UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

CARRERA INGENIERIA EN SOFTWARE

TRABAJO DE INTEGRACIÓN CURRICULAR PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN SOFTWARE

TEMA:

"IMPLEMENTACIÓN DE UN SISTEMA DE BANCA ELECTRÓNICA EMPRESARIAL PARA LA GESTIÓN DE PRODUCTOS FINANCIEROS DE LA MUTUALISTA IMBABURA, ALINEADO A LOS CONTROLES SEPS-009 Y CON PRUEBAS OWASP TOP 10 INTEGRADAS."

AUTOR: Rodman Joel Guerrero Malquin

DIRECTOR: MSc. Diego Javier Trejo España

Ibarra-Ecuador

2026

UNIVERSIDAD TÉCNICA DEL NORTE
BIBLIOTECA UNIVERSITARIA

IDENTIFICACIÓN DE LA OBRA

La Universidad Técnica del Norte dentro del proyecto Repositorio Digital Institucional, determinó la necesidad de disponer de textos completos en formato digital con la finalidad de apoyar los procesos de investigación, docencia y extensión de la Universidad.

Por medio del presente documento dejo sentada mi voluntad de participar en este proyecto, para lo cual pongo a disposición la siguiente información:

DATOS DE CONTACTO			
CÉDULA DE IDENTIDAD:	0450080940		
APELLIDOS Y NOMBRES:	Guerrero Malquin Rodman Joel		
DIRECCIÓN:	Tulcán, Rafael Arellano y Rocafuerte		
EMAIL:	rjguerrerom@utn.edu.ec, jg38903@gmail.com		
TELÉFONO FIJO:	S/N	**TELF. MOVIL**	0998673590

DATOS DE LA OBRA	
TÍTULO:	Implementación de un sistema de Banca Electrónica Empresarial para la gestión de productos financieros de la Mutualista Imbabura, alineado a los controles SEPS-009 y con pruebas OWASP top 10 integradas.
AUTOR (ES):	Guerrero Malquin Rodman Joel
FECHA: AAAAMMDD	2026/02/04
CARRERA/PROGRAMA:	☒ **GRADO** ☐ **POSGRADO**
TITULO POR EL QUE OPTA:	INGENIERÍA EN SOFTWARE
DIRECTOR:	MSc. Diego Javier Trejo España

AUTORIZACIÓN DE USO A FAVOR DE LA UNIVERSIDAD

Yo, Rodman Joel Guerrero Malquin, con cédula de identidad Nro. 0401876543, en calidad de autor y titular de los derechos patrimoniales de la obra o trabajo de integración curricular descrito anteriormente, hago entrega del ejemplar respectivo en formato digital y autorizo a la Universidad Técnica del Norte, la publicación de la obra en el Repositorio Digital Institucional y uso del archivo digital en la Biblioteca de la Universidad con fines académicos, para ampliar la disponibilidad del material y como apoyo a la educación, investigación y extensión; en concordancia con la Ley de Educación Superior Artículo 144.

Ibarra, a los 4 días del mes de Febrero de 2026

EL AUTOR:

Firma_____

Firmado electrónicamente por:
RODMAN JOEL
GUERRERO MALQUIN
Validar únicamente con FirmaEC

Nombre: Rodman Joel Guerrero Malquin

CONSTANCIAS

El autor manifiesta que la obra objeto de la presente autorización es original y se la desarrolló, sin violar derechos de autor de terceros, por lo tanto, la obra es original y que es el titular de los derechos patrimoniales, por lo que asume la responsabilidad sobre el contenido de la misma y saldrá en defensa de la Universidad en caso de reclamación por parte de terceros.

Ibarra, a los 4 días del mes de Febrero de 2026

EL AUTOR:

Firma 

_____

Nombre: Rodman Joel Guerrero Malquin

CERTIFICACIÓN DEL DIRECTOR DEL TRABAJO DE INTEGRACIÓN CURRICULAR

Ibarra, 4 de Febrero de 2026

MSc. Diego Javier Trejo España
DIRECTOR DEL TRABAJO DE INTEGRACIÓN CURRICULAR

CERTIFICA:
Haber revisado el presente informe final del trabajo de Integración Curricular, el mismo que se ajusta a las normas vigentes de la Universidad Técnica del Norte; en consecuencia, autorizo su presentación para los fines legales pertinentes.

DIEGO JAVIER TREJO ESPAÑA
Firmado digitalmente por DIEGO JAVIER TREJO ESPAÑA
Fecha: 2026.02.04 14:55:40 -05'00'

(f) _____
MSc. Diego Javier Trejo España
C.C.: 1002149290

DEDICATORIA

Dedico este trabajo a mis padres, los pilares fundamentales de mi vida. En especial a mi madre, **María Magdalena**, quien fue la persona que me brindó toda la educación que poseo y me formó con los valores que me definen hoy. Gracias mamá por ser mi guía constante, por enseñarme con tu ejemplo que con esfuerzo todo es posible y por ser el motor que me impulsó a llegar hasta aquí. Eres la razón principal de este logro y de la persona en la que me he convertido.

Asimismo, dedico esto a mi hermano por su apoyo y su ayuda práctica en el día a día. Gracias por cuidarme y facilitarme el camino cuando el tiempo y las fuerzas me faltaban. Este éxito también te pertenece.

AGRADECIMIENTO

Agradezco a la Universidad Técnica del Norte por ser el espacio donde crecí académica y personalmente durante estos años de formación.

Agradezco profundamente al Ing. Luis Yaguapaz y a la Ing. Gabriela Toledo, quienes confiaron en mi capacidad. Gracias por compartir su experiencia y brindarme las oportunidades necesarias para mejorar profesionalmente. Especialmente agradezco al Ing. Luis por su guía en el perfeccionamiento de mis habilidades de desarrollo y por enseñarme la importancia de la calidad y las buenas prácticas en la programación.

Al MSc. Diego Javier Trejo España, mi director de tesis, le agradezco por su guía experta y por orientarme con claridad durante todo el proceso de este trabajo. Su apoyo fue fundamental para culminar esta etapa con éxito.

A mis dos mejores amigos, les agradezco por ser mi soporte incondicional. Gracias por caminar a mi lado y, sobre todo, por no dejarme caer en esos momentos personales tan difíciles. Su amistad fue el refugio que necesité para levantar el ánimo y seguir adelante con mis metas

RESUMEN

La presente investigación surge ante la necesidad de la Mutualista Imbabura de modernizar sus servicios para clientes empresariales, quienes actualmente dependen de procesos manuales que afectan su eficiencia operativa. El objetivo general consistió en implementar un sistema de Banca Electrónica Empresarial para la gestión de productos financieros, el cual se encuentra alineado a los controles normativos SEPS-009 y cuenta con pruebas de seguridad OWASP Top 10 integradas. La metodología empleada incluyó un enfoque aplicado y el uso del marco de trabajo ágil Scrum para lograr un desarrollo iterativo y eficiente. Para definir las funciones del sistema, se realizó un levantamiento de requerimientos mediante reuniones directas con el personal clave de la institución, lo que permitió identificar las necesidades reales del software de primera mano. Como resultados más relevantes, se logró el desarrollo de una plataforma con módulos de consulta de saldos, transferencias interbancarias y pagos masivos, integrando además mecanismos de seguridad como la autenticación multifactor.

Palabras clave: Banca electrónica, SEPS-009, OWASP, Scrum, Seguridad informática, Gestión financiera.

ABSTRACT

This research arose from Mutualista Imbabura's need to modernize its services for business customers, who currently rely on manual processes that affect their operational efficiency. The overall objective was to implement a Business Electronic Banking system for financial product management, which is aligned with SEPS-009 regulatory controls and has integrated OWASP Top 10 security tests. The methodology employed included an applied approach and the use of the agile Scrum framework to achieve iterative and efficient development. To define the system's functions, requirements were gathered through direct meetings with key personnel at the institution, which made it possible to identify the actual needs of the software firsthand. The most relevant results were the development of a platform with modules for balance inquiries, interbank transfers, and bulk payments, as well as the integration of security mechanisms such as multi-factor authentication.

Keywords: Electronic banking, SEPS-009, OWASP, Scrum, IT security, Financial management.

ÍNDICE DE CONTENIDOS

Contenido

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

ÍNDICE DE ANEXOS

INTRODUCCIÓN

1.1 Problema de investigación.

Mutualista Imbabura, institución financiera ecuatoriana, se enfrenta a un desafío crítico: su cartera de clientes empresariales requiere gestionar productos financieros de manera eficiente y segura mediante canales digitales, pero actualmente carece de una plataforma de Banca Empresas que ofrezca un portal multiusuario para este fin. Esta carencia limita la eficiencia operativa de las empresas y podría afectar la competitividad de Mutualista Imbabura en el mercado financiero, ya que la digitalización de los servicios financieros es trascendental para mantener la competitividad en el mercado actual [1]. Esta limitación no solo afecta la eficiencia operativa de las empresas (que dependen de procesos manuales o presenciales para operaciones bancarias, aumentando costos y tiempos [2]), sino que también pone en riesgo la competitividad institucional en un mercado donde la digitalización es un factor clave para retener clientes [3].

La problemática surge principalmente por dos factores: 1) la ausencia de digitalización en servicios empresariales, que impide a las empresas gestionar autónomamente sus productos financieros en línea, y 2) la dependencia de métodos tradicionales, como trámites presenciales, que generan retrasos y errores en operaciones críticas [2]. Estas causas tienen consecuencias directas: por un lado, las empresas enfrentan ineficiencias operativas (estudios demuestran que soluciones tecnológicas podrían reducir hasta un 30% el tiempo de procesamiento de información financiera [3]), y por otro, Mutualista Imbabura podría perder clientes ante competidores con plataformas más modernas [3].

Para abordar este desafío desde la ingeniería, se propone implantar un sistema de Banca Empresas con un portal multiusuario seguro e intuitivo. La solución incluirá funcionalidades clave como consulta de saldos, transferencias, pagos y administración de cuentas y un módulo de seguridad MFA, priorizando estándares de seguridad y usabilidad. El desarrollo seguirá un enfoque estructurado: análisis de requerimientos, diseño técnico, desarrollo en fases iterativas, pruebas rigurosas y despliegue en el entorno productivo de la institución. Adicionalmente, se brindará capacitación a usuarios finales para garantizar una adopción efectiva, asegurando que la transición desde procesos manuales hacia la plataforma digital sea exitosa y sostenible.

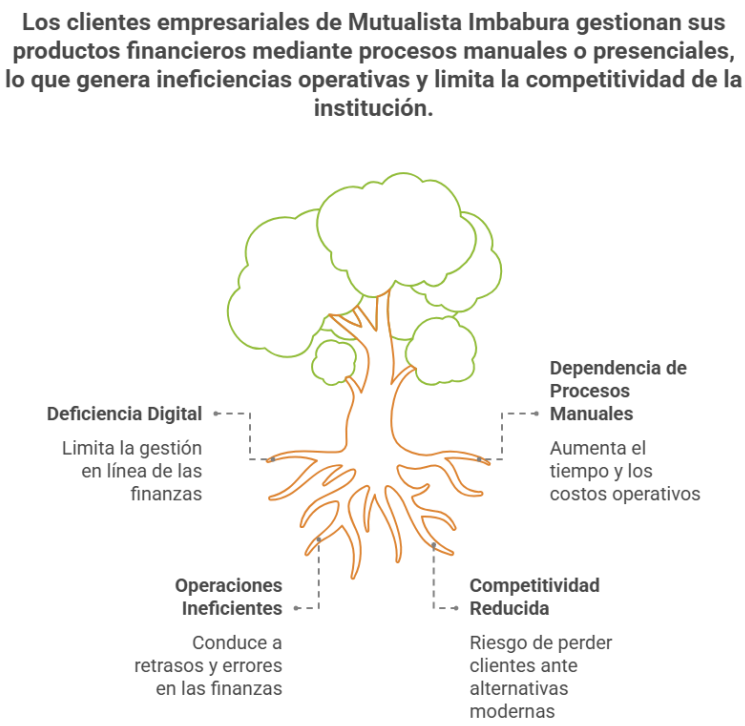


Figura 1: Mapa de problemas.

1.2 Justificación

El sistema de Banca Empresas para Mutualista Imbabura cuenta con un criterio pues atiende a una necesidad urgente que resolver con eficacia y optimización: la falta de acceso a servicios financieros digitales especializados para clientes tipo empresas. Los clientes tipo empresas vinculadas a Mutualista aún deben asistir personalmente para trámites de igual prioridad como transferir o revisar su saldo, lo que las deja muy detrás de la competencia que ya goza del sistema en la banca digital en instituciones ajenas, generando un retraso injusto del financiamiento.

En primer lugar, el proyecto proporcionará autonomía y eficiencia. Al proporcionar a los clientes tipo empresas el portal web que incluye las funciones de verificar los saldos al instante, transferencias que se validarán automáticamente y producción de certificados digitales, el tiempo gastado para los clientes se reducirá significativamente.

La seguridad es otro pilar fundamental. El sistema integrará prácticas avaladas por Microsoft para entornos .NET [4], como cifrado de datos y arquitecturas multicapa que separan lógica de negocio, presentación y acceso a datos. Estas medidas son esenciales en un contexto global donde la ciberseguridad financiera es prioritaria, y más aún en Ecuador, que ha fortalecido sus regulaciones para proteger transacciones electrónicas (como la Ley Orgánica de

Protección de Datos Personales). Para Mutualista Imbabura, esto no solo mitigará riesgos de fraude, sino que reforzará su reputación como institución confiable.

Para la ingeniería de software, el proyecto mostrará cómo puede adaptarse, en entornos financieros altamente regulados, a metodologías ágiles como Scrum, que se usan sobre todo en startups tecnológicas. El trabajo se hará en sprints, con la posibilidad de ajustar, en cada uno de ellos, el rumbo del proyecto según la retroalimentación que dé el jefe de TI de Mutualista, que también será uno de los usuarios para los que se está construyendo este sistema.

La plataforma es, en términos económicos, una inversión estratégica. La digitalización de los servicios reduce costos operativos a mediano plazo, y eso resulta trascendental para instituciones como Mutualista Imbabura. Una optimización en la reducción de trámites presenciales en los servicios financieros llevará a una optimización en el uso de los recursos humanos, y los aliados financieros de Mutualista Imbabura podrán volver a poner en servicio a sus colaboradores en tareas que realmente les son productivas. Esto, en resumidas cuentas, no solamente hace competitiva a la institución, sino que también aumenta la productividad del país.

1.3 Objetivos

1.3.1 Objetivo General

Implementar un sistema de Banca Electrónica Empresarial para la gestión de productos financieros de la Mutualista Imbabura, alineado a los controles SEPS-009 y con pruebas OWASP top 10 integradas.

1.3.2 Objetivos Específicos

- Fundamentar el diseño del sistema de Banca Electrónica Empresarial mediante la revisión sistemática de la literatura existente sobre sistemas de banca en línea, normativas SEPS-009, estándares de seguridad OWASP top 10 y técnicas de cifrado AES-256.
- Implementar el sistema de Banca Electrónica Empresarial, incluyendo módulos para consulta de saldos, transferencias, pagos y administración de cuentas y un módulo de seguridad MFA, asegurando la integración de los controles de seguridad y la usabilidad del sistema.
- Validar la eficacia y seguridad del sistema de Banca Electrónica Empresarial mediante la aplicación de pruebas técnicas, pruebas de usuario y auditorías de seguridad basadas en los controles SEPS-009 y OWASP top 10, para garantizar su correcto funcionamiento en entornos reales.

CAPÍTULO II
MARCO TEÓRICO

2.1. Antecedentes

2.2.1 Design and Implementation of an Efficient Electronic Bank Management Information System Based Data Warehouse and Data Mining Processing

Luo et al. [1] desarrollaron un sistema de información de gestión de bancos electrónicos eficiente basado en un almacén de datos (DW) y procesamiento de minería de datos (EEBMIS-DWMP) para mejorar la toma de decisiones. La metodología implicó la preparación de datos de marketing bancario, la aplicación de procesos ETL (Extract, Transform, Load) y la implementación de vistas indexadas (agrupadas y no agrupadas) en el DW. Luego, se aplicaron y evaluaron seis algoritmos de minería de datos (MLPNN, Naïve Bayes, Random Forest, Regresión Logística, SVM y C5.0) usando métricas de rendimiento y tiempo de ejecución. El resultado más relevante fue que el EEBMIS-DWMP, especialmente con las vistas indexadas, redujo drásticamente el tiempo de respuesta de las consultas y mejoró la precisión, con C5.0 mostrando la mejor eficiencia. Una limitación identificada es que las vistas indexadas podrían requerir mantenimiento si las filas modificadas demandan más capacidad, lo que sugiere la necesidad de pruebas en un entorno práctico.

2.1.2 Decision as a Service for Transaction Banking Using Service-Oriented Modeling Architecture Methodology

Gaol et al. [2]buscaron transformar la unidad de banca transaccional de un sistema con dependencias generales a un sistema independiente y escalable que operara a pequeña escala funcional, con el fin de obtener una ventaja competitiva en la industria bancaria. Esto aborda la lentitud en la implementación de reglas de decisión y los riesgos asociados a los sistemas tradicionales. La metodología se basó en la arquitectura de modelado orientada a servicios (SOMA), que incluye fases de modelado de negocio, gestión de soluciones, identificación, especificación y realización. La solución propuesta integra API, ESB (Enterprise Service Bus), BPM (Business Process Management) y BRM (Business Rule Management). El resultado más relevante es que el modelo "Decisión como Servicio (DaaS)" mejoró significativamente los tiempos de respuesta y la eficiencia operativa, demostrando escalabilidad y flexibilidad en comparación con los sistemas monolíticos, al separar las cargas funcionales. Una limitación es que el estudio se realizó con una versión "sandbox" de la API, lo que podría afectar la

generalizabilidad a entornos de producción reales y se necesita investigación adicional para la optimización de costos.

2.1.3 Effective Filter for Common Injection Attacks in Online Web Applications

Ibarra-Fiallos et al. [3] se propusieron diseñar e implementar un filtro de protección eficaz contra ataques de inyección comunes (como SQLi, CI, XSS) en aplicaciones web, especialmente para aquellas que no pueden ser reescritas. La metodología se centró en un filtro de validación de campos de entrada basado en OWASP Stinger, un conjunto de expresiones regulares y un proceso de sanitización. El filtro, desarrollado en Java y desplegado como un módulo Jboss/Wildfly, valida tanto caracteres fundamentales como declaraciones complejas (JSON y XML) mediante esquemas. El resultado más relevante fue una precisión del 98.4% en la detección de ataques y un tiempo de procesamiento promedio de 50 ms, lo que demuestra su alta fiabilidad sin requerir recursos computacionales adicionales. Una limitación es que el uso de listas blancas de expresiones regulares podría prohibir cadenas benignas si no están incluidas explícitamente, y la validación de JSON/XML mediante esquemas podría ser insuficiente si los propios esquemas no incluyen validaciones adecuadas.

2.1.4 Testing and Exploiting Tools to Improve OWASP Top Ten Security Vulnerabilities Detection

Aljabri et al. [4] investigaron y probaron herramientas existentes para la detección y explotación de las diez principales vulnerabilidades de seguridad web de OWASP (lista 2021), con el fin de medir sus tiempos de ejecución y categorizarlas según sus características. La metodología incluyó el estudio y la evaluación de diversas herramientas, categorizándolas por su interfaz (GUI o línea de comandos), comportamiento (estático o dinámico), estructura (caja blanca o caja negra), formato de informe, compatibilidad con sistemas operativos y protocolos objetivo. Las pruebas se realizaron en una máquina estándar, promediando los resultados de tres ejecuciones por herramienta. El resultado más relevante es la taxonomía de herramientas de detección y explotación de vulnerabilidades de OWASP Top 10, que muestra que las herramientas con escaneo activo tardan más pero detectan más vulnerabilidades, mientras que otras son más rápidas pero ofrecen menos características. La limitación es que el trabajo no presenta la herramienta combinada propuesta, dejándola como trabajo futuro, y se destaca que una sola herramienta no es suficiente para detectar la mayoría de las vulnerabilidades.

2.1.5 Securing Open Banking with Model-View-Controller Architecture and OWASP

Kellezi et al. [9] buscaron desarrollar una solución web innovadora para la banca abierta (Open Banking) que permitiera a los usuarios ahorrar dinero y fomentar hábitos positivos, al tiempo que garantizaba un alto nivel de seguridad. La metodología propuso una arquitectura basada en Modelo-Vista-Controlador (MVC) para la aplicación web, combinada con el microframework Flask, la plataforma Heroku y PostgreSQL para el almacenamiento de datos. La seguridad se analizó utilizando la metodología OWASP Top 10 y un modelo de amenaza. El resultado más relevante fue que muchas de las medidas de seguridad se manejan automáticamente por los componentes de la pila tecnológica (como Flask y SQLAlchemy), previniendo eficazmente inyecciones y mejorando la gestión de sesiones y la protección CSRF. La principal limitación es el manejo comprometido de la capa TLS en la API de Nordea (versión sandbox), que causaba fallas al usar HTTPS y obligaba a usar HTTP, poniendo en riesgo la confidencialidad de los paquetes enviados, un problema que no pudo ser mitigado por la aplicación y que carece de documentación suficiente.

