UNIVERSIDAD NACIONAL DE CHIMBORAZO
FACULTAD DE INGENIERIA
CARRERA DE SISTEMAS Y COMPUTACIÓN

Aplicación móvil de pasarela de pagos para procesos E-commerce B2C en PYMES, utilizando la arquitectura MVVM.

Trabajo de Titulación para optar al título de Ingeniero en Sistemas y Computación

Autor:
Constante Vinocunga, Fausto Fabricio

Tutor:
Ing. Delgado Altamirano, Jorge Edwin

Riobamba, Ecuador. 2025

DERECHOS DE AUTORÍA

Yo, **Fausto Fabricio Constante Vinocunga,** con cédula de ciudadanía **1727653055**, autor del trabajo de investigación titulado: **Aplicación móvil de pasarela de pagos para procesos de e-commerce B2C en PYMES, utilizando la arquitectura MVVM,** certifico que la producción, ideas, opiniones, criterios, contenidos y conclusiones expuestas son de mí exclusiva responsabilidad.

Asimismo, cedo a la Universidad Nacional de Chimborazo, en forma no exclusiva, los derechos para su uso, comunicación pública, distribución, divulgación y/o reproducción total o parcial, por medio físico o digital; en esta cesión se entiende que el cesionario no podrá obtener beneficios económicos. La posible reclamación de terceros respecto de los derechos de autor (a) de la obra referida, será de mi entera responsabilidad; librando a la Universidad Nacional de Chimborazo de posibles obligaciones.

En Riobamba, 20 de mayo de 2025.

Fausto Fabricio Constante Vinocunga

C.I: 172765305-5

DICTAMEN FAVORABLE DEL TUTOR Y MIEMBROS DE TRIBUNAL

Quienes suscribimos, catedráticos designados Miembros del Tribunal de Grado del trabajo de investigación **Aplicación móvil de pasarela de pagos para procesos de e-commerce B2C en PYMES, utilizando la arquitectura MVVM**, presentado por Fausto Fabricio Constante Vinocunga, con cédula de identidad número 1727653055, emitimos el DICTAMEN FAVORABLE, conducente a la APROBACIÓN de la titulación. Certificamos haber revisado y evaluado el trabajo de investigación y cumplida la sustentación por parte de su autor; no teniendo más nada que observar.

De conformidad a la normativa aplicable firmamos, en Riobamba 25 de junio de 2025.

Gonzalo Allauca Mgs.
PRESIDENTE DELEGADO

Milton López Mgs.
MIEMBRO DEL TRIBUNAL DE GRADO

Miryan Narváez, PhD.
MIEMBRO DEL TRIBUNAL DE GRADO

Jorge Edwin Delgado Altamirano Mgs.
TUTOR

CERTIFICADO DE LOS MIEMBROS DEL TRIBUNAL

Quienes suscribimos, catedráticos designados Miembros del Tribunal de Grado para la evaluación del trabajo de investigación **Aplicación móvil de pasarela de pagos para procesos de e-commerce B2C en PYMES, utilizando la arquitectura MVVM**, presentado por **Fausto Fabricio Constante Vinocunga**, con cédula de identidad número **1727653055**, bajo la tutoría del **Ing. Jorge Edwin Delgado Altamirano**; certificamos que recomendamos la APROBACIÓN de este con fines de titulación. Previamente se ha evaluado el trabajo de investigación y escuchada la sustentación por parte de su autor; no teniendo más nada que observar.

De conformidad a la normativa aplicable firmamos, en Riobamba 25 de junio de 2025.

Presidente del Tribunal de Grado
Mgs. Gonzalo Allauca

Miembro del Tribunal de Grado
PhD. Miryan Estela Narváez Vilema

Miembro del Tribunal de Grado
Mgs. Milton Paul López R.

C E R T I F I C A C I Ó N

Que, **CONSTANTE VINOCUNGA FAUSTO FABRICIO con C.C. 1727653055**, estudiante de la carrera **INGENIERÍA EN SISTEMAS Y COMPUTACIÓN , NO VIGENTE,** Facultad de **INGENIERÍA**; ha trabajado bajo mi tutoría el trabajo de investigación titulado "**APLICACIÓN MOVIL DE PASARELA DE PAGOS PARA PROCESOS E- COMMERCE B2C EN PYMES, UTILIZANDO LA ARQUITECTURA MVVM**", cumple con el 4 %, de acuerdo al reporte del sistema Anti plagio **COMPILATIO**, porcentaje aceptado de acuerdo a la reglamentación institucional, por consiguiente autorizo continuar con el proceso.

Riobamba, 13 de mayo de 2025

JORGE EDWIN DELGADO ALTAMIRANO

Mg. Jorge Delgado
TUTOR TRABAJO DE INVESTIGACIÓN

DEDICATORIA

Dedico este trabajo a mi madre, Marica Clemencia Vinocunga Analuisa, quien, con su amor inquebrantable y fortaleza infinita, me ha enseñado que la perseverancia es la clave para alcanzar cualquier meta. Su ejemplo ha sido mi guía, su sacrificio mi inspiración.

A mi hermano, Edison Danilo García Vinocunga, con la esperanza de que este esfuerzo sea una muestra de que los sueños se alcanzan con determinación y trabajo duro. Que encuentre en mí un ejemplo de lucha y crecimiento.

A mi mejor amigo, que más que un amigo ha sido un hermano, Anthony Gabriel Pazmiño Solís, por estar siempre a mi lado, por sus palabras de aliento en los momentos difíciles y por recordarme que rendirse nunca es una opción.

A todos quienes han sido parte de este camino, gracias por su apoyo, por su fe en mí y por enseñarme que la verdadera fuerza nace de quienes nos rodean.

Fausto Fabricio Constante Vinocunga

AGRADECIMIENTO

A Dios, por su infinita misericordia y por darme la fortaleza para superar cada desafío en este camino académico. A Él, por cada bendición recibida y por iluminar mi sendero en los momentos de incertidumbre.

A mi madre, Marica Clemencia Vinocunga Analuisa, por su amor incondicional, por su esfuerzo incansable y por ser la base sobre la que construyo mis sueños. Su ejemplo de determinación y sacrificio me ha dado la fuerza para seguir adelante.

A mi hermano, Edison Danilo García Vinocunga, por su apoyo y compañía, por recordarme que con esfuerzo y constancia todo es posible. Que este logro sea una inspiración para que siga persiguiendo sus propios sueños.

A mi mejor amigo, Anthony Gabriel Pazmiño Solís, por ser un pilar fundamental en mi vida, por sus palabras de ánimo en los momentos difíciles y por motivarme a seguir adelante sin rendirme.

A mi tutor de tesis, el Ing. Jorge Edwin Delgado Altamirano, por su invaluable orientación, paciencia y compromiso, por dedicar su tiempo y conocimientos para guiarme en la elaboración de este trabajo.

A todos mis docentes de la carrera de Ingeniería en Sistemas y Computación, por compartir sus conocimientos y contribuir a mi crecimiento profesional y personal a lo largo de estos años.

A mis compañeros de aula, por hacer de esta etapa un viaje enriquecedor, lleno de aprendizaje, experiencias y amistad.

A mi familia en su totalidad, por ser mi refugio y mi mayor fuente de motivación. Sin su amor, apoyo y comprensión, este logro no habría sido posible.

Finalmente, a mi querida U.N.A.C.H, por abrirme sus puertas, por brindarme la oportunidad de aprender y crecer, y por ser el espacio donde he formado la base de mi carrera profesional.

Fausto Fabricio Constante Vinocunga

ÍNDICE GENERAL

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

La automatización de procesos es un factor clave en la evolución de las organizaciones, especialmente en la gestión de pagos digitales y la optimización de la experiencia del usuario. En este contexto, la presente investigación se enfoca en el desarrollo de una aplicación móvil de pasarela de pagos orientada a los procesos de comercio electrónico B2C en pequeñas y medianas empresas (PYMES), implementando la arquitectura Model-View-ViewModel (MVVM).

El estudio adopta un enfoque cuantitativo con un diseño bibliográfico-documental, considerando una población infinita. Para evaluar la seguridad de las transacciones digitales, se empleó la herramienta OWASP ZAP, la cual permitió detectar y corregir vulnerabilidades en pasarelas de pago y garantizar la protección de los datos sensibles. Los resultados mostraron un alto porcentaje de cumplimiento con los controles de la Norma ISO 27001, así como una robusta implementación de cifrado para la información confidencial.

Además, se detallan los principios clave de la arquitectura MVVM aplicados en el desarrollo del sistema, junto con un análisis de aquellos que no fueron incorporados en la implementación. Asimismo, se examina el impacto de la metodología Clean Architecture, resaltando su capacidad para garantizar la separación de responsabilidades, la independencia tecnológica y la escalabilidad del sistema, facilitando su mantenibilidad.

Finalmente, se aborda la seguridad de la información en las pasarelas de pago de la aplicación, tomando como referencia la Norma ISO 27001, con el fin de reforzar los protocolos de protección y asegurar la integridad de las transacciones digitales. Las pruebas realizadas demostraron la efectividad de las medidas implementadas contra accesos no autorizados validando la robustez del sistema. Los resultados del estudio demuestran la viabilidad de la solución propuesta y su potencial para mejorar la seguridad y eficiencia en la gestión de pagos dentro del comercio electrónico B2C en PYMES.

Palabras claves: Seguridad informática, protección de datos, comercio electrónico B2C, PYMES, MVVM, Clean Architecture, OWASP, ISO 27001.

ABSTRACT

Process automation is a key factor in the evolution of organizations, especially in the management of digital payments and the optimization of the user experience. In this context, the present research focuses on developing a mobile payment gateway application tailored to B2C e-commerce processes in small and medium-sized enterprises (SMEs), utilizing the Model-View-ViewModel (MVVM) architecture.

The study adopts a quantitative approach with a bibliographic-documentary design, considering an infinite population. To evaluate the security of digital transactions, the OWASP ZAP tool was utilized to detect and correct vulnerabilities in payment gateways, thereby ensuring the protection of sensitive data. The results showed a high percentage of compliance with ISO 27001 controls, as well as a robust implementation of encryption for confidential information. Additionally, the key principles of the MVVM architecture applied in the system's development are detailed, along with an analysis of those that were not incorporated into the implementation. The impact of the Clean Architecture methodology is also examined, highlighting its ability to ensure the separation of responsibilities, technological independence, and scalability of the system, facilitating its maintainability.

Finally, information security in the application's payment gateways is addressed, using ISO 27001 as a reference, to reinforce protection protocols and ensure the integrity of digital transactions. The tests performed demonstrated the effectiveness of the measures implemented against unauthorized access, validating the robustness of the system. The study's results demonstrate the viability of the proposed solution and its potential to enhance security and efficiency in the management of payments within B2C e-commerce for SMEs.

Keywords: Cybersecurity, data protection, B2C e-commerce, SMEs, MVVM, Clean Architecture, OWASP, ISO 27001.

Reviewed by:
Ms.C. Ana Maldonado León
ENGLISH PROFESSOR
C.I.0601975980

CAPÍTULO I. INTRODUCCIÓN

El sistema que se propone tiene como meta optimizar la comercialización de productos y servicios entre empresas y consumidores, incorporando medidas de seguridad que garanticen la protección de la información durante las transacciones digitales. En un contexto de incertidumbre económica, la digitalización se revela como una estrategia clave para fomentar el crecimiento empresarial y satisfacer de manera efectiva las necesidades de los clientes.

Según un informe de (Orienteed, 2023), Se prevé que para el año 2026, las compras minoristas en línea experimenten un aumento del 24%, alcanzando un volumen cercano a los 8. 1 billones de dólares. Esto consolidará el comercio electrónico como una de las principales estrategias comerciales a largo plazo. A su vez, un análisis de (SALESFORCE, 2021), indica que la pandemia ha acelerado notablemente la adopción de canales digitales, lo que ha llevado a una transformación significativa en el comercio global. En la actualidad, un 68% de los consumidores afirma que seguirá comprando productos esenciales en línea, lo que refleja una tendencia persistente en este sector. Desde 2019, muchos líderes empresariales han intensificado sus inversiones en el comercio digital, motivados por tres factores clave: la crisis sanitaria, el aumento en la demanda y la presión de la competencia.

De hecho, más de la mitad de las empresas (56%) anticipa que, durante los próximos tres años, la mayor parte de sus ingresos provendrá de canales digitales. En el ámbito del desarrollo de aplicaciones móviles, diversos frameworks han ganado popularidad por su eficiencia y versatilidad. Tecnologías como React Native, Flutter, Ionic, Adobe y NativeScript se distinguen por su facilidad de uso, su capacidad para desarrollar aplicaciones multiplataforma y el fuerte apoyo de comunidades de desarrolladores. En particular, React Native ha ganado una amplia aceptación en la creación de aplicaciones móviles nativas, gracias a su habilidad para reutilizar código en diferentes sistemas operativos. Además, ofrece recursos especializados en seguridad que abordan aspectos cruciales, tales como el almacenamiento seguro de datos sensibles, la autenticación de usuarios y la protección en la comunicación con servidores externos (REACTNATIVE, 2023).

A pesar de los avances tecnológicos, la seguridad en aplicaciones móviles sigue siendo un desafío crítico. Un informe de (VERIZON, 2022) indica que el 43% de las empresas ha comprometido la seguridad en sus desarrollos tecnológicos, y un 39% ha enfrentado vulnerabilidades que impactaron directamente su negocio. Estas cifras reflejan la

importancia de reforzar los protocolos de seguridad y adoptar buenas prácticas en el diseño de software.

El comercio electrónico confronta múltiples amenazas digitales, lo que hace necesaria la implementación de medidas de ciberseguridad en todas las etapas del desarrollo de aplicaciones. Según (INCIBE, 2019), garantizar la seguridad de los sistemas e-commerce requiere un enfoque integral que considere la protección de datos, la prevención de fraudes y el cumplimiento de normativas internacionales.

Mediante una aplicación móvil, los consumidores tienen la posibilidad de acceder a información sobre productos y servicios, realizar compras y efectuar pagos en línea. Esta plataforma almacenará datos en la cuenta del usuario, lo que permitirá facilitar futuras adquisiciones al tener en cuenta sus patrones de comportamiento y preferencias de compra.

1.1 PLANTEAMIENTO DEL PROBLEMA

El auge del comercio electrónico B2C ha tenido un impacto notable en la economía digital, motivando a grandes empresas y pequeñas y medianas empresas (PYMES) a adoptar plataformas móviles para la venta de sus productos y servicios. Según (Statista, 2023) Se estima que los ingresos globales del comercio electrónico B2C experimentarán un crecimiento de más del 50% entre 2021 y 2025, consolidándose, así como una estrategia clave para la expansión de negocios en el entorno digital. No obstante, a pesar de esta tendencia alentadora, las pequeñas y medianas empresas (PYMES) en América Latina enfrentan desafíos en la implementación de aplicaciones móviles, lo que restringe su competitividad en el mercado digital. Este auge en el comercio electrónico B2C ha tenido un impacto significativo en la economía digital, impulsando tanto a grandes empresas como a PYMES a adoptar plataformas móviles para la comercialización de productos y servicios.

Diversos estudios han identificado los principales desafíos que afectan la adopción de plataformas de comercio electrónico en PYMES (EMarketer, 2019) señala que estas empresas se ven limitadas por factores como la escasez de recursos financieros y técnicos, el desconocimiento en la implementación de aplicaciones digitales, la inseguridad respecto a las transacciones electrónicas y las restricciones para acceder a servicios de pago en línea. Asimismo, un análisis de (Statista, 2023), menciona que la falta de confianza en la seguridad de las transacciones representa uno de los principales obstáculos para el crecimiento del comercio electrónico en América Latina. En 2020, el 47% de los consumidores identificó la seguridad como su mayor preocupación al realizar compras en línea.

En Ecuador, las PYMES B2C no están exentas de estos problemas, pues la implementación de aplicaciones móviles con pasarelas de pago sigue siendo un desafío (Matute et al., 2023), identifican que la inseguridad en los pagos electrónicos como un factor crucial que limita el crecimiento de estas empresas en el entorno digital. La ausencia de protocolos sólidos para salvaguardar la información financiera de los usuarios genera vulnerabilidades que pueden socavar la confianza de los consumidores y afectar la rentabilidad de los negocios.

De acuerdo con un artículo de Paycomet, incorporar una pasarela de pago en una aplicación móvil puede impulsar las ventas, aunque es fundamental considerar diversos aspectos. Previamente, es crucial evaluar las necesidades del negocio y las preferencias de los usuarios para determinar cuál es la opción más adecuada y cómo debería operar la pasarela de pago. Asimismo, es esencial garantizar que esta funcione de manera efectiva y cumpla con aspectos clave como la seguridad y la facilidad de uso (PAYCOMET, 2021).

Para reducir estos riesgos, es esencial implementar arquitecturas de software que prioricen la seguridad de las aplicaciones móviles. La arquitectura MVVM (Modelo-Vista-Modelo de Vista) se ha consolidado como una opción eficaz para optimizar la calidad y escalabilidad de las aplicaciones de comercio electrónico, lo que a su vez simplifica su mantenimiento y las pruebas unitarias (Angleritech, 2020). Además, su estructura modular permite aplicar estrategias de seguridad en diferentes capas del sistema, reduciendo el riesgo de vulnerabilidades y optimizando el manejo de datos sensibles.

