protecciones contra Cross-Site Request Forgery (CSRF) y otros vectores de ataque web. Al validar que cada acción iniciada en el sistema provenga de una fuente confiable y verificada, se protege al usuario de ejecuciones involuntarias de transacciones. Esta capa de seguridad es vital en la arquitectura de microservicios para mantener la persistencia de la confianza en cada punto de acceso del ecosistema bancario.

Definición de Usuarios

La identificación de los sujetos que interactúan con la plataforma es un paso crítico para garantizar que el diseño de las interfaces y los niveles de acceso respondan a necesidades reales. Según Arias (2012), en todo proyecto de investigación es imperativo definir claramente las unidades de estudio o sujetos, ya que esto determina el alcance operativo de la solución propuesta.

En el contexto del sistema de pagos por reconocimiento facial para el Banco de Venezuela, S.A., se han identificado tres perfiles de usuarios diferenciados, cada uno con roles y privilegios específicos dentro del ecosistema transaccional:

1. Usuario Cliente (Titular de Cuenta) Es el usuario final y el eje central de la propuesta. Este perfil corresponde a los clientes naturales de la institución, con especial énfasis en aquellos que, según el diagnóstico, presentan dificultades con el BioPago dactilar (86,67% de la muestra crítica).

Acciones: Realiza la vinculación de su cuenta mediante el registro biométrico facial, gestiona su perfil de seguridad a través del Segundo Factor de Autenticación (2FA) y autoriza pagos en puntos de venta utilizando su rostro como identificador único.

Privilegios: Acceso exclusivo a sus datos personales y consulta de su historial de transacciones vinculadas a la biometría facial.

2. Usuario Administrador (Personal del Banco) Representa al equipo técnico y de seguridad de la institución bancaria encargado de la gestión de la plataforma en el Backend.

Acciones: Supervisa el rendimiento de los microservicios, monitorea los tiempos de latencia (asegurando el cumplimiento del estándar de 3 segundos) y gestiona las alertas de seguridad emitidas por los módulos de cifrado (HSM).

Privilegios: Acceso total a los registros de auditoría del sistema, gestión de parámetros del algoritmo de reconocimiento facial y administración de permisos de red. No tiene acceso a las imágenes directas de los usuarios, sino a los hashes matemáticos resguardados.

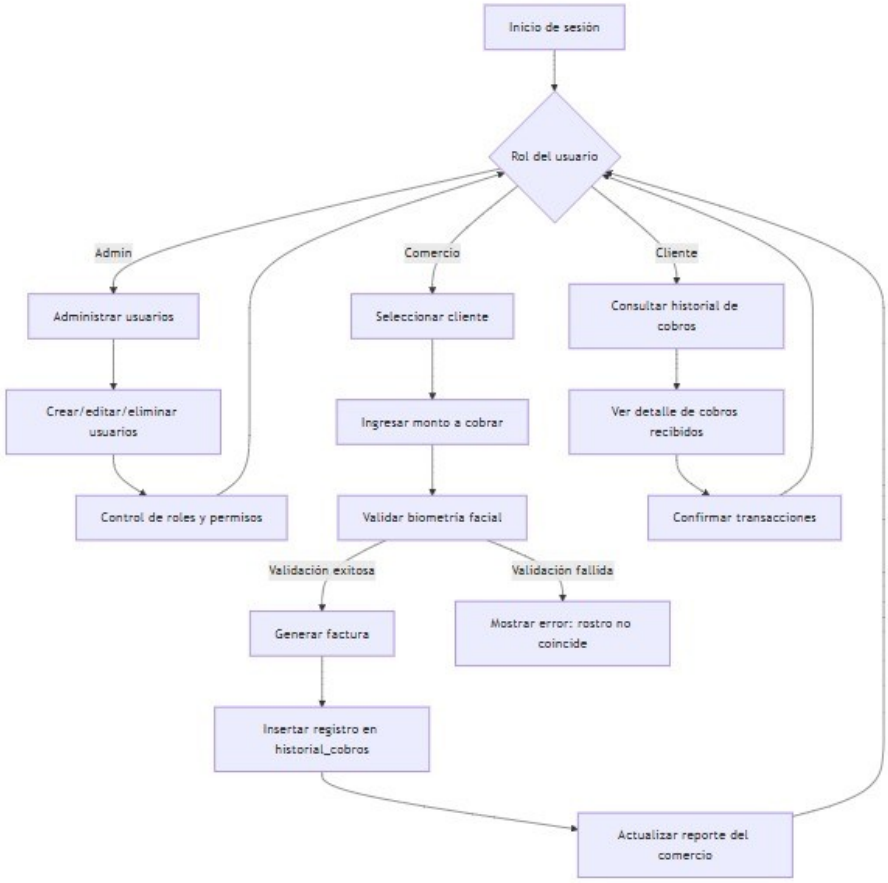
3. Usuario Comercio (Agente de Venta) Es el intermediario operativo que facilita la transacción en el punto de contacto físico.