2.1.6 Overview of Intelligent Online Banking System Based on HERCULES Architecture

Luo aet al [10]. presenta el diseño e implementación de un sistema de banca en línea inteligente basado en la arquitectura HERCULES, con el objetivo de superar los desafíos de seguridad, complejidad y frecuentes actualizaciones que enfrentan los sistemas bancarios tradicionales, así como de mejorar la inteligencia del negocio. La metodología empleada combina la ingeniería de software con algoritmos de aprendizaje automático, tales como redes neuronales (para depósitos inteligentes), árboles de decisión (para préstamos a "cuello blanco") y K-means (para la clasificación de clientes). Asimismo, el trabajo aborda la seguridad de las transacciones con mecanismos robustos y una novedosa implementación de balanceo de carga "suave" (soft load balancing) que reduce la dependencia del hardware costoso. El resultado más relevante es la notable mejora en la inteligencia y seguridad del sistema de banca en línea respecto a las soluciones existentes, lo que optimiza la automatización y disminuye los costos operativos. No obstante, el sistema tiene la limitación de exigir un alto nivel de experiencia y conocimientos especializados en finanzas y en la propia arquitectura HERCULES a usuarios, analistas y desarrolladores, además de presentar deficiencias en los modos de control de código abierto y MVC.

2.1.7 A Study Using OWASP On Secure Open Banking Architecture

Kumar et al [11]. propone un marco tecnológico seguro para una aplicación web de banca abierta, con el objetivo de abordar las vulnerabilidades inherentes de ciberseguridad

cuando los bancos exponen datos a través de APIs, centrándose específicamente en la API de Nordea. La metodología implica la construcción de una aplicación utilizando un stack tecnológico que incluye el microframework Flask, la plataforma en la nube Heroku y PostgreSQL con SQLAlchemy para el almacenamiento de datos, mientras se adapta una arquitectura Modelo-Vista-Controlador (MVC) con una Capa de Abstracción de API para facilitar la interacción segura. El sistema propuesto fue evaluado rigurosamente contra los 10 principales riesgos de seguridad de aplicaciones web de OWASP. El resultado más relevante es la provisión de recomendaciones detalladas y un marco robusto que mejora significativamente la seguridad y la comunicación con APIs financieras abiertas, demostrando que muchas precauciones de seguridad son manejadas por las tecnologías elegidas o fácilmente implementadas dentro de la plataforma Flask. No obstante, una limitación clave identificada es el procesamiento inadecuado de las capas TLS por parte de la propia API de Nordea, lo que provoca fallos operativos con HTTPS y presenta riesgos para los datos del usuario, y la evaluación se vio limitada por el uso de un entorno de prueba (sandbox), restringiendo la capacidad de estimar el impacto comercial real y los agentes de amenaza debido a la falta de contexto de usuario y negocio.

2.2 Banca Electrónica Empresarial

2.2.1 Definición y características

La banca electrónica empresarial, o banca corporativa digital, permite a las empresas gestionar transacciones y operaciones financieras mediante plataformas electrónicas, optimizando eficiencia, accesibilidad y comodidad, transformando el panorama financiero con herramientas que agilizan la gestión [12]. Impulsada por el cambio en los hábitos de los consumidores, que demandan servicios financieros accesibles 24/7 similares a las redes sociales, y por la competencia de fintechs y gigantes tecnológicos, que ofrecen soluciones ágiles como pagos o crowdfunding con menor presión regulatoria, la transformación digital de los bancos tradicionales sigue tres etapas: reacción, desarrollando canales y productos digitales como apps móviles y billeteras digitales; adaptación tecnológica, rediseñando infraestructuras para mayor flexibilidad con tecnologías como cloud computing y automatización mediante inteligencia artificial para experiencias omnicanal; y posicionamiento estratégico, adoptando cambios organizativos y metodologías ágiles para fidelizar clientes mediante analíticas avanzadas, aunque enfrenta resistencias internas y desafíos regulatorios [13]. Esta digitalización genera nuevas formas de interacción con clientes, transforma oficinas en centros de ventas, reorienta el rol de empleados hacia productos de alto valor, implementa metodologías

ágiles y métricas para evaluar el rendimiento digital, esperando reducciones de costos a corto plazo y mayores ingresos a largo plazo, siendo las entidades más avanzadas las mejor preparadas para competir. La seguridad es crucial, aplicando protocolos como cifrado y SSL/TLS para proteger transacciones y datos, aunque estudios en Ecuador muestran que el 20% de las entidades bancarias tienen debilidades en certificados digitales, exponiendo a usuarios a ciberriesgos, por lo que implementar medidas robustas es esencial para garantizar confianza en los servicios digitales [14].

2.2.2 Diferencias entre banca personal y empresarial

La banca personal y la banca empresarial, si bien se enmarcan dentro del objetivo general de la inclusión financiera, entendida como el acceso de personas y empresas a productos y servicios financieros adecuados[12], presentan diferencias sustanciales en su enfoque, productos y desafíos, lo que impacta directamente la experiencia del usuario y la operativa bancaria.

Una distinción fundamental radica en la segmentación de clientes y la oferta de productos y servicios[12]. La banca personal se centra en clientes individuales (personas), ofreciendo servicios básicos como la apertura de cuentas de ahorro que facilitan transacciones y el acceso a medios de pago electrónicos[12] Las plataformas de banca virtual para este segmento han sido objeto de estudios específicos sobre su seguridad[14] En contraste, la banca empresarial atiende a una diversidad de entidades que van desde microempresas, PYMES, hasta el sector comercial y corporativo[12]. La segunda fuente analiza la oferta de créditos dirigidos a estos diferentes segmentos empresariales[12]

El volumen y el tipo de crédito también varían notablemente entre los segmentos[12]. Según el estudio empírico de la segunda fuente para el año 2016, el microcrédito, dirigido a microempresas o unidades económicas de bajos ingresos, representó menos del 5% del total de la cartera de créditos en tres de los cuatro bancos grandes analizados, mientras que el crédito al segmento comercial tuvo la mayor participación[12]. Además, se destaca que el otorgamiento de crédito a las MIPYMES representa un alto riesgo para las instituciones financieras[12], una consideración que puede influir en la disponibilidad y las condiciones de los productos ofrecidos a este segmento en comparación con otros de la banca personal o empresarial.

En cuanto a la atención a grupos específicos, la banca puede diseñar productos o modificar los existentes para atender a grupos vulnerables (como beneficiarios de pensiones alimenticias) o microempresarios/mujeres empresarias[12]. Algunas metodologías, como las

Microfinanzas Grupales, atienden a personas con negocios similares que se garantizan solidariamente, mostrando cómo la inclusión financiera puede combinar aspectos personales y microempresariales, a menudo enfocándose en áreas con índices de pobreza o baja densidad poblacional[12].

2.2.3 Beneficios de la digitalización financiera

La digitalización en el ámbito financiero representa una evolución significativa que ofrece ventajas considerables tanto para los individuos que utilizan los servicios bancarios como para las instituciones que los proveen[15].

Para los usuarios de servicios financieros, la digitalización se traduce principalmente en mayor conveniencia y accesibilidad El E-Banking, por ejemplo, permite acceder a las operaciones bancarias en cualquier momento y desde cualquier lugar, utilizando dispositivos conectados a internet. Esta flexibilidad es especialmente apreciada por las generaciones más familiarizadas con la tecnología. Al poder gestionar las finanzas de forma remota, los usuarios ahorran una cantidad significativa de tiempo al evitar desplazamientos a sucursales físicas y filas. Los datos de encuestas en Machala, por ejemplo, revelan que una gran mayoría de usuarios percibe un ahorro de más de cinco horas gracias al E-Banking [15].

Otro beneficio fundamental es la seguridad mejorada que ofrecen las plataformas digitales. Estas plataformas proporcionan un entorno protegido para realizar operaciones financieras, lo que contribuye a reducir el riesgo de robos asociados a las transacciones presenciales. La mayoría de los usuarios encuestados se siente seguro o muy seguro utilizando estos servicios, y una abrumadora mayoría reporta no haber experimentado problemas de seguridad[15].

Además, la digitalización empodera a los usuarios al brindarles un mayor control sobre sus finanzas personales. El acceso fácil y constante a la información de cuentas y la posibilidad de monitorear transacciones permiten una mejor gestión financiera. Una proporción muy alta de usuarios siente que el E-Banking ha mejorado definitivamente o en cierta medida su control financiero. Las plataformas digitales también ponen a disposición de los usuarios una amplia variedad de servicios sin necesidad de visitar una sucursal, siendo las transferencias bancarias el servicio más utilizado con alta frecuencia, seguido de pagos de servicios básicos, pagos de tarjetas, consultas de saldo y otras operaciones como pagos de facturas, recargas móviles, inversiones y solicitudes de préstamos. En general, el E-Banking ha supuesto una mejoría significativa en la experiencia financiera general de los usuarios, siendo percibido como mucho

mejor o mejor en comparación con otros métodos de banca tradicional por una amplia mayoría. La digitalización también es clave para la inclusión financiera, facilitando el acceso a servicios formales a poblaciones que tradicionalmente han estado excluidas del sistema[15], [16].

Un beneficio económico fundamental para las instituciones es la reducción de costos operativos. La optimización de la red de oficinas físicas, la externalización de servicios y la automatización contribuyen a esta disminución de gastos. En Machala, por ejemplo, una parte considerable de las instituciones financieras reportó una reducción de costos operativos superior al 51% gracias al E-Banking. La digitalización también impulsa un aumento en los ingresos y la rentabilidad, evidenciado por el incremento en el volumen de transacciones digitales. De hecho, todas las instituciones encuestadas en Machala reportaron que sus ingresos han aumentado con la implementación del E-Banking[15].

Para mantener la competitividad en el mercado actual, la digitalización es esencial, permitiendo a los bancos adaptarse y responder a la aparición de nuevos competidores y tecnologías [15]. El uso de tecnologías como el Big Data facilita un mejor conocimiento del cliente, permitiendo a los bancos analizar grandes cantidades de datos para comprender el comportamiento y las necesidades de los usuarios, personalizar la oferta y descubrir nuevas oportunidades de negocio. La digitalización también es crucial para la gestión de riesgos y la prevención de fraude, habilitando el análisis de datos en tiempo real y el monitoreo constante de transacciones. Las medidas comunes incluyen la autenticación de dos factores, el cifrado de datos y el monitoreo de transacciones. Finalmente, la inversión en tecnologías digitales fomenta la innovación y el desarrollo de nuevos productos y servicios, y la disponibilidad y análisis de datos de calidad soporta una mejor toma de decisiones estratégicas[17].

2.2.4 Plataformas tecnológicas utilizadas

La seguridad es un pilar fundamental de la información que un usuario debe recibir en el servicio de banca virtual. Las plataformas financieras utilizan protocolos de seguridad como SSL (Secure Sockets Layer), que fue concebido para establecer seguridad en las comunicaciones por internet, y TLS (Transport Layer Security). TLS es el protocolo de cifrado más utilizado en Internet y tiene como objetivo garantizar la integridad y confidencialidad del mensaje que transita por la red en la capa de transporte. Permite la comunicación segura de extremo a extremo, evitando la intercepción y alteración de la información. El protocolo HTTPS (Hypertext Transfer Protocol Secure), la versión segura del HTTP, utiliza protocolos de seguridad como TLS para cifrar la información que transita entre el cliente y el servidor. La

aplicación de certificados de seguridad, técnicas de encriptación, uso de llaves simétricas y asimétricas, y la combinación de suites de cifrados convierten al protocolo HTTP en HTTPS, evitando que personas mal intencionadas intercepten y utilicen los datos para usos indebidos. Un certificado válido y fuerte, junto con una clave privada fuerte, son primordiales para la seguridad de la comunicación. Los conjuntos de cifrado son grupos de algoritmos y reglas utilizados para cifrar y descifrar información, diseñados para garantizar la seguridad y confidencialidad de los datos. Se recomienda la aplicación y configuración de TLS 1.3 y TLS 1.2 del lado del servidor, y deshabilitar versiones anteriores. La aplicación de HSTS (HTTP Strict Transport Security) también se recomienda para mitigar vulnerabilidades al proteger el tráfico HTTP (HTTPS), impidiendo que un atacante convierta una conexión HTTPS en HTTP[14].

Más allá de la seguridad subyacente, las plataformas de banca digital utilizan diversas herramientas tecnológicas. El Big Data es fundamental en el sector financiero, ya que la información representa un insumo principal para realizar un adecuado análisis de riesgo y es considerada una ventaja competitiva. Implica procesos computacionales para analizar grandes cantidades de datos y extraer información relevante. Entre sus características se encuentran el volumen, variedad, velocidad, valor y veracidad. En el sector financiero, el Big Data ayuda a gestionar riesgos mediante información en tiempo real, detectar y prevenir fraude, lanzar ofertas personalizadas, facilitar la retención de clientes, y descubrir nuevas oportunidades de negocio mediante modelos predictivos que analizan el comportamiento del cliente[17].

Además, las API (Application Programming Interface) y la banca abierta (Open Banking) surgen como oportunidades para que los bancos ofrezcan nuevos servicios financieros y no financieros en colaboración con otras organizaciones. La automatización de procesos es otra parte de la transformación digital, que busca eliminar tareas manuales y repetitivas, mejorando la eficiencia y agilidad[13], [15], [16].

2.3 Normativa SEPS-009

2.3.1 Contexto legal y regulatorio en Ecuador

En Ecuador, el marco legal y regulatorio de la banca electrónica se fundamenta en el Código Orgánico Monetario y Financiero, la Ley Orgánica de Economías Populares y Solidarias y las normativas complementarias emitidas por la Superintendencia de Economía Popular y Solidaria (SEPS). Esta entidad, conforme a los artículos 62 y 74 del mencionado Código, tiene la responsabilidad de vigilar, auditar, controlar y supervisar el funcionamiento de

las entidades financieras, así como el cumplimiento de las medidas de seguridad establecidas para los canales electrónicos. En particular, la normativa SEPS-009 estandariza la seguridad en los canales electrónicos de entidades como cooperativas de ahorro y crédito, cajas centrales y asociaciones mutualistas, con el objetivo de proteger los activos de información críticos, prevenir fraudes y garantizar la implementación rigurosa de mecanismos de autenticación y control de acceso, alineándose con la Ley Orgánica de Protección de Datos Personales para consolidar un ecosistema normativo robusto que responda a los desafíos de la digitalización en el sector financiero ecuatoriano[18].

2.3.2 Requisitos técnicos para sistemas financieros

La normativa SEPS-009 establece requisitos técnicos específicos que las entidades financieras deben implementar para garantizar operaciones seguras en entornos electrónicos. Estos incluyen el uso de algoritmos de cifrado reconocidos internacionalmente, como AES-256, para proteger la información crítica tanto en reposo como en tránsito, asegurando que, en caso de interceptación, los datos permanezcan inaccesibles a accesos no autorizados. Asimismo, se exige la implementación de mecanismos de registro y trazabilidad de transacciones, mediante herramientas como registros inalterables en SQL Server o, en algunos casos, tecnologías de blockchain, que permiten auditar y verificar detalladamente cada operación electrónica. Además, los entornos tecnológicos deben garantizar una adecuada segregación de funciones y controles de acceso, mediante la gestión de privilegios basada en niveles y la implementación de autenticación multifactor, para evitar conflictos de interés y reforzar la seguridad [18], [19].

2.3.3 Controles exigidos por la SEPS

La normativa SEPS-009 establece controles específicos que las entidades financieras deben implementar para mitigar los riesgos asociados al uso de canales electrónicos. Entre estos, destaca la autenticación multifactor (MFA), que combina al menos dos factores como algo que el usuario sabe, tiene o es para validar la identidad en el acceso inicial al sistema y en transacciones de alto valor, reduciendo significativamente el riesgo de accesos fraudulentos. Asimismo, se exige realizar pruebas de penetración periódicas, que simulan ataques cibernéticos, junto con auditorías de seguridad internas y externas, para identificar vulnerabilidades, validar la efectividad de los controles y establecer medidas correctivas de manera oportuna. Además, los sistemas deben generar notificaciones inmediatas al usuario ante transacciones, especialmente en casos de actividades inusuales o intentos fallidos de acceso,

fortaleciendo el control del usuario y facilitando la detección rápida de posibles fraudes. Por último, se requiere implementar herramientas de monitoreo continuo en tiempo real, como el registro de direcciones IP, el seguimiento de sesiones y la configuración de alertas automáticas para detectar patrones anómalos que puedan indicar brechas de seguridad [18], [19].

2.4 Estándares de Seguridad OWASP Top 10

2.4.1 Introducción a OWASP

El Open Web Application Security Project (OWASP), fundado en 2001 como una organización sin fines de lucro, se dedica a mejorar la seguridad de las aplicaciones web mediante recursos, guías, herramientas y proyectos educativos de acceso abierto, orientados a desarrolladores, evaluadores de seguridad y organizaciones para identificar y mitigar riesgos en entornos digitales. Entre sus aportes más destacados se encuentra el OWASP Top 10, una lista actualizada periódicamente que identifica las vulnerabilidades más críticas en aplicaciones web, reflejando la evolución de las amenazas y las tendencias en ciberseguridad, y proporcionando un marco de referencia para el desarrollo seguro, así como para auditorías y pruebas de penetración; este recurso promueve mejores prácticas que fomentan una cultura de desarrollo centrada en la integridad, confidencialidad y disponibilidad de los sistemas [20], [21].

2.4.2 Las 10 principales vulnerabilidades web

La versión más reciente del OWASP Top 10, actualizada en 2021, identifica las vulnerabilidades más críticas que comprometen la seguridad de las aplicaciones web. Entre estas, la pérdida de control de acceso permite a usuarios no autorizados acceder o modificar recursos y datos sensibles debido a mecanismos de restricción inadecuados. Los fallos criptográficos, relacionados con la protección deficiente de datos sensibles en reposo o en tránsito, como el uso inadecuado de algoritmos como AES-256, pueden exponer información confidencial. Las vulnerabilidades de inyección, como inyección SQL o de comandos, permiten a atacantes ejecutar comandos maliciosos o acceder a datos protegidos a través de entradas inseguras. El diseño inseguro, derivado de la falta de controles de seguridad en las fases iniciales del desarrollo, requiere una arquitectura de seguridad integrada para prevenir errores. La configuración de seguridad incorrecta, como configuraciones por defecto o desactualizadas en servidores, deja vulnerabilidades explotables. El uso de componentes y software desactualizados, como bibliotecas o frameworks con vulnerabilidades conocidas, representa un riesgo si no se actualizan. Los fallos en la identificación y autenticación, como una gestión

inadecuada de sesiones, permiten la suplantación de usuarios legítimos. Los fallos en la integridad del software y los datos afectan la confiabilidad de actualizaciones y dependencias. La ausencia o deficiencia en el registro y monitoreo de seguridad dificulta la detección temprana de incidentes. Por último, la falsificación de solicitudes del lado del servidor (SSRF) permite a atacantes inducir solicitudes maliciosas desde el servidor, accediendo a recursos internos o desviando datos sensibles [22], [23].

2.4.3 Recomendaciones para mitigación

El Open Web Application Security Project (OWASP) proporciona estrategias prácticas para mitigar las vulnerabilidades identificadas en su Top 10. Estas incluyen la implementación de controles de acceso robustos, mediante autenticación multifactor (MFA) y políticas de gestión de sesiones seguras, asegurando que los usuarios tengan solo los permisos necesarios para sus roles y evitando la elevación indebida de privilegios. También se recomienda proteger los datos sensibles en reposo y en tránsito con algoritmos criptográficos modernos, como AES-256, revisando periódicamente su implementación y actualizando bibliotecas criptográficas. La validación rigurosa de entradas, mediante consultas parametrizadas o declaraciones preparadas, es crucial para prevenir inyecciones de código malicioso, como inyección SQL. Incorporar la seguridad desde la fase de planificación, adoptando metodologías de diseño seguro y modelos de amenaza, requiere revisiones extensivas de arquitectura y código. La gestión proactiva de configuraciones implica estandarizar y fortalecer servidores y aplicaciones, eliminando configuraciones por defecto. Mantener componentes actualizados, aplicando parches de seguridad oportunamente, y automatizar la gestión de versiones refuerza la integridad del sistema. El registro y monitoreo continuo de actividades, mediante soluciones que alerten sobre comportamientos inusuales, permite la detección temprana de incidentes. Por último, fomentar una cultura de seguridad mediante capacitación continua, prácticas recomendadas y participación en comunidades como OWASP fortalece el desarrollo seguro [24], [25].

2.5 Técnicas de Cifrado y Protección de Datos

2.5.1 Fundamentos de criptografía

Los fundamentos de la criptografía se centran en la ciencia de ocultar la escritura, derivada del griego "Kriptos" (ocultar) y "Graphos" (escritura). Su meta principal es mantener la seguridad de la información al codificar mensajes para hacerlos ilegibles, de manera que solo el receptor autorizado pueda comprenderlos. El mensaje inicial se conoce como "texto claro", mientras que el mensaje codificado se denomina "texto cifrado". El proceso de convertir el texto

claro en texto cifrado es el "cifrado", y el proceso inverso para recuperar el texto claro del texto cifrado es el "descifrado". Las claves son un elemento esencial de los algoritmos criptográficos. Una clave es como una llave física: se necesita la clave correcta, con el patrón de bits y la longitud apropiados, para descifrar la información cifrada. La criptografía es un campo de estudio que involucra Ciencias Computacionales, Matemáticas, Teoría de Números y Complejidad Computacional. Se apoya en matemáticas complejas para fortalecer la seguridad de las transacciones informáticas. Los algoritmos y protocolos criptográficos son los principales medios para ofrecer servicios de seguridad informática como autenticación, confidencialidad, integridad y no repudio. Por ejemplo, un criptosistema asimétrico es un conjunto de algoritmos que facilitan las operaciones de cifrado y descifrado, construidos en capas desde definiciones matemáticas hasta protocolos de seguridad. A pesar de sus capacidades, los sistemas criptográficos tienen limitaciones que evolucionan con los avances tecnológicos, como algoritmos que pueden perder efectividad con el tiempo debido al aumento en la velocidad y potencia de los equipos de cómputo[26], [27], [28].