Las amenazas cibernéticas como la falta de autenticación robusta, la ausencia de cifrado de datos, ataques de inyección SQL y el phishing representan riesgos significativos para las aplicaciones de comercio electrónico (INCIBE, 2019). Para abordar estos problemas, se sugiere la implementación de ISO/IEC 27001, un estándar que establece los requisitos para un Sistema de Gestión de Seguridad de la Información (SGSI) (Tovar, 2022).

Este enfoque permite a las empresas implementar una serie de controles de seguridad, tales como la autenticación de dos factores, el cifrado de datos, las pruebas de penetración y las actualizaciones periódicas. De esta manera, se asegura la integridad de la información y se fomenta la confianza de los usuarios.

De acuerdo con la investigación realizada por los autores antes mencionados, se puede concluir que la implementación de tiendas virtuales tiene un aporte importante al crecimiento del negocio y, como resultado, logra la satisfacción del cliente a través de la gestión de diversos procesos de compra de productos mediante pasarelas de pagos.

1.1.1 Formulación de la pregunta de investigación

¿Cómo la implementación de la Arquitectura MVVM en una aplicación móvil de pasarela de pagos puede mejorar la seguridad de los procesos e-commerce B2C en PYMES, alineándose con el estándar ISO/IEC 27001?

La adopción de la arquitectura MVVM en una aplicación móvil de pasarela de pagos fortalece la seguridad en los procesos de comercio electrónico B2C para pequeñas y medianas empresas (PYMES) al permitir una clara separación de responsabilidades entre la lógica de negocio, la presentación y la interacción con los datos. Esta estructura facilita la implementación de medidas de seguridad, como el cifrado, la validación de datos y la gestión de tokens en el modelo. A su vez, reduce la exposición de información sensible en la ViewModel y minimiza las vulnerabilidades en la vista. Además, esta arquitectura simplifica las auditorías, el control de acceso y las pruebas de seguridad, cumpliendo con los principios de la norma ISO/IEC 27001, que aboga por la protección de datos, la gestión de riesgos y la trazabilidad. De este modo, se garantiza un manejo seguro de la información durante las transacciones.

1.1.2 Justificación

En el comercio electrónico B2C, la seguridad de las transacciones en línea es un aspecto crítico para la protección de la información de los usuarios y la confianza en las plataformas digitales. De acuerdo con (INCIBE, 2019), las aplicaciones móviles manejan una cantidad significativa de datos sensibles, los cuales pueden estar en riesgo debido a diversas amenazas, como la inyección de código, el almacenamiento inseguro, la protección inadecuada en la capa de transporte, la fuga involuntaria de información, la autenticación débil y la utilización de algoritmos de cifrado vulnerables. Ante estas problemáticas, es esencial implementar arquitecturas de software que minimicen riesgos y garanticen la integridad de la información en plataformas de comercio electrónico.

En este contexto, la arquitectura Model-View-ViewModel (MVVM) ha demostrado ser una estrategia eficiente en el desarrollo de aplicaciones móviles de comercio electrónico. Según (Garcia, 2021), MVVM permite una clara separación entre la lógica de presentación y la lógica de negocio, facilitando el desacoplamiento de componentes, la reutilización de código, la facilidad de mantenimiento y la ejecución de pruebas unitarias. Estas características resultan fundamentales para asegurar la estabilidad de las aplicaciones, reduciendo errores en la manipulación de datos y mejorando la experiencia del usuario.

La integración de React con la arquitectura MVVM ofrece significativas ventajas en términos de escalabilidad y mantenibilidad, facilitando la creación de aplicaciones dinámicas que se adaptan fácilmente a los cambios en los requerimientos del mercado. Para asegurar que estas aplicaciones cumplan con los estándares de seguridad de la información, se adoptará la norma ISO/IEC 27001, la cual proporciona un marco sólido para la gestión de la seguridad. Este estándar incluye controles fundamentales como la autenticación de dos factores, el cifrado de datos, las pruebas de penetración y las actualizaciones periódicas, garantizando así que las transacciones digitales sean confiables y estén protegidas contra amenazas externas.

Por consiguiente, este estudio se centra en la creación de una aplicación móvil destinada a servir como pasarela de pagos. Para llevar a cabo este proyecto, se utilizará la arquitectura MVVM y se aplicarán los principios de la norma ISO/IEC 27001, con el objetivo de reforzar la seguridad en los procesos de comercio electrónico B2C en pequeñas y medianas empresas (PYMES). De esta manera, se pretende aumentar la confianza de los usuarios, optimizar la gestión de datos sensibles y contribuir al crecimiento de las PYMES en el ámbito digital.

1.2 OBJETIVOS

1.2.1 Objetivo General

Implementar una aplicación móvil de pasarela de pagos para procesos e-commerce B2C para las PYMES, utilizando la arquitectura MVVM.

1.2.2 Objetivos Específicos

- Investigar el desarrollo de aplicaciones móviles utilizando la arquitectura MVVM.
- Desarrollar la aplicación móvil para procesos e-commerce B2C para las PYMES.
- Evaluar la seguridad de la información en las pasarelas de pago en la aplicación móvil para procesos e-commerce utilizando la NORMA ISO 27001

CAPÍTULO II. MARCO TEÓRICO

2.1 Comercio Electrónico

El comercio electrónico constituye la incorporación de tecnología en los procesos de compra y venta, abarcando diversos modelos de transacción, tales como B2B (empresa a empresa), B2C (empresa a consumidor) y C2B (consumidor a empresa). Más allá de facilitar el intercambio de bienes y servicios, el comercio electrónico integra sistemas de gestión que optimizan pedidos, inventarios y análisis de datos, proporcionando herramientas esenciales para la eficiencia en los procesos empresariales (Castro, 2022).

Tabla 1: Ventajas y Desventajas del Comercio Electrónico

Aspecto	Ventajas	Desventajas
Acceso a una audiencia global	Permite a las empresas llegar a clientes en cualquier parte del mundo, ampliando oportunidades de crecimiento.	Puede aumentar la competencia con otras empresas internacionales, dificultando la diferenciación en el mercado.
Optimización de procesos	La automatización reduce costos operativos y mejora la eficiencia empresarial.	Requiere inversión inicial en plataformas digitales y capacitación del personal para su correcta implementación.
Mayor rentabilidad	La eliminación de infraestructura física reduce gastos, permitiendo reinversión en productos y experiencia del usuario.	Los costos de mantenimiento de la plataforma pueden ser elevados, dependiendo de la complejidad del sistema.
Interacción con los clientes	Facilita la recopilación de comentarios y permite mejorar estrategias comerciales mediante redes sociales y marketing digital.	La falta de contacto físico puede afectar la confianza y lealtad de los consumidores.
Flexibilidad y adaptabilidad	Permite actualizar inventarios, modificar precios y lanzar promociones con facilidad.	La personalización de la experiencia del usuario requiere algoritmos sofisticados y análisis constante de datos.
Costos de envío y logística	Puede reducir costos operativos al optimizar la distribución de productos.	La gestión de envíos internacionales puede ser compleja y afectar la experiencia del consumidor debido a tiempos de entrega prolongados.

Realizado por: (Proscont, 2022)

2.2 Pasarelas de Pago

Las pasarelas de pago son sistemas diseñados para que los clientes puedan realizar transacciones en línea de una forma segura y eficiente. En el ámbito del comercio electrónico, estas plataformas son esenciales, ya que simplifican la compra de productos y servicios al encargarse de la validación y el procesamiento de los pagos digitales (Rodriguez, 2023).

Las pasarelas de pago, actuando como intermediarias entre compradores, vendedores y entidades bancarias, aseguran una experiencia fluida en las transacciones financieras. Al

realizar una compra en línea, el sistema verifica la disponibilidad de fondos en la cuenta del cliente y, una vez aprobado, transfiere el monto al comerciante, ofreciendo una confirmación inmediata de la operación.

Además de cumplir con su función principal, las pasarelas de pago cuentan con sofisticados mecanismos de seguridad, como el cifrado de datos y la autenticación de usuarios. Estos sistemas están diseñados para salvaguardar la información sensible y minimizar los riesgos de fraudes y accesos no autorizados. Su integración en el comercio digital ha permitido a las empresas optimizar sus procesos de pago, aumentar la confianza del consumidor y ampliar su presencia en mercados internacionales.

Tabla 2: Ventajas y Desventajas de las Pasarelas de Pago

Aspecto	Ventajas	Desventajas
Seguridad	Implementan tecnología de cifrado avanzada para proteger la información financiera y reducir fraudes.	Pueden ser vulnerables a ciberataques si no cuentan con medidas de seguridad adecuadas.
Comodidad	Permiten a los consumidores realizar compras en línea en cualquier momento y lugar, mejorando la accesibilidad.	Algunos usuarios pueden encontrar complicado el proceso de pago digital, especialmente si la plataforma no es intuitiva.
Rapidez	Agilizan las transacciones, reduciendo tiempos de espera para compradores y vendedores.	Si la pasarela de pago presenta fallos técnicos, el proceso de compra se ve afectado, causando retrasos.
Costos	Eliminan la necesidad de manejar efectivo, reduciendo ciertos costos operativos.	Cobran tarifas por transacción, lo que puede incrementar los costos para los comerciantes.
Accesibilidad	Facilitan la expansión de negocios al permitir pagos internacionales y en diversas plataformas.	Algunas pasarelas tienen restricciones en los tipos de tarjetas que aceptan, limitando las opciones de pago para los clientes.

Realizado por: (Rodriguez, 2023)

2.3 Framework

De acuerdo con investigadores de Unir, un framework es un concepto que ofrece una estructura fundamental para el desarrollo de proyectos con objetivos concretos. Es, en esencia, un modelo que sirve como punto de partida para la creación y gestión de software.

Un Framework puede simplificar una tarea o proceso. Por lo tanto, los marcos son una de las herramientas comunes utilizadas por los trabajadores digitales, ya que ayudan a aumentar la eficiencia y la productividad.

2.3.1 Framework de desarrollo móvil

El desarrollo móvil se ha convertido en un área fundamental en la actualidad, y seleccionar el framework adecuado puede influir significativamente en la eficiencia y calidad de las aplicaciones.

A continuación, detallaré algunos frameworks populares para el desarrollo móvil.

Tabla 3: frameworks populares para desarrollo móvil

Framework	Descripción	Ventajas
React Native	React Native es un framework de código abierto creado por Facebook. Puede crear aplicaciones móviles para Android e iOS utilizando JavaScript y React.	- Reutilización de código entre plataformas. - Comunidad activa y abundantes bibliotecas. - Rendimiento cercano al de aplicaciones nativas.
Flutter	Flutter es un framework de trabajo de Google que utiliza el lenguaje Dart para crear aplicaciones móviles para Android, iOS y la web.	- Interfaz de usuario atractiva y personalizable. - Rendimiento cercano al de aplicaciones nativas. - Hot reload para una rápida iteración de desarrollo.
Xamarin	Xamarin es un framework de Microsoft para desarrollar aplicaciones móviles utilizando C# y .NET.	- Reutilización de código entre plataformas. - Acceso completo a las API nativas. - Integración con Visual Studio.
NativeScript	NativeScript le permite crear aplicaciones móviles utilizando JavaScript o TypeScript. Proporciona acceso directo a las API nativas.	- Rendimiento cercano al de aplicaciones nativas. - Amplia comunidad y soporte.
Ionic	Ionic es un framework basado en web para crear aplicaciones móviles utilizando HTML, CSS y JavaScript. Se ejecuta en un WebView.	- Fácil desarrollo multiplataforma. - Amplia variedad de componentes y plugins.

Realizado por: Fausto Constante

2.3.2 Aplicaciones móviles

Las aplicaciones móviles han revolucionado la forma en que los usuarios acceden a información y servicios, estableciéndose como un elemento fundamental de la tecnología contemporánea. Su versatilidad facilita la interacción entre empresas y consumidores en tiempo real, sin importar la ubicación, lo que no solo mejora la eficiencia operativa, sino que también abre un abanico de nuevas oportunidades comerciales (Ortega, 2020). Además, el desarrollo de aplicaciones móviles ha sido moldeado por diversos patrones de arquitectura, diseñados para mejorar la escalabilidad, el mantenimiento y la seguridad de los sistemas.

Uno de los patrones recomendados en el desarrollo de aplicaciones nativas es Model-View-ViewModel (MVVM). Según Google, este enfoque permite una separación clara entre la interfaz de usuario y la lógica de negocio, mejorando la reutilización de código y la capacidad de prueba. Para facilitar su implementación, Google ha desarrollado un conjunto de bibliotecas que incluyen componentes diseñados específicamente para estructurar aplicaciones bajo este patrón, ofreciendo herramientas robustas para la gestión de datos y la interacción con la interfaz de usuario.

2.3.3 Patrones arquitectónicos MVVM, MVC, MVP, MVI

A partir del estudio de (Moskala, 2017) se elaboró una tabla comparativa de los patrones de diseño de arquitectura de software MVC, MVP, MVVM y MVI.

Tabla 4: Comparativa de los patrones de diseño

Patrón arquitectónico	Descripción	Ventajas	Desventajas
MVC	El patrón Modelo-Vista-Controlador separa la presentación y la lógica empresarial de una aplicación de su interfaz de usuario (UI).	- Gestionar las pruebas, el mantenimiento y el desarrollo de aplicaciones. - Mejorar enormemente las áreas de reutilización de código.	- esto puede resultar difícil de implementar en aplicaciones grandes. : Las vistas y los controladores están demasiado limitados.
MVP	El patrón Modelo-Vista-Presentador separa la lógica de presentación y negocios de una aplicación de su interfaz de usuario (UI).	- Gestionar las pruebas, el mantenimiento y el desarrollo de aplicaciones. - Mejorar enormemente las áreas de reutilización de código.	- Esto puede resultar difícil de implementar en aplicaciones grandes. - Se pueden combinar vista y presentador. .
MVVM	El patrón Modelo-Vista-Modelo de Vista separa la lógica de presentación y negocios de una aplicación de su interfaz de usuario (UI).	- Facilita la prueba, el mantenimiento y la evolución de una aplicación. - Mejora considerablemente las oportunidades de reutilización del código. - Permite una mejor separación de preocupaciones.	- Esto puede resultar difícil de implementar en aplicaciones grandes. - Difícil de entender para nuevos desarrolladores. .
MVI	El patrón Modelo-Vista-Intención separa la lógica de presentación y negocios de una aplicación de su interfaz de usuario (UI).	- Ayuda en las pruebas, mantenimiento y desarrollo de aplicaciones. - Mejorar enormemente las áreas de reutilización de código. - Aislar mejor los problemas.	: esto puede resultar difícil de implementar en aplicaciones grandes. : Difícil de entender para los nuevos desarrolladores.

2.4 Arquitectura MVVM

La arquitectura MVVM (Model-View-ViewModel) es un patrón de diseño de software que promueve la separación entre la interfaz de usuario (UI) y la lógica empresarial de una

aplicación. Este enfoque no solo facilita la mantenibilidad y escalabilidad del software, sino que también mejora las pruebas, abordando así varios desafíos comunes en el desarrollo de aplicaciones, según lo señalan investigadores de (microsoft, 2023).

MVVM se fundamenta en tres componentes esenciales:

Modelo (Model): Este componente representa los datos y la lógica de negocio de la aplicación, ocupándose del acceso a la información y de la gestión de los procesos internos.

Vista (View): Se refiere a la interfaz de usuario, la cual se encarga de presentar los datos y de captar las interacciones de los usuarios.

Modelo de Vista (ViewModel): Este elemento actúa como un intermediario entre el modelo y la vista, gestionando la lógica de presentación y garantizando la sincronización entre la interfaz y los datos.

Adoptar este patrón de diseño favorece la reutilización de código, simplifica la colaboración entre desarrolladores y diseñadores de interfaces, y permite estructurar aplicaciones de manera modular y eficiente. Google avala el uso de MVVM para el desarrollo de aplicaciones nativas y ha creado un conjunto de bibliotecas especializadas que optimizan su implementación, ofreciendo herramientas clave para la gestión de datos y el diseño de la interfaz de usuario.

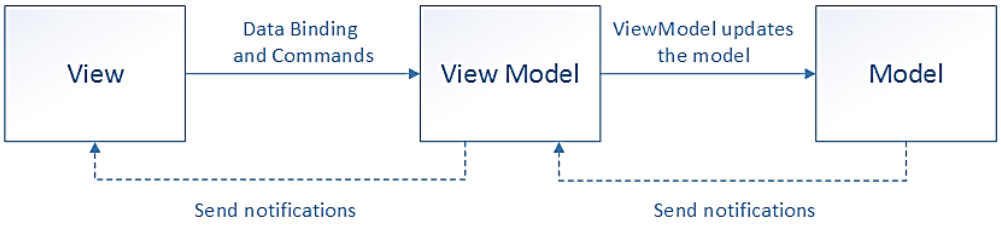


Figura 1: Componentes principales de MVVM
Fuente: (microsoft, 2023)

2.4.1 Ventajas de la Arquitectura MVVM

El patrón MVVM (Modelo-Vista-VistaModelo) se presenta como una arquitectura de diseño muy efectiva para organizar la interacción entre la lógica de negocio y la interfaz de usuario de manera eficiente. Los investigadores de (microsoft, 2023) resaltan varias ventajas clave de este enfoque:

1. Mejora en la separación de responsabilidades: La interfaz de usuario se gestiona de forma independiente a la lógica de negocio, lo que conduce a aplicaciones más limpias y modulares.