Acciones: Inicia la solicitud de cobro en el terminal de venta, selecciona la opción de pago facial y recibe la confirmación de éxito o rechazo de la transacción en tiempo real.

Privilegios: Limitado estrictamente a la ejecución de cobros y visualización del estatus de la transacción. No posee acceso a información sensible del cliente ni a la configuración del sistema biométrico.

Diagrama de Flujo

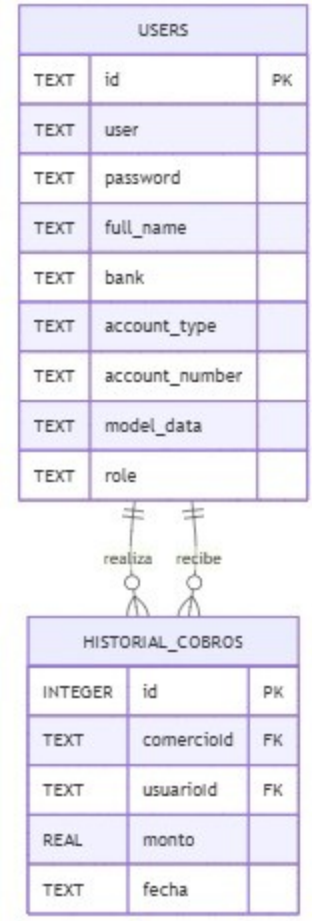
Figura N.º 1



Fuente: Terán, G. (2025)

Modelo Relacional: Modelo Lógico, Tablas, Campos, Tipos de Datos, PF, FK, Clases Primarias y Foráneas