2.5.2 Cifrado AES-256: estructura y aplicación

En cuanto al cifrado, el Advanced Encryption Standard (AES) es presentado como uno de los algoritmos de cifrado simétrico de bloque más ampliamente utilizados en la actualidad. Originalmente llamado "Rijndael", fue creado por Vincent Rijmen y Joan Daemen. AES opera como un cifrado por bloques y, aunque inicialmente diseñado con longitud variable, el estándar lo define con un tamaño de bloque de 128 bits. Esto implica que los datos se dividen en segmentos de 16 bytes, que pueden visualizarse como una matriz de 4x4. Las fuentes indican que AES está comenzando a reemplazar algoritmos más antiguos como DES. Su aplicación se da en el cifrado simétrico, a menudo después de un intercambio seguro de claves utilizando métodos asimétricos como RSA. Es relevante notar que las fuentes proporcionadas describen el algoritmo AES con un tamaño de bloque estándar de 128 bits, como se mencionó, pero no hacen referencia específica al cifrado AES-256, su estructura particular, o aplicaciones concretas de esta variante[27], [28].

2.5.3 Cumplimiento con la Ley de Protección de Datos Personales en Ecuador

Respecto al cumplimiento con la Ley de Protección de Datos Personales en Ecuador, las fuentes consultadas no contienen información directa sobre leyes o regulaciones específicas de protección de datos personales en Ecuador. Sin embargo, sí enfatizan la fundamental

importancia de la seguridad para proteger la información sensible tanto de los usuarios como de las empresas involucradas en transacciones electrónicas. Se resalta que la insuficiencia en la seguridad puede acarrear problemas significativos, tanto económicos como legales, para usuarios y plataformas. Específicamente, se menciona la preocupación relacionada con el no repudio de las transacciones comerciales cuando los datos han sido vulnerados. Las referencias sugieren que las actividades comerciales electrónicas deberían contar con la certificación correspondiente ante el sector financiero y proponen como futuras áreas de investigación la mejora de los sistemas de verificación de usuarios en las plataformas para reforzar la seguridad[28].

2.6 Autenticación Multifactor (MFA)

2.6.1 Tipos de factores de autenticación

La autenticación es el proceso fundamental para verificar la identidad de un usuario que busca acceder a un sistema o información específicos, garantizando que solo los usuarios autorizados tengan acceso. Los sistemas de autenticación pueden clasificarse, por ejemplo, según lo que el usuario sabe. El método más básico es la autenticación de factor único (SFA), que se basa en la verificación de un solo dato, típicamente un nombre de usuario y una contraseña. Históricamente, estos sistemas evolucionaron desde prácticas antiguas como los sellos romanos hasta adaptarse a la necesidad de proteger la información en la era digital. Como respuesta a las vulnerabilidades del SFA, surgió la autenticación de dos factores (2FA). Esta utiliza dos formas diferentes de verificación de identidad, como una contraseña y un código de seguridad enviado a un dispositivo móvil, añadiendo una segunda "llave" o un "token", que es un código o serie de caracteres generada aleatoriamente. Las fuentes mencionan diversos métodos específicos de 2FA como los PINs basados en SMS, TOTP, HOTP, Google Authenticator y FIDO U2F. La autenticación multifactor (MFA) se presenta como una expansión o una combinación de factores adicionales, pudiendo incluir elementos como nombre de usuario, contraseña, un número aleatorio y datos biométricos como la huella dactilar. Además, la autenticación biométrica es otro tipo destacado que emplea características físicas únicas del usuario, difíciles de falsificar, como huellas dactilares, reconocimiento facial, voz o iris, para verificar la identidad. Estas características biométricas pueden usarse como un segundo token o llave secundaria. Se señala que cada método tiene sus pros y contras, y la elección adecuada depende de las necesidades de seguridad y la comodidad del usuario. También se mencionan los autenticadores de hardware como dispositivos físicos que generan

códigos de seguridad, siendo más seguros que los métodos basados en SMS o aplicaciones y que pueden incluir funciones biométricas[29], [30].

2.6.2 Implementación de MFA en sistemas financieros

El sector financiero está atravesando una intensa transformación digital, lo que hace que la seguridad de la información sensible sea fundamental tanto para los usuarios como para las empresas. La seguridad insuficiente puede generar inconvenientes financieros y legales. En este contexto, la implementación de la autenticación multifactor (MFA) es presentada como una estrategia clave para aumentar la seguridad y dificultar el acceso no autorizado a sistemas y datos, recomendada como parte de las políticas de acceso seguro. Las referencias describen un esquema seguro de autenticación multifactor propuesto en el contexto de la nube, que podría ser relevante para sistemas financieros digitalizados. Este esquema incluye fases de registro y un procedimiento de inicio de sesión donde las credenciales tradicionales como el nombre de usuario y la contraseña actúan como el primer factor, mientras que la verificación exitosa del segundo factor o factores requiere elementos adicionales como un certificado en la nube, una OTP por correo electrónico y una OTP por móvil. El objetivo general es mejorar los sistemas de verificación de usuarios, aunque las fuentes no profundizan en los detalles técnicos específicos de cómo los sistemas financieros implementan la MFA más allá de este esquema propuesto y la mención de aplicar políticas de acceso seguro. Se sugiere que las actividades comerciales electrónicas con datos sensibles deberían contar con certificación ante el sector financiero[29], [30], [31].

2.6.3 Seguridad y experiencia de usuario

La seguridad en los sistemas de autenticación tiene como objetivo principal proteger la información y los sistemas al verificar la identidad de los usuarios, permitiendo el acceso solo a quienes están autorizados. Las referencias destacan que, aunque sistemas como SFA y 2FA son importantes, presentan vulnerabilidades como contraseñas débiles, phishing, ataques de intermediarios, reutilización de contraseñas para SFA; e ingeniería social, intercepción de mensajes y malware para 2FA, lo cual subraya los riesgos de seguridad. El ecosistema financiero digitalizado se enfrenta a riesgos significativos, incluyendo ciberamenazas. La insuficiencia de seguridad puede tener consecuencias negativas importantes. Sin embargo, también se resalta que los sistemas financieros están diseñados para generar la confianza necesaria en sus operaciones. En cuanto a la experiencia del usuario, la transformación digital del sector busca beneficiar al cliente, enfocándose en la receptividad, confianza y seguridad. El

uso de canales digitales, especialmente los smartphones, ha cambiado los hábitos de consumo y se ha popularizado debido a la facilidad y comodidad para realizar operaciones. No obstante, la adaptación a estas nuevas tecnologías puede ser un desafío para algunos segmentos de la población, como los adultos mayores, quienes pueden preferir la atención presencial debido a la falta de familiarización con productos digitales y aplicaciones, lo que impacta su experiencia de usuario y la inclusión. Las referencias sugieren que los proveedores deben comunicarse con los clientes para generar confianza, mejorar las aplicaciones y convertirse en herramientas preferidas, adaptándose a las preferencias y hábitos del cliente. A pesar de que la 2FA, por ejemplo, puede presentar inconvenientes de compatibilidad, ofrece una capa adicional de seguridad que dificulta el acceso no autorizado. La autenticación biométrica es percibida por algunos como más rápida y cómoda. Se reconoce la necesidad de alfabetización digital y financiera, ya que una parte significativa de los usuarios desconoce conceptos básicos de seguridad como el phishing o el uso de autenticadores, y muchos perciben la seguridad de los pagos por internet como poco segura. En última instancia, la seguridad en línea se ve como un esfuerzo conjunto entre proveedores de servicios y usuarios[29], [30], [31].

2.7 Metodología Ágil Scrum

2.7.1 Fundamentos de Scrum

Scrum es definido como un marco de trabajo ligero diseñado para ayudar a personas, equipos y organizaciones a generar valor a través de soluciones adaptables para problemas complejos. Su esencia radica en ser un enfoque empírico y basado en el pensamiento Lean, donde el conocimiento proviene de la experiencia y las decisiones se toman basándose en lo observado, mientras se reducen los desperdicios y se centra en lo esencial. Scrum emplea un enfoque iterativo e incremental para optimizar la previsibilidad y controlar el riesgo. Se apoya en tres pilares empíricos fundamentales que dan vida a sus eventos: la Transparencia, la Inspección, y la Adaptación. La transparencia asegura que el proceso y el trabajo sean visibles para quienes lo realizan y quienes lo reciben, basando las decisiones importantes en el estado percibido de los artefactos formales. La inspección implica la revisión frecuente y diligente de los artefactos y el progreso hacia los objetivos acordados para detectar variaciones o problemas. La adaptación requiere ajustar el proceso o los materiales lo antes posible si algún aspecto se desvía de los límites aceptables o si el producto es inaceptable. El uso exitoso de Scrum depende de que las personas vivan cinco valores clave: Compromiso, Enfoque, Apertura, Respeto y Coraje. Estos valores guían al Equipo Scrum en su trabajo y comportamiento, y su asimilación ayuda a que los pilares empíricos cobren vida construyendo confianza. El marco de Scrum es

deliberadamente incompleto, definiendo solo las partes necesarias para implementar su teoría, y se basa en la inteligencia colectiva de sus usuarios. Define roles específicos, eventos formales y artefactos que juntos conforman su estructura. Los roles esenciales son el Scrum Master, responsable de establecer Scrum y asegurar su comprensión y efectividad; el Propietario del Producto (Product Owner), responsable de maximizar el valor del producto y gestionar el Product Backlog; y los Desarrolladores, quienes se comprometen a crear un incremento útil en cada Sprint[32], [33], [34].

2.7.2 Ventajas de su uso en entornos regulados

La referencia señala que SCRUM posee diversos beneficios, entre los cuales se destacan la entrega de resultados en plazos cortos, ya sean mensuales o quincenales, asegurando que los requisitos prioritarios sean atendidos en primer lugar. Contribuye a la gestión de las expectativas del cliente, quien tiene la capacidad de definir sus propias expectativas, asignar valor a cada requisito y especificar el tiempo estimado para su finalización. Permite la obtención de resultados anticipados, lo que posibilita al cliente utilizar las funcionalidades más importantes incluso antes de que el proyecto concluya, facilitando así una recuperación temprana de la inversión y el uso de un producto al que solo le restan características de menor relevancia. Esto se logra mediante la priorización de requisitos basada en el costo y el valor que aportan al cliente. Otra ventaja es la flexibilidad y adaptación, permitiendo al cliente reorientar el proyecto según sus nuevas prioridades, lo cual se consigue a través de la replanificación de requisitos y prioridades al inicio de cada ciclo iterativo. Se menciona también la maximización del Retorno de Inversión (ROI) mediante la priorización de requisitos medidos por su valor. En caso de que el beneficio previsto sea inferior al costo de desarrollo, el cliente tiene la opción de finalizar el proyecto. La metodología facilita la definición y mitigación temprana de riesgos desde la primera iteración, con la filosofía de que es preferible identificar y abordar los errores lo antes posible. Esto se logra implementando un desarrollo iterativo e incremental que evita postergar actividades riesgosas vinculadas a la entrega de requisitos. Se observa una mayor productividad y calidad debido a que el equipo perfecciona y simplifica su metodología de trabajo en cada iteración al analizar retrospectivamente sus procesos, apoyándose en una comunicación constante. Promueve el trabajo conjunto entre el cliente y el equipo, involucrándolos desde el planteamiento inicial de los requisitos y detalles hasta el análisis de los resultados obtenidos. Finalmente, fomenta un equipo autogestionado y motivado, donde los individuos pueden emplear su creatividad para solucionar problemas y determinar la mejor forma de organizar su trabajo para completar los requisitos definidos en una iteración[35].

2.7.3 Ciclo de desarrollo iterativo

El Sprint es el evento contenedor fundamental en Scrum y representa el latido del corazón de este marco. Es un período de tiempo fijo de un mes o menos, o típicamente de una a cuatro semanas, durante el cual se crea valor. Un nuevo Sprint comienza inmediatamente después de que concluye el anterior. Todos los eventos de Scrum ocurren dentro del Sprint, incluyendo la Planificación del Sprint, el Daily Scrum, la Revisión del Sprint y la Retrospectiva del Sprint. Durante un Sprint, no se hacen cambios que pongan en peligro el Objetivo del Sprint, no disminuye la calidad, se refina el Product Backlog según sea necesario, y el alcance puede clarificarse y renegociarse con el Propietario del Producto. Los Sprints permiten la previsibilidad al asegurar la inspección y adaptación del progreso hacia un objetivo. Sprints más cortos pueden generar más ciclos de aprendizaje y limitar el riesgo. Cada Sprint puede verse como un proyecto corto, con el objetivo de producir un Incremento utilizable del producto, que es un paso concreto hacia el Objetivo del Producto. Al final del Sprint, el equipo realiza una Revisión del Sprint para inspeccionar el resultado y una Retrospectiva del Sprint para planificar mejoras para el siguiente. Este ciclo completo se repite para el siguiente Sprint, proporcionando múltiples oportunidades de aprendizaje y mejora, lo cual es considerado la esencia de Agile[32], [33], [34].

2.8 Arquitectura de Software en N Capas

2.8.1 Principios y beneficios

La arquitectura N-Capas es un enfoque fundamental para gestionar la complejidad en aplicaciones empresariales, basada en la división lógica de la aplicación según sus responsabilidades. Esto adhiere al principio de separación de intereses y facilita a los desarrolladores encontrar funcionalidades específicas. Una ventaja clave es la reutilización de código común de bajo nivel, lo que estandariza implementaciones y reduce la cantidad de código. Las capas también permiten aplicar restricciones en su comunicación, logrando encapsulación y minimizando el impacto de los cambios: si una capa se modifica, solo las capas que interactúan directamente con ella deberían verse afectadas. Un diseño robusto implica alta cohesión interna y bajo acoplamiento entre capas, comunicándose a través de interfaces bien definidas. Es crucial distinguir entre capas (divisiones lógicas) y niveles (distribución física en servidores separados), lo que permite mayor flexibilidad y escalabilidad. Como se dice, "Si cree que una buena arquitectura es cara, pruebe una mala arquitectura"[36], [37], [38].

El Diseño Orientado al Dominio (DDD) no es solo una arquitectura, sino una aproximación para diseñar software centrada en el Dominio del Negocio. Es ideal para aplicaciones empresariales complejas con mucha lógica de negocio. Su objetivo principal, al integrarse con arquitecturas N-Capas, es lograr un acoplamiento mínimo entre el Modelo del Dominio y otras capas como la presentación o la infraestructura. DDD promueve un Lenguaje Ubicuo, acordado con expertos del negocio, para modelar el Dominio, e identifica patrones clave como Repositorios, Entidades y Servicios. Sus beneficios incluyen mejor comunicación en el equipo, mayor extensibilidad al desacoplar el Dominio de la infraestructura, y una mejor capacidad de prueba y mocking gracias al bajo acoplamiento[36], [37].

La Inyección de Dependencias (DI) y la Inversión de Control (IoC) son técnicas esenciales para lograr el desacoplamiento entre componentes. Se basan en el Principio de Inversión de Dependencias (DIP): las capas de alto nivel no deben depender de las de bajo nivel; ambas deben depender de abstracciones (interfaces). Esto hace que los componentes de alto nivel sean independientes de las implementaciones concretas de los de bajo nivel, favoreciendo el diseño de clases con una única responsabilidad (SRP) y facilitando enormemente el testing unitario. Aunque no son obligatorias para una arquitectura orientada al Dominio, favorecen el aislamiento del Dominio. La división en Módulos también es útil para organizar y particionar modelos de dominio complejos, reduciendo la complejidad y aplicando alta cohesión interna con bajo acoplamiento entre módulos[36].

2.8.2 Aplicación en desarrollo con .NET

La implementación de estos estilos arquitecturales en el ecosistema .NET es clave. Aunque las aplicaciones .NET tradicionales a menudo se desarrollan como unidades únicas, las aplicaciones de negocio importantes se benefician de la separación lógica en capas. En Visual Studio, las aplicaciones de ASP.NET Core suelen evolucionar de un monolito inicial (organizado por carpetas) a soluciones de múltiples proyectos (.DLL), donde cada proyecto reside lógicamente en una capa. Cada capa o sub-capa puede tener su propio proyecto para mayor flexibilidad y desacoplamiento[36].

La Capa de Infraestructura de Persistencia de Datos es la encargada de acceder y persistir datos, utilizando frecuentemente frameworks ORM como Entity Framework (EF), que se adapta bien a patrones DDD como Repositorios y Unit of Work. Las entidades POCO (Plain Old CLR Objects) se recomiendan para la Capa de Dominio por su independencia de la tecnología de persistencia. Los contratos de Repositorios se definen en la Capa de Dominio,

mientras que su implementación está en la Capa de Infraestructura. Para la Capa de Servicios Distribuidos, tecnologías como WCF o ASMX se utilizan, comunicando datos a través de los límites físicos con DTOs (Data Transfer Objects) o entidades serializadas. La Capa de Presentación puede usar tecnologías como WPF, Silverlight o ASP.NET MVC, y patrones como MVVM, que facilitan la separación entre la vista y el ViewModel permitiendo el trabajo independiente de diseñadores y desarrolladores. La gestión de transacciones en .NET se recomienda con System.Transactions. La autenticación y autorización pueden implementarse con arquitecturas orientadas a Claims (con WIF y ADFS 2.0). La gestión de caché puede usar tecnologías como Microsoft AppFabric-Cache, y la validación de datos el Validation Block de Microsoft Enterprise Library. El desacoplamiento interno, especialmente entre la Capa de Dominio y la de Infraestructura, se logra usando interfaces y contenedores IoC/DI como Unity[36].

2.8.3 Escalabilidad y mantenibilidad

La arquitectura N-Capas contribuye significativamente a la escalabilidad y mantenibilidad al dividir la aplicación en partes manejables con responsabilidades claras. La separación de intereses y el bajo acoplamiento entre capas minimizan el impacto de los cambios, lo que facilita el mantenimiento y reduce costos. El DDD, al centrarse en un Modelo de Dominio desacoplado de la infraestructura, permite que la lógica de negocio, que cambia con frecuencia, se modifique y pruebe de forma más sencilla e independiente. Un bajo acoplamiento entre módulos también reduce la complejidad y mejora la mantenibilidad[36].

La escalabilidad se relaciona con la capacidad de la aplicación para manejar una carga creciente. Mientras que los monolitos se escalan en su totalidad, las arquitecturas N-Niveles permiten distribuir físicamente las capas en servidores separados, permitiendo escalar niveles específicos para mayor eficiencia. La capa de base de datos relacional suele ser el punto más crítico para la escalabilidad horizontal. El uso de un cache distribuido (como Microsoft AppFabric-Cache) puede mejorar significativamente la escalabilidad, el rendimiento y la disponibilidad al minimizar el acceso a la base de datos. El control de concurrencia optimista también mejora la escalabilidad al evitar bloqueos de datos prolongados[36].

En cuanto a la mantenibilidad, la posibilidad de sustituir implementaciones de capas o componentes gracias a las interfaces y la inyección de dependencias (DI/IoC) mejora la flexibilidad y reduce el código a modificar. La automatización de pruebas unitarias, facilitada por el diseño desacoplado, ayuda a mantener la calidad y detectar problemas rápidamente,

reduciendo los costos de mantenimiento. Aunque la complejidad arquitectural inicial de una N-Capas orientada al Dominio es mayor que la de una aplicación simple orientada a datos, la mantenibilidad y el desacoplamiento resultantes son mucho mayores a largo plazo. La capacidad de adaptar la arquitectura para soportar escenarios de escalabilidad (Web-Farms) y alta disponibilidad mediante la gestión adecuada de estados y caches distribuidos es crucial. En resumen, la arquitectura N-Capas facilita la reutilización, estandarización, desarrollo independiente y mejor mantenibilidad, lo que reduce costos y permite que el sistema sea escalable ante los cambios[36].

2.9 Bases de Datos y Transacciones en SQL Server.

2.9.1 Propiedades ACID

Las propiedades ACID (Atomicidad, Consistencia, Aislamiento y Durabilidad) son fundamentales para la arquitectura de las bases de datos relacionales modernas como SQL Server. Una transacción de base de datos se define como una secuencia de operaciones que se tratan como una sola unidad bajo el principio de "hacer todo o no hacer nada". Para que una transacción sea exitosa, debe cumplir con las pruebas ACID. Una transacción puede incluir operaciones como leer, escribir, eliminar o actualizar datos. Por ejemplo, una operación de retiro de dinero de un cajero automático implica leer el saldo, actualizarlo y registrar la transacción, todas tratadas como una sola unidad. SQL Server soporta diferentes modos de transacción, incluyendo el modo de confirmación automática (predeterminado), implícito y explícito[39].