2. Facilita pruebas y mantenimiento: Al desacoplar la lógica de presentación de la lógica de negocio, se simplifican las pruebas y el mantenimiento del código.
3. Reutilización de código: Este patrón promueve la creación de componentes que pueden ser reutilizados en diferentes secciones de una misma aplicación e incluso en múltiples proyectos.
4. Colaboración más efectiva: Gracias a la clara distinción entre la estructura del modelo y la vista, desarrolladores y diseñadores pueden trabajar de manera paralela, optimizando así el proceso de desarrollo.

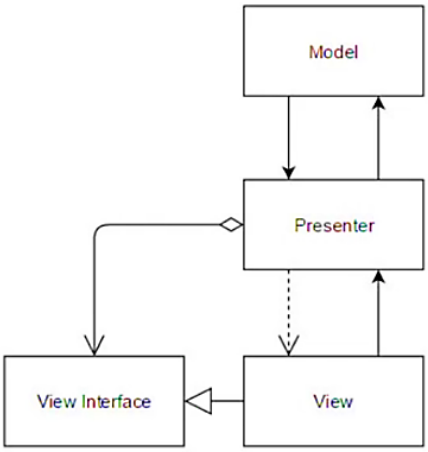


Figura 2: Funcionalidad de los componentes de MVVM
Fuente: *(microsoft, 2023)*

2.4.2 Componentes de la Arquitectura MVVM

Los componentes de la arquitectura MVVM (Model-View-ViewModel) según (microsoft, 2023) se basa en tres componentes esenciales: el modelo, la vista y el modelo vista controlador. Cada uno de estos elementos desempeña un papel específico y se interrelaciona de tal manera que se asegura una división clara de responsabilidades.

Tabla 5: Componentes de MVVM

Componente	Descripción	Funciones principales
Modelo	Representa los datos y la lógica empresarial de la aplicación.	- Recuperar y almacenar datos. - Proporcionar una interfaz para que el modelo de vista acceda a los datos.
Vista	Es la interfaz gráfica de usuario que muestra datos al usuario e interactúa con él.	- Presentar los datos al usuario. - Facilitar la interacción entre el usuario y la aplicación.
Modelo vista controlador	Actúa como intermediario entre el modelo y la vista, gestionando la lógica empresarial y la presentación.	- Transformar los datos del modelo para que sean adecuados en la vista. - Manejar interacciones del usuario y reflejarlas en el modelo.

2.4.3 Mejores Prácticas de la Arquitectura MVVM

De acuerdo con (microsoft, 2023), las siguientes son algunas de las mejores prácticas recomendadas para implementar cada componente de la arquitectura MVVM:

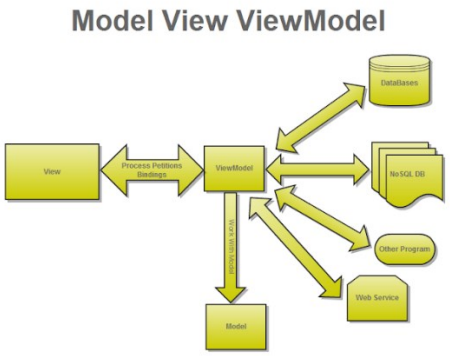


Figura 3: (MVVM) Model - View - ViewModel
Fuente: *(microsoft, 2023)*

Modelo:

- Debe estar completamente separado de la vista y del modelo de vista.
- Proporcionar una interfaz clara y consistente para facilitar el acceso a los datos desde el modelo de vista.
- Ser reutilizable y fácil de ampliar para admitir cambios futuros.

Vista:

- Debe ser independiente tanto del modelo como del modelo de vista.
- Diseñarse para ser fácilmente configurable y ampliable.
- Ser sencilla de probar y depurar, lo que facilita el mantenimiento del sistema.

Modelo de vista:

- Debe operar de forma independiente de la vista base para mantener la separación de responsabilidades.
- Proveer una interfaz clara y coherente para que las vistas accedan a los datos y la lógica de presentación.
- Diseñarse para ser reutilizable y fácilmente adaptable a nuevos requisitos.

2.4.4 Importancia de MVVM en Seguridad de Pasarelas de Pagos B2C

Según los investigadores de (microsoft, 2023) y la especialista en seguridad Marisol Morelos, la arquitectura MVVM (Model-View-ViewModel) es ampliamente utilizada en el

desarrollo de aplicaciones móviles. Esta arquitectura es particularmente útil en el contexto de las pasarelas de pagos de comercio electrónico B2C debido a sus capacidades para separar responsabilidades y gestionar la seguridad (Morelos, 2023).

Tabla 6: Importancia de MVVM con B2C

Aspecto	Descripción	Beneficios Clave
Separación de preocupaciones	MVVM permite una separación clara entre la lógica de presentación (vistas) y la lógica de negocios (modelos).	- Evitar que datos confidenciales, como información financiera, sean accesibles desde la interfaz de usuario. - Facilitar medidas de seguridad específicas por capa.
Seguridad de datos sensibles	Garantiza la protección de los datos de los clientes durante los métodos de pago.	- Separar la lógica empresarial del código de la interfaz de usuario. - Minimizar el riesgo de exposición accidental de datos.
Pruebas unitarias y seguridad	Permite realizar pruebas unitarias en la lógica empresarial y el modelo de vista sin depender de la interfaz gráfica.	- Validar la seguridad de las transacciones de pago. - Garantizar que el modelo de vista cumpla con los estándares de seguridad.

Además, se destaca que la ciberseguridad cobra mayor relevancia en el contexto de la acelerada digitalización, generando oportunidades tanto para grandes empresas como para emprendedores en el ámbito del comercio electrónico.

2.5 Norma ISO 27001

La norma internacional ISO 27001, según los investigadores de la Escuela Europea de Excelencia, está diseñada para proteger tanto la información física como la digital. Su objetivo principal es garantizar una gestión eficaz de la seguridad de la información en las empresas (Escuelaeuropeaexcelencia, 2022).

2.6 Importancia de ISO 27001 en Pasarelas de Pago

De acuerdo con (Escuelaeuropeaexcelencia, 2022), Las pasarelas de pago en el comercio electrónico B2C manejan datos financieros sensibles, como números de tarjetas de crédito y transacciones. La seguridad de estas pasarelas es crucial para:

Tabla 7: ISO 27001 aplicada a pasarelas de pagos

Aspectos Claves	Descripción
Protección de la confianza del cliente	Garantizar que los clientes se sientan seguros al compartir información financiera.
Cumplimiento normativo	La ISO 27001 proporciona un marco para gestionar riesgos de seguridad en las pasarelas de pago.

2.6.1 Beneficios de utilizar ISO 27001 en pasarelas de pago

Tabla 8: Beneficios de la ISO para pasarelas de pagos

Beneficio	Descripción
Gestión integral de riesgos	Ayuda a identificar, evaluar y mitigar riesgos de seguridad en los canales de pago.
Cumplimiento de regulaciones	Demuestra el compromiso con la seguridad de la información y facilita el cumplimiento de requisitos legales.
Mejora continua	Promueve la adaptación y el fortalecimiento de controles de seguridad frente a nuevas amenazas.

2.7 OWASP ZAP (Zed Attack Proxy)

OWASP ZAP es una herramienta gratuita y de código abierto creada para detectar vulnerabilidades en aplicaciones web y móviles. Su utilidad se destaca en la evaluación de la seguridad de pasarelas de pago, ya que facilita la simulación de ataques en el flujo de datos y en las comunicaciones entre la aplicación y el servidor (Venera, 2024).

- **Análisis Automatizado y Manual:** Realiza un escaneo automático de las interacciones entre la aplicación móvil y la pasarela de pago, con el objetivo de identificar vulnerabilidades como la exposición de datos sensibles y fallos en la autenticación. Además, ofrece herramientas manuales avanzadas que permiten a los desarrolladores realizar pruebas específicas con mayor profundidad (Venera, 2024).
- **Interceptación de Tráfico HTTP/HTTPS**: Facilita el análisis de las solicitudes y respuestas de las APIs utilizadas por la aplicación en conjunto con las pasarelas de pago. Esto es fundamental para asegurar que los datos confidenciales, tales como credenciales de usuario o tokens de autenticación, se encuentren debidamente cifrados (Venera, 2024).
- **Compatibilidad con Pruebas de APIs REST:** Dado que muchas pasarelas de pago operan mediante APIs REST, OWASP ZAP se encuentra capacitado para examinarlas en busca de configuraciones incorrectas, como la ausencia de autenticación o autorización adecuadas (Venera, 2024).
- **Integración con Metodologías Ágiles:** Se adapta fácilmente al proceso de desarrollo, garantizando que las vulnerabilidades sean detectadas y corregidas antes de que se realice el despliegue (Venera, 2024).

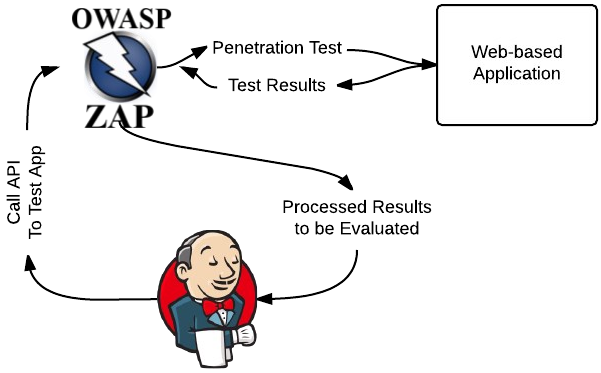


Figura 4: Funcionamiento de OWASP Zap
Obtenido de: https://devopedia.org/owasp-zap

En una arquitectura MVVM, en la que la ViewModel se conecta con APIs externas, OWASP ZAP desempeña un papel crucial al identificar posibles riesgos en los datos que se envían desde el Model hacia la pasarela de pago. Este proceso de identificación se alinea con los controles de seguridad establecidos en la norma ISO 27001.

CAPÍTULO III. METODOLOGIA.

3.1 Metodología

El objetivo del proyecto de investigación es desarrollar una aplicación móvil de pasarelas de pago orientada a procesos e-commerce B2C en PYMES, aplicando la arquitectura Model-View-ViewModel (MVVM). Esta investigación utilizará herramientas adaptadas para evaluar el cumplimiento de las métricas de seguridad establecidas por la norma ISO 27001.

3.2 Enfoque

El enfoque de la investigación es cuantitativo. Este enfoque permitirá medir el rendimiento y la seguridad del sistema, utilizando herramientas específicas que evalúan métricas relacionadas con ISO 27001, proporcionando datos objetivos sobre la eficiencia, escalabilidad y seguridad de la aplicación móvil.

3.3 Método de la investigación

El método aplicado será deductivo, partiendo de un análisis teórico y estructurado de arquitecturas de software, como MVVM, y de normativas internacionales como ISO 27001. El desarrollo permitirá arribar a conclusiones prácticas basadas en la implementación de controles de seguridad en las pasarelas de pago.

3.4 Tipo de investigación

La investigación será de tipo bibliográfica-documental. Se recopilará y analizará información relevante a través de libros, artículos académicos, revistas científicas y foros especializados que respalden los conceptos relacionados con pasarelas de pago, ISO 27001 y la arquitectura MVVM.

3.5 Técnicas de recolección de datos

Para recopilar datos se utilizará la siguiente técnica:

- Pruebas de rendimiento y seguridad: Se utilizará una herramienta especializada que evalúe métricas de seguridad y rendimiento, alineadas con ISO 27001. La herramienta considerada es OWASP ZAP, para analizar riesgos y detectar vulnerabilidades críticas en el sistema.

3.6 Población y muestra

La población es infinita debido al alcance teórico de la investigación, pero los datos experimentales serán obtenidos mediante pruebas que serán realizadas con la herramienta de

evaluación OWASP. Esta herramienta generará la métrica como tiempos de respuesta, detección de vulnerabilidades y cumplimiento de las medidas de seguridad de la norma ISO 27001.

3.7 Identificación de variables

3.7.1 Variable independiente

Aplicación móvil utilizando la arquitectura MVVM

3.7.2 Variable Dependiente

Seguridad de pasarelas de pago para procesos e-commerce B2C en PYMES.

3.8 Operación con variables

Tabla 9: Operaciones con variables

PROBLEMA	TEMA	OBJETIVOS	VARIABLES	CONCEPTUALZACION	DIMENSION	INDICADORES
¿Cómo el uso de la Arquitectura MVVM incidirá en la seguridad de la Aplicación móvil de pasarela de pagos para procesos e-commerce B2C para PYMES?	APLICACIÓN MOVIL DE PASARELA DE PAGOS PARA PROCESOS E-COMMERCE B2C EN PYMES, UTILIZANDO LA ARQUITECTURA MVVM.	GENERAL Implementar una aplicación móvil de pasarela de pagos para procesos e-commerce B2C para las PYMES, utilizando la arquitectura MVVM.	INDEPENDIENTE Aplicación Móvil.	Las aplicaciones móviles funcionan como programas de software diseñados específicamente para dispositivos móviles. Utilizan los recursos del dispositivo, como el procesador, la memoria y las conexiones a Internet, para ofrecer diversas funcionalidades.	Desarrollo software	Independiente: • Tiempo de desarrollo • Número de líneas de código •Número de funcionalidades
		ESPECIFICOS • Investigar el desarrollo de aplicaciones móviles utilizando la arquitectura MVVM. • Desarrollar la aplicación móvil para procesos e-commerce B2C para las PYMES. • Evaluar la seguridad de la información en las pasarelas de pago en la aplicación móvil para procesos e-commerce utilizando la NORMA ISO 27001	DEPENDIENTE Seguridad de pasarelas de pago utilizando MVVM para procesos E-commerce B2C en PYMES	• La seguridad de pago en pasarelas de pago se refiere a las medidas de seguridad implementadas en las plataformas de pago en línea para proteger la información financiera y personal de los clientes durante las transacciones en línea. • MVVM permite aislar la lógica de negocios (donde se manejan los datos) del código de la interfaz de usuario. • La Norma ISO es una serie de estándares internacionales que establecen directrices y requisitos para garantizar la calidad, seguridad y eficiencia en diversos campos para lo cual se utilizara OWASP que es un proyecto de código abierto dedicado a determinar y combatir las causas que hacen que el software sea inseguro.	Seguridad	Dependiente: • # de vulnerabilidades • % cumplimiento de controles ISO 27001 • Nivel de robustez de cifrado de datos sensibles

3.9 Desarrollo de la aplicación

Para la creación de la aplicación, se comenzó con la instalación y ajuste de las herramientas necesarias para asegurar un entorno de trabajo adecuado. La imagen mostrada ofrece un esquema del proceso, subrayando las etapas esenciales en la elaboración del sistema de entrega móvil.

En la primera fase, se utilizó Visual Studio Code junto con el entorno de React Native, lo que permitió organizar la interfaz y aplicar funcionalidades utilizando componentes que se pueden reutilizar. Luego, se incorporaron Android Studio y Expo Go, herramientas clave para la visualización, diagnóstico y prueba de la aplicación en dispositivos móviles.

Finalmente, se añadió Node.js como entorno de ejecución para el backend, lo que facilita la conexión con bases de datos y la administración de solicitudes del servidor. Esta metodología de trabajo asegura un desarrollo eficaz y continuo, permitiendo llevar la aplicación desde su diseño inicial hasta su funcionamiento práctico en un entorno real.

Figura 5: Flujo de Desarrollo de la Aplicación Móvil para Delivery

Se usó la metodología SCRUM para el desarrollo de la aplicación móvil, que está orientada para el comercio e-commerce que ayude a las PYMES, la misma que está integrada por cinco fases a ejecutarse en el siguiente Sprint realizado conforme al modelo en cascada. y que a continuación se describen las actividades realizadas en cada una:

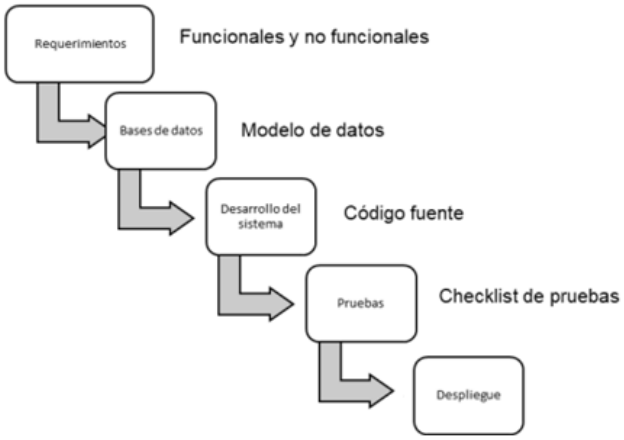


Figura 6: Fases del proyecto realizadas por Sprint

3.9.1 Requerimientos

En la fase de planificación se consideró el análisis de requerimientos para el desarrollo del proyecto de investigación, el cual busca proporcionar a las pequeñas y medianas empresas (PYMES) una solución eficiente para la integración de pasarelas de pago en procesos E-commerce B2C mediante una aplicación móvil. El objetivo principal es superar la problemática detectada en los procesos de pago actuales de las PYMES, como limitaciones en la seguridad, baja eficiencia en la experiencia de usuario y falta de integración con métodos de pago modernos.