Figura N.º 2

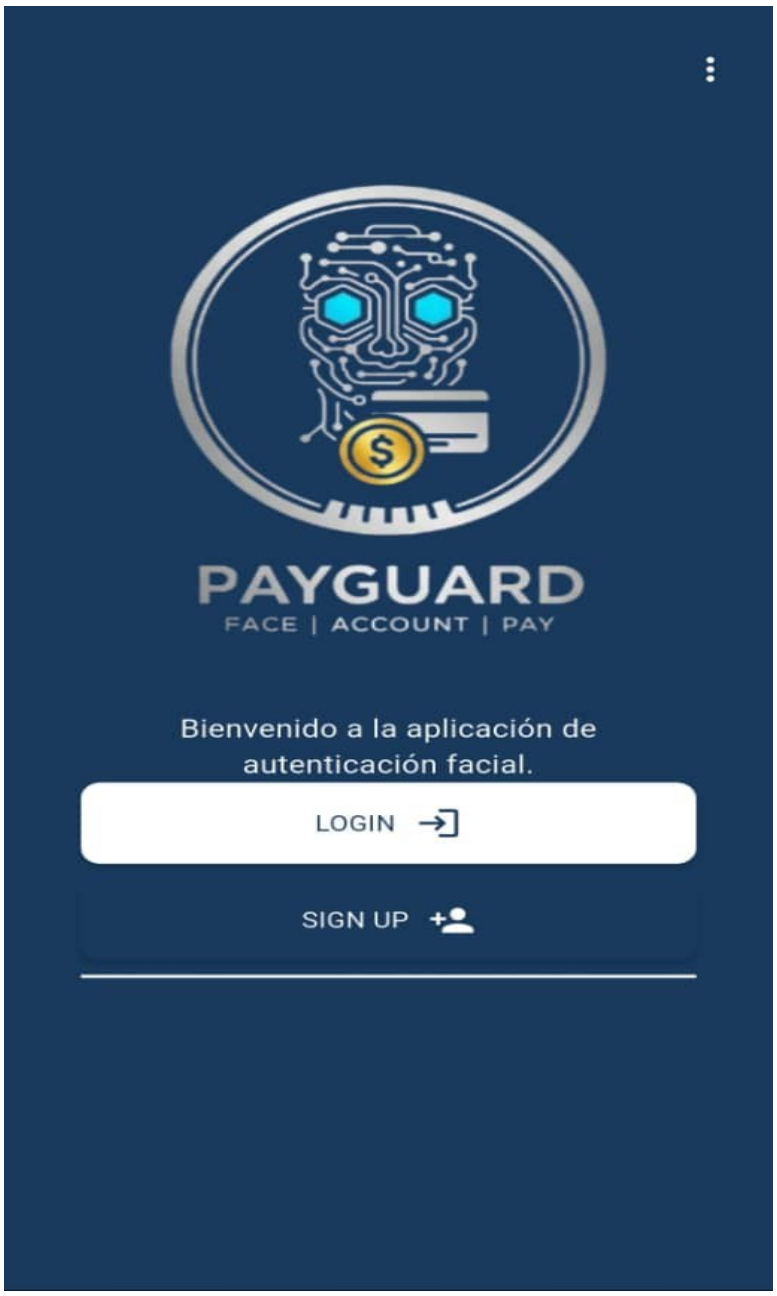


Fuente: Terán, G. (2025)

Pantallas del Sistema de Pagos

Figura N.º 3

Interfaz Principal



Fuente: Terán, G. (2025)

Análisis: La interfaz principal constituye el núcleo de gestión de identidad del cliente dentro del ecosistema del Banco de Venezuela. Su diseño no solo busca la modernización visual, sino que representa la solución directa a la exclusión detectada en el diagnóstico inicial.

Figura N.º 4

Interfaz de Registro

Fuente: Terán, G. (2025)

Análisis: La interfaz del sistema constituye el ecosistema visual donde la inclusión social y la seguridad bancaria convergen, funcionando como un puente intuitivo que transforma la identidad física del cliente en una firma digital blindada. Representa la solución definitiva a la exclusión del BioPago dactilar, devolviendo al usuario la autonomía y confianza sobre su cuenta mediante un diseño de baja carga cognitiva y alta eficiencia.

Figura N.º 5

Interfaz de Usuario

Fuente: Terán, G. (2025)

Análisis: La interfaz del Usuario constituye el punto de gestión de identidad digital, diseñada bajo un enfoque de baja carga cognitiva para garantizar la inclusión del 86,67% de los usuarios con dificultades dactilares. Representa la autonomía y el control del titular sobre sus activos, funcionando como un tablero centralizado donde el usuario activa su vinculación de cuenta mediante 2FA, supervisa su estatus biométrico y autoriza pagos.

Figura N.º 6

Interfaz de Comercio

Fuente: Terán, G. (2025)

Análisis: La interfaz comercial constituye la herramienta operativa de cobro diseñada para optimizar el flujo de ventas en el punto de contacto físico. Representa la eficiencia y la seguridad del negocio, funcionando como el terminal digital donde el comerciante gestiona las solicitudes de pago, valida la identidad facial del comprador y recibe confirmaciones financieras inmediatas. Su funcionamiento es simplificado para evitar errores humanos: el comercio ingresa el monto, selecciona el método de pago facial y activa la cámara del terminal para que los microservicios del banco procesen la biometría.

Figura N.º 7

Interfaz de Administrador

Fuente: Terán, G. (2025)

Análisis: La interfaz de administración constituye el centro de monitoreo y gobernanza técnica de la plataforma, diseñada para ofrecer una visión global del estado del sistema. Representa la integridad y la supervisión del servicio, funcionando como el panel de control donde el personal del banco audita la operatividad de los microservicios y asegura la continuidad del sistema de pagos.

REFERENCIAS

Aerospike. (2023). ***What is a database management system?*** [Articulo en linea]. Disponible en: https://aerospike.com/glossary/database-management-system/ [Consultado en:]

Akeyless. (2021). ***What Is Vault?*** [Articulo en linea]. Disponible en: https://www.akeyless.io/secrets-management-glossary/what-is-vault/ [Consultado en:]

Arias, F. (2012). El proyecto de investigación: ***Introducción a la metodología científica.*** [Libro en línea] Disponible: https://t.me/c/1708242346/4 [Consultado: 2025, Marzo 03]

AWS. (2026). ***¿Qué es el reconocimiento facial?*** [Articulo en linea]. Disponible en: https://aws.amazon.com/es/what-is/facial-recognition/ [Consultado en:]