Atomicidad garantiza que todas las operaciones dentro de una transacción DML (insertar, actualizar, eliminar) se completen con éxito o, si alguna falla, todas se reviertan, asegurando que la base de datos no quede en un estado inconsistente. La Consistencia asegura que la base de datos esté en un estado válido y coherente antes de iniciar la transacción y permanezca así después de que se complete. Esto implica mantener las reglas y restricciones de integridad. Por ejemplo, en una transferencia bancaria, la suma total de dinero debe ser la misma antes y después de la transacción. El Aislamiento asegura que el estado intermedio de una transacción no sea visible para otras transacciones concurrentes, evitando inconsistencias que podrían surgir si las transacciones se leyeran o modificaran datos que están siendo alterados por otra transacción en curso. Finalmente, la Durabilidad asegura que una vez que una transacción se completa con éxito, los cambios realizados son permanentes y persistirán incluso en caso de fallas del sistema, interrupciones de energía o cualquier otro evento anormal[39].

2.9.2 Integridad y seguridad de los datos financieros

La integridad y seguridad de los datos financieros almacenados en SQL Server son cruciales, ya que estas bases de datos a menudo contienen información sensible como registros personales y datos financieros. La implementación de una metodología de seguridad por capas proporciona una defensa en profundidad. SQL Server incluye varias características de seguridad para contrarrestar amenazas y proteger las aplicaciones de base de datos[40], [41].

Para proteger los datos sensibles, se pueden aplicar medidas en diferentes niveles. A nivel de columna, SQL Server ofrece Always Encrypted para cifrar datos tanto en reposo como en tránsito, y Enmascaramiento Dinámico de Datos (DDM) para ofuscar datos sensibles en los resultados de consultas basándose en roles de usuario. Se recomienda usar Always Encrypted sobre DDM siempre que sea posible. También se pueden conceder permisos GRANT específicos a nivel de columna. A nivel de fila, la Seguridad de Nivel de Fila (RLS) permite controlar el acceso a las filas de una tabla basándose en el contexto de ejecución del usuario, asegurando que los usuarios solo vean los registros que les corresponden. RLS se puede usar junto con Always Encrypted o DDM para maximizar la postura de seguridad. Para la protección de datos en reposo a nivel de archivo, el Cifrado de Datos Transparente (TDE) cifra los archivos de base de datos, copias de seguridad y archivos tempdb, impidiendo que puedan ser leídos sin los certificados adecuados. TDE se admite para trabajar con otras funcionalidades de seguridad[40].

Además de la protección de datos, la identidad y autenticación son clave. SQL Server soporta autenticación de Windows y autenticación de SQL Server (modo mixto). Las estrategias de seguridad basada en roles con privilegios mínimos y el uso de grupos de Windows/Active Directory son prácticas recomendadas. Se prefiere la autenticación de Active Directory siempre que sea posible. Requerir contraseñas seguras y complejas, así como el uso de autenticación multifactor para cuentas de alto privilegio, ayuda a proteger contra robos de credenciales. Las cuentas de servicio administradas de grupo (gMSA) mejoran la seguridad al automatizar la administración de contraseñas. Limitar los derechos concedidos a las cuentas de DBA y usar CONTROL SERVER en lugar del rol sysadmin también aumenta la seguridad. El mantenimiento de registros históricos de los cambios de datos mediante tablas temporales puede ayudar a abordar cambios accidentales o malintencionados y es útil para la auditoría de cambios. Las herramientas de evaluación de seguridad como la Evaluación de Vulnerabilidades y la Clasificación y Detección de Datos ayudan a identificar y reportar sensibilidades y vulnerabilidades. Conocer las amenazas comunes como la inyección de código SQL, ataques

de canal lateral, fuerza bruta, difusión de contraseñas y ransomware es importante para implementar las protecciones adecuadas.

2.9.3 Herramientas para trazabilidad y auditoría

La auditoría es esencial para rastrear accesos, cambios y posibles brechas en bases de datos que contienen datos sensibles. SQL Server ofrece herramientas de auditoría nativas y se pueden complementar con herramientas de terceros[41].

La herramienta principal nativa es la función de Auditoría de SQL Server. Permite crear auditorías de servidor que contienen especificaciones de auditoría de servidor para eventos de servidor, y especificaciones de auditoría de base de datos para eventos de base de datos. Estas auditorías pueden capturar eventos a nivel de servidor y de base de datos utilizando especificaciones de auditoría. Los administradores pueden definir qué acciones rastrear, dónde guardar los registros (archivo binario, Visor de Eventos de Windows o registro de seguridad de Windows) y el formato. Los resultados de la auditoría se envían a un destino. Se pueden leer los registros de eventos de Windows con el Visor de Eventos o, para destinos de archivo, usar el Visor del Archivo de Registros en SSMS o la función fn_get_audit_file. Todas las ediciones de SQL Server soportan auditorías a nivel de servidor, y a nivel de base de datos desde SQL Server 2016 SP1. Aunque potentes, las herramientas nativas tienen limitaciones, como monitoreo limitado en tiempo real sin integración externa y dependencia de informes manuales o de terceros. La documentación oficial de Microsoft detalla cómo el sistema genera y almacena registros de auditoría[41], [42], [43].

Los Eventos Extendidos son el método preferido actualmente para rastrear eventos de forma granular, sustituyendo a SQL Trace. SQL Server Audit utiliza Eventos Extendidos para facilitar la creación de auditorías. Se pueden integrar con vistas del sistema para consultar registros[41], [42], [43].

Otras técnicas para auditoría y trazabilidad incluyen Desencadenadores de SQL Server, que pueden rastrear eventos DML/DDL para tablas específicas pero requieren esfuerzo de creación y mantenimiento. La Lectura de Registros de Transacciones registra todo lo que ocurre en SQL Server sin sobrecarga adicional, pero los archivos son difíciles de leer directamente sin herramientas. Las Tablas Temporales ofrecen una solución complementaria al mantener versiones históricas de registros, permitiendo ver el historial de cambios, pero requieren la creación de tablas de historial e interacción con T-SQL para ver resultados. Change Tracking y Change Data Capture (CDC) también rastrean cambios de datos, siendo CDC una mejora sobre

Change Tracking con mejor información de auditoría, aunque carece de una interfaz de usuario fácil para visualización[40], [42].

Integrar DataSunrise mejora las capacidades de auditoría nativas de SQL Server, añadiendo políticas contextuales, mejor seguimiento del comportamiento de los usuarios y registro inteligente. DataSunrise se despliega como proxy o agente para capturar y analizar tráfico. Ofrece un ámbito de auditoría más detallado que rastrea consultas, resultados y contexto de acceso. Proporciona monitoreo en tiempo real con alertas basadas en reglas e integraciones, mayor flexibilidad de configuración con reglas personalizadas, un motor de informes integrado y opciones de almacenamiento flexibles. DataSunrise también soporta enmascaramiento de datos tanto estático como dinámico, a diferencia del enmascaramiento dinámico nativo de SQL Server. La configuración de DataSunrise para auditar SQL Server implica instalar la plataforma, registrar la instancia de SQL Server y configurar reglas de auditoría para eventos y criterios específicos. Esto centraliza y visualiza los resultados de la auditoría, permitiendo filtrar eventos, generar informes y exportar a sistemas SIEM. Al manejar grandes volúmenes de datos sensibles en entornos complejos, combinar las herramientas nativas de SQL Server con una solución como DataSunrise hace que las auditorías sean más potentes y accionables[41].

CAPÍTULO III
MATERIALES Y MÉTODOS

3.1 Descripción del área de estudio

El desarrollo del presente proyecto se llevará a cabo en la Mutualista Imbabura, institución financiera ecuatoriana con una amplia trayectoria en la promoción del ahorro y el financiamiento responsable, que en los últimos años ha emprendido un proceso integral de transformación digital, orientado a fortalecer su infraestructura tecnológica, modernizar sus canales de atención y ofrecer soluciones innovadoras que respondan a las necesidades cambiantes de sus clientes.

En este contexto, la implementación de un sistema de Banca Electrónica Empresarial constituye un componente estratégico que permitirá optimizar la gestión de productos financieros mediante un entorno web seguro, escalable y alineado a las disposiciones normativas de la Superintendencia de Economía Popular y Solidaria (SEPS), específicamente a los controles SEPS-009; adicionalmente, el proyecto incorpora mecanismos de seguridad fundamentados en las pruebas OWASP Top 10 que permitirán prevenir vulnerabilidades y garantizar la integridad, confidencialidad y disponibilidad de la información.

3.2 Enfoque y Tipo de Investigación

La presente investigación adopta un enfoque cualitativo ya que permite analizar de manera objetiva las necesidades tecnológicas y funcionales de la Mutualista Imbabura en el ámbito de la gestión de productos financieros empresariales, mediante la recolección y procesamiento de información de los actores principales del sistema recabada mediante entrevistas.

Así también, se ha considerado que el tipo de investigación aplicada es la más pertinente, ya que mediante el diseño e implementación del sistema de Banca Electrónica Empresarial la presente investigación se orienta a la resolución de una necesidad real dentro de un contexto organizacional específico al interior de la Mutualista Imbabura.

3.3 Recolección de información

El proceso de recolección de información se desarrollará de manera sistemática, combinando técnicas de análisis documental, entrevistas estructuradas y observación directa de los procesos financieros y tecnológicos que actualmente se ejecutan en la Mutualista Imbabura:

- En una primera etapa, se realizará la revisión de documentos institucionales como políticas de seguridad de la información, manuales de procedimientos financieros, y lineamientos de cumplimiento normativo relacionados con la SEPS-009, con el propósito de identificar los estándares regulatorios y los requerimientos mínimos que el nuevo sistema debe cumplir.
- En una segunda etapa, se aplicarán entrevistas estructuradas y reuniones de levantamiento de información con personal de las áreas de Tecnologías de la Información, Banca Empresarial, Seguridad Informática y Cumplimiento Normativo, a fin de identificar y priorizar los requisitos funcionales y no funcionales del sistema.

Este proceso permitirá estructurar de manera ordenada el desarrollo incremental del sistema de banca electrónica, facilitando la planificación de los sprints de desarrollo, la trazabilidad de los requisitos y la alineación con los objetivos estratégicos de la transformación digital de la Mutualista Imbabura.

3.4 Procesamiento de la información

El procesamiento de la información se desarrollará de forma estructurada y rigurosa, con el propósito de garantizar la confiabilidad y validez de los datos obtenidos en la fase de recolección.

- En una primera etapa, se realizará la organización, depuración y codificación de la información proveniente de las distintas fuentes, diferenciando entre datos cualitativos (obtenidos de entrevistas y observación directa) y datos cuantitativos (provenientes de encuestas).
- En el caso específico de las encuestas aplicadas se efectuará la tabulación de los resultados mediante herramientas estadísticas SPSS, permitiendo cuantificar las respuestas y obtener frecuencias, porcentajes y gráficos comparativos que facilitarán la interpretación de los datos y la identificación de patrones o tendencias relacionados con el uso de servicios digitales, las percepciones sobre seguridad, usabilidad y confiabilidad del sistema actual, así como las expectativas frente al nuevo sistema de Banca Electrónica Empresarial.

3.5 Desarrollo del sistema

3.5.1 Análisis

3.5.1.1 Definición de requisitos funcionales

Definir los requisitos funcionales permite establecer con claridad qué debe hacer el sistema para satisfacer las necesidades del usuario y cumplir con los objetivos del proyecto, garantizando que el sistema responda a las operaciones reales de la Mutualista Imbabura; a continuación, en la Tabla 1 se describen todos los requisitos funcionales definidos para el presente proyecto.

Requisitos Funcionales (RF)	**Breve descripción**
RF-01 Validar credenciales	Autenticar al usuario verificando usuario y contraseña en la base de datos.
RF-02 Bloquear tras N intentos	Inhabilitar el acceso temporalmente tras varios intentos fallidos consecutivos.
RF-03 Registrar eventos de acceso	Registrar en bitácora cada inicio de sesión exitoso o fallido para auditoría.
RF-04 Generar OTP	Crear un código temporal de seis dígitos como segundo factor de autenticación.
RF-05 Expiración de OTP	Definir el tiempo máximo de validez del código OTP antes de caducar.
RF-06 Validar OTP en servidor	Comprobar que el código OTP ingresado sea correcto y esté vigente.
RF-07 Generar token de recuperación	Emitir un enlace único para restablecer la contraseña del usuario.
RF-08 Enviar correo de restablecimiento	Enviar al correo del usuario el enlace seguro para cambiar su contraseña.
RF-09 Invalidar token usado	Desactivar automáticamente el enlace de recuperación tras su uso.
RF-10 Crear/editar/desactivar usuarios	Gestionar el ciclo de vida de los usuarios desde el panel administrativo.

Requisitos Funcionales (RF)	Breve descripción
RF-11 Búsqueda y paginación de usuarios	Localizar usuarios aplicando filtros y paginación.
RF-12 Validaciones de datos de usuario	Evitar duplicados y garantizar integridad de la información registrada.
RF-13 Definir roles	Crear y gestionar perfiles de acceso (Administrador, Operador, Aprobador).
RF-14 Asignar permisos por acción	Definir qué acciones puede realizar cada rol dentro del sistema.
RF-15 Consultar saldos	Mostrar el saldo actual y disponible de las cuentas asociadas.
RF-16 Filtrar movimientos	Permitir consultar transacciones aplicando filtros por fecha, tipo o canal.
RF-17 Exportar movimientos CSV	Descargar los resultados de consulta de movimientos a un archivo CSV.
RF-18 Validar saldo previo a transferencia	Comprobar que exista saldo suficiente antes de ejecutar la operación.
RF-19 Crear transacción interna	Registrar movimientos entre cuentas del mismo cliente.
RF-20 Generar comprobante PDF	Producir un comprobante digital de la transacción realizada.
RF-21 Registrar beneficiario externo	Ingresar y guardar información de beneficiarios interbancarios.
RF-22 Enviar datos al core bancario	Transmitir la instrucción de pago al sistema central o red interbancaria.
RF-23 Gestionar estados de transferencia	Controlar los estados Pendiente, Aprobada y Rechazada.
RF-24 Flujo solicitante/aprobador	Implementar el principio de doble control para aprobar transacciones.

Requisitos Funcionales (RF)	Breve descripción
RF-25 Límites por monto	Establecer umbrales monetarios que requieren aprobación adicional.
RF-26 Registro de evidencias	Guardar trazas y comprobantes digitales de cada aprobación.
RF-27 Bitácora de acciones	Registrar toda acción relevante del usuario en el sistema.
RF-28 Consulta y exportación de auditoría	Visualizar y descargar los registros de auditoría.
RF-29 Política de contraseñas	Aplicar reglas de complejidad, expiración e historial de contraseñas.
RF-30 Aviso de caducidad de contraseña	Notificar al usuario antes de la expiración de su clave.
RF-31 Generar PDF contractual	Crear documentos contractuales en PDF a partir de plantillas HTML.
RF-32 Firma y verificación OTP en documentos	Asociar una firma o verificación de seguridad mediante OTP.
RF-33 Enviar documentos por correo	Enviar automáticamente los documentos firmados al correo del cliente.
RF-34 Expiración de sesión	Cerrar sesión automáticamente tras un tiempo de inactividad configurado.
RF-35 Renovación de token de sesión	Extender la sesión activa de forma segura sin reautenticación completa.
RF-36 Protección CSRF	Evitar ataques de falsificación de solicitudes entre sitios mediante tokens.
RF-37 Delegar permisos temporalmente	Permitir a un usuario transferir permisos a otro por un tiempo definido.
RF-38 Revocación anticipada de delegación	Cancelar manualmente una delegación antes de su fecha de expiración.

Requisitos Funcionales (RF)	Breve descripción
RF-39 Auditoría de delegaciones	Registrar las acciones de delegación y revocación realizadas.
RF-40 Búsqueda avanzada de movimientos	Filtrar transacciones por rango, monto, canal o beneficiario.
RF-41 Paginación y orden de resultados	Facilitar la navegación y organización de los resultados de búsqueda.
RF-42 Totales parciales	Calcular totales agrupados de los movimientos filtrados.
RF-43 Exportación masiva a XLSX	Descargar grandes volúmenes de datos de movimientos en Excel.
RF-44 Firma o folio del reporte	Añadir un identificador único de seguridad a los reportes generados.
RF-45 Alta de beneficiario	Registrar nuevos beneficiarios en el sistema.
RF-46 Validación CCI/IBAN	Verificar la validez del número de cuenta y entidad financiera.
RF-47 Verificación de beneficiario	Confirmar la titularidad mediante microdepósito o código OTP.
RF-48 Carga de pagos masivos	Admitir la carga de archivos CSV/XLSX con múltiples pagos.
RF-49 Validación línea a línea	Verificar los datos de cada registro del archivo cargado.
RF-50 Simulación de errores	Previsualizar errores antes de ejecutar los pagos.
RF-51 Ejecución de pagos masivos	Procesar los lotes de transferencias validadas.
RF-52 Validación previa de nómina	Comprobar estructura y consistencia de los archivos de nómina.
RF-53 Totales por banco/cuenta	Calcular los montos totales por institución o cuenta destino.

Requisitos Funcionales (RF)	Breve descripción
RF-54 Detección de cuentas inválidas	Identificar cuentas inexistentes o erróneas antes del pago.
RF-55 Generar orden de pago individual	Crear la instrucción de pago para cada empleado o proveedor.
RF-56 Emitir comprobante PDF de pago	Generar recibos individuales en formato PDF.
RF-57 Reversos controlados	Permitir revertir operaciones de nómina con registro de motivo.
RF-58 Alta/edición de proveedores	Registrar y actualizar información de proveedores.
RF-59 Validación de cuenta bancaria	Comprobar la validez de la cuenta registrada del proveedor.
RF-60 Bloqueo de pagos no verificados	Impedir realizar pagos a cuentas sin verificación.
RF-61 Flujo de aprobación por niveles	Definir jerarquías para autorizar pagos según monto o tipo.
RF-62 Reglas por monto/día	Aplicar límites transaccionales diarios o por operación.
RF-63 Programación de pagos automáticos	Agendar pagos según calendario configurado.
RF-64 Alertas por días de mora	Notificar al usuario sobre obligaciones vencidas.
RF-65 Semáforo de riesgo	Clasificar deudores por nivel de riesgo visualmente.
RF-66 Recordatorios automáticos	Enviar notificaciones periódicas de vencimiento.
RF-67 Simulación de tasa/plazo CDP	Calcular proyecciones de intereses para depósitos a plazo.
RF-68 Cálculo de intereses CDP	Determinar el valor de intereses según tasa y plazo.
RF-69 Renovación de CDP	Permitir renovar automáticamente el depósito vencido.

Requisitos Funcionales (RF)	Breve descripción
RF-70 Reglas de barrido (sweep)	Definir transferencias automáticas entre cuentas.
RF-71 Ejecución programada de barridos	Ejecutar las transferencias en los horarios establecidos.
RF-72 Comprobante de barrido	Generar registro y comprobante de cada barrido ejecutado.
RF-73 Panel de KPIs	Mostrar métricas y estadísticas de uso del sistema.
RF-74 Exporte mensual de KPIs	Permitir descargar indicadores en formato de reporte.
RF-75 Logging estructurado	Registrar eventos con estructura uniforme para análisis.
RF-76 Correlación de trazas (traceId)	Relacionar operaciones entre servicios mediante un identificador común.
RF-77 Retención y rotación de logs	Administrar la duración y reemplazo automático de archivos de registro.
RF-78 Endpoints de salud	Exponer el estado operativo de los servicios del sistema.
RF-79 Métricas de rendimiento	Registrar tiempos de respuesta, errores y disponibilidad.
RF-80 Panel de disponibilidad	Visualizar la salud general de la aplicación y sus componentes.
RF-81 Adaptadores core bancario	Integrar la aplicación con el sistema central bancario (sandbox y producción).
RF-82 Configuración de tiempos y reintentos	Definir límites de espera y reintentos en las operaciones externas.
RF-83 Conciliación de estados	Sincronizar los estados entre el sistema de banca electrónica y el core.

Tabla 1: Definición de requisitos funcionales.

3.5.1.2 Definición de requisitos no funcionales

Definir los requisitos no funcionales permita garantizar la manera en que debe comportarse el sistema, asegurando no solo que funcione, sino que lo haga de forma segura, eficiente, confiable y conforme a la normativa, para este caso específico se deben considerar

aspectos clave como la seguridad de la información (SEPS-009 y OWASP Top 10), tiempos de respuesta, disponibilidad, usabilidad, escalabilidad y trazabilidad, los cuales son fundamentales para generar confianza en los usuarios empresariales y proteger las operaciones financieras; a continuación, en la Tabla 2 se describen todos los requisitos funcionales definidos para el presente proyecto.

Requisito no funcional	**Descripción del Requisito**
RNF-01 Seguridad de Autenticación	El sistema debe permitir el acceso mediante autenticación segura con usuario, contraseña y doble factor (2FA) para usuarios empresariales.
RNF-02 Cifrado de Datos	Toda la información debe viajar cifrada mediante protocolos HTTPS/TLS y mantenerse en reposo con cifrado AES-256.
RNF-03 Disponibilidad del Sistema	La plataforma debe estar disponible al menos el 99,5% del tiempo, garantizando continuidad operativa para clientes empresariales.
RNF-04 Rendimiento y Tiempo de Respuesta	Las operaciones principales (login, transferencias, consulta de saldos) deben ejecutarse en menos de 3 segundos.
RNF-05 Usabilidad	La interfaz debe ser intuitiva, accesible y fácil de usar para usuarios empresariales sin conocimientos técnicos especializados.
RNF-06 Escalabilidad	El sistema debe permitir el incremento de usuarios y transacciones sin degradar su rendimiento.
RNF-07 Cumplimiento Normativo SEPS-009	Debe cumplir con los controles de seguridad, auditoría, gestión de riesgos y trazabilidad exigidos por la SEPS-009.
RNF-08 Auditoría y Trazabilidad	Debe registrar los accesos, transacciones y modificaciones en logs auditables, vinculados a usuarios, fechas y direcciones IP.
RNF-09 Protección ante Vulnerabilidades (OWASP Top 10)	El sistema debe incorporar pruebas de seguridad para evitar inyecciones, fallos de autenticación, exposición de datos, y demás riesgos OWASP Top 10.