Requerimientos funcionales

Los requerimientos funcionales están definidos por las funcionalidades que debe cumplir el módulo, las cuales se determinaron en conjunto con los diferentes stakeholders.

Tabla 10: Requerimientos funcionales

Identificación	Nombre	Descripción	Prioridad
RF01	Registro de usuarios	El usuario podrá registrarse proporcionando su información personal y de contacto.	Alta
RF02	Inicio de sesión seguro	El usuario podrá iniciar sesión utilizando credenciales verificadas o autenticación social.	Alta
RF03	Selección de productos	El usuario podrá navegar por el catálogo y seleccionar productos para su pedido.	Alta
RF04	Carrito de compras	El usuario podrá añadir y gestionar productos en su carrito antes de realizar la compra.	Alta

RF05	Opciones de pago	El usuario podrá realizar pagos utilizando diferentes pasarelas de pago, como tarjetas de crédito, débito, etc.	Alta
RF06	Seguimiento de pedidos	El usuario podrá ver en tiempo real el estado y la ubicación de su pedido.	Alta
RF07	Gestión de direcciones	El usuario podrá guardar y editar múltiples direcciones de entrega.	Alta

Requerimientos no funcionales

Los requisitos no funcionales describen criterios del funcionamiento general de la aplicación móvil, estos requisitos comprenden características de seguridad, disponibilidad, compatibilidad, etc.

Tabla 11: Requerimientos no funcionales

Identificación	Nombre	Descripción	Prioridad
RNF01	Disponibilidad	La aplicación debe estar disponible el 99.9% del tiempo para garantizar un servicio confiable a los usuarios.	Alta
RNF02	Seguridad	Todos los datos sensibles, como las credenciales y la información de tarjetas de crédito, deben cifrarse mediante TOKENS.	Alta
RNF03	Compatibilidad	La aplicación debe ser compatible con dispositivos Android e iOS en versiones recientes (al menos las últimas dos versiones).	Alta
RNF04	Escalabilidad	La aplicación debe manejar picos de usuarios simultáneos sin degradar significativamente el rendimiento.	Alta
RNF05	Experiencia de usuario (UX)	La interfaz debe ser intuitiva, con un diseño limpio y funcional, optimizado para pantallas móviles de diferentes tamaños.	Alta
RNF06	Consumo de batería	La aplicación debe ser eficiente y minimizar el impacto en el consumo de batería del dispositivo.	Media

3.9.2 Base de Datos

Para la elaboración del modelo de datos, se esquematizaron las necesidades del módulo de gestión de pedidos y logística, tomando como referencia el sistema previamente establecido, con el objetivo de optimizar la eficiencia y funcionalidad del servicio de entrega.

Se identificaron y clasificaron los atributos esenciales para la estructuración de las tablas necesarias dentro del sistema de delivery, garantizando la integración adecuada de información relacionada con clientes, pedidos, repartidores y productos.

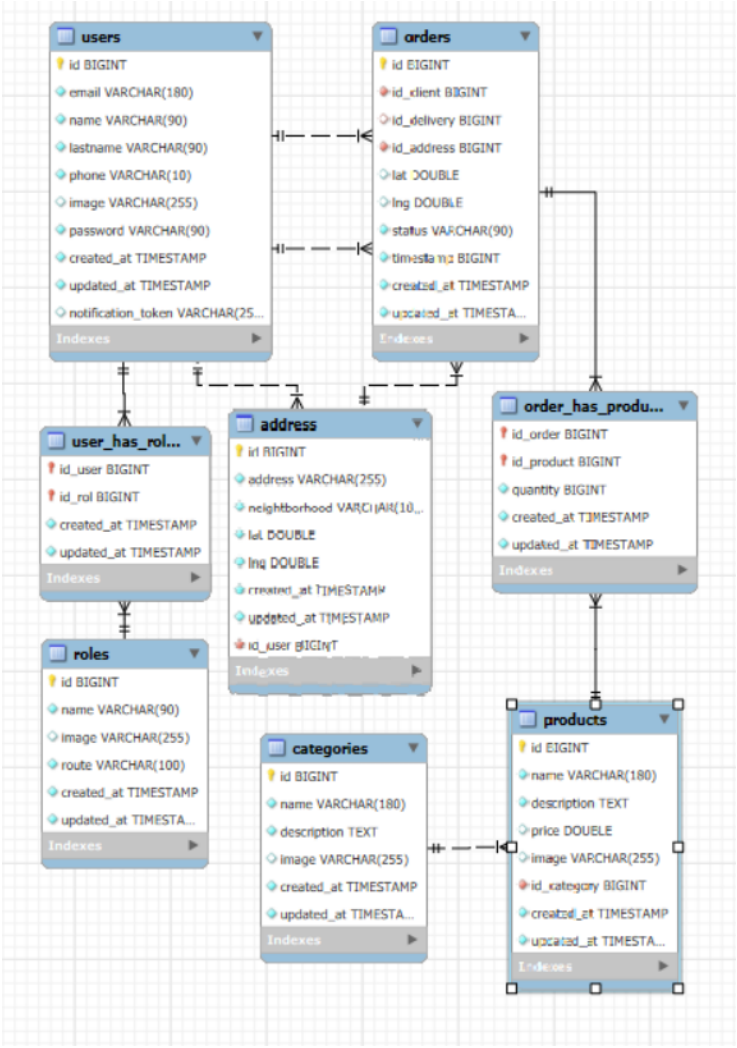


Figura 7: Diagrama Entidad Relación

3.9.3 Desarrollo del código Fuente

El desarrollo del proyecto comenzó con la configuración del entorno de desarrollo en Visual Studio Code, utilizando React Native para la implementación de la aplicación móvil. Para las pruebas, se empleó un dispositivo físico, lo que permitió evaluar el comportamiento real de la aplicación en condiciones de uso concretas.

Además, se instaló Expo-CLI en el entorno de desarrollo, facilitando la visualización de cambios en tiempo real y el acceso a un puerto específico desde el cual se monitoreó el funcionamiento

de la aplicación. Esto permitió una evaluación detallada de las modificaciones implementadas a lo largo del proceso de desarrollo.

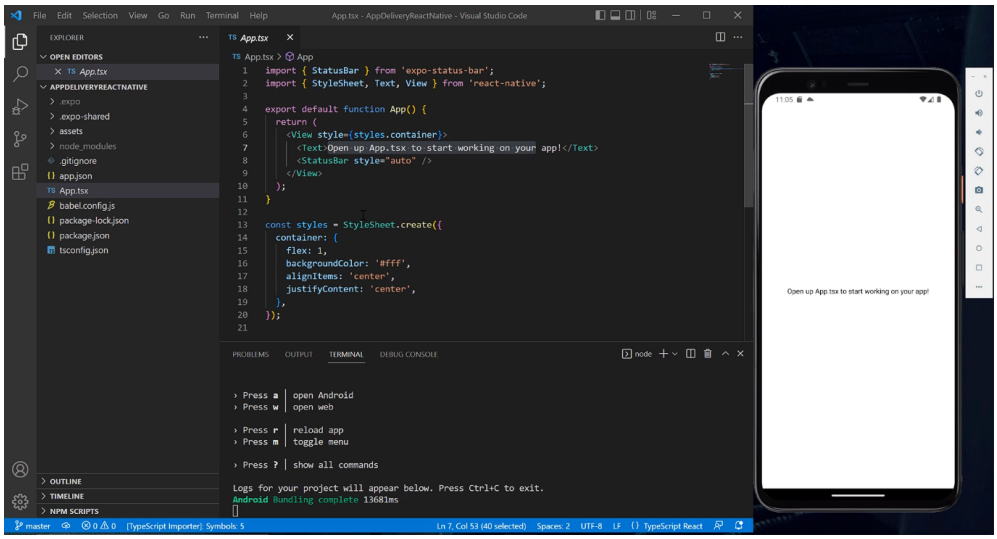


Figura 8: Entorno de desarrollo e instalación de expo-cli

Una vez ejecutado el sistema, se procede a configurar los stacks de navegaciones internos que serán utilizados por el usuario.

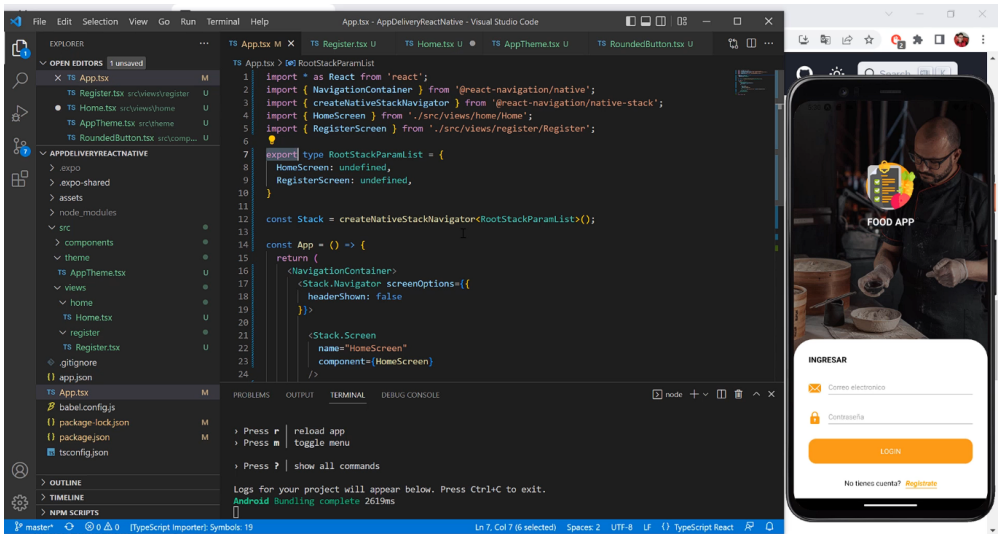


Figura 9: Implementación de los StackNavigations

Una vez completada la configuración del entorno de desarrollo, se procede con la configuración del servidor. En esta etapa, el servidor es parametrizado para gestionar y procesar eficientemente toda la información proveniente de la aplicación, asegurando una comunicación fluida entre el sistema y los datos transmitidos.

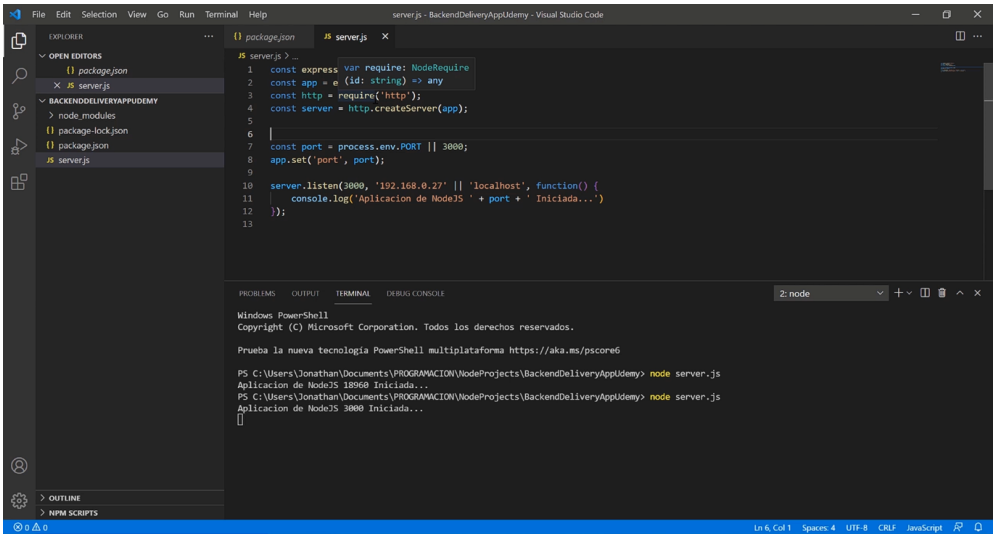


Figura 10: Creación del servidor en NodeJS

Una vez que se completó la configuración del servidor, se procedió con la implementación del gestor de base de datos. En esta etapa, se configuró MySQL para garantizar el almacenamiento eficiente de la información procesada por el servidor, optimizando la gestión de datos y la accesibilidad de los registros dentro del sistema.

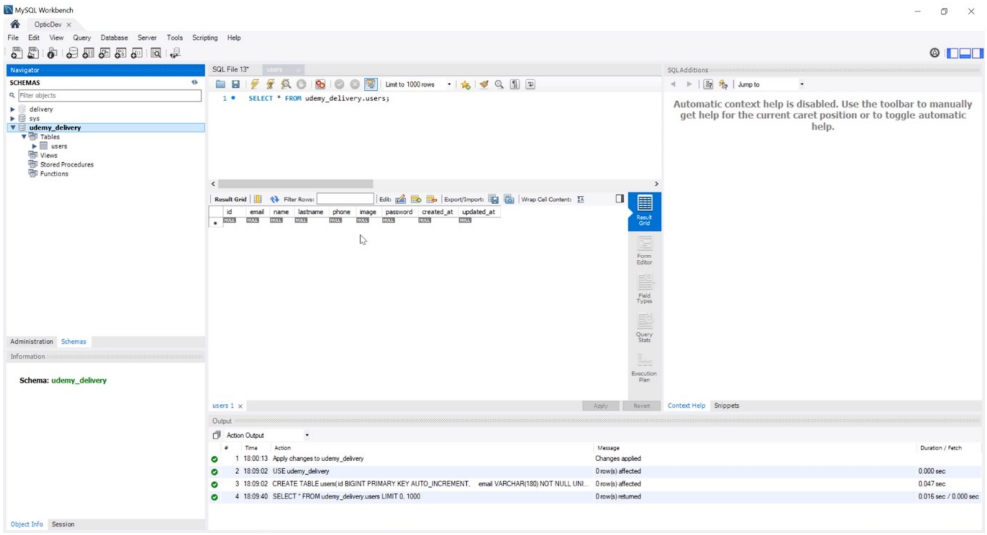


Figura 11: MYSQL y la creación de su primera tabla

3.9.4 Implementación y desarrollo de la aplicación

Autenticación y gestión de usuarios

Se implementó la distribución de MVVM junto con Clean Architecture con el objetivo de estructurar la aplicación y aplicar buenas prácticas de desarrollo. Asimismo, se llevó a cabo la

distribución de funciones según los principios de MVVM, organizándolas en sus respectivas capas y asegurando el cumplimiento de protocolos de seguridad.

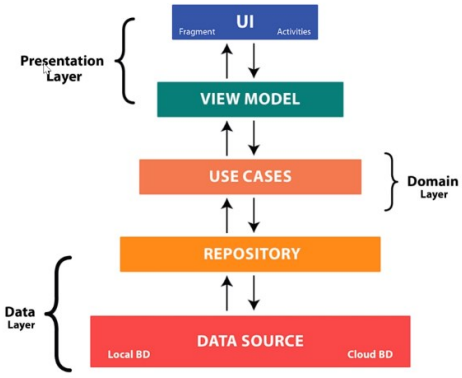


Figura 12: Distribución de las capas de MVVM

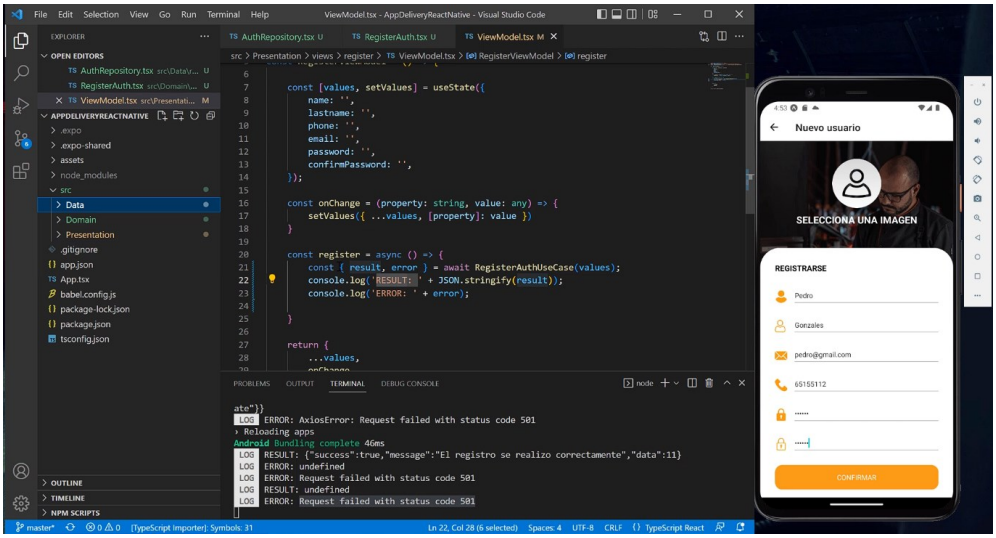


Figura 13: Aplicación de MVVM

Una vez aplicada la arquitectura MVVM, se procedió con la implementación de un sistema de seguridad para el usuario. Se encriptó su clave de acceso antes de almacenarla en la base de datos, garantizando la protección de los datos sensibles. Además, se generó un JWT (JSON Web Token) para establecer un sistema de autenticación robusto, alineado con la ISO 27001, con el objetivo de asegurar la integridad y confidencialidad de la información.