Banco Central de la República Argentina. ***Sistema de Pagos.*** [Blog en línea]. Disponible en: https://www.bcra.gob.ar/SistemasFinancierosYdePagos/Sistemas_de_Pago.asp#:~:text=seguridad%20y%20eficiencia.-,Medios%20de%20Pago%20Electr%C3%B3nicos,en%20l%C3%ADnea)%20por%20el%20canal [Consultado: 2025, Marzo 02]

BBVA. (2020). ***'Pagar por la cara' gracias a la estrategia de 'pagos invisibles' de BBVA*** [Articulo en linea]. Disponible en: https://www.bbva.com/es/bbva-pone-marcha-estrategia-pagos-invisibles/ [Consultado en:]

Buehler, T. (2024). ***The Risks of Contactless Payment Are High Despite Security*** [Blog en linea]. Disponible en: https://www.amu.apus.edu/area-of-study/business-administration-and-management/resources/the-risks-of-contactless-payment-are-high-despite-security/ [Consultado en:]

Campillo, R. (2024). ***Aplicación de tecnologías biométricas en la industria financiera*** [Blog en linea]. Disponible en: https://www.mobbeel.com/blog/aplicacion-tecnologias-biometricas-industria-financiera/ [Consultado en:]

Castillo, R. y Mora, M. (2015). ***DESARROLLO DE UN SISTEMA TRANSACCIONAL QUE PERMITE REALIZAR PAGOS ELECTRONICOS IMPLEMENTANDO NFC.*** [Trabajo de grado en línea]. Disponible en: http://biblioteca2.ucab.edu.ve/anexos/biblioteca/marc/texto/AAT2032.pdf [Consultado: 2025, Abril 24]

Castillo, M. y Romero, P. (2021). ***ESTUDIO DE FACTIBILIDAD DE UNA ALTERNATIVA DE PAGO CON RECONOCIMIENTO FACIAL EN ESTACIONES DE TRANSMILENIO, BOGOTÁ.*** [Trabajo de grado en línea]. Fundación Universidad de América, Colombia. Disponible en: https://repository.uamerica.edu.co/server/api/core/bitstreams/70b85856-0956-49e0-becb-dbdb560a868b/content [Consultado: 2025, Abril 22]

CEC. (2022). ***Frameworks de Ciberseguridad*** [Articulo en linea]. Disponible en: https://www.cec.es/frameworks-de-ciberseguridad-tipos-estrategias-implementacion-y-beneficios/ [Consultado en:]

Chakray. (2021). ***APIs Open Banking: La guía definitiva para dominar el nuevo ecosistema financiero*** [Articulo en linea]. Disponible en: https://chakray.com/es/apis-open-banking-guia-definitiva-beneficios-ejemplos-estrategias/ [Consultado en:]

Chirinos, J. (2023). ***SISTEMA DE ACCESO POR MEDIO DE UN DISPOSITIVO DE RECONOCIMIENTO FACIAL, PARA SISTEMAS INFORMÁTICOS.*** [Trabajo de grado en línea]. Universidad José Antonio Páez, Venezuela. Disponible en: https://riujap.ujap.edu.ve/server/api/core/bitstreams/a655ee57-ea1e-4c51-8885-5a9a5c69d55d/content [Consultado: 2025, Abril 24]

Cosmikal. (2024). ***¿Qué es y cómo funciona un Vault Encriptado?*** [Articulo en linea]. Disponible en: https://www.cosmikal.es/que-es-y-como-funciona-un-vault-encriptado/ [Consultado en:]

CyberArk. (2025). ***What is Security Framework?*** [Articulo en linea]. Disponible en: https://www.cyberark.com/what-is/security-framework/ [Consultado en:]

De Sousa, K. y Mora, C. (2016). ***Sistema de seguridad basado en reconocimiento facial utilizando una Raspberry Pi.*** [Trabajo de grado en línea]. Universidad Central de Venezuela, Venezuela. Disponible en: http://saber.ucv.ve/bitstream/10872/14700/1/TEG%20-%20De%20Sousa%2C%20Mora.pdf [Consultado: 2025, Abril 23]

Díaz, J. (2022). ***Fallas en el sistema de BiopagoBDV: ¿qué hacer si no reconoce la huella dactilar?*** [Articulo en linea]. Disponible en: https://eldiario.com/2022/08/11/que-hacer-si-no-reconoce-la-huella-dactilar-del-sistema-de-biopagobdv/ [Consultado en:]