Requisito no funcional	Descripción del Requisito
RNF-10 Recuperación ante Desastres	Debe contar con copias de seguridad automatizadas y procedimientos de recuperación para volver a operar en menos de 2 horas tras una falla crítica.

Tabla 2: Definición de requisitos no funcionales.

3.5.1.3 Definición de los actores del sistema

Definir los actores del sistema permite identificar claramente quiénes interactúan con la plataforma, qué funciones realizan y qué nivel de acceso requieren, lo que garantiza un diseño organizado, seguro y alineado a los procesos reales de la entidad; a continuación, en la Tabla 3 se describen todos los requisitos funcionales definidos para el presente proyecto.

Actor	Descripción / Rol en el sistema
Cliente Empresarial (Usuario Principal)	Cliente autorizado que utiliza la plataforma para gestionar productos financieros, realizar transferencias, pagos, consultas de saldos y generación de reportes.
Administrador del Sistema (Área de TI)	Personal técnico que gestiona la configuración de la plataforma, crea perfiles, asigna permisos avanzados, monitorea el sistema, realiza mantenimiento y gestiona incidentes técnicos.
Oficial de Cumplimiento / Auditor Interno	Encargado de supervisar que las transacciones, registros y procesos cumplan con la normativa SEPS-009, monitorea operaciones inusuales, auditoría de logs y verificación de trazabilidad.
Superintendencia de Economía Popular y Solidaria (SEPS)	Entidad externa reguladora que no interactúa directamente con el sistema, pero establece las normas (SEPS-009) que condicionan su funcionamiento, seguridad y control.

Tabla 3: Definición de actores del sistema.

3.5.2 Planificación

3.5.2.1 Definición de las épicas de usuario

Para definir las épicas de usuario se aplicaron los siguientes criterios:

- Cada épica representa una parte significativa del sistema
- Una épica debe ser lo suficientemente grande para dividirse en varias historias de usuario, pero no tan amplia que resulte ambigua o infinita.
- Su descripción se redacta desde la perspectiva del usuario: Como [tipo de usuario], quiero [funcionalidad general], para [beneficio o propósito]
- Una épica debe tener definido cuándo se considera completada, es decir, qué condiciones generales debe cumplir.

Épica	**Descripción**	**Criterio de aceptación**
EPIC01 - Autenticación y Seguridad	Como administrador de seguridad, quiero que los usuarios accedan al sistema mediante autenticación segura y doble factor, para proteger mis cuentas y evitar accesos no autorizados.	• El sistema permite iniciar sesión con usuario, contraseña y código 2FA • Se bloquea el acceso tras varios intentos fallidos • Las sesiones expiran tras un tiempo de inactividad.
EPIC 02 - Gestión de Usuarios y Roles	Como administrador del sistema, quiero crear usuarios, asignar roles y definir permisos, para que cada empleado tenga acceso solo a las funciones autorizadas.	• Es posible crear, modificar o eliminar usuarios. • Los roles limitan correctamente las funciones disponibles. • Toda modificación queda registrada en la auditoría.
EPIC 03 - Integración y Disponibilidad	Como institución financiera, quiero que la banca electrónica esté integrada con el core bancario, para que las operaciones reflejen saldos reales y el sistema esté disponible en todo momento.	• Las transacciones se sincronizan con el core bancario. • Disponibilidad del sistema igual o superior al 99,5%. • Notificaciones automáticas operativas.
EPIC 04 - Auditoría y Cumplimiento	Como oficial de cumplimiento, quiero que todas las acciones realizadas en el sistema se	• Cada operación queda registrada con usuario, fecha e IP.

Épica	Descripción	Criterio de aceptación
	registren, para garantizar trazabilidad y cumplir la normativa SEPS-009.	• Se pueden generar reportes de auditoría exportables.
EPIC 05 - Observabilidad (Logging Técnico)	Como área de TI, quiero monitorear errores, caídas de servicio y alertas técnicas, para reaccionar rápidamente ante fallas del sistema.	• Se registran errores y eventos críticos. • Se generan alertas automáticas ante fallas o caídas.
EPIC 06 - Consultas y Movimientos	Como usuario empresarial, quiero consultar saldos y movimientos de mis cuentas, para mantener control financiero en tiempo real.	• Los saldos y movimientos se muestran actualizados. • Es posible filtrar movimientos y exportarlos en PDF o Excel.
EPIC 07 - Transacciones Internas y Externas	Como usuario, quiero realizar transferencias a cuentas propias, de terceros y otros bancos, para efectuar pagos de forma rápida y segura.	• Se validan fondos antes de ejecutar la transacción. • Se genera comprobante digital tras la operación.
EPIC 08 - Aprobaciones y Control de Riesgo	Como administrador empresarial, quiero aprobar o rechazar transacciones de alto valor, para controlar riesgos y evitar movimientos no autorizados.	• Las transacciones superiores al límite configurado requieren aprobación. • Los registros de aprobación o rechazo quedan documentados.
EPIC 09 - Documentación Digital	Como usuario, quiero descargar comprobantes, reportes y documentos electrónicos, para respaldar y verificar mis operaciones realizadas en el sistema.	• Cada transacción genera comprobante en PDF o XML. • Los documentos incluyen código único o QR de autenticidad.

Épica	Descripción	Criterio de aceptación
EPIC 10 - Nómina y Proveedores	Como empresa, quiero cargar archivos de pagos a empleados o proveedores, para procesar transferencias masivas de forma eficiente.	• El sistema acepta archivos Excel o CSV. • Se muestran pagos procesados, pendientes y errores.
EPIC 11 - Cartera y Productos Financieros	Como usuario empresarial, quiero consultar mis créditos, inversiones y productos financieros, para gestionar mis obligaciones y decisiones económicas.	• Es posible visualizar saldos, cuotas, cronogramas y vencimientos. • Se permite realizar pagos, prepagos o solicitudes de refinanciamiento.
EPIC 12 - Cash Management y KPIs	Como gerente financiero, quiero visualizar indicadores, flujo de caja y KPIs en tiempo real, para tomar decisiones basadas en datos.	• Los dashboards muestran saldos consolidados e indicadores financieros. • Los datos se actualizan desde el core bancario en tiempo real.

Tabla 4: Épicas de usuario.

3.5.2.2 Definición de las historias de usuario

Para definir las épicas de usuario se aplicaron los siguientes criterios:

- Cada historia debe describir una sola funcionalidad específica, sin incluir varios objetivos o condiciones.
- Cada historia debe estar asociada a una épica, que agrupe un conjunto de funcionalidades relacionadas.
- Las historias deben estar escritas en lenguaje natural, evitando tecnicismos innecesarios, de modo que puedan ser entendidas tanto por el equipo de desarrollo.
- Su descripción se redacta desde la perspectiva del usuario: Como [tipo de usuario], quiero [funcionalidad general], para [beneficio o propósito]

Épica	Historia de Usuario	Descripción
01 - Autenticación y Seguridad	HU-01 Validar credenciales	Como administrador de seguridad, quiero validar credenciales, para autenticar al

Épica	Historia de Usuario	Descripción
		usuario verificando usuario y contraseña en la base de datos.
01 - Autenticación y Seguridad	HU-02 Bloquear tras N intentos	Como administrador de seguridad, quiero bloquear tras n intentos, para inhabilitar el acceso temporalmente tras varios intentos fallidos consecutivos.
01 - Autenticación y Seguridad	HU-03 Registrar eventos de acceso	Como administrador de seguridad, quiero registrar eventos de acceso, para registrar en bitácora cada inicio de sesión exitoso o fallido para auditoría.
01 - Autenticación y Seguridad	HU-04 Generar OTP	Como administrador de seguridad, quiero generar otp, para crear un código temporal de seis dígitos como segundo factor de autenticación.
01 - Autenticación y Seguridad	HU-05 Expiración de OTP	Como administrador de seguridad, quiero expiración de otp, para definir el tiempo máximo de validez del código otp antes de caducar.
01 - Autenticación y Seguridad	HU-06 Validar OTP en servidor	Como administrador de seguridad, quiero validar otp en servidor, para comprobar que el código otp ingresado sea correcto y esté vigente.
01 - Autenticación y Seguridad	HU-07 Generar token de recuperación	Como administrador de seguridad, quiero generar token de recuperación, para emitir un enlace único para restablecer la contraseña del usuario.
01 - Autenticación y Seguridad	HU-08 Enviar correo de restablecimiento	Como administrador de seguridad, quiero enviar correo de restablecimiento, para enviar al correo del usuario el enlace seguro para cambiar su contraseña.
01 - Autenticación y Seguridad	HU-09 Invalidar token usado	Como administrador de seguridad, quiero invalidar token usado, para desactivar

Épica	Historia de Usuario	Descripción
		automáticamente el enlace de recuperación tras su uso.
01 - Autenticación y Seguridad	HU-29 Política de contraseñas	Como administrador de seguridad, quiero política de contraseñas, para aplicar reglas de complejidad, expiración e historial de contraseñas.
01 - Autenticación y Seguridad	HU-30 Aviso de caducidad de contraseña	Como administrador de seguridad, quiero aviso de caducidad de contraseña, para notificar al usuario antes de la expiración de su clave.
01 - Autenticación y Seguridad	HU-34 Expiración de sesión	Como administrador de seguridad, quiero expiración de sesión, para cerrar sesión automáticamente tras un tiempo de inactividad configurado.
01 - Autenticación y Seguridad	HU-35 Renovación de token de sesión	Como administrador de seguridad, quiero renovación de token de sesión, para extender la sesión activa de forma segura sin reautenticación completa.
01 - Autenticación y Seguridad	HU-36 Protección CSHU	Como administrador de seguridad, quiero protección csrf, para evitar ataques de falsificación de solicitudes entre sitios mediante tokens.
02 - Gestión de Usuarios y Roles	HU-10 Crear/editar/desactivar usuarios	Como administrador del sistema, quiero crear/editar/desactivar usuarios, para gestionar el ciclo de vida de los usuarios desde el panel administrativo.
02 - Gestión de Usuarios y Roles	HU-11 Búsqueda y paginación de usuarios	Como administrador del sistema, quiero búsqueda y paginación de usuarios, para localizar usuarios aplicando filtros y paginación.
02 - Gestión de Usuarios y Roles	HU-12 Validaciones de datos de usuario	Como administrador del sistema, quiero validaciones de datos de usuario, para evitar

Épica	Historia de Usuario	Descripción
		duplicados y garantizar integridad de la información registrada.
02 - Gestión de Usuarios y Roles	HU-13 Definir roles	Como administrador empresarial, quiero definir roles, para crear y gestionar perfiles de acceso (administrador, operador, aprobador).
02 - Gestión de Usuarios y Roles	HU-14 Asignar permisos por acción	Como administrador empresarial, quiero asignar permisos por acción, para definir qué acciones puede realizar cada rol dentro del sistema.
02 - Gestión de Usuarios y Roles	HU-37 Delegar permisos temporalmente	Como administrador del sistema, quiero delegar permisos temporalmente, para permitir a un usuario transferir permisos a otro por un tiempo definido.
02 - Gestión de Usuarios y Roles	HU-38 Revocación anticipada de delegación	Como administrador del sistema, quiero revocación anticipada de delegación, para cancelar manualmente una delegación antes de su fecha de expiración.
02 - Gestión de Usuarios y Roles	HU-39 Auditoría de delegaciones	Como administrador del sistema, quiero auditoría de delegaciones, para registrar las acciones de delegación y revocación realizadas.
03 - Integración y Disponibilidad	HU-78 Endpoints de salud	Como área de ti, quiero endpoints de salud, para exponer el estado operativo de los servicios del sistema.
03 - Integración y Disponibilidad	HU-79 Métricas de rendimiento	Como área de ti, quiero métricas de rendimiento, para registrar tiempos de respuesta, errores y disponibilidad.
03 - Integración y Disponibilidad	HU-80 Panel de disponibilidad	Como área de ti, quiero panel de disponibilidad, para visualizar la salud general de la aplicación y sus componentes.

Épica	Historia de Usuario	Descripción
03 - Integración y Disponibilidad	HU-81 Adaptadores core bancario	Como área de ti, quiero adaptadores core bancario, para integrar la aplicación con el sistema central bancario (sandbox y producción).
03 - Integración y Disponibilidad	HU-82 Configuración de tiempos y reintentos	Como área de ti, quiero configuración de tiempos y reintentos, para definir límites de espera y reintentos en las operaciones externas.
03 - Integración y Disponibilidad	HU-83 Conciliación de estados	Como área de ti, quiero conciliación de estados, para sincronizar los estados entre el sistema de banca electrónica y el core.
04 - Auditoría y Cumplimiento	HU-27 Bitácora de acciones	Como administrador del sistema, quiero bitácora de acciones, para registrar toda acción relevante del usuario en el sistema.
04 - Auditoría y Cumplimiento	HU-28 Consulta y exportación de auditoría	Como oficial de cumplimiento, quiero consulta y exportación de auditoría, para visualizar y descargar los registros de auditoría.
05 - Observabilidad (Logging)	HU-75 Logging estructurado	Como oficial de cumplimiento, quiero logging estructurado, para registrar eventos con estructura uniforme para análisis.
05 - Observabilidad (Logging)	HU-76 Correlación de trazas (traceId)	Como área de ti, quiero correlación de trazas (traceid), para relacionar operaciones entre servicios mediante un identificador común.
05 - Observabilidad (Logging)	HU-77 Retención y rotación de logs	Como oficial de cumplimiento, quiero retención y rotación de logs, para administrar la duración y reemplazo automático de archivos de registro.
06 - Consultas y Movimientos	HU-15 Consultar saldos	Como usuario, quiero consultar saldos, para mostrar el saldo actual y disponible de las cuentas asociadas.

Épica	Historia de Usuario	Descripción
06 - Consultas y Movimientos	HU-16 Filtrar movimientos	Como usuario, quiero filtrar movimientos, para permitir consultar transacciones aplicando filtros por fecha, tipo o canal.
06 - Consultas y Movimientos	HU-17 Exportar movimientos CSV	Como usuario, quiero exportar movimientos csv, para descargar los resultados de consulta de movimientos a un archivo csv.
06 - Consultas y Movimientos	HU-40 Búsqueda avanzada de movimientos	Como usuario, quiero búsqueda avanzada de movimientos, para filtrar transacciones por rango, monto, canal o beneficiario.
06 - Consultas y Movimientos	HU-41 Paginación y orden de resultados	Como usuario, quiero paginación y orden de resultados, para facilitar la navegación y organización de los resultados de búsqueda.
06 - Consultas y Movimientos	HU-42 Totales parciales	Como usuario, quiero totales parciales, para calcular totales agrupados de los movimientos filtrados.
06 - Consultas y Movimientos	HU-43 Exportación masiva a XLSX	Como usuario, quiero exportación masiva a xlsx, para descargar grandes volúmenes de datos de movimientos en excel.
06 - Consultas y Movimientos	HU-44 Firma o folio del reporte	Como usuario, quiero firma o folio del reporte, para añadir un identificador único de seguridad a los reportes generados.
07 - Transacciones Internas y Externas	HU-18 Validar saldo previo a transferencia	Como usuario, quiero validar saldo previo a transferencia, para comprobar que exista saldo suficiente antes de ejecutar la operación.
07 - Transacciones Internas y Externas	HU-19 Crear transacción interna	Como usuario, quiero crear transacción interna, para registrar movimientos entre cuentas del mismo cliente.
07 - Transacciones Internas y Externas	HU-20 Generar comprobante PDF	Como usuario, quiero generar comprobante pdf, para producir un comprobante digital de la transacción realizada.

Épica	Historia de Usuario	Descripción
07 - Transacciones Internas y Externas	HU-21 Registrar beneficiario externo	Como usuario, quiero registrar beneficiario externo, para ingresar y guardar información de beneficiarios interbancarios.
07 - Transacciones Internas y Externas	HU-22 Enviar datos al core bancario	Como usuario, quiero enviar datos al core bancario, para transmitir la instrucción de pago al sistema central o red interbancaria.
07 - Transacciones Internas y Externas	HU-23 Gestionar estados de transferencia	Como usuario, quiero gestionar estados de transferencia, para controlar los estados pendiente, aprobada y rechazada.
07 - Transacciones Internas y Externas	HU-45 Alta de beneficiario	Como usuario, quiero alta de beneficiario, para registrar nuevos beneficiarios en el sistema.
07 - Transacciones Internas y Externas	HU-46 Validación CCI/IBAN	Como usuario, quiero validación cci/iban, para verificar la validez del número de cuenta y entidad financiera.
07 - Transacciones Internas y Externas	HU-47 Verificación de beneficiario	Como usuario, quiero verificación de beneficiario, para confirmar la titularidad mediante microdepósito o código otp.
07 - Transacciones Internas y Externas	HU-48 Carga de pagos masivos	Como usuario, quiero carga de pagos masivos, para admitir la carga de archivos csv/xlsx con múltiples pagos.
07 - Transacciones Internas y Externas	HU-49 Validación línea a línea	Como usuario, quiero validación línea a línea, para verificar los datos de cada registro del archivo cargado.
07 - Transacciones Internas y Externas	HU-50 Simulación de errores	Como área de ti, quiero simulación de errores, para previsualizar errores antes de ejecutar los pagos.
07 - Transacciones Internas y Externas	HU-51 Ejecución de pagos masivos	Como usuario, quiero ejecución de pagos masivos, para procesar los lotes de transferencias validadas.
08 - Aprobaciones y Control de Riesgo	HU-24 Flujo solicitante/aprobador	Como administrador empresarial, quiero flujo solicitante/aprobador, para

Épica	Historia de Usuario	Descripción
		implementar el principio de doble control para aprobar transacciones.
08 - Aprobaciones y Control de Riesgo	HU-25 Límites por monto	Como administrador empresarial, quiero límites por monto, para establecer umbrales monetarios que requieren aprobación adicional.
08 - Aprobaciones y Control de Riesgo	HU-26 Registro de evidencias	Como administrador empresarial, quiero registro de evidencias, para guardar trazas y comprobantes digitales de cada aprobación.
08 - Aprobaciones y Control de Riesgo	HU-61 Flujo de aprobación por niveles	Como usuario, quiero flujo de aprobación por niveles, para definir jerarquías para autorizar pagos según monto o tipo.
08 - Aprobaciones y Control de Riesgo	HU-62 Reglas por monto/día	Como administrador empresarial, quiero reglas por monto/día, para aplicar límites transaccionales diarios o por operación.
08 - Aprobaciones y Control de Riesgo	HU-63 Programación de pagos automáticos	Como usuario, quiero programación de pagos automáticos, para agendar pagos según calendario configurado.
09 - Documentación Digital	HU-31 Generar PDF contractual	Como usuario, quiero generar pdf contractual, para crear documentos contractuales en pdf a partir de plantillas html.
09 - Documentación Digital	HU-32 Firma y verificación OTP en documentos	Como usuario, quiero firma y verificación otp en documentos, para asociar una firma o verificación de seguridad mediante otp.
09 - Documentación Digital	HU-33 Enviar documentos por correo	Como usuario, quiero enviar documentos por correo, para enviar automáticamente los documentos firmados al correo del cliente.
10 - Nómina y Proveedores	HU-52 Validación previa de nómina	Como usuario, quiero validación previa de nómina, para comprobar estructura y consistencia de los archivos de nómina.

Épica	Historia de Usuario	Descripción
10 - Nómina y Proveedores	HU-53 Totales por banco/cuenta	Como usuario, quiero totales por banco/cuenta, para calcular los montos totales por institución o cuenta destino.
10 - Nómina y Proveedores	HU-54 Detección de cuentas inválidas	Como usuario, quiero detección de cuentas inválidas, para identificar cuentas inexistentes o erróneas antes del pago.
10 - Nómina y Proveedores	HU-55 Generar orden de pago individual	Como usuario, quiero generar orden de pago individual, para crear la instrucción de pago para cada empleado o proveedor.
10 - Nómina y Proveedores	HU-56 Emitir comprobante PDF de pago	Como usuario, quiero emitir comprobante pdf de pago, para generar recibos individuales en formato pdf.
10 - Nómina y Proveedores	HU-57 Reversos controlados	Como usuario, quiero reversos controlados, para permitir revertir operaciones de nómina con registro de motivo.
10 - Nómina y Proveedores	HU-58 Alta/edición de proveedores	Como usuario, quiero alta/edición de proveedores, para registrar y actualizar información de proveedores.
10 - Nómina y Proveedores	HU-59 Validación de cuenta bancaria	Como usuario, quiero validación de cuenta bancaria, para comprobar la validez de la cuenta registrada del proveedor.
10 - Nómina y Proveedores	HU-60 Bloqueo de pagos no verificados	Como usuario, quiero bloqueo de pagos no verificados, para impedir realizar pagos a cuentas sin verificación.
11 - Cartera y Productos Financieros	HU-64 Alertas por días de mora	Como administrador del sistema, quiero alertas por días de mora, para notificar al usuario sobre obligaciones vencidas.
11 - Cartera y Productos Financieros	HU-65 Semáforo de riesgo	Como usuario, quiero semáforo de riesgo, para clasificar deudores por nivel de riesgo visualmente.