Para ello, se instalaron los siguientes paquetes en el entorno de desarrollo:

- npm i passport (para la gestión de autenticación de usuarios).
- npm i passport-jwt (para la validación de tokens JWT en el proceso de autenticación).
- npm i jsonwebtoken (para la generación y verificación de JWT)

Esta estructura técnica optimiza la seguridad del sistema, cumpliendo con estándares internacionales de protección de datos.

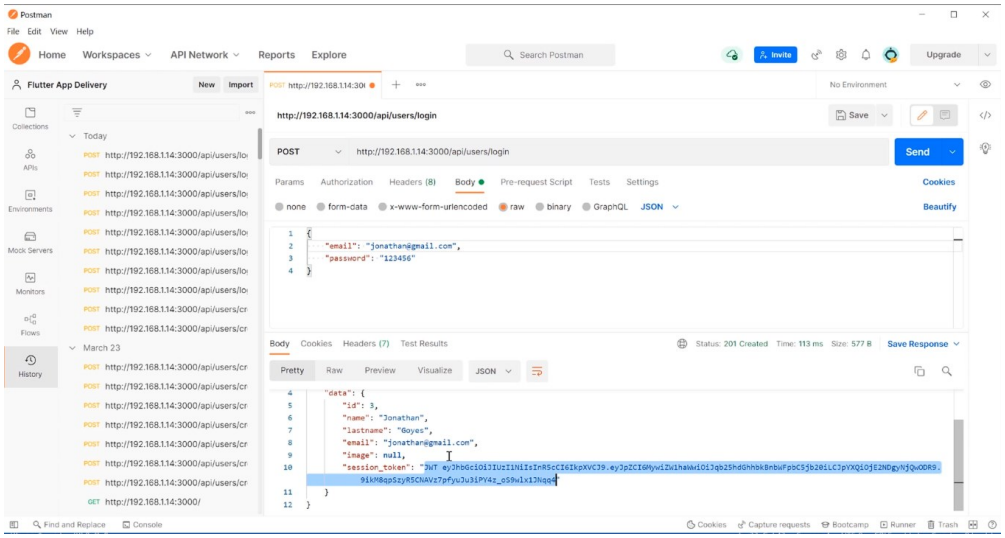


Figura 14: Postman y la visualización del JWT

Vista de gestión de usuarios

La aplicación permite el registro de nuevos usuarios directamente desde la pantalla de **login**. Durante el proceso de registro, cada usuario es asignado por defecto con el rol de **cliente**, asegurando un acceso adecuado a las funcionalidades destinadas a este tipo de usuario dentro del sistema.

Para gestionar los distintos niveles de acceso y roles en la plataforma, se implementa un sistema de control basado en permisos, lo que permite una administración eficiente y segura de las cuentas registradas.

Figura 15: Vista de registro de Usuario

Vista de rol

Una vez que el usuario completa el proceso de registro, inicia sesión en la aplicación, accediendo a la interfaz de selección de rol. Dado que la asignación de roles es una función exclusiva del administrador, la vista de rol varía según el tipo de usuario.

- Clientes: Al iniciar sesión, visualizan únicamente las opciones y funcionalidades permitidas para su rol, manteniendo acceso restringido a configuraciones administrativas.

- Administradores: Cuentan con permisos para gestionar roles, pudiendo modificar y asignar privilegios a los usuarios dentro del sistema.

Este enfoque garantiza una separación clara de responsabilidades y un control preciso sobre los niveles de acceso dentro de la aplicación.

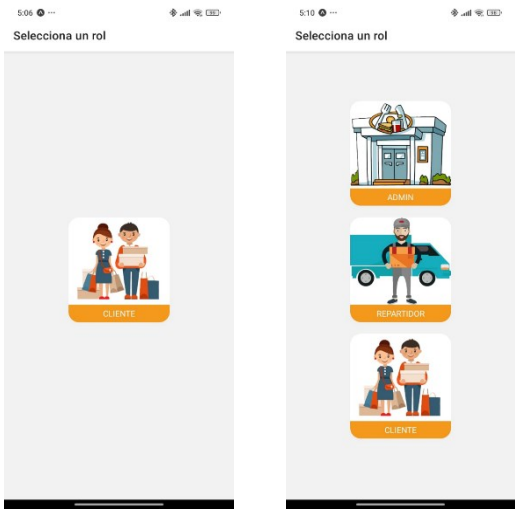


Figura 16: Vista Roles cliente vs admin

Vista de categoría

Una vez que el usuario elige su rol, accede a la interfaz de selección de categoría de productos. Sin embargo, el rol de repartidor no dispone de esta opción, ya que su función se limita exclusivamente a la entrega de los productos solicitados por los clientes.

Por otro lado, el administrador cuenta con una vista diferenciada, que le permite gestionar y registrar nuevas categorías de productos dentro del sistema. Esta configuración garantiza una distribución clara de responsabilidades y optimiza la operatividad del servicio de delivery.

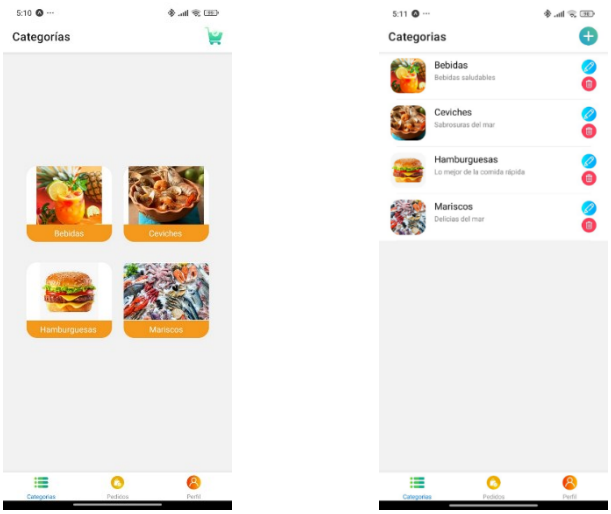


Figura 17: Vista de Categorías cliente vs admin

Vista de productos

Una vez que el usuario elige la categoría, accede a la pantalla de selección de productos. Para el cliente, la interfaz presenta un listado con información básica de cada producto, permitiéndole ingresar a la vista detallada para consultar características específicas antes de realizar una compra.

Por otro lado, el administrador dispone de una vista diferente, que le permite registrar, editar y eliminar productos dentro del sistema. Esta configuración garantiza un control eficiente de la base de datos de productos, asegurando una gestión dinámica y organizada.

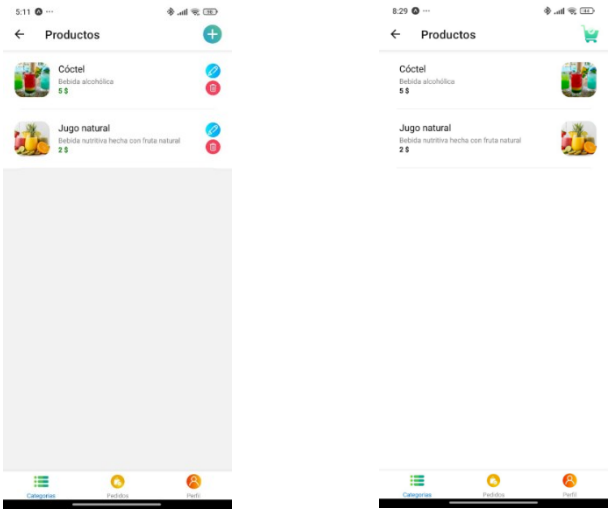


Figura 18: Vista de Productos cliente vs admin

Vista de órdenes

Una vez que el usuario selecciona los productos, accede al módulo de órdenes, donde se visualiza un listado con los artículos elegidos. En esta interfaz, el usuario tiene la opción de modificar la cantidad de cada producto antes de proceder con la compra.

Además, se muestra de manera dinámica el valor total a pagar, reflejando cualquier cambio realizado en las cantidades seleccionadas. Finalmente, el usuario cuenta con la opción de confirmar la orden, asegurando que el proceso de compra se complete de manera eficiente dentro del sistema.

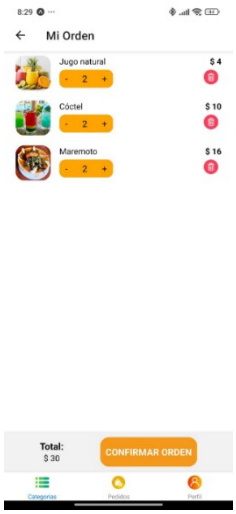


Figura 19: Vista del módulo órdenes

Vista de direcciones

Una vez confirmada la orden, el usuario accede al módulo de direcciones, donde puede visualizar las ubicaciones previamente registradas. En esta sección, tiene la posibilidad de editar sus direcciones existentes o agregar nuevas, definiendo el punto de entrega para el servicio de delivery.

Además, el sistema permite la geolocalización de las direcciones en el mapa, garantizando una mayor precisión en la entrega y optimizando la experiencia del usuario.

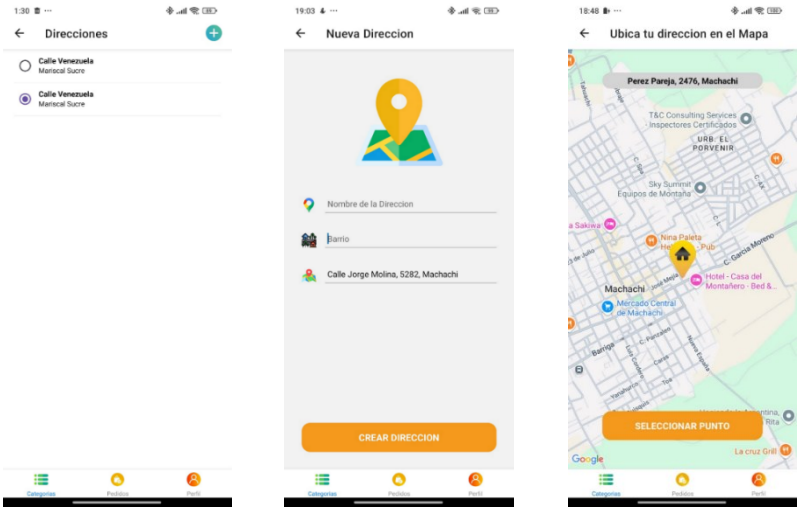


Figura 20: Vista del Módulo de Direcciones

Vista del formulario de pago

Tras confirmar la orden, el usuario accede al módulo de pagos, donde puede ingresar los datos de su tarjeta de crédito o débito. La información proporcionada es validada de manera segura a través de la pasarela de pagos Stripe, garantizando la integridad de la transacción y la protección de los datos financieros.

El sistema incorpora mecanismos de autenticación y cifrado para asegurar un proceso de pago confiable y eficiente, optimizando la experiencia del usuario dentro de la aplicación.

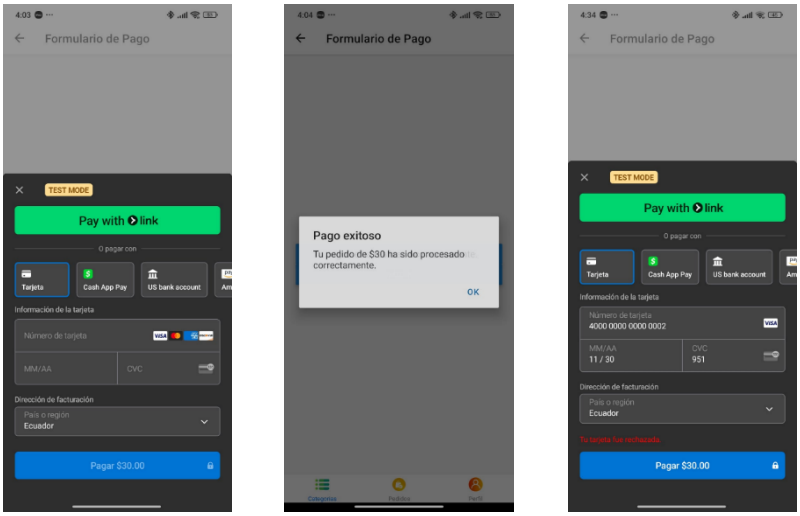


Figura 21: Vista del Formulario de pagos

Vista del módulo de delivery

Una vez confirmado el pago, el pedido es registrado en el módulo de delivery, donde se gestionan sus diferentes estados: "PAGADO", "DESPACHADO", "EN CAMINO" y "ENTREGADO".

El administrador tiene la capacidad de asignar un repartidor responsable de la entrega del pedido. Una vez seleccionado, el sistema permite despachar el pedido, asegurando un flujo de distribución eficiente y controlado.

Este proceso garantiza un seguimiento claro del estado de los pedidos, optimizando la logística y la experiencia del usuario.

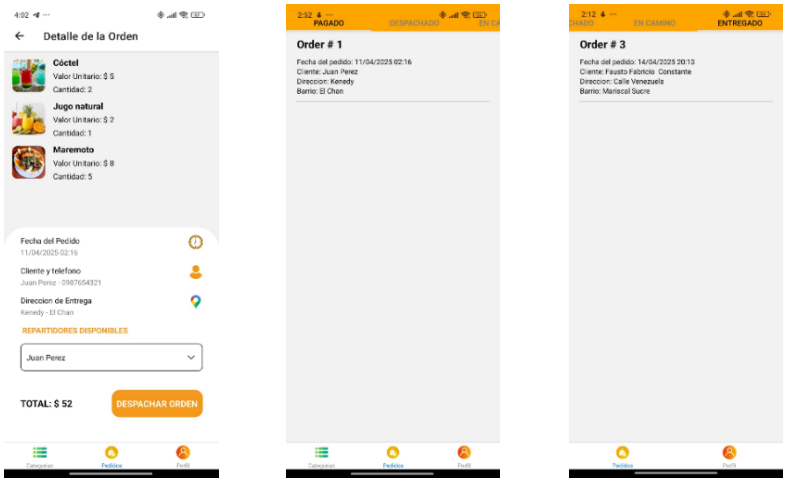


Figura 22: *Vista del Módulo Delivery*

Vista del módulo de delivery para el repartidor

Una vez que el administrador asigna el repartidor y despacha la orden, el repartidor accede al módulo de delivery, donde puede visualizar los pedidos en uno de los siguientes estados: "DESPACHADO", "EN CAMINO" y "ENTREGADO".

A medida que avanza en el proceso de entrega, el repartidor actualiza el estado del pedido, lo que permite al usuario hacer un seguimiento en tiempo real de la ubicación y progreso de su solicitud hasta la confirmación de la entrega.

Este sistema optimiza la gestión de envíos y mejora la experiencia del usuario, proporcionando transparencia y eficiencia en el servicio de delivery.

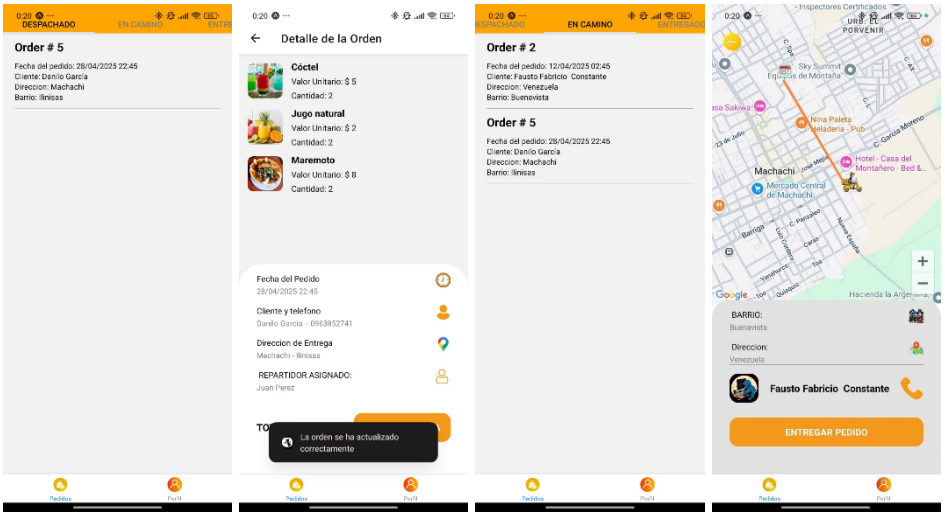


Figura 23: Vista del Módulo Delivery para el Repartidor

Vista del API/REST

La implementación del API REST se realizó de manera continua, utilizando Postman para verificar la comunicación entre la aplicación móvil y el servidor. A través de estas pruebas, se comprobó la correcta transmisión de datos y la integridad de las respuestas obtenidas.

Además, la aplicación de estos protocolos garantiza que todos los dispositivos conectados puedan realizar peticiones y obtener resultados uniformes, asegurando la interoperabilidad y el acceso eficiente a la información dentro del sistema.