Deyli. (2025). ***Adiós al efectivo: China implementa pagos faciales.*** [Artículo en línea]. Disponible en: https://saganoticias.com/ciencia-y-tecnologia/adios-al-efectivo-china-implementa-pagos-faciales [Consultado: 2025, Marzo 03]

Entrust. (2024). ***¿Qué es un módulo de seguridad de hardware (HSM) y cuáles son sus servicios?*** [Blog en linea]. Disponible en: https://www.entrust.com/es/resources/learn/what-are-hardware-security-modules [Consultado en:]

Fernández, V. (2006). ***Desarrollo de sistemas de información.*** [Libro en línea]. Disponible en: https://books.google.co.ve/books?id=Sqm7jNZS_L0C&newbks=0&printsec=frontcover&hl=es-419&redir_esc=y#v=onepage&q&f=false [Consultado: 2025, Marzo 02]

Fortinet. (2021). ***Significado del módulo de seguridad de hardware (HSM).*** [Articulo en linea]. Disponible en: https://www.fortinet.com/lat/resources/cyberglossary/hardware-security-module [Consultado en:]

Glover, E. (2024). ***Facial Recognition Software: 20 Tools to Know.*** [Página web]. Disponible en: https://builtin.com/artificial-intelligence/facial-recognition-software [Consultado: 2025, Abril 24]

Google Cloud. (2024). ***Framework de seguridad y resiliencia*** [Articulo en linea]. Disponible en: https://cloud.google.com/security/solutions/security-and-resilience?hl=es [Consultado en:]

Gutter, R. (2024). ***Aprovechamiento del Potencial del Sector Bancario Mediante la Tecnología de Reconocimiento Facial*** [Blog en linea]. Disponible en: https://revistaseguridad.cl/2024/05/08/tecnologia-de-reconocimiento-facial/ [Consultado en:]

InvestGlass. (2024). ***Racionalización del proceso de aprobación de transacciones bancarias: Guía paso a paso*** [Articulo en linea]. Disponible en: https://www.investglass.com/es/agilizar-el-proceso-de-aprobacion-de-transacciones-bancarias-guia-paso-a-paso/ [Consultado en:]

Innovatrics. (2023). ***Reconocimiento Facial*** [Articulo en linea]. Disponible en: https://www.innovatrics.com/es/glosario/reconocimiento-facial/ [Consultado en:]

IONOS. (2025). ***Facial Recognition: ¿qué es el reconocimiento facial?*** [Articulo en linea]. Disponible en: https://www.ionos.com/es-us/digitalguide/paginas-web/desarrollo-web/reconocimiento-facial/ [Consultado en:]

iProUP. (2024). ***Mastercard lanzó el Pago Biométrico global: ¿llegó el fin de las tarjetas de débito y crédito?*** [Blog en línea]. Disponible en: https://www.iproup.com/innovacion/48064-mastercard-permite-ahora-pagar-palma-de-la-mano [Consultado: 2025, Marzo 02]

Kaspersky. (2025). ***Reconocimiento facial: definición y explicación.*** [Articulo en linea]. Disponible en: https://latam.kaspersky.com/resource-center/definitions/what-is-facial-recognition [Consultado en:]

Keyless. (2024). ***Facial Recognition: applications, benefits and challenges*** [Blog en linea]. Disponible en: https://keyless.io/blog/post/facial-recognition-applications-benefits-and-challenges [Consultado en:]

Khudiar, R. y Muttasher, G. (2022). ***Payment Systems Based on Face Recognition: A Survey*** [Articulo en linea]. Disponible en: https://www.researchgate.net/publication/360972928_Payment_Systems_Based_on_Face_Recognition_A_Survey#read [Consultado en:]

Mayen, J. (2025). ***¡Adiós al dinero en efectivo! En China solo necesitas tu cara para pagar (video).*** [Artículo en línea]. Disponible en: https://www.dineroenimagen.com/actualidad/adios-dinero-efectivo-china-solo-necesitas-tu-cara-para-pagar-video [Consultado: 2025, Marzo 02]

Meca, G. (2024). ***Todo tu dinero en la palma de la mano: así pagan ya en las tiendas en China***. [Artículo en línea]. Disponible en: https://okdiario.com/curiosidades/todo-tu-dinero-palma-mano-asi-pagan-ya-tiendas-china-12785441 [Consultado: 2025, Marzo 03]