Épica	Historia de Usuario	Descripción
11 - Cartera y Productos Financieros	HU-66 Recordatorios automáticos	Como usuario, quiero recordatorios automáticos, para enviar notificaciones periódicas de vencimiento.
11 - Cartera y Productos Financieros	HU-67 Simulación de tasa/plazo CDP	Como usuario, quiero simulación de tasa/plazo cdp, para calcular proyecciones de intereses para depósitos a plazo.
11 - Cartera y Productos Financieros	HU-68 Cálculo de intereses CDP	Como usuario, quiero cálculo de intereses cdp, para determinar el valor de intereses según tasa y plazo.
11 - Cartera y Productos Financieros	HU-69 Renovación de CDP	Como usuario, quiero renovación de cdp, para permitir renovar automáticamente el depósito vencido.
12 - Cash Management y KPIs	HU-70 Reglas de barrido (sweep)	Como usuario, quiero reglas de barrido (sweep), para definir transferencias automáticas entre cuentas.
12 - Cash Management y KPIs	HU-71 Ejecución programada de barridos	Como usuario, quiero ejecución programada de barridos, para ejecutar las transferencias en los horarios establecidos.
12 - Cash Management y KPIs	HU-72 Comprobante de barrido	Como usuario, quiero comprobante de barrido, para generar registro y comprobante de cada barrido ejecutado.
12 - Cash Management y KPIs	HU-73 Panel de KPIs	Como gerente financiero, quiero panel de kpis, para mostrar métricas y estadísticas de uso del sistema.
12 - Cash Management y KPIs	HU-74 Exporte mensual de KPIs	Como usuario, quiero exporte mensual de kpis, para permitir descargar indicadores en formato de reporte.

Tabla 5: Historias de usuario.

3.5.2.3 Conformación del equipo SCRUM

Definir claramente los roles del equipo Scrum (ver Tabla 6) es fundamental porque garantiza una organización efectiva del trabajo, una comunicación fluida y una correcta ejecución del proyecto bajo los principios ágiles.

Rol	Descripción
Product Owner	• Gerente
Scrum Master	• Director de Tesis
Equipo de Desarrollo	• Tesista

Tabla 6: Equipo SCRUM.

3.5.2.4 Definición de los sprint de desarrollo

Definir los sprints durante la gestión de proyectos ágiles permite organizar y estructurar el trabajo en ciclos cortos que permiten una rápida adaptación a los cambios, mejora el uso de recursos y mejora la capacidad de respuesta a las necesidades de los usuarios finales, en la Tabla 7 se describen los sprint que serán desarrollados.

Sprint	Épica
Sprint 1	EPIC01 - Autenticación y Seguridad
Sprint 2	EPIC 02 - Gestión de Usuarios y Roles
Sprint 3	EPIC 03 - Integración y Disponibilidad
Sprint 4	EPIC 04 - Auditoría y Cumplimiento
Sprint 5	EPIC 05 - Observabilidad (Logging Técnico)
Sprint 6	EPIC 06 - Consultas y Movimientos
Sprint 7	EPIC 07 - Transacciones Internas y Externas
Sprint 8	EPIC 08 - Aprobaciones y Control de Riesgo
Sprint 9	EPIC 09 - Documentación Digital
Sprint 10	EPIC 10 - Nómina y Proveedores
Sprint 11	EPIC 11 - Cartera y Productos Financieros

Tabla 7: Definición de los Sprint de desarrollo.

3.5.2.5 Definición de las herramientas de desarrollo

Las herramientas de desarrollo seleccionadas para el presente proyecto se encuentran alineadas a la arquitectura tecnológica de la Cooperativa:

- Lenguaje de desarrollo: Visual Basic
- Base de datos: SQL Server
- Entorno de Desarrollo Integrado: Visual Studio Code (VS Code)

3.5.3 Desarrollo del Sprint 1

3.5.3.1 Planificación del Sprint 1

- *Objetivo:* Este sprint se enfoca en establecer la base tecnológica para la validación de credenciales, mecanismos de autenticación multifactor, políticas de seguridad y registro de eventos, conforme a los lineamientos de control normativo SEPS-009 y prácticas OWASP Top 10.
- *Duración estimada:* 2 semanas
- *Equipo involucrado:* Product Owner, Scrum Master, Desarrollador

La fase de planificación del Sprint 1 se centró en revisar y validar una a una las historias seleccionadas descritas en la Tabla 8.

Historia de Usuario	Descripción
HU-01 Validar credenciales	Como administrador de seguridad, quiero validar credenciales, para autenticar al usuario verificando usuario y contraseña en la base de datos.
HU-02 Bloquear tras N intentos	Como administrador de seguridad, quiero bloquear tras n intentos, para inhabilitar el acceso temporalmente tras varios intentos fallidos consecutivos.
HU-03 Registrar eventos de acceso	Como administrador de seguridad, quiero registrar eventos de acceso, para registrar en bitácora cada inicio de sesión exitoso o fallido para auditoría.
HU-04 Generar OTP	Como administrador de seguridad, quiero generar otp, para crear un código temporal de seis dígitos como segundo factor de autenticación.
HU-05 Expiración de OTP	Como administrador de seguridad, quiero expiración de otp, para definir el tiempo máximo de validez del código otp antes de caducar.
HU-06 Validar OTP en servidor	Como administrador de seguridad, quiero validar otp en servidor, para comprobar que el código otp ingresado sea correcto y esté vigente.
HU-07 Generar token de recuperación	Como administrador de seguridad, quiero generar token de recuperación, para emitir un enlace único para restablecer la contraseña del usuario.

Historia de Usuario	Descripción
HU-08 Enviar correo de restablecimiento	Como administrador de seguridad, quiero enviar correo de restablecimiento, para enviar al correo del usuario el enlace seguro para cambiar su contraseña.
HU-09 Invalidar token usado	Como administrador de seguridad, quiero invalidar token usado, para desactivar automáticamente el enlace de recuperación tras su uso.
HU-29 Política de contraseñas	Como administrador de seguridad, quiero política de contraseñas, para aplicar reglas de complejidad, expiración e historial de contraseñas.
HU-30 Aviso de caducidad de contraseña	Como administrador de seguridad, quiero aviso de caducidad de contraseña, para notificar al usuario antes de la expiración de su clave.
HU-34 Expiración de sesión	Como administrador de seguridad, quiero expiración de sesión, para cerrar sesión automáticamente tras un tiempo de inactividad configurado.
HU-35 Renovación de token de sesión	Como administrador de seguridad, quiero renovación de token de sesión, para extender la sesión activa de forma segura sin reautenticación completa.
HU-36 Protección CSHU	Como administrador de seguridad, quiero protección csrf, para evitar ataques de falsificación de solicitudes entre sitios mediante tokens.

Tabla 8: Planificación del Sprint 1.

Durante la planificación también se analizaron los aspectos técnicos necesarios: integración con servicios de correo seguro, uso de almacenamiento cifrado, implementación de tokens temporales, protección contra ataques de fuerza bruta, manejo de sesiones y cumplimiento de requisitos regulatorios.

3.5.3.2 Ejecución del Sprint 1

El trabajo inició con el traslado de las historias del Sprint Backlog a la columna “To Do” del tablero de tareas, para luego ser tomadas para el desarrollo, posteriormente cada historia de usuario (HU-01 a HU-36) se descompuso en tareas técnicas, tales como diseño de endpoints, implementación de lógica de autenticación, validación de credenciales, generación de OTP,

codificación del manejo seguro de sesiones, integración con servicios de correo, configuración de políticas de contraseñas y registro de logs de acceso según las exigencias normativas.

Durante toda la ejecución se realizó la Daily Scrum, una reunión breve diaria para sincronizar actividades, revisar el progreso, identificar impedimentos y reorganizar el trabajo cuando sea necesario con el objetivo de mantener visibilidad sobre el desarrollo del sprint, detectar bloqueos, ajustar prioridades técnicas y asegurar la coordinación entre desarrollo backend, middleware, servicios de seguridad y pruebas.

La ejecución también incluyó actividades de pruebas continuas, asegurando que las funcionalidades implementadas cumplan con los criterios de aceptación definidos, esto abarca pruebas unitarias, de integración, manejo de errores, simulación de ataques de fuerza bruta, validación de tokens temporales, expiración de sesión, políticas de contraseñas robustas, pruebas de logging y auditoría, y validaciones técnicas relacionadas con los procesos de autenticación multifactor.

Cada historia fue marcada como "completada" únicamente cuando cumplió con la Definition of Done (DoD), que incluyó: funcionalidad operativa, código revisado, pruebas superadas y despliegue en el entorno de pruebas; de este modo, la ejecución del sprint permitió consolidar un conjunto funcional robusto y listo para su revisión en la siguiente fase.

3.5.3.3 Revisión del Sprint 1

Durante la reunión de revisión del sprint, el equipo presentó las funcionalidades desarrolladas al Product Owner:

- Se mostró el flujo completo para la autenticación y seguridad.
- Se valido que cada una de las historias de usuario funcionen correctamente mediante el uso de datos de prueba o de casos específicos que los interesados solicitaron se usaran.
- Se valido que se cumplan con todos los criterios de aceptación de la épica de usuario.

Al finalizar la revisión, el Product Owner aprobó el avance y realizó observaciones menores del diseño visual con el objetivo de mejorar la navegación entre módulos.

3.5.3.4 Resultado del Sprint 1

Como resultado del trabajo colaborativo, se obtuvo un incremento funcional que incluye todas las historias de usuario descritas durante la fase de planificación y cuyas evidencias se describen en las siguientes Figuras.

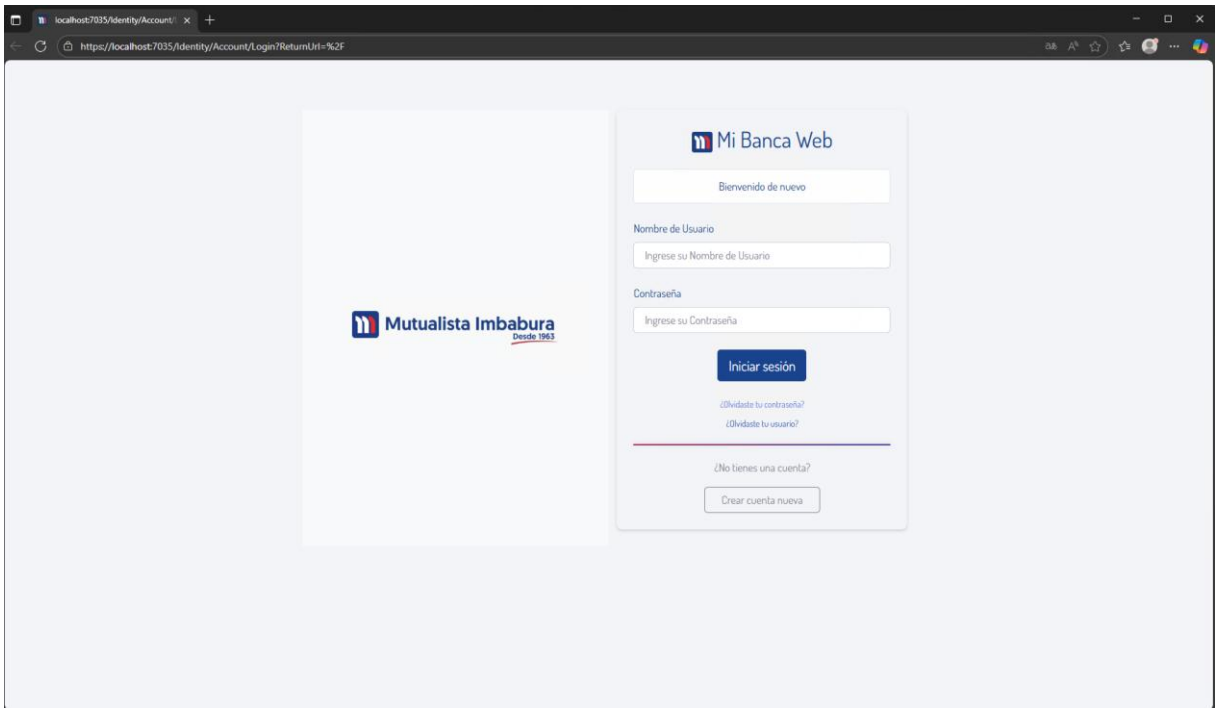


Figura 2: Validación de credenciales.

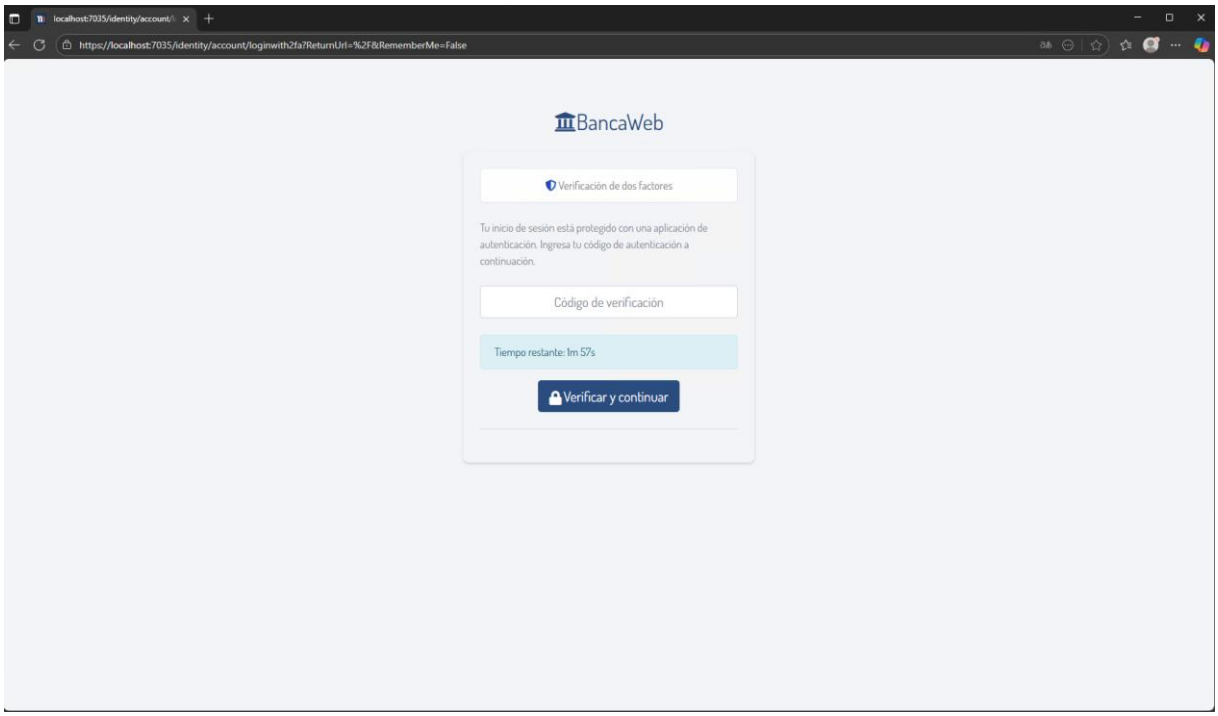


Figura 3: Generación de OTP.

3.5.4 Desarrollo del Sprint 2

3.5.4.1 Planificación del Sprint 2

- *Objetivo:* Implementar las funcionalidades del módulo de Gestión de Usuarios y Roles, permitiendo administrar el ciclo de vida de los usuarios, configurar roles, definir permisos y gestionar delegaciones temporales con sus respectivas auditorías.
- *Duración estimada:* 2 semanas
- *Equipo involucrado:* Product Owner, Scrum Master, Desarrollador

La fase de planificación del Sprint 2 se centró en revisar y validar una a una las historias seleccionadas descritas en la Tabla 9.

Historia de Usuario	**Descripción**
HU-10 Crear/editar/desactivar usuarios	Como administrador del sistema, quiero crear/editar/desactivar usuarios, para gestionar el ciclo de vida de los usuarios desde el panel administrativo.
HU-11 Búsqueda y paginación de usuarios	Como administrador del sistema, quiero búsqueda y paginación de usuarios, para localizar usuarios aplicando filtros y paginación.
HU-12 Validaciones de datos de usuario	Como administrador del sistema, quiero validaciones de datos de usuario, para evitar duplicados y garantizar integridad de la información registrada.
HU-13 Definir roles	Como administrador empresarial, quiero definir roles, para crear y gestionar perfiles de acceso (administrador, operador, aprobador).
HU-14 Asignar permisos por acción	Como administrador empresarial, quiero asignar permisos por acción, para definir qué acciones puede realizar cada rol dentro del sistema.
HU-37 Delegar permisos temporalmente	Como administrador del sistema, quiero delegar permisos temporalmente, para permitir a un usuario transferir permisos a otro por un tiempo definido.
HU-38 Revocación anticipada de delegación	Como administrador del sistema, quiero revocación anticipada de delegación, para cancelar manualmente una delegación antes de su fecha de expiración.
HU-39 Auditoría de delegaciones	Como administrador del sistema, quiero auditoría de delegaciones, para registrar las acciones de delegación y revocación realizadas.

Tabla 9: Planificación del Sprint 2.

3.5.4.2 Ejecución del Sprint 2

El trabajo inició con el traslado de las historias del Sprint Backlog a la columna “To Do” del tablero de tareas, para luego ser tomadas para el desarrollo, se descompuso en tareas técnicas específicas para el desarrollo del módulo de administración de roles (RBAC), construcción del flujo de asignación de permisos por acción, definición de mecanismos de delegación temporal y la integración de auditoría para registrar eventos de delegación y revocación.

Durante la Daily Scrum, se revisó tareas en progreso, identificó impedimentos (como redefinición de reglas de negocio o ajustes en el modelo de roles), y coordinó esfuerzos para asegurar un desarrollo continuo, evitar cuellos de botella y cumplir con los requisitos de control interno, seguridad normativa y trazabilidad exigidos por la SEPS-009.

3.5.4.3 Revisión del Sprint 2

Durante la reunión de revisión del sprint, el equipo presentó las funcionalidades desarrolladas al Product Owner:

- Se mostró el flujo completo para la gestión de usuarios y roles.
- Se valido que cada una de las historias de usuario funcionen correctamente mediante el uso de datos de prueba o de casos específicos que los interesados solicitaron se usaran.
- Se valido que se cumplan con todos los criterios de aceptación de la épica de usuario.

Al finalizar la revisión, el Product Owner aprobó el avance y realizó observaciones menores del diseño visual con el objetivo de mejorar la navegación entre módulos.

3.5.4.4 Resultado del Sprint 2

Como resultado del trabajo colaborativo, se obtuvo un incremento funcional que incluye todas las historias de usuario descritas durante la fase de planificación y cuyas evidencias se describen en las siguientes Figuras.

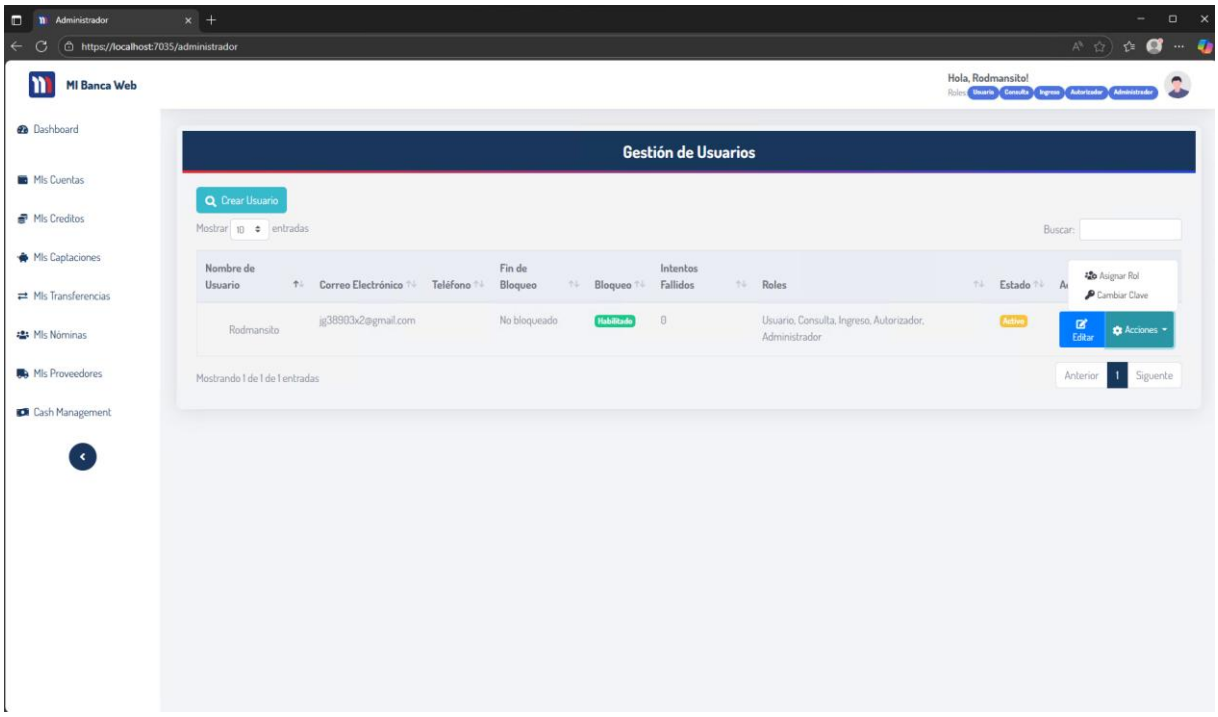


Figura 4: Crear/editar/desactivar usuarios.