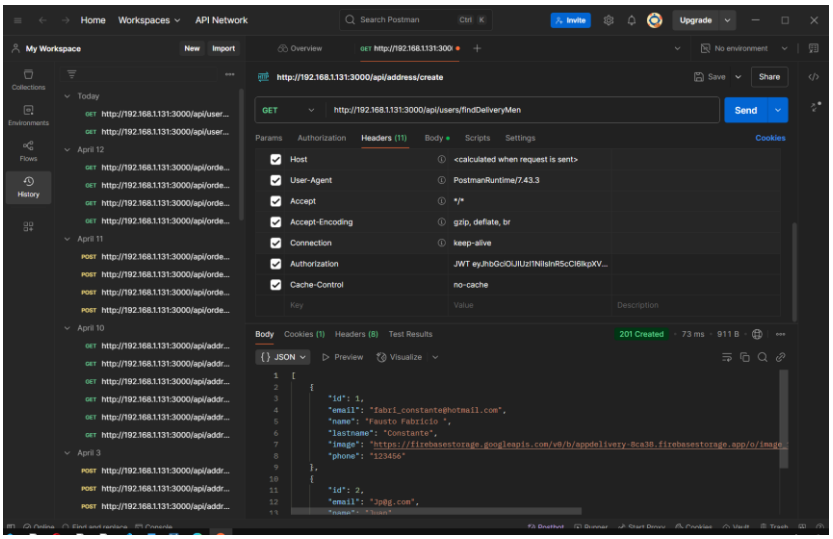


Figura 24: Peticiones con Postman

3.9.5 PRUEBAS

Una vez finalizado el desarrollo, se realizaron pruebas de seguridad en las pasarelas de pago, utilizando la herramienta OWASP para la evaluación de posibles vulnerabilidades. Durante este proceso, se definieron las rutas específicas de las pasarelas con el propósito de identificar riesgos y puntos críticos en la protección de los datos transaccionales.

El análisis permitió verificar si la implementación de la arquitectura MVVM cumple con los estándares de seguridad establecidos por la ISO 27001, garantizando la integridad y confidencialidad de la información financiera dentro del sistema.

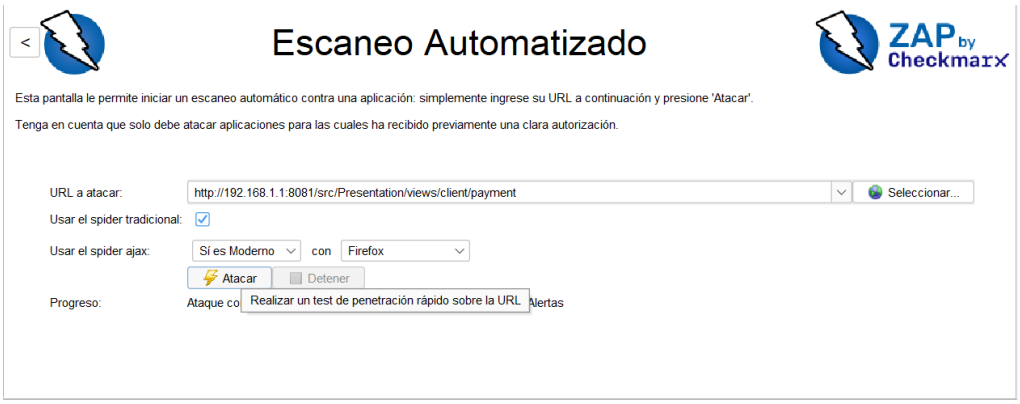


Figura 25: OWASP y enrutamiento de las pasarelas de pago

Vista general de resultados

Se implementó el escaneo automático mediante OWASP para identificar posibles vulnerabilidades en la comunicación entre la aplicación y el servidor. Este análisis permitió detectar fallos en la transmisión de datos, evaluando la seguridad de los protocolos utilizados y garantizando la integridad de la información intercambiada.

El uso de esta herramienta contribuyó a fortalecer la protección del sistema, asegurando que las medidas de seguridad aplicadas cumplan con los estándares requeridos y minimizando los riesgos de exposición a ataques externos.

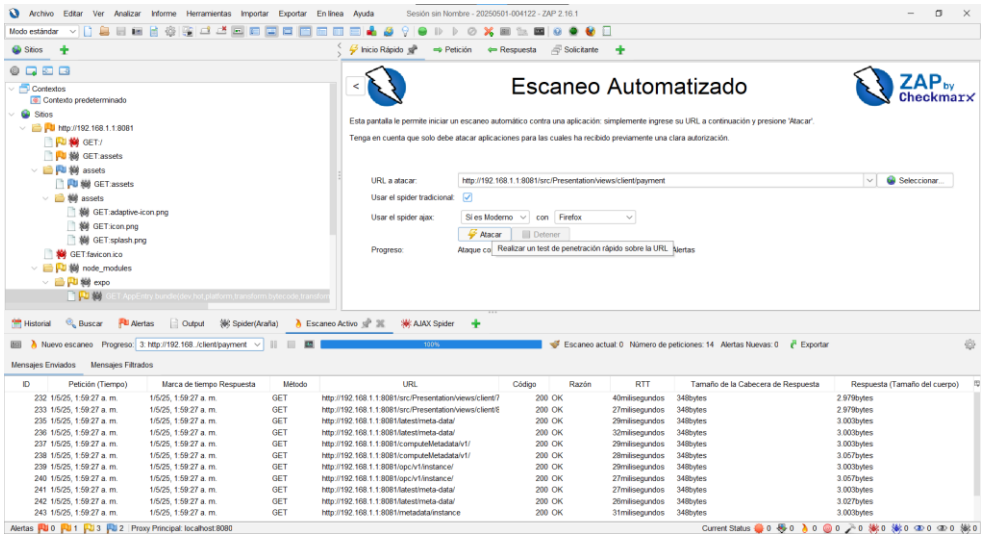


Figura 26: OWASP - Escaneo Automatizado

Análisis del funcionamiento de la comunicación entre el servidor y el sistema

Tras realizar las peticiones correspondientes, se obtuvo un desglose detallado del funcionamiento de la comunicación entre el servidor y el sistema. Este análisis permitió examinar el intercambio de datos, verificar la respuesta a las solicitudes y evaluar la estabilidad de la conexión, garantizando que los procesos de transmisión sean eficientes y seguros.

A continuación, se presentan los resultados obtenidos, donde se evidencia el comportamiento del sistema en relación con las interacciones establecidas con el servidor.

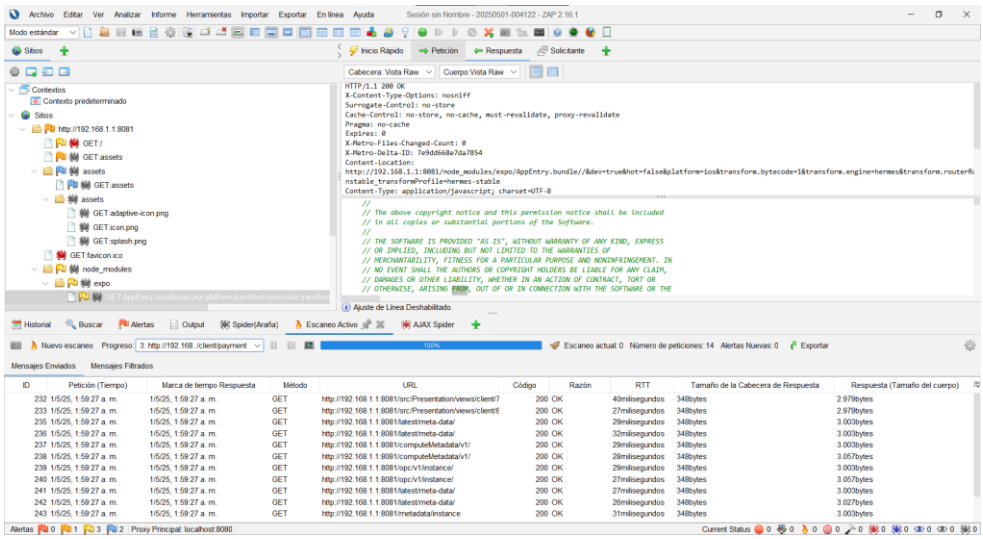


Figura 27: Resultados de OWASP

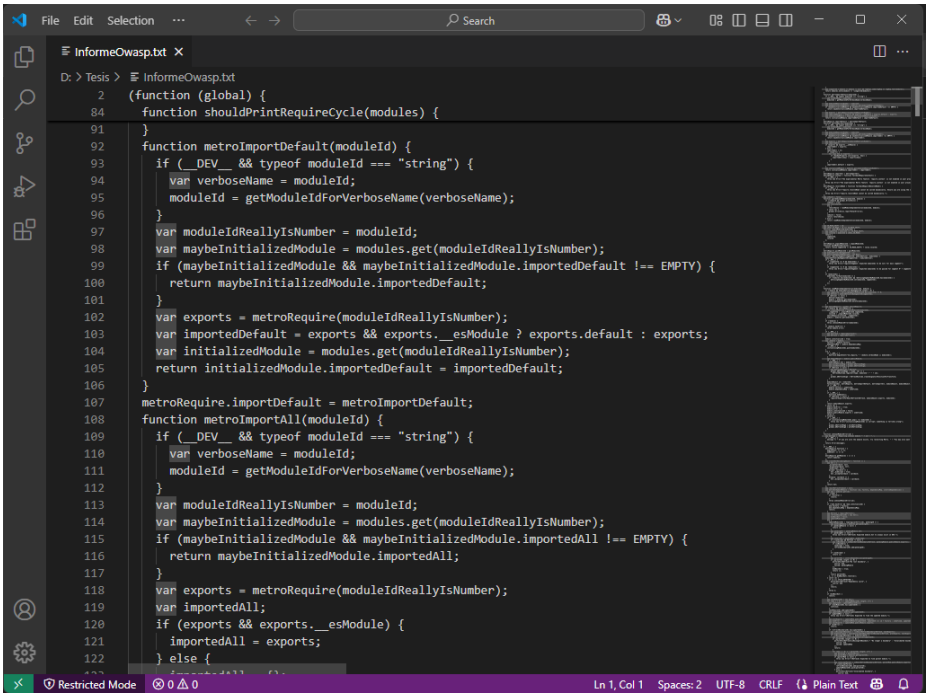


Figura 28: Informe de OWASP

CAPÍTULO IV. RESULTADOS Y DISCUSIÓN

El propósito de este capítulo es presentar y analizar los resultados obtenidos tras la implementación de los controles de seguridad en la aplicación móvil. A través de diversas pruebas y verificaciones, se busca evaluar el cumplimiento de los estándares de la ISO 27001, garantizando la integridad y protección de los datos dentro del sistema.

El cumplimiento de la ISO 27001 es un aspecto fundamental en la seguridad de la información, ya que establece un conjunto de buenas prácticas para la gestión y protección de datos sensibles. En este contexto, el análisis de los resultados permitirá determinar si las medidas aplicadas en la arquitectura de la aplicación cumplen con los requisitos exigidos, asegurando un entorno confiable para los usuarios y optimizando la seguridad en el procesamiento de información.

4.1 Resultados

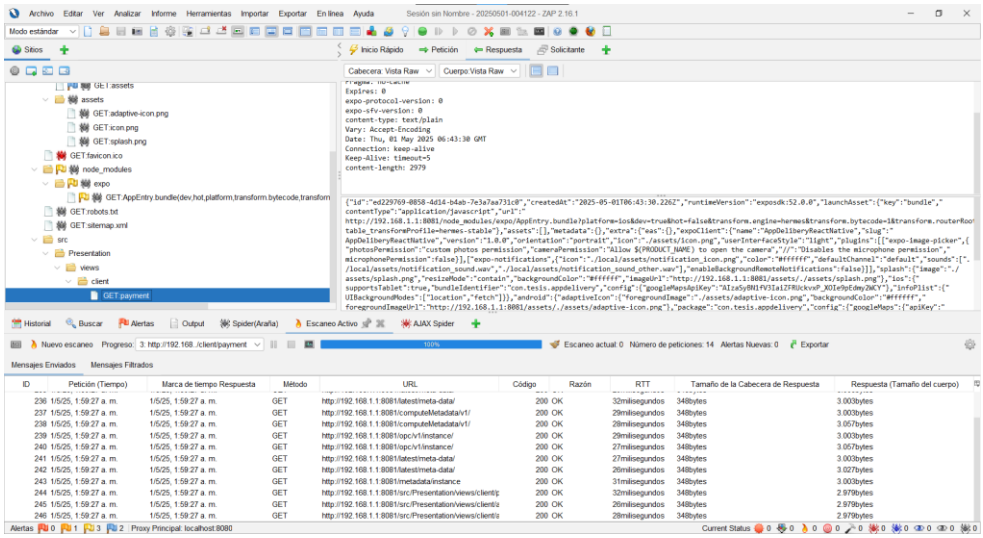


Figura 29: Ataque a las pasarelas de Pagos

Como se observa en la figura 29, la implementación de los controles de seguridad definidos por la ISO 27001, junto con la aplicación de la arquitectura MVVM, ha permitido fortalecer la protección de los datos sensibles dentro de la aplicación móvil.

Gracias al uso de autenticación basada en JWT (JSON Web Tokens) y la adopción de protocolos de cifrado avanzados (TLS 1.2+), se garantiza la confidencialidad y integridad de la información transmitida entre el usuario y la pasarela de pago.

Además, la segmentación de responsabilidades dentro de la arquitectura MVVM asegura que la manipulación de estos tokens se realice exclusivamente en el Model, evitando su exposición

innecesaria en otras capas de la aplicación, lo que reduce el riesgo de vulnerabilidades y mejora la seguridad del sistema.

4.2 Análisis de los Resultados Obtenidos

Los resultados obtenidos en las pruebas realizadas confirman que el sistema cumple con los estándares de seguridad exigidos por la ISO 27001, asegurando una protección robusta de los datos y minimizando el riesgo de accesos no autorizados.

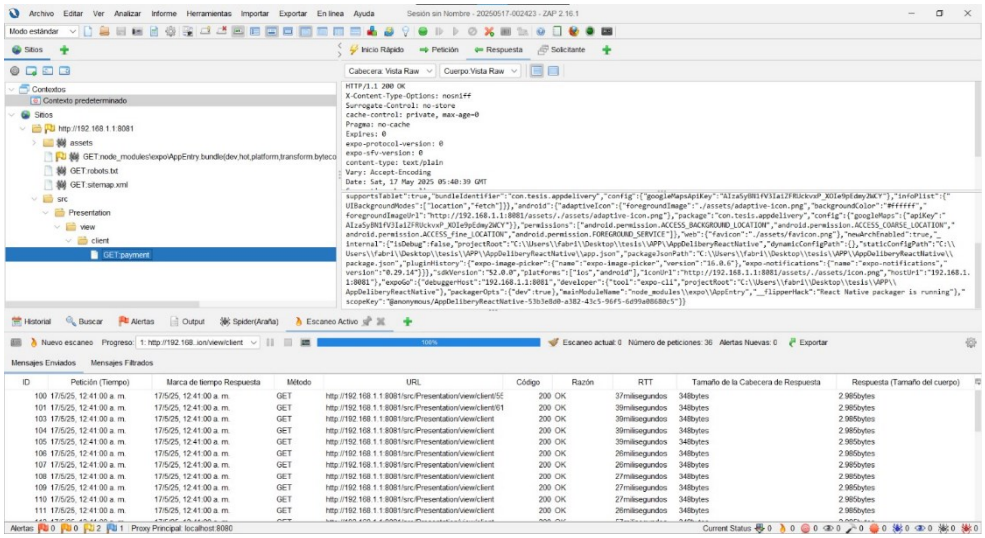


Figura 30: Control de datos sensibles

En la figura 30, se muestra un análisis de acceso no autorizado a información sensible dentro de la aplicación. En la interfaz de OWASP ZAP, se visualizan intentos de acceso a datos protegidos, junto con el estado de autenticación y las respuestas generadas por el servidor. Se incluyen detalles de las solicitudes HTTP interceptadas, evidenciando el manejo seguro de credenciales y sesiones.