Mendoza, V. y Falcón, G. (2018). ***DESARROLLO DE UN SISTEMA DE SEGURIDAD BASADO EN EL RECONOCIMIENTO FACIAL PARA LA UNIVERSIDAD JOSÉ ANTONIO PÁEZ.*** [Trabajo de grado en línea]. Universidad José Antonio Páez, Venezuela. Disponible en: https://riujap.ujap.edu.ve/server/api/core/bitstreams/052bfe17-b641-418b-98d9-23f6a09a5320/content [Consultado: 2025, Abril 24]

Morillo, G. (2020). ***APLICACIÓN DE GESTIÓN BANCARIA CON FIRMA DIGITAL PARA VALIDACIÓN DE OPERACIONES.*** [Trabajo de grado en linea]. Universidad Politécnica de Madrid. Disponible en: https://oa.upm.es/66293/1/TFG_GABRIEL_MORILLO_PILENO.pdf [Consultado en:]

Nebreda, P. (2024). ***Frameworks de ciberseguridad, ¿qué debes saber?*** [Articulo en linea]. Disponible en: https://www.factum.es/articulos/frameworks-de-ciberseguridad-que-debes-saber/ [Consultado en:]

Niu. (2022). ***Aplicaciones del reconocimiento facial en la industria bancaria*** [Blog en linea]. Disponible en: https://blog.niu.solutions/soluciones-tecnologicas/aplicaciones-del-reconocimiento-facial-en-la-industria-bancaria [Consultado en:]

Nutanix. (2025). ***¿Qué es un Sistema de Gestión de Bases de Datos (DBMS)?*** [Articulo en linea]. Disponible en: https://www.nutanix.com/es/info/database-management [Consultado en:]

OVHcloud. (2020). ***¿Qué es el SGBD?*** [Articulo en linea]. Disponible en: https://www.ovhcloud.com/es/learn/what-is-dbms/ [Consultado en:]

Ramirez, O. (2025). ***Frameworks de Ciberseguridad: Protege tus Aplicaciones*** [Articulo en linea]. Disponible en: https://bambu-mobile.com/frameworks-de-ciberseguridad/#:~:text=Un%20framework%20de%20ciberseguridad%20es,de%20amenazas%20de%20seguridad%20inform%C3%A1tica. [Consultado en:]

Revista Ciberseguridad. (2025). ***Los riesgos de los pagos sin contacto y recomendaciones de cómo protegerse*** [Articulo en linea]. Disponible en: https://www.revistaciberseguridad.com/2025/04/los-riesgos-de-los-pagos-sin-contacto-y-recomendaciones-de-como-protegerse/ [Consultado en:]

Stankevičiūtė, G. (2023). ***Los 5 principales casos de uso de la biometría en la banca.*** [Página web]. Disponible en: https://www.idenfy.com/blog/biometrics-in-banking/ [Consultado: 2025, Abril 23]

Silva, H. (2025). ***API bancaria: qué es y cómo integrarla en tu negocio*** [Blog en linea]. Disponible en: https://www.sydle.com/es/blog/api-bancaria-667af1a1a14707634f35cd5a [Consultado en:]

Stripe. (2023). ***Aspectos básicos de la verificación de cuentas bancarias: qué es y***

cómo funciona [Articulo en linea]. Disponible en: https://stripe.com/es/resources/more/bank-account-verification-101 [Consultado en:]

Stripe. (2024) ***¿Qué son los pagos biométricos? Guía rápida para empresas.*** [Articulo en linea]. Disponible en: https://stripe.com/es/resources/more/what-are-biometric-payments-a-quick-guide-for-businesses?allow-unsupported-browser=true [Consultado: 2025, Marzo 02]

Stripe. (2024). ***Explicación de las API financieras:: Qué son, cómo funcionan y cómo están cambiando el fintech*** [Articulo en linea]. Disponible en: https://stripe.com/es-us/resources/more/financial-apis-explained-what-they-are-how-they-work-and-how-they-are-changing-fintech [Consultado en:]

Stripe. (2024). ***¿Qué son los pagos biométricos? Guía rápida para las empresas*** [Articulo en linea]. Disponible en: https://stripe.com/es-us/resources/more/what-are-biometric-payments-a-quick-guide-for-businesses [Consultado en:]