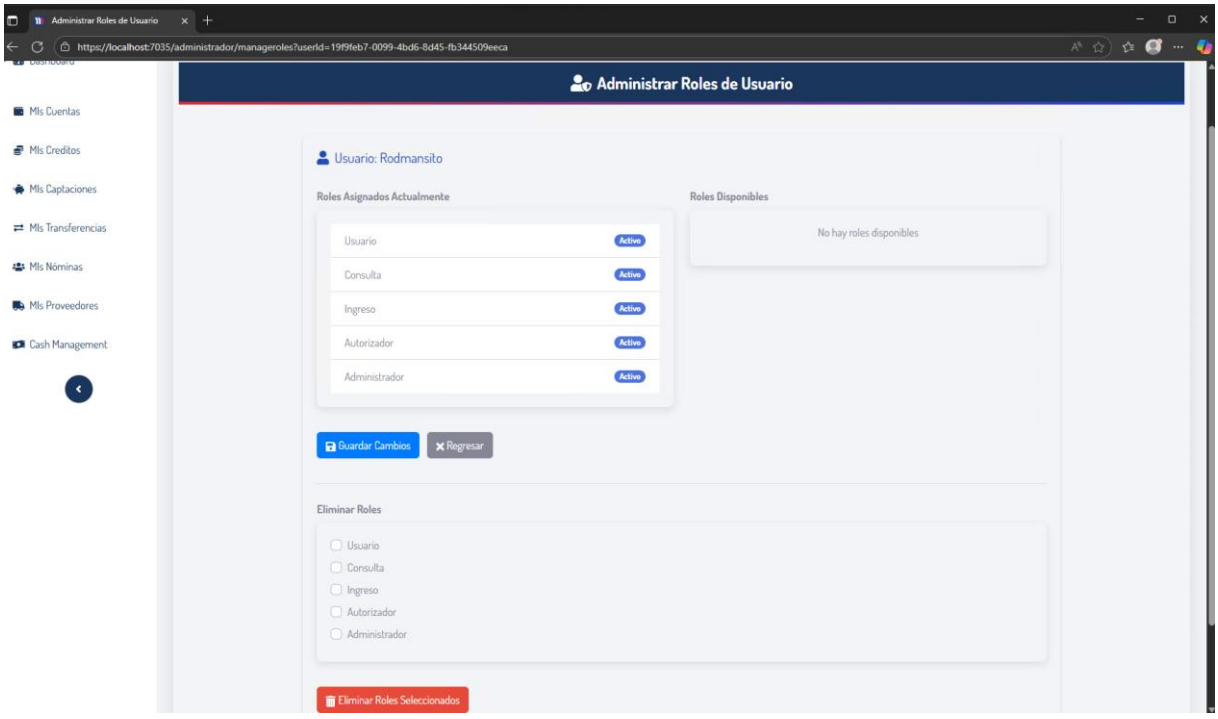


Figura 5: Asignar permisos por acción.

3.5.5 Desarrollo del Sprint 3

3.5.5.1 Planificación del Sprint 3

- *Objetivo:* Implementar los mecanismos de integración, disponibilidad y monitoreo del sistema, garantizando su conectividad estable con el core bancario, la observabilidad en tiempo real y la conciliación correcta de los estados transaccionales.
- *Duración estimada:* 2 semanas
- *Equipo involucrado:* Product Owner, Scrum Master, Desarrollador

La fase de planificación del Sprint 3 se centró en revisar y validar una a una las historias seleccionadas descritas en la Tabla 10.

Historia de Usuario	Descripción
HU-78 Endpoints de salud	Como área de ti, quiero endpoints de salud, para exponer el estado operativo de los servicios del sistema.
HU-79 Métricas de rendimiento	Como área de ti, quiero métricas de rendimiento, para registrar tiempos de respuesta, errores y disponibilidad.
HU-80 Panel de disponibilidad	Como área de ti, quiero panel de disponibilidad, para visualizar la salud general de la aplicación y sus componentes.
HU-81 Adaptadores core bancario	Como área de ti, quiero adaptadores core bancario, para integrar la aplicación con el sistema central bancario (sandbox y producción).
HU-82 Configuración de tiempos y reintentos	Como área de ti, quiero configuración de tiempos y reintentos, para definir límites de espera y reintentos en las operaciones externas.
HU-83 Conciliación de estados	Como área de ti, quiero conciliación de estados, para sincronizar los estados entre el sistema de banca electrónica y el core.

Tabla 10: Planificación del Sprint 3.

3.5.5.2 Ejecución del Sprint 3

Durante esta fase se trasladó cada historia de usuario al tablero de tareas, donde se descompusieron en actividades técnicas específicas para la implementación del sistema de búsqueda y paginación, desarrollo del modelo de roles (RBAC), asignación de permisos por acción, lógica para delegación temporal de permisos, revocación anticipada y mecanismos de auditoría para registrar dichas acciones.

Para mantener la sincronización del trabajo diario, se realizaron las Daily Scrum, donde se reportó avances, identificó bloqueos y ajustó prioridades que permitieron sobrellevar los inconvenientes que surgían y para aclarar dudas sobre los flujos de negocio, roles autorizados y criterios de aceptación vinculados a la segregación de funciones.

3.5.5.3 Revisión del Sprint 3

Durante la reunión de revisión del sprint, el equipo presentó las funcionalidades desarrolladas al Product Owner:

- Se mostró el flujo completo para la Integración y Disponibilidad.
- Se valido que cada una de las historias de usuario funcionen correctamente mediante el uso de datos de prueba o de casos específicos que los interesados solicitaron se usaran.
- Se valido que se cumplan con todos los criterios de aceptación de la épica de usuario.

Al finalizar la revisión, el Product Owner aprobó el avance y realizó observaciones menores del diseño visual con el objetivo de mejorar la navegación entre módulos.

3.5.5.4 Resultado del Sprint 3

Como resultado del trabajo colaborativo, se obtuvo un incremento funcional que incluye todas las historias de usuario descritas durante la fase de planificación y cuyas evidencias se describen en las siguientes Figuras.

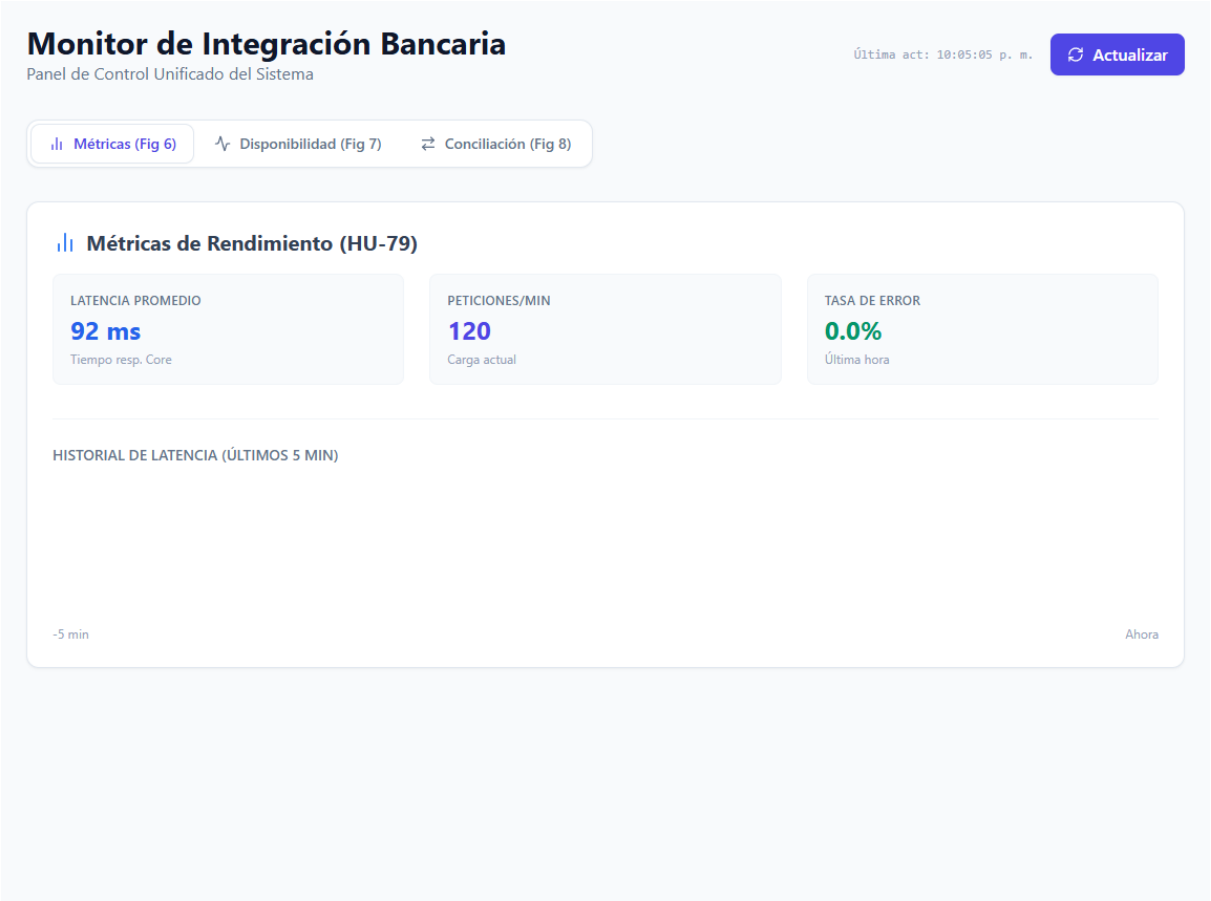


Figura 6: Métricas de rendimiento.

Figura 7: Panel de disponibilidad.

3.5.6 Desarrollo del Sprint 4

3.5.6.1 Planificación del Sprint 4

- *Objetivo:* Implementar el módulo de auditoría del sistema, incorporando el registro seguro de acciones y la consulta y exportación de la bitácora, garantizando trazabilidad, transparencia y cumplimiento normativo SEPS-009.
- *Duración estimada:* 2 semanas
- *Equipo involucrado:* Product Owner, Scrum Master, Desarrollador

La fase de planificación del Sprint 4 se centró en revisar y validar una a una las historias seleccionadas descritas en la Tabla 11.

Historia de Usuario	Descripción
HU-27 Bitácora de acciones	Como administrador del sistema, quiero bitácora de acciones, para registrar toda acción relevante del usuario en el sistema.
HU-28 Consulta y exportación de auditoría	Como oficial de cumplimiento, quiero consulta y exportación de auditoría, para visualizar y descargar los registros de auditoría.

Tabla 11: Planificación del Sprint 4.

3.5.6.2 Ejecución del Sprint 4

Durante esta fase se trasladaron las historias de usuario al tablero Scrum, donde se dividieron en tareas técnicas específicas que permitieron el desarrollo de la interfaz de búsqueda y filtrado, construcción de exportaciones en formatos estándar y validaciones de acceso para garantizar que solo usuarios autorizados puedan consultar la información registrada.

Durante la ejecución, las Daily Scrum fueron fundamentales para sincronizar el trabajo diario, resolver impedimentos, redistribuir tareas y asegurar que las decisiones técnicas estuvieran alineadas con los criterios normativos y de negocio; así también, el PO facilitó la gestión de bloqueos, aclaró dudas sobre requisitos funcionales, restricciones de acceso y la correcta interpretación de las políticas de integridad del registro de auditoría.

3.5.6.3 Revisión del Sprint 4

Durante la reunión de revisión del sprint, el equipo presentó las funcionalidades desarrolladas al Product Owner:

- Se mostró el flujo completo para la auditoría y cumplimiento.
- Se valido que cada una de las historias de usuario funcionen correctamente mediante el uso de datos de prueba o de casos específicos que los interesados solicitaron se usaran.
- Se valido que se cumplan con todos los criterios de aceptación de la épica de usuario.

Al finalizar la revisión, el Product Owner aprobó el avance y realizó observaciones menores del diseño visual con el objetivo de mejorar la navegación entre módulos.

3.5.6.4 Resultado del Sprint 4

Como resultado del trabajo colaborativo, se obtuvo un incremento funcional que incluye todas las historias de usuario descritas durante la fase de planificación y cuyas evidencias se describen en las siguientes Figuras.

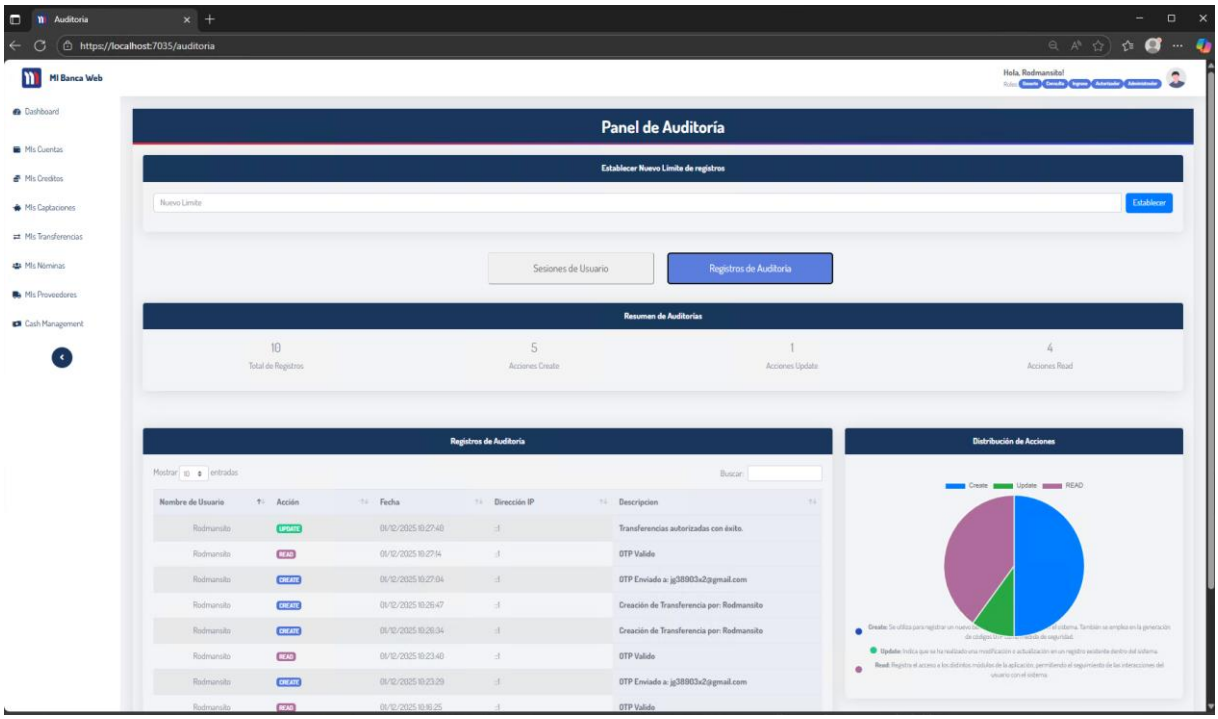


Figura 8: Bitácora de acciones.

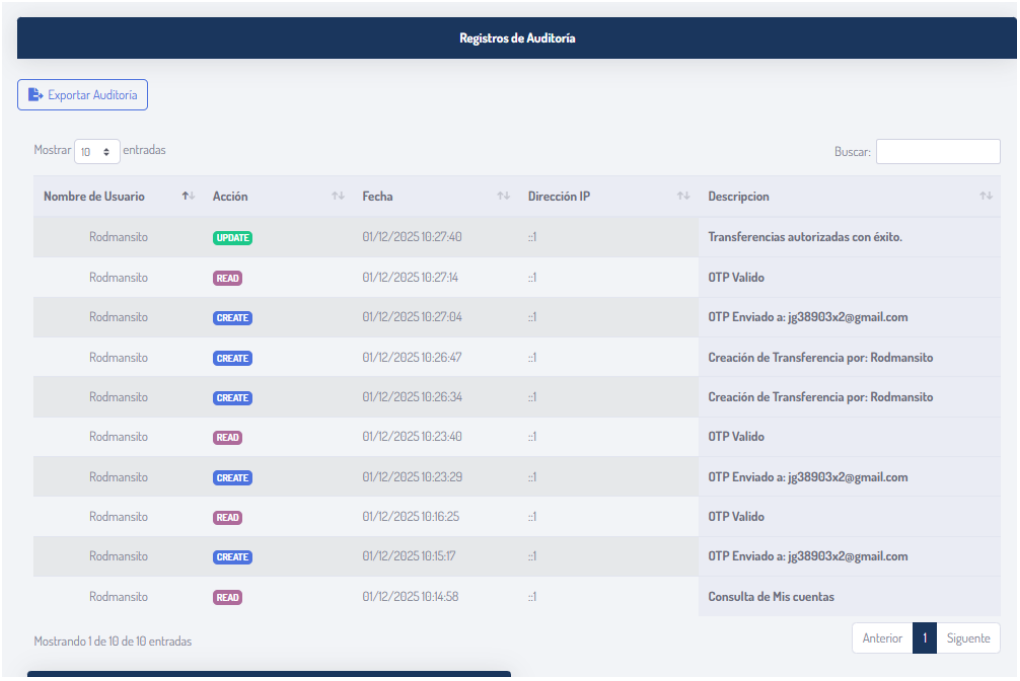


Figura 9: Consulta y exportación de auditorías.

3.5.7 Desarrollo del Sprint 5

3.5.7.1 Planificación del Sprint 5

- *Objetivo:* Implementar el módulo de observabilidad mediante logging estructurado, trazas correlacionadas y políticas de retención y rotación, garantizando la trazabilidad técnica y el monitoreo confiable del sistema de banca electrónica empresarial.
- *Duración estimada:* 2 semanas
- *Equipo involucrado:* Product Owner, Scrum Master, Desarrollador

La fase de planificación del Sprint 5 se centró en revisar y validar una a una las historias seleccionadas descritas en la Tabla 12.

Historia de Usuario	Descripción
HU-75 Logging estructurado	Como oficial de cumplimiento, quiero logging estructurado, para registrar eventos con estructura uniforme para análisis.
HU-76 Correlación de trazas (traceId)	Como área de ti, quiero correlación de trazas (traceid), para relacionar operaciones entre servicios mediante un identificador común.
HU-77 Retención y rotación de logs	Como oficial de cumplimiento, quiero retención y rotación de logs, para administrar la duración y reemplazo automático de archivos de registro.

Tabla 12: Planificación del Sprint 5.

Finalmente se centró en definir el alcance y las tareas técnicas necesarias para implementar las funcionalidades del módulo de Observabilidad, revisando las historias de usuario relacionadas con el registro y monitoreo del sistema.

3.5.7.2 Ejecución del Sprint 5

Se inició la ejecución trasladando las historias HU-75, HU-76 y HU-77 al tablero Scrum, dividiéndolas en tareas técnicas específicas, entre estas tareas se incluyeron: diseño del formato estandarizado de logs en JSON, instrumentación del backend para generar eventos estructurados, incorporación de identificadores únicos de trazas (traceId) en cada solicitud entrante y saliente, integración del traceId en las comunicaciones internas, configuración de librerías de rotación automatizada de archivos de log, definición de políticas de retención basadas en normativas y buenas prácticas, y verificación de que los registros no incluyan información sensible conforme a principios de seguridad y privacidad.

Durante las Daily Scrum, se compartió los avances, identificó impedimentos y coordinó dependencias técnicas con los demás miembros del equipo, el PO facilitó la resolución de bloqueos y gestionó la comunicación con las áreas de Seguridad y Arquitectura para validar las políticas de registro y retención.

3.5.7.3 Revisión del Sprint 5

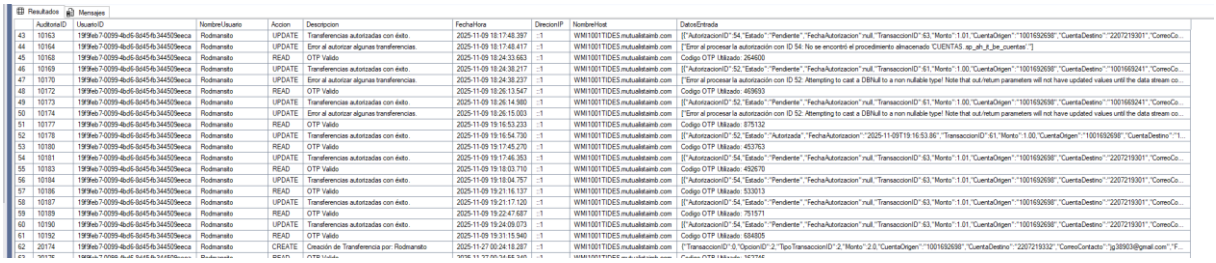
Durante la reunión de revisión del sprint, el equipo presentó las funcionalidades desarrolladas al Product Owner:

- Se mostró el flujo completo para la Observabilidad (Logging Técnico).
- Se valido que cada una de las historias de usuario funcionen correctamente mediante el uso de datos de prueba o de casos específicos que los interesados solicitaron se usaran.
- Se valido que se cumplan con todos los criterios de aceptación de la épica de usuario.