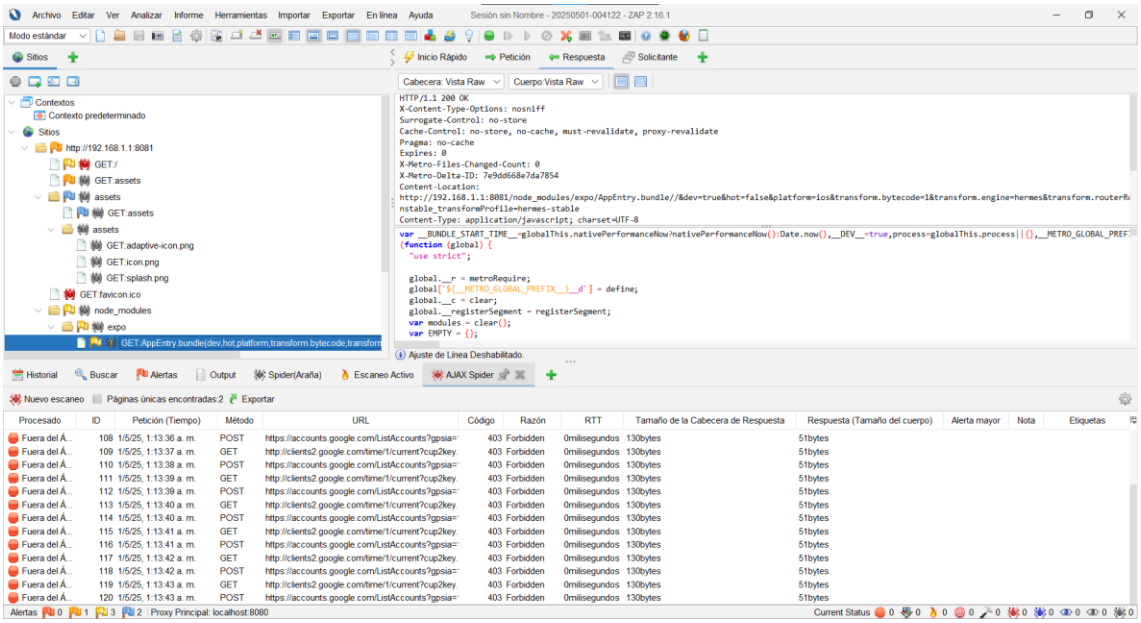


Figura 31: Cifrado de datos en transito

En la figura 31, se muestra un análisis de tráfico de red en OWASP ZAP, donde se verifican los protocolos de cifrado utilizados en la comunicación entre la aplicación y el servidor. Se observan solicitudes HTTPS con TLS 1.2+, asegurando que la transmisión de datos está protegida contra interceptaciones y ataques MITM (Man-in-the-Middle).

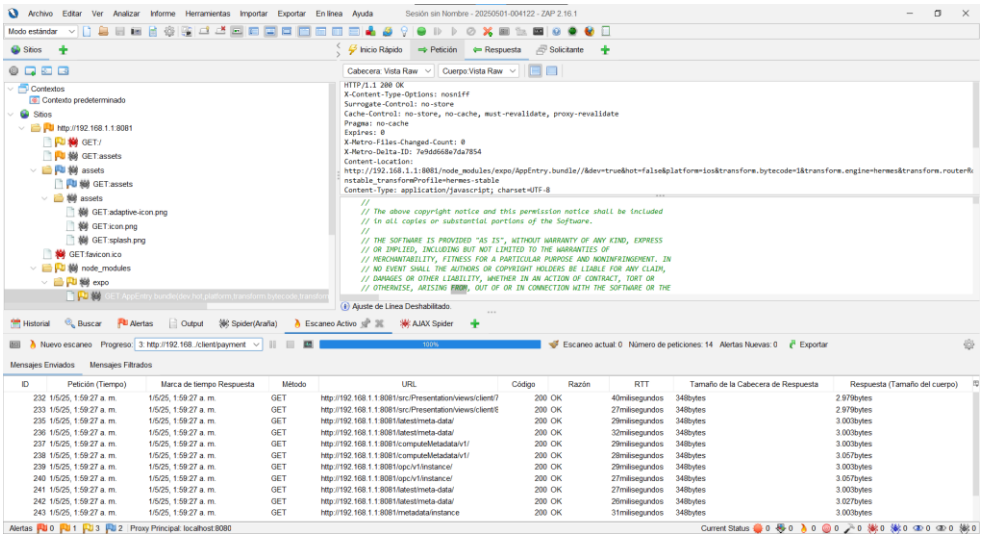


Figura 32: Validación de datos

En la figura 32, se muestra pruebas de manipulación de datos realizadas con OWASP ZAP, donde se analiza la integridad de los datos procesados por la pasarela de pago. Se visualizan solicitudes y respuestas interceptadas, verificando si el sistema detecta alteraciones o intentos de modificación no autorizados en la estructura de los datos

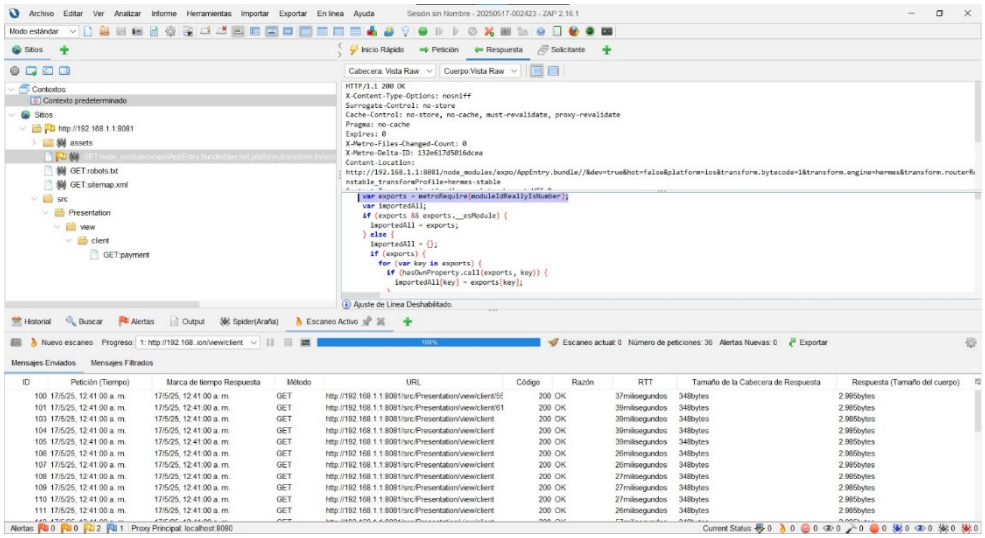


Figura 33: Seguridad de transacciones

En la figura 33, se exhibe pruebas de seguridad en transacciones financieras dentro de OWASP ZAP. Se muestran análisis de sesiones y validación de autenticación, comprobando la resistencia del sistema contra ataques de repetición y uso indebido de tokens. También se observa la implementación de JWT, asegurando que cada transacción cuente con medidas de verificación adecuadas.

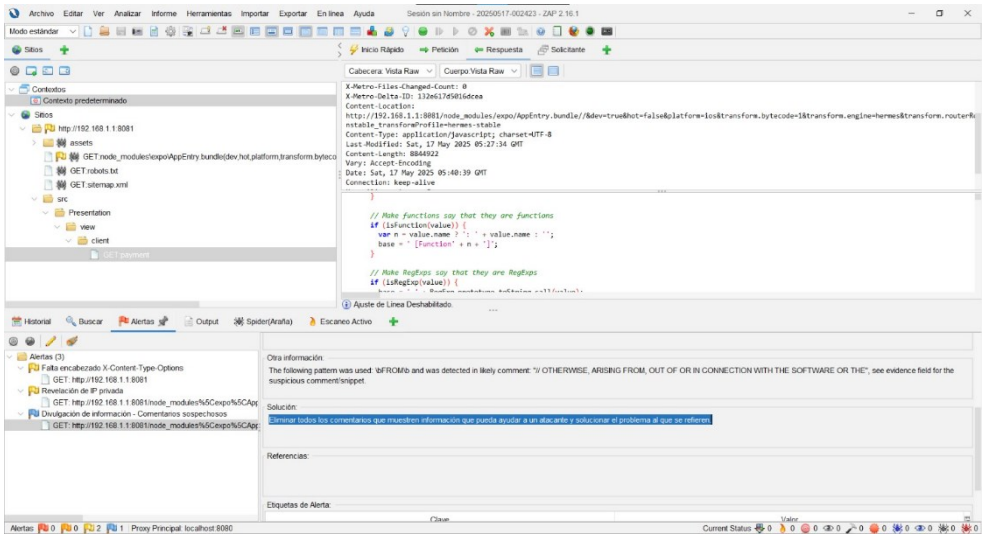


Figura 34: Gestión de incidentes de seguridad

En la figura 34, se muestra registros de eventos de seguridad y análisis de posibles vulnerabilidades detectadas por OWASP ZAP. Se evidencia la identificación de riesgos, el monitoreo de logs y la respuesta del sistema ante incidentes simulados.

4.3 Verificación del cumplimiento de la ISO 27001

Los resultados obtenidos confirman que las protecciones aplicadas han sido efectivas, asegurando la integridad y confidencialidad de la información manejada por el sistema.

A continuación, se presenta la tabla 12, en donde se detallan los controles evaluados y sus respectivos resultados:

Tabla 12: Tabla de verificación de la ISO 27001

Control ISO 27001	Descripción	Prueba de Seguridad con OWASP ZAP	Resultado
A.10.1.1 - Control de acceso a datos sensibles	Protección de la información transmitida por la pasarela de pago.	Simulación de ataques para identificar accesos no autorizados a datos financieros.	✅ Aprobado – No se detectaron accesos indebidos.
A.10.1.2 - Cifrado de datos en tránsito	Aplicación de protocolos como TLS para proteger la comunicación.	Prueba de interceptación de tráfico para verificar cifrado de datos.	✅ Aprobado – Cifrado TLS activo y funcional.
A.12.2.1 - Validación de datos	Verificación de integridad y autenticidad de datos de pago.	Análisis de manipulación en solicitudes y respuestas de pago.	✅ Aprobado – No se detectaron alteraciones.
A.14.1.3 - Seguridad en las transacciones	Implementación de controles para evitar transacciones fraudulentas.	Evaluación de la gestión de sesiones y protección contra ataques de repetición.	✅ Aprobado – Protección efectiva contra ataques de repetición.
A.16.1 - Gestión de incidentes de seguridad	Registro y monitoreo de posibles vulnerabilidades en el sistema de pagos.	Análisis de logs de seguridad y respuesta ante incidentes simulados.	✅ Aprobado – Detección y gestión de eventos de seguridad eficiente.

4.4 Discusión

La adopción de la arquitectura MVVM (Modelo-Vista-Modelo de Vista) en aplicaciones móviles ha demostrado ser una estrategia eficaz para separar responsabilidades y mejorar la seguridad en los procesos de pago. En el ámbito de las pasarelas de pago para comercio electrónico, MVVM permite disminuir la exposición de datos sensibles, fortaleciendo así las medidas de protección de la información en cada una de las capas de la aplicación.

- Separación de responsabilidades y mitigación de vulnerabilidades

  Investigaciones previas han señalado que la segmentación adecuada en arquitecturas como MVVM no solo optimiza la eficiencia, sino que también incrementa la seguridad frente a enfoques tradicionales como el MVC (Modelo-Vista-Controlador). Según (A Bucchiarone,

2020), la separación lógica que propone MVVM facilita la protección de datos al restringir el acceso directo a información crítica en la capa de presentación. En el contexto de las pasarelas de pago, este enfoque reduce significativamente el riesgo de exposición de tokens de autenticación o credenciales de usuario, dado que los datos confidenciales se gestionan exclusivamente en el Modelo, sin reflejarse en la Vista o en el Modelo de Vista.

- Cifrado y seguridad en el manejo de datos

  Una investigación llevada a cabo por (Sharma & Singh, 2021) sobre la seguridad en arquitecturas móviles destaca que el cifrado aplicado en la capa del Modelo dentro de MVVM disminuye la probabilidad de ataques por interceptación de tráfico. Este mecanismo se alinea con los estándares de la norma ISO 27001, específicamente con el control A. 10. 1. 1 (Protección de datos en tránsito), asegurando que la información financiera enviada a las pasarelas de pago esté cifrada utilizando protocolos como TLS 1. 2 o superior. Además, estudios realizados por (Patel, 2019) han evidenciado que la gestión de claves y tokens de pago dentro del Modelo evita la filtración de datos sensibles en la interfaz de usuario, donde ataques como el Man-in-the-Middle (MITM) podrían comprometer la seguridad.

- Prevención de ataques mediante validaciones en la arquitectura MVVM

  Las pruebas de seguridad realizadas con OWASP ZAP han confirmado que la arquitectura MVVM favorece una implementación más robusta de validaciones en el flujo de pago. Según (García, 2022), la seguridad de las transacciones mejora notablemente cuando las validaciones se manejan en el Modelo, dificultando las manipulaciones en la Vista o Modelo de Vista por parte del usuario final. Este enfoque ayuda a prevenir vulnerabilidades comunes, tales como la inyección de código, la alteración de montos de pago y accesos no autorizados.

En resumen, la implementación de la arquitectura MVVM no solo mejora la organización y la eficiencia de las aplicaciones móviles, sino que también actúa como un baluarte en la seguridad de los procesos de pago, convirtiéndose en una elección preferida para el desarrollo de aplicaciones en el ámbito del comercio electrónico.

La adopción del patrón MVVM en aplicaciones de pago móvil contribuye significativamente a mejorar la seguridad. Esto se logra al estructurar la lógica de negocio en capas independientes,

lo que reduce la exposición de datos y optimiza el manejo de cifrado y autenticación. Los resultados obtenidos a través de OWASP ZAP y estudios anteriores respaldan la idea de que esta arquitectura cumple con los estándares internacionales de seguridad. De este modo, las pasarelas de pago se convierten en opciones más confiables para las PYMES que desean asegurar la protección de los datos financieros de sus clientes.

CAPÍTULO V. CONCLUSIONES y RECOMENDACIONES

CONCLUSIONES

La implementación de la arquitectura MVVM ha resultado ser una táctica efectiva para desarrollar aplicaciones móviles actuales. Su diseño permite un claro reparto de roles, lo que se traduce en una mejor estructuración del código y una mayor capacidad de ampliación del sistema. La división en Model, View y ViewModel ha mejorado la administración de datos, favoreciendo una mayor reutilización de los elementos y facilitando el mantenimiento del software. Igualmente, la arquitectura MVVM ha potenciado la interacción entre los usuarios y la aplicación, asegurando que la actualización de las vistas sea ágil y eficaz. La utilización de este modelo ha brindado mayor adaptabilidad en el proceso de desarrollo y ha ayudado a simplificar las interdependencias entre los diferentes módulos del sistema.

El sistema creado se ha centrado en ofrecer una solución efectiva para el comercio electrónico B2C en pequeñas y medianas empresas, garantizando una administración óptima de productos, órdenes y entregas. Gracias a la introducción de un proceso de compra bien definido, los usuarios pueden desplazarse de manera sencilla por la aplicación, realizando transacciones de forma segura y precisa. Las características implementadas en la plataforma garantizan una experiencia mejorada tanto para los clientes como para los gerentes, asegurando un manejo adecuado del catálogo de productos y una logística eficiente en el control de envíos. La incorporación de tecnologías avanzadas ha permitido asegurar que el sistema sea escalable y capaz de ajustarse a las necesidades comerciales contemporáneas.

La protección de los datos ha sido un elemento fundamental en la creación de esta aplicación. Mediante varias pruebas ejecutadas con OWASP ZAP, se ha verificado la efectividad de las medidas de seguridad adoptadas en la pasarela de pago. La implementación de JWT (JSON Web Tokens) ha hecho posible gestionar la autenticación de los usuarios de forma segura, garantizando la salvaguarda de las credenciales en cada sesión. Además, la adopción de cifrado TLS 1. 2+ ha garantizado la integridad y privacidad de la información enviada entre el usuario y el servidor. Los resultados obtenidos han corroborado que la aplicación se ajusta a los criterios de seguridad requeridos por la norma ISO 27001, asegurando un entorno seguro y reduciendo los riesgos de accesos no autorizados. La distribución de la arquitectura MVVM ha sido crucial en el manejo de datos sensibles, asegurando que los tokens de autenticación sean gestionados únicamente en el Model, evitando su exposición en otras partes del sistema.

RECOMENDACIONES

Se recomienda mejorar la gestión del Model, asegurando que la manipulación de datos se realice de manera eficiente y segura, evitando la exposición innecesaria de información en otras capas.

Para garantizar la competitividad en el mercado de PYMES, se sugiere integrar módulos adicionales que optimicen la experiencia del usuario, como personalización de compras y métodos de pago alternativos al estilo nacional.

Aunque la aplicación cumple con la ISO 27001, es recomendable realizar auditorías periódicas con herramientas como OWASP ZAP, asegurando que las medidas de protección se mantengan actualizadas frente a nuevas amenazas.

BIBLIOGRAFÍA

A Bucchiarone, N. D. (2020). *Academia.edu.* Obtenido de https://www.academia.edu/73073283/From_Monolithic_to_Microservices_An_Experience_Report_from_the_Banking_Domain

Angleritech. (2020). Obtenido de https://www.angleritech.com/case_studies/b2c-ecommerce-application-development/

Castro, J. (10 de 2022). *CORPONET.* Obtenido de https://blog.corponet.com/e-commerce-que-es-sus-caracteristicas-ventajas-y-desventajas#:~:text=Ventajas%20y%20desventajas%20del%20e-commerce%201%20Oportunidad%20de,por%20servicios%20p%C3%BAblicos%2C%20alquiler%2C%20entre%20otros.%20M%C3%A1s%20elementos

EMarketer. (Junio de 2019). *Ecommerce continues Strong Gains Amid Global Economic Uncertainty.* Obtenido de https://www.insiderintelligence.com/content/ecommerce-continues-strong-gains-amid-global-economic-uncertainty

Emprendedores. (2019). *Las empresas sin una web optimizada pierden.* Titania Compañia Editorial. Obtenido de Titania Compañia Editorial,.