Stripe. (2025). ***Funcionamiento del procesamiento de las transacciones de pago: guía rápida*** [Articulo en linea]. Disponible en: https://stripe.com/es/resources/more/how-payment-transaction-processing-works [Consultado en:]

Tomych, I. (2025). ***Bank API in Modern Finance: Use Cases, Classifications, and Integration*** [Blog en linea]. Disponible en: https://dashdevs.com/blog/api-in-banking-classification/ [Consultado en:]

Universidad Isabel I. (2023). ***¿Qué es la Gestión de bases de datos?*** [Blog en linea]. Disponible en: https://www.ui1.es/blog-ui1/que-es-la-gestion-de-bases-de-datos [Consultado en:]

Varela, M. (2018). ***BBVA lanza un sistema de pagos por reconocimiento facial.*** [Blog en línea]. Disponible en: https://www.bbva.com/es/innovacion/bbva-lanza-sistema-pagos-reconocimiento-facial/ [Consultado: 2025, Marzo 02]

Wei, M. (2021). ***El uso de tecnología de reconocimiento facial en el proceso de pago para promover la economía en México durante la pandemia*** [Trabajo de grado en línea]. Universidad Autónoma de Querétaro, México. Disponible en: https://static1.squarespace.com/static/55564587e4b0d1d3fb1eda6b/t/60a2901a923fb71ca3054761/1621266459669/H084MaoWei+--+Exploratoris+V10N1+2021+--+32-39.pdf [Consultado en: 2021, Abril 21]

[ANEXO “A”]

[Modelo del Instrumento: El Cuestionario]

UNIVERSIDAD ALEJANDRO DE HUMBOLDT
FACULTAD DE INGENIERÍA
INGENIERÍA EN INFORMÁTICA

Cuestionario

Este cuestionario forma parte de un trabajo de investigación enfocado en el desarrollo de un sistema de pagos mediante vinculación de cuenta a través de Reconocimiento Facial para el Banco de Venezuela, S.A. Banco Universal. El objetivo principal de este estudio es recopilar información técnica valiosa sobre las herramientas y componentes necesarios para diseñar esta solución innovadora.

El este cuestionario es totalmente anónimo y confidencial, sus respuestas nos ayudarán a definir y establecer los requerimientos para esta nueva tecnología de pago, asegurando que el sistema sea seguro, eficiente y se ajuste a la infraestructura actual del banco. Responder a estas preguntas solo le tomará unos minutos y es de gran importancia para el éxito del proyecto.

Instrucciones

- Por favor lea detenidamente todo el instrumento antes de responder.
- Marque con una X la opción de respuesta que considere para cada pregunta.
- Asegúrese de no dejar ninguna pregunta sin responder.
- Marque solo una alternativa de respuesta por cada pregunta.

Items	SI	NO
1. - ¿Considera que el sistema BioPago presenta una limitación de accesibilidad para adultos mayores o trabajadores manuales cuyas huellas dactilares se han deteriorado, impidiéndoles completar transacciones de manera efectiva?		
2. - ¿Cree usted que los sistemas de pago Contactless utilizados actualmente por el banco son vulnerables a ataques de lectura no autorizada o clonación de datos a corta distancia?		
3. - ¿Considera usted que la frecuencia de intentos de fraude o transacciones no reconocidas en los sistemas de pago actuales del Banco de Venezuela justifica la necesidad de una autenticación biométrica más segura como el reconocimiento facial?		

4. - ¿Considera usted que para vincular una cuenta por primera vez se debería requerirse obligatoriamente un segundo factor de autenticación además de la validación biométrica inicial?		
5. - ¿Considera usted que el Flujo de Autenticación por Reconocimiento Facial debe incorporar mecanismos de detección de vida (liveness detection) activos para mitigar ataques de suplantación (spoofing)?		
6. - ¿Considera adecuado un tiempo de latencia máximo de 3 segundos para la Ejecución y Confirmación de Transacciones de pago por reconocimiento facial, desde la autenticación hasta la respuesta final del core bancario?		
7. - ¿Cree usted que es indispensable utilizar herramientas y programas especializados en el desarrollo de Reconocimiento Facial para construir la funcionalidad de identificación?		
8. - ¿Considera que la arquitectura del Backend Seguro y Escalable debe estar basada en microservicios para soportar las proyecciones de concurrencia de pagos?		
9. ¿Cree usted que sea necesario implementar un Módulo de Seguridad y Cifrado dedicado (ej. HSM o Key Vault) para la gestión y protección de las claves criptográficas utilizadas en el sistema?		
10. - ¿Cree que la frecuencia de fallas en la autenticación biométrica de BioPago deteriora la experiencia de pago del cliente y justifica la implementación de una biometría alternativa (como el reconocimiento facial)?		

