 **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.**

**(Proyecto de investigación)**

**Autor: Terán Gabriel**

**C.I: V-26.546.735**

**Profesor: Franklin Cedeño**

**Caracas, Agosto 2025.**

**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**

**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)**

**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.

https://www.mobbeel.com/blog/aplicacion-tecnologias-biometricas-industria-financiera/

https://www-nngroup-com.translate.goog/articles/facial-recognition-payment/?\_x\_tr\_sl=en&\_x\_tr\_tl=es&\_x\_tr\_hl=es&\_x\_tr\_pto=tc

<https://revistaseguridad.cl/2024/05/08/tecnologia-de-reconocimiento-facial/>

***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

**CAPÍTULO III**

**MARCO METODOLÓGICO**

**Diseño de Investigación**

El proyecto que se está desarrollando actualmente tiene como aplicación dos tipos de propiedades: diseño de Investigación de Campo (I.C.). 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**

Esta investigación desarrollará un nivel de tipo 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 las doce (12) 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 12  bancarias del Banco de Venezuela,  S.A. Banco Universal |

**Fuente: Gabriel Terán (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 doce (12) 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 doce (12) 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 12  bancarias del Banco de Venezuela,  S.A. Banco Universal |

**Fuente: Gabriel Terán (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 doce (12) empleados de la Gerencia de linea de sistemas financieros y colocaciones bancarias del Banco de Venezuela, S.A. Banco Universal, (Ver Anexo “A”).

**REFERENCIAS**

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]

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](https://www.bcra.gob.ar/SistemasFinancierosYdePagos/Sistemas_de_Pago.asp" \l ":~:text=seguridad y eficiencia.-,Medios de Pago Electrónicos,en línea) por el canal) [Consultado: 2025, Marzo 02]

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]

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]

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](http://saber.ucv.ve/bitstream/10872/14700/1/TEG - De Sousa%2C Mora.pdf) [Consultado: 2025, Abril 23]

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]

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](https://books.google.co.ve/books?id=Sqm7jNZS_L0C&newbks=0&printsec=frontcover&hl=es-419&redir_esc=y" \l "v=onepage&q&f=false) [Consultado: 2025, Marzo 02]

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]

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]

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]

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]

Stripe. (2024) ***¿Qué son los pagos biométricos? Guía rápida para empresas.*** [Página

web]. 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]

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]**

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)? |  |  |