Escuelaeuropeaexcelencia. (12 de 2022). *escuelaeuropeaexcelencia*. Obtenido de https://www.escuelaeuropeaexcelencia.com/2022/12/norma-iso-270012022-todo-lo-que-debes-saber-sobre-el-nuevo-estandar-de-seguridad-de-la-informacion/

García. (2022). Obtenido de Security Testing Framework for Web Applications: Benchmarking ZAP V2.12.0 and V2.13.0 by OWASP as an example: https://arxiv.org/abs/2501.05907

Garcia, C. (2021). *appmaster.io.* Obtenido de https://appmaster.io/es/blog/patrones-arquitectonicos-mvc-mvp-y-mvvm

INCIBE. (2019). Obtenido de Seguridad en el comercio electrónico: Principales amenazas y recomendaciones. Instituto Nacional de Ciberseguridad de España.: https://www.incibe.es/empresas/blog/aspectos-clave-proteger-tu-tienda-online

INCIBE. (2019). Obtenido de https://www.incibe.es/empresas/blog/aspectos-clave-proteger-tu-tienda-online

Jesús Maceira. (13 de 07 de 2023). *ORIENTEED.* Obtenido de https://orienteed.com/es/estadisticas-de-ecommerce-en-2023/

Matute-Celi, V., Viñansaca-Eras, X., & Capa-Tejedor, M. (2023). *dialnet.unirioja.es.* Obtenido de https://dialnet.unirioja.es/servlet/articulo?codigo=9124169

microsoft. (08 de junio de 2023). *learn.microsoft*. Obtenido de https://learn.microsoft.com/es-es/dotnet/architecture/maui/mvvm

Montoya, J. (2025). Obtenido de innovaciondigital360: https://www.innovaciondigital360.com/cyber-security/burp-suite-que-es-como-se-utiliza/

Morelos, M. (11 de 05 de 2023). *blog.clip.mx*. Obtenido de https://blog.clip.mx/articulo/seguridad-en-las-pasarelas-de-pago

Moskala, M. (22 de 11 de 2017). *REALM*. Obtenido de https://academy.realm.io/posts/mvc-vs-mvp-vs-mvvm-vs-mvi-mobilization-moskala/

Orienteed. (2023). Obtenido de El crecimiento del comercio electrónico minorista y sus proyecciones para 2026.: https://orienteed.com/es/estadisticas-de-ecommerce-en-2023/

Ortega, C. (Julio de 2020). *SEIDOR*. Obtenido de https://www.opentrends.net/es/articulo/la-importancia-de-las-arquitecturas-modulares-en-las-aplicaciones-moviles

Patel, M. (2019). *Allcommercejournal.* Obtenido de Cyber security in digital payments: An empirical study.: https://www.allcommercejournal.com/article/274/5-1-40-607.pdf

PAYCOMET. (2021). *www.paycomet.com.* Obtenido de Integrar una pasarela de pago en tu app : https://www.paycomet.com/news/integrar-pasarela-pago-app/

Proscont. (2022). *PROSCONT*. Obtenido de https://www.proscont.com/ventajas-y-desventajas-de-e-commerce/

ReactNative. (21 de 06 de 2023). Obtenido de https://reactnative.dev/docs/security

REACTNATIVE. (21 de 06 de 2023). Obtenido de https://reactnative.dev/docs/security

Rodríguez, A. G. (2019). El comercio electrónico: diseño e implantación de una tienda online. Coruña.

Rodriguez, J. (2023). *Hubspot*. Obtenido de https://blog.hubspot.es/sales/pasarelas-de-pago

Salesforce. (19 de 04 de 2021). Obtenido de E-commerce trends and digital transformation: Market analysis. Salesforce Research.: https://www.salesforce.com/es/blog/2021/04/commcerce_b2b_b2c.html

SALESFORCE. (19 de 04 de 2021). Obtenido de https://www.salesforce.com/es/blog/2021/04/commcerce_b2b_b2c.html

Segovia, A. J. (24 de 04 de 2018). *advisera*. Obtenido de https://advisera.com/27001academy/blog/2018/04/24/how-to-use-open-web-application-security-project-owasp-for-iso-27001/

Sharma, S., & Singh, P. (2021). *Middlesex University Research Repository*. Obtenido de https://repository.mdx.ac.uk/item/89639

spdigitalagency. (2023). *spdigitalagency*. Obtenido de https://spdigitalagency.com/es/blog/popular-frameworks-in-2023-for-mobile-application-development

Statista. (6 de 2023). *Statista.com.* Obtenido de https://www.statista.com/markets/413/topic/457/b2c-e-commerce/#overview

Tovar, F. (27 de 09 de 2022). *sana.* Obtenido de https://www.sana-commerce.com/es/blog-es/seguridad-en-ecommerce/

Venera, D. (2024). *OWASP ZAP: Herramienta de seguridad de aplicaciones web*. Obtenido de community.listopro: https://community.listopro.com/owasp-zap-herramienta-de-seguridad-de-aplicaciones-web/

VERIZON. (08 de 11 de 2022). Obtenido de https://theblackboxlab.com/2022/11/08/aplicaciones-moviles-desarrollo-de-software-ciberseguridad-big-data/

ANEXOS

MANUAL DE USUARIO APLICACIÓN MÓVIL

FOOD APP

Aplicación Móvil de Pasarela de Pagos para Procesos E-commerce B2C en PYMES.

Elaborado Por: Fausto Fabricio Constante Vinocunga

Versión: 1.0

CONTENIDO

INTRODUCCIÓN

La tecnología ha evolucionado significativamente en los últimos años, transformando la manera en que las personas realizan diversas actividades cotidianas. En este contexto, los dispositivos móviles han adquirido un papel esencial, proporcionando acceso a una amplia gama de aplicaciones diseñadas para mejorar la eficiencia en distintos ámbitos como comercio, entretenimiento, educación y servicios financieros.

El aplicativo móvil desarrollado busca optimizar la gestión de procesos de e-commerce B2C, ofreciendo una solución eficiente para la compra y distribución de productos. A través de su arquitectura basada en MVVM, el sistema garantiza una experiencia de usuario fluida, asegurando una correcta administración de pedidos, pagos y entregas dentro de la plataforma. Este manual de usuario tiene como propósito proporcionar instrucciones claras sobre el funcionamiento de la aplicación, permitiendo que los usuarios interactúen con cada módulo de manera óptima. El documento explica detalladamente cómo registrarse en la plataforma, seleccionar productos, realizar pagos, gestionar pedidos y monitorear el estado de las entregas, asegurando que el usuario pueda aprovechar al máximo las funcionalidades ofrecidas.

Siguiendo los pasos descritos en este manual, los usuarios podrán navegar de manera intuitiva por la aplicación, facilitando la integración con el sistema de compras y garantizando la seguridad en sus transacciones.

Requisitos del sistema

Sistemas Operativos Compatibles:

- Android 5.0 o superior
- iOS 11.0 o superior

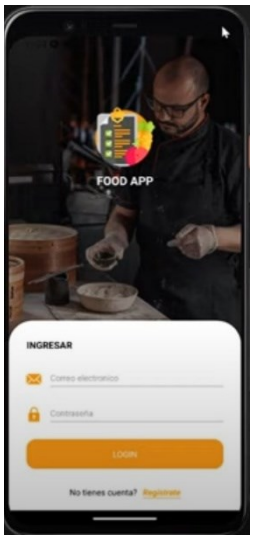
Conexión a Internet: Se requiere una conexión estable para el funcionamiento óptimo de la aplicación.

- Permisos Necesarios:
- Acceso a la ubicación (para determinar la dirección de entrega)
- Acceso a la Cámara (para agregar una foto de datos en la app)

Inicio de sesión

Al cargar la aplicación, se mostrará la pantalla de inicio de sesión, donde el usuario deberá ingresar sus credenciales en los campos correspondientes. Una vez completada esta información, el sistema habilitará el botón de Inicio de Sesión, permitiendo el acceso al menú principal de la aplicación.

Si el usuario no tiene una cuenta registrada, deberá seleccionar la opción "Regístrate", donde podrá completar el proceso de creación de perfil antes de acceder a la plataforma.



Registro de nuevo usuario

Para acceder a la aplicación móvil, el usuario debe completar el formulario de registro, ingresando la siguiente información requerida:

- Nombre y apellido de usuario
- Correo electrónico

- Número telefónico
- Contraseña

Una vez que todos los campos han sido llenados correctamente, el sistema habilitará el botón de "Registrar", permitiendo al usuario completar el proceso de creación de cuenta y acceder a la plataforma.

Selección de categoría

Después de elegir su rol, el usuario accede a la pantalla de selección de categoría de productos. Pueden explorar las categorías disponibles y seleccionar los productos de su interés.

Esta configuración facilita la gestión del sistema y define claramente las funciones de cada tipo de usuario.

Selección de la lista de productos

Después de elegir una categoría, el usuario accede a la pantalla de selección de productos.

Visualizarán un listado con información básica de cada producto. Pueden ingresar a la vista detallada para consultar características específicas antes de realizar una compra.

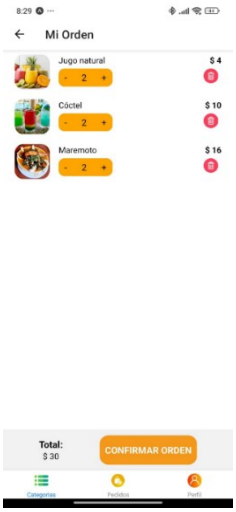
Esta configuración optimiza la administración de productos y define claramente las funciones de cada usuario dentro de la aplicación.

Vista del producto

Cuando el usuario selecciona un producto desde la lista de categorías, accede a la vista detallada del producto, donde podrá consultar información específica antes de realizar una compra.

Podrán visualizar detalles como nombre, descripción, precio, disponibilidad, y características adicionales del producto. También tendrán la opción de agregarlo al carrito o proceder directamente con la compra.

Esta vista proporciona una experiencia interactiva y clara para los usuarios, permitiendo un acceso rápido a la información relevante de cada artículo disponible en la tienda.

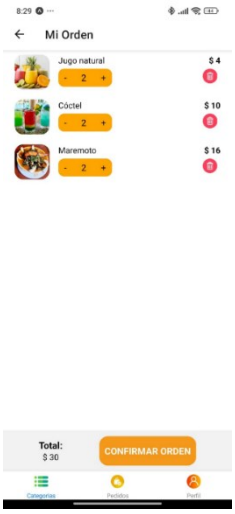


Vista de órdenes

Después de seleccionar los productos, el usuario accede al módulo de órdenes, donde podrá visualizar el listado de los artículos elegidos antes de proceder con la compra.

Podrán revisar los productos añadidos, modificar la cantidad de cada artículo y visualizar el total a pagar en tiempo real. También tendrán la opción de confirmar la orden, asegurando que el pedido sea procesado correctamente.

Este módulo garantiza una experiencia intuitiva y organizada, asegurando que los usuarios tengan control sobre sus compras y que la gestión de pedidos dentro del sistema sea eficiente.



Vista de direcciones y agregar nuevas direcciones

El módulo de direcciones permite a los usuarios administrar los puntos de entrega de sus pedidos de manera eficiente.

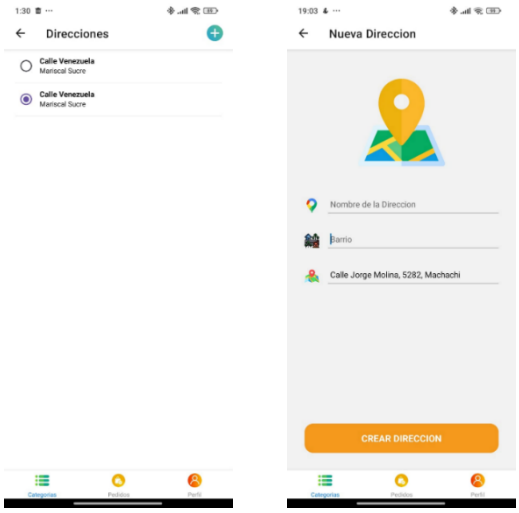
1. Vista de direcciones

- Una vez dentro de la aplicación, el usuario puede acceder a la sección de direcciones, donde se visualizarán las ubicaciones previamente registradas. Desde esta pantalla, el usuario puede:
- Seleccionar una dirección existente para el envío.
- Modificar los datos de una dirección registrada.
- Eliminar ubicaciones que ya no sean necesarias.

2. Agregar nuevas direcciones

- Para añadir una nueva dirección, el usuario debe:
- Seleccionar la opción "Agregar dirección".
- Ingresar los datos requeridos, como nombre de la ubicación, dirección exacta y referencias.
- Utilizar la función de geolocalización en el mapa para ubicar con precisión el destino.
- Confirmar los datos ingresados y guardar la nueva dirección.

Esta funcionalidad garantiza una administración organizada de las direcciones de entrega, mejorando la experiencia del usuario en la gestión de pedidos dentro de la aplicación.



Vista del formulario de pago

El formulario de pago permite a los usuarios completar su transacción de manera segura dentro de la aplicación.

1. Acceso al formulario

- Después de confirmar la orden, el usuario será dirigido al módulo de pagos, donde podrá ingresar la información requerida para procesar la compra.

2. Información requerida

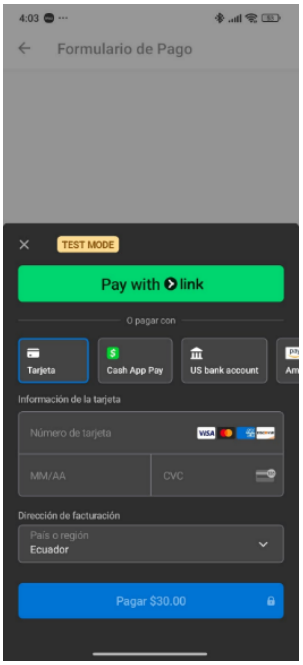
- Para completar el pago, el usuario deberá proporcionar los siguientes datos:
- Número de tarjeta (crédito o débito).
- Fecha de vencimiento.
- Código de seguridad (CVV).
- Nombre del titular de la tarjeta.

3. Validación y procesamiento

- Una vez ingresados los datos, la pasarela de pagos Stripe verificará la información y procesará la transacción. Se utiliza cifrado TLS 1.2+ para garantizar la seguridad de los datos financieros.

4. Confirmación de pago

- Si la transacción es exitosa, el sistema mostrará un mensaje de confirmación, y el usuario será redirigido al módulo de gestión de pedidos para el seguimiento del envío.
- Esta vista proporciona una experiencia de pago segura y estructurada, asegurando que las transacciones se realicen de manera eficiente.



Gestión de pedidos

El módulo de pedidos permite a los usuarios realizar un seguimiento de sus compras, verificando el estado y la ubicación de los productos en tiempo real.

1. Visualización de pedidos

- Después de completar el pago, el usuario puede acceder al apartado de pedidos, donde visualizará una lista de las compras realizadas con los siguientes detalles:
- Número de pedido.
- Productos adquiridos.
- Fecha de compra.
- Estado del pedido (PAGADO, DESPACHADO, EN CAMINO, ENTREGADO).

2. Seguimiento de entrega

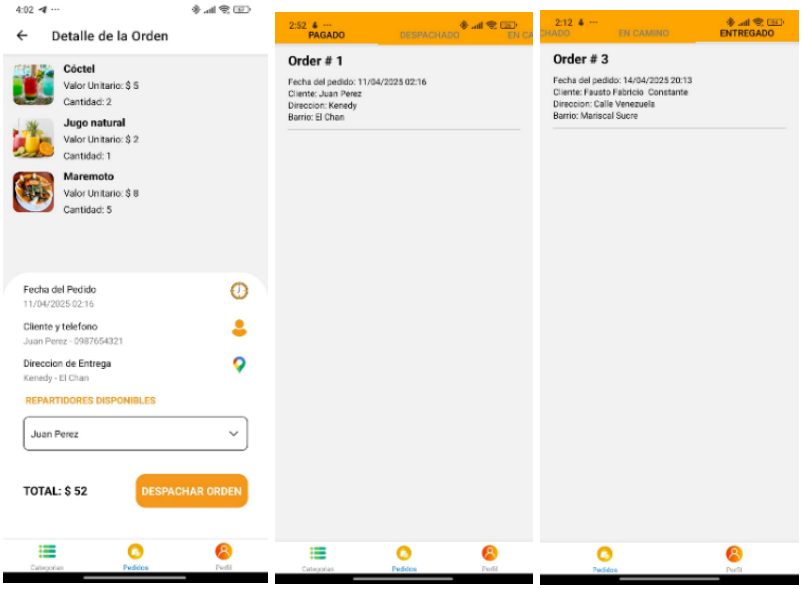
- El usuario puede realizar un seguimiento del estado de su pedido a medida que avanza en el proceso de distribución. La aplicación proporciona actualizaciones en tiempo real, mostrando cuándo el producto ha sido despachado y está en camino.

3. Funciones para administradores

Los administradores cuentan con herramientas adicionales dentro del módulo de pedidos, como:

- Asignación de repartidores a los pedidos en estado “DESPACHADO”.
- Gestión y modificación del estado del pedido según el progreso de la entrega.
- Historial de compras, permitiendo revisar registros previos y optimizar la logística.

Este módulo garantiza una administración eficiente de las órdenes de compra y una experiencia de usuario transparente, mejorando la operatividad del sistema.



Editar perfil

El usuario en caso de haber cometido algún error a la hora de registrarse podrá actualizar su información que considere necesario modificar, una vez actualizado pulsará el botón actualizar y se procederá a guardar los datos registrados.