[ANEXO "B"]

[Matriz de Validación: Instrumento de Recolección de Datos]

Matriz de validación del instrumento de recolección de datos. Ing. Ofelia Sanchez / Msc. Profesora de la UAH. Presentada como componente Metodológico.

UNIVERSIDAD ALEJANDRO DE HUMBOLDT
FACULTAD DE INGENIERÍA
CARRERA INGENIERÍA EN INFORMÁTICA

MATRIZ DE VALIDACIÓN DEL INSTRUMENTO DE RECOLECCIÓN DE DATOS

Ítem	Criterio				Juicios					
	Claridad		Congruencia		Eliminar		Modificar		Aceptar	
	Si	No	Si	No	Si	No	Si	No	Si	No
1	✓		✓			✓		✓	—	
2	✓		✓			✓		✓	✓	
3	✓		✓			✓		✓	✓	
4	✓		✓			✓		✓	✓	
5	✓		✓			✓		—	✓	
6	✓		✓			✓		—	—	
7	✓		✓			✓		—	—	
8	✓		✓			✓		—	—	
9	✓		✓			✓		—	✓	
10	✓		✓			✓		—	—	

Observaciones:

Nombre del Especialista: Ofelio Sanchez

C.I: 9597058

Profesión: Ingeniero en Sistemas / MSc

Firma

[ANEXO “C”]

[Matriz de Validación: Instrumento de Recolección de Datos]

Matriz de validación del instrumento de recolección de datos. Ing. Oscar Lozano, profesor de la UAH. Presentado como componente Tecnológico.

UNIVERSIDAD ALEJANDRO DE HUMBOLDT
FACULTAD DE INGENIERÍA
CARRERA INGENIERÍA EN INFORMÁTICA

MATRIZ DE VALIDACIÓN DEL INSTRUMENTO DE RECOLECCIÓN DE DATOS

Ítem	Criterio				Juicios					
	Claridad		Congruencia		Eliminar		Modificar		Aceptar	
	Si	No	Si	No	Si	No	Si	No	Si	No
1	✓		✓			✓		✓	✓	
2	✓		✓			✓		✓	✓	
3	✓		✓			✓		✓	✓	
4	✓		✓			✓		✓	✓	
5	✓		✓			✓		✓	✓	
6	✓		✓			✓		✓	✓	
7	✓		✓			✓		✓	✓	
8	✓		✓			✓		✓	✓	
9	✓		✓			✓		✓	✓	
10	✓		✓			✓		✓	✓	

Observaciones: _____

Nombre del Especialista: Oscar Lozano

C.I: V-6425667

Profesión: Esp. Ing. Sistemas Firma _____

[ANEXO “D”]

[Matriz de Validación: Instrumento de Recolección de Datos]

Matriz de validación del instrumento de recolección de datos. Lic. Juan Bernardini, profesor de la UAH. Presentado como componente Estadistico.

UNIVERSIDAD ALEJANDRO DE HUMBOLDT
FACULTAD DE INGENIERÍA
CARRERA INGENIERÍA EN INFORMÁTICA

MATRIZ DE VALIDACIÓN DEL INSTRUMENTO DE RECOLECCIÓN DE DATOS

Ítem	Criterio				Juicios					
	Claridad		Congruencia		Eliminar		Modificar		Aceptar	
	Si	No	Si	No	Si	No	Si	No	Si	No
1	✓		✓			✓		✓	✓	
2	✓		✓			✓		✓	✓	
3	✓		✓			✓		✓	✓	
4	✓		✓			✓		✓	✓	
5	✓		✓			✓		✓	✓	
6	✓		✓			✓		✓	✓	
7	✓		✓			✓		✓	✓	
8	✓		✓			✓		✓	✓	
9	✓		✓			✓		✓	✓	
10	✓		✓			✓		✓	✓	

Observaciones:

Nombre del Especialista: Juan Bernardini

C.I: V-17610918

Profesión: Contador

Firma