Al finalizar la revisión, el Product Owner aprobó el avance y realizó observaciones menores del diseño visual con el objetivo de mejorar la navegación entre módulos.

3.5.7.4 Resultado del Sprint 5

Como resultado del trabajo colaborativo, se obtuvo un incremento funcional que incluye todas las historias de usuario descritas durante la fase de planificación y cuyas evidencias se describen en las siguientes Figuras.



	AuditoriaID	UsuarioID	NombreUsuario	Accion	Descripcion	FechaHora	DireccionIP	NombreHost	DatosEntrada
43	10163	1f9fbeb7-0099-4bd6-8d45-fb344509eeca	Rodmansito	UPDATE	Transferencias autorizadas con éxito.	2025-11-09 18:17:48.397	::1	WIN10011TIDES.mutualistaimb.com	[{"AutorizacionID":54,"Estado":"Pendiente","FechaAutorizacion":null,"TransaccionID":63,"Monto":1.01,"CuentaOrigen":"1001692698","CuentaDestino":"2207219301","CorreoCo...
44	10164	1f9fbeb7-0099-4bd6-8d45-fb344509eeca	Rodmansito	UPDATE	Error al autorizar algunas transferencias.	2025-11-09 18:17:48.417	::1	WIN10011TIDES.mutualistaimb.com	["Error al procesar la autorización con ID 54: No se encontró el procedimiento almacenado 'CUENTAS_sp_ah_tr_be_cuentas'."]
45	10168	1f9fbeb7-0099-4bd6-8d45-fb344509eeca	Rodmansito	READ	OTP Valido	2025-11-09 18:24:33.663	::1	WIN10011TIDES.mutualistaimb.com	Codigo OTP Utilizado: 264600
46	10169	1f9fbeb7-0099-4bd6-8d45-fb344509eeca	Rodmansito	UPDATE	Transferencias autorizadas con éxito.	2025-11-09 18:24:38.217	::1	WIN10011TIDES.mutualistaimb.com	[{"AutorizacionID":52,"Estado":"Pendiente","FechaAutorizacion":null,"TransaccionID":61,"Monto":1.00,"CuentaOrigen":"1001692698","CuentaDestino":"1001669241","CorreoCo...
47	10170	1f9fbeb7-0099-4bd6-8d45-fb344509eeca	Rodmansito	UPDATE	Error al autorizar algunas transferencias.	2025-11-09 18:24:38.237	::1	WIN10011TIDES.mutualistaimb.com	["Error al procesar la autorización con ID 52: Attempting to cast a DBNull to a non nullable type! Note that out/return parameters will not have updated values until the data stream co...
48	10172	1f9fbeb7-0099-4bd6-8d45-fb344509eeca	Rodmansito	READ	OTP Valido	2025-11-09 18:26:13.547	::1	WIN10011TIDES.mutualistaimb.com	Codigo OTP Utilizado: 469693
49	10173	1f9fbeb7-0099-4bd6-8d45-fb344509eeca	Rodmansito	UPDATE	Transferencias autorizadas con éxito.	2025-11-09 18:26:14.980	::1	WIN10011TIDES.mutualistaimb.com	[{"AutorizacionID":52,"Estado":"Pendiente","FechaAutorizacion":null,"TransaccionID":61,"Monto":1.00,"CuentaOrigen":"1001692698","CuentaDestino":"1001669241","CorreoCo...
50	10174	1f9fbeb7-0099-4bd6-8d45-fb344509eeca	Rodmansito	UPDATE	Error al autorizar algunas transferencias.	2025-11-09 18:26:15.003	::1	WIN10011TIDES.mutualistaimb.com	["Error al procesar la autorización con ID 52: Attempting to cast a DBNull to a non nullable type! Note that out/return parameters will not have updated values until the data stream co...
51	10177	1f9fbeb7-0099-4bd6-8d45-fb344509eeca	Rodmansito	READ	OTP Valido	2025-11-09 19:16:53.233	::1	WIN10011TIDES.mutualistaimb.com	Codigo OTP Utilizado: 875132
52	10178	1f9fbeb7-0099-4bd6-8d45-fb344509eeca	Rodmansito	UPDATE	Transferencias autorizadas con éxito.	2025-11-09 19:16:54.730	::1	WIN10011TIDES.mutualistaimb.com	[{"AutorizacionID":52,"Estado":"Autorizada","FechaAutorizacion":"2025-11-09T19:16:53.86","TransaccionID":61,"Monto":1.00,"CuentaOrigen":"1001692698","CuentaDestino":"1...
53	10180	1f9fbeb7-0099-4bd6-8d45-fb344509eeca	Rodmansito	READ	OTP Valido	2025-11-09 19:17:45.270	::1	WIN10011TIDES.mutualistaimb.com	Codigo OTP Utilizado: 453763
54	10181	1f9fbeb7-0099-4bd6-8d45-fb344509eeca	Rodmansito	UPDATE	Transferencias autorizadas con éxito.	2025-11-09 19:17:46.353	::1	WIN10011TIDES.mutualistaimb.com	[{"AutorizacionID":54,"Estado":"Pendiente","FechaAutorizacion":null,"TransaccionID":63,"Monto":1.01,"CuentaOrigen":"1001692698","CuentaDestino":"2207219301","CorreoCo...
55	10183	1f9fbeb7-0099-4bd6-8d45-fb344509eeca	Rodmansito	READ	OTP Valido	2025-11-09 19:18:03.710	::1	WIN10011TIDES.mutualistaimb.com	Codigo OTP Utilizado: 452670
56	10184	1f9fbeb7-0099-4bd6-8d45-fb344509eeca	Rodmansito	UPDATE	Transferencias autorizadas con éxito.	2025-11-09 19:18:04.757	::1	WIN10011TIDES.mutualistaimb.com	[{"AutorizacionID":54,"Estado":"Pendiente","FechaAutorizacion":null,"TransaccionID":63,"Monto":1.01,"CuentaOrigen":"1001692698","CuentaDestino":"2207219301","CorreoCo...
57	10186	1f9fbeb7-0099-4bd6-8d45-fb344509eeca	Rodmansito	READ	OTP Valido	2025-11-09 19:21:16.137	::1	WIN10011TIDES.mutualistaimb.com	Codigo OTP Utilizado: 533013
58	10187	1f9fbeb7-0099-4bd6-8d45-fb344509eeca	Rodmansito	UPDATE	Transferencias autorizadas con éxito.	2025-11-09 19:21:17.120	::1	WIN10011TIDES.mutualistaimb.com	[{"AutorizacionID":54,"Estado":"Pendiente","FechaAutorizacion":null,"TransaccionID":63,"Monto":1.01,"CuentaOrigen":"1001692698","CuentaDestino":"2207219301","CorreoCo...
59	10189	1f9fbeb7-0099-4bd6-8d45-fb344509eeca	Rodmansito	READ	OTP Valido	2025-11-09 19:22:47.687	::1	WIN10011TIDES.mutualistaimb.com	Codigo OTP Utilizado: 751571
60	10190	1f9fbeb7-0099-4bd6-8d45-fb344509eeca	Rodmansito	UPDATE	Transferencias autorizadas con éxito.	2025-11-09 19:24:09.073	::1	WIN10011TIDES.mutualistaimb.com	[{"AutorizacionID":54,"Estado":"Pendiente","FechaAutorizacion":null,"TransaccionID":63,"Monto":1.01,"CuentaOrigen":"1001692698","CuentaDestino":"2207219301","CorreoCo...
61	10192	1f9fbeb7-0099-4bd6-8d45-fb344509eeca	Rodmansito	READ	OTP Valido	2025-11-09 19:31:15.940	::1	WIN10011TIDES.mutualistaimb.com	Codigo OTP Utilizado: 684805
62	20174	1f9fbeb7-0099-4bd6-8d45-fb344509eeca	Rodmansito	CREATE	Creación de Transferencia por: Rodmansito	2025-11-27 00:24:18.287	::1	WIN10011TIDES.mutualistaimb.com	{"TransaccionID":0,"OpcionID":2,"TipoTransaccionID":2,"Monto":2.0,"CuentaOrigen":"1001692698","CuentaDestino":"2207219332","CorreoContacto":"jg38903@gmail.com","F...

Figura 10: Logging estructurado.

3.5.8 Desarrollo del Sprint 6

3.5.8.1 Planificación del Sprint 6

- *Objetivo:* Implementar el módulo de Consultas y Movimientos, habilitando la consulta de saldos, filtrado avanzado, paginación, totales parciales y exportaciones en distintos formatos, garantizando precisión, rendimiento y cumplimiento normativo.
- *Duración estimada:* 2 semanas
- *Equipo involucrado:* Product Owner, Scrum Master, Desarrollador

La fase de planificación del Sprint 6 se centró en revisar y validar una a una las historias seleccionadas descritas en la Tabla 13.

Historia de Usuario	Descripción
HU-15 Consultar saldos	Como usuario, quiero consultar saldos, para mostrar el saldo actual y disponible de las cuentas asociadas.
HU-16 Filtrar movimientos	Como usuario, quiero filtrar movimientos, para permitir consultar transacciones aplicando filtros por fecha, tipo o canal.
HU-17 Exportar movimientos CSV	Como usuario, quiero exportar movimientos csv, para descargar los resultados de consulta de movimientos a un archivo csv.
HU-40 Búsqueda avanzada de movimientos	Como usuario, quiero búsqueda avanzada de movimientos, para filtrar transacciones por rango, monto, canal o beneficiario.
HU-41 Paginación y orden de resultados	Como usuario, quiero paginación y orden de resultados, para facilitar la navegación y organización de los resultados de búsqueda.
HU-42 Totales parciales	Como usuario, quiero totales parciales, para calcular totales agrupados de los movimientos filtrados.
HU-43 Exportación a XLSX	Como usuario, quiero exportación a xlsx, para descargar grandes volúmenes de datos de movimientos en excel.
HU-44 Firma o folio del reporte	Como usuario, quiero firma o folio del reporte, para añadir un identificador único de seguridad a los reportes generados.

Tabla 13: Planificación del Sprint 6.

3.5.8.2 Ejecución del Sprint 6

Se inició con la construcción de servicios para consultas de saldos, integración con el core bancario utilizando los adaptadores creados en el Sprint 3, procesamiento eficiente de grandes volúmenes de movimientos, diseño de algoritmos de filtrado avanzado y ordenamiento, implementación de paginación basada en parámetros dinámicos, cálculo automático de totales parciales y desarrollo de mecanismos de exportación en formatos XLSX.

Durante las Daily Scrum, se revisó el progreso, definió prioridades técnicas y resolvió impedimentos relacionados con la optimización de consultas, tiempos de respuesta y manejo de volúmenes elevados de transacciones, estas reuniones permitieron sincronizar el trabajo

diario y garantizar que todos los desarrolladores mantuvieran una comprensión compartida del avance del sprint y de los elementos críticos del módulo.

3.5.8.3 Revisión del Sprint 6

Durante la reunión de revisión del sprint, el equipo presentó las funcionalidades desarrolladas al Product Owner:

- Se mostró el flujo completo para las consultas y movimientos.
- Se valido que cada una de las historias de usuario funcionen correctamente mediante el uso de datos de prueba o de casos específicos que los interesados solicitaron se usaran.
- Se valido que se cumplan con todos los criterios de aceptación de la épica de usuario.

Al finalizar la revisión, el Product Owner aprobó el avance y realizó observaciones menores del diseño visual con el objetivo de mejorar la navegación entre módulos.

3.5.8.4 Resultado del Sprint 6

Como resultado del trabajo colaborativo, se obtuvo un incremento funcional que incluye todas las historias de usuario descritas durante la fase de planificación y cuyas evidencias se describen en las siguientes Figuras.

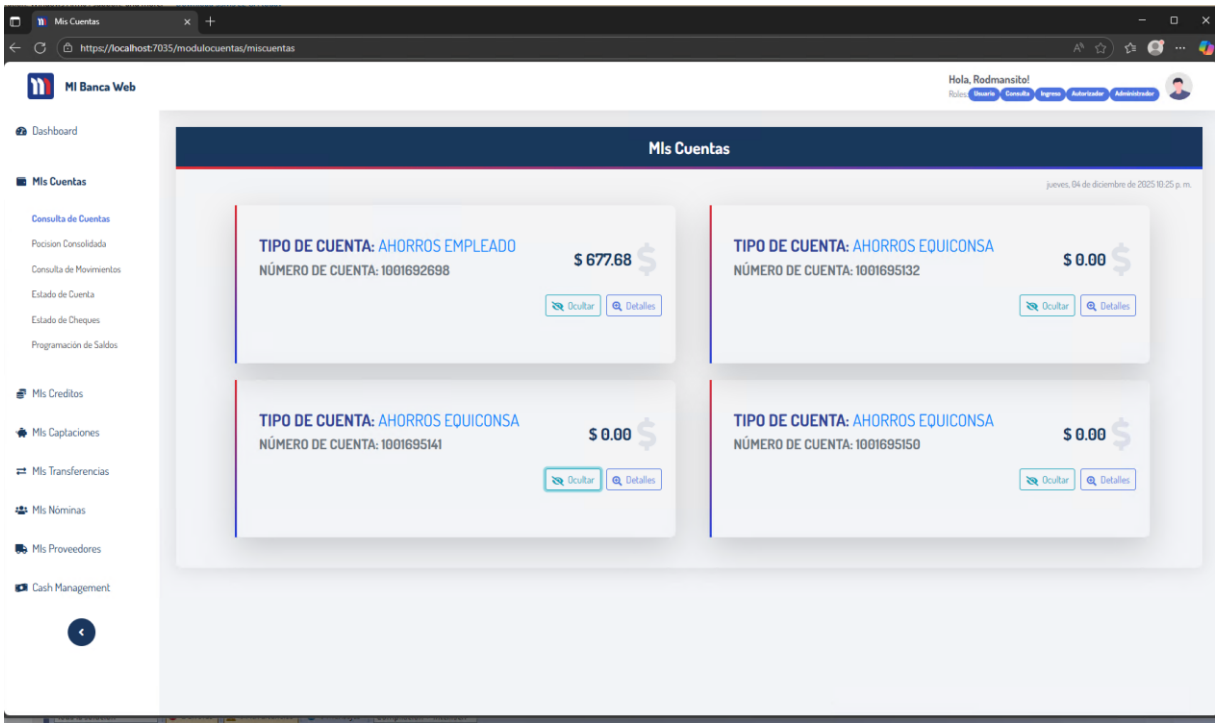


Figura 11: Consultar saldos.

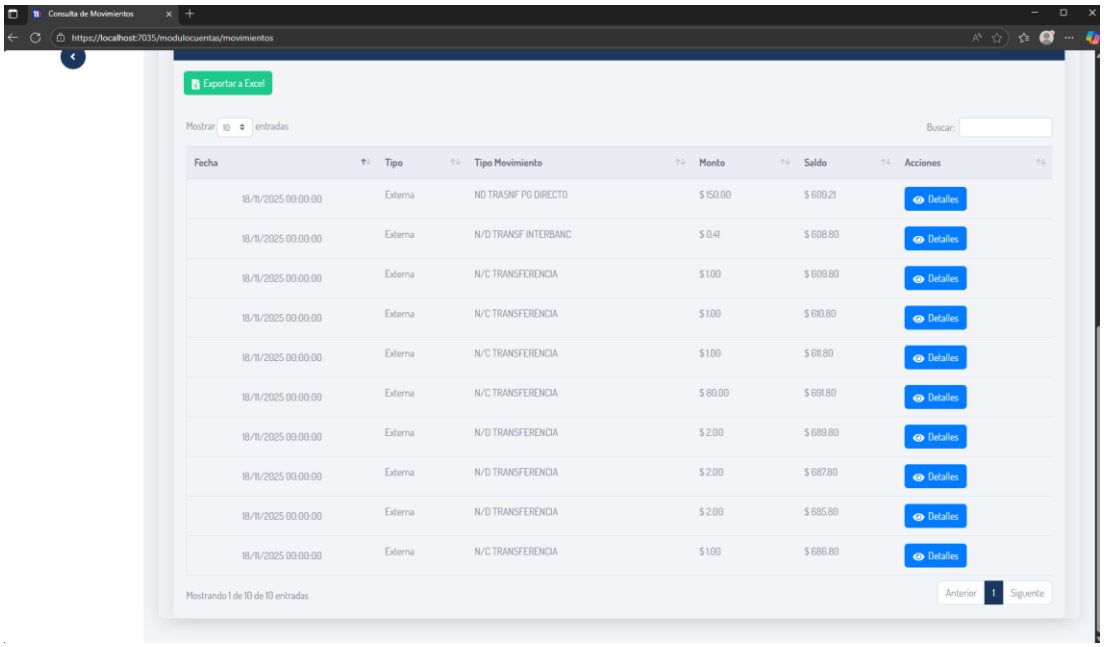


Figura 12: Exportación Excel.

3.5.9 Desarrollo del Sprint 7

3.5.9.1 Planificación del Sprint 7

- *Objetivo:* Implementar el módulo de Transacciones Internas y Externas, habilitando operaciones individuales y masivas, con validaciones de saldo, beneficiarios, estados transaccionales y comunicación segura con el core bancario.
- *Duración estimada:* 2 semanas
- *Equipo involucrado:* Product Owner, Scrum Master, Desarrollador

La fase de planificación del Sprint 7 se centró en revisar y validar una a una las historias seleccionadas descritas en la Tabla 14.

Historia de Usuario	Descripción
HU-18 Validar saldo previo a transferencia	Como usuario, quiero validar saldo previo a transferencia, para comprobar que exista saldo suficiente antes de ejecutar la operación.
HU-19 Crear transacción interna	Como usuario, quiero crear transacción interna, para registrar movimientos entre cuentas del mismo cliente.
HU-20 Generar comprobante PDF	Como usuario, quiero generar comprobante pdf, para producir un comprobante digital de la transacción realizada.

Historia de Usuario	Descripción
HU-21 Registrar beneficiario externo	Como usuario, quiero registrar beneficiario externo, para ingresar y guardar información de beneficiarios interbancarios.
HU-22 Enviar datos al core bancario	Como usuario, quiero enviar datos al core bancario, para transmitir la instrucción de pago al sistema central o red interbancaria.
HU-23 Gestionar estados de transferencia	Como usuario, quiero gestionar estados de transferencia, para controlar los estados pendiente, aprobada y rechazada.
HU-45 Alta de beneficiario	Como usuario, quiero alta de beneficiario, para registrar nuevos beneficiarios en el sistema.
HU-46 Validación CCI/IBAN	Como usuario, quiero validación cci/iban, para verificar la validez del número de cuenta y entidad financiera.
HU-47 Verificación de beneficiario	Como usuario, quiero verificación de beneficiario, para confirmar la titularidad mediante microdepósito o código otp.
HU-48 Carga de pagos masivos	Como usuario, quiero carga de pagos masivos, para admitir la carga de archivos csv/xlsx con múltiples pagos.
HU-49 Validación línea a línea	Como usuario, quiero validación línea a línea, para verificar los datos de cada registro del archivo cargado.
HU-50 Simulación de errores	Como área de ti, quiero simulación de errores, para previsualizar errores antes de ejecutar los pagos.
HU-51 Ejecución de pagos masivos	Como usuario, quiero ejecución de pagos masivos, para procesar los lotes de transferencias validadas.

Tabla 14: Planificación del Sprint 7.

Cada historia fue descompuesta en tareas técnicas específicas, identificando actividades como: diseño de APIs transaccionales, integración con adaptadores del core bancario implementados en Sprint 3, validación de saldos por microservicios, construcción de motores de procesamiento masivo, generación de PDF transaccionales, cifrado de datos sensibles, aplicación de controles antifraude, y manejo de colas para garantizar consistencia en operaciones de alto volumen.

3.5.9.2 Ejecución del Sprint 7

Se inició con el desarrollo de tareas técnicas detalladas como: validación automática de saldos antes de iniciar una transacción (HU-18), creación del flujo completo de transferencias internas (HU-19) y generación automatizada de comprobantes en formato PDF utilizando plantillas con códigos de verificación (HU-20).

Adicionalmente, se trabajó en el registro, validación y verificación de beneficiarios para transferencias externas, desarrollando funcionalidades específicas para su alta (HU-45), validación de CCI/IBAN (HU-46) y verificación de identidad del beneficiario mediante servicios externos o internos (HU-47). Para garantizar la trazabilidad y seguridad, se implementaron controles antifraude y validaciones adicionales sobre los datos financieros procesados.

En relación con la comunicación con el core bancario, se implementó el envío seguro de operaciones (HU-22) utilizando los adaptadores construidos en el Sprint 3 y mecanismos de mensajería o colas para tolerancia a fallos y se desarrolló la lógica para gestionar el ciclo de vida de las transacciones (HU-23), incluyendo estados como pendiente, procesando, completado, rechazado, error técnico y reintento automático.

Uno de los bloques más complejos desarrollado durante la ejecución fue el procesamiento de pagos masivos, el cual incluyó: carga de archivos con cientos o miles de líneas (HU-48), validación específica para cada fila del archivo (HU-49), simulación de errores y escenarios atípicos (HU-50) para anticipar fallos comunes, y la ejecución final de los pagos masivos (HU-51).

Durante las Daily Scrum, se sincronizó avances, identificó impedimentos y coordinó aspectos críticos como desempeño en operaciones de alto volumen, latencia en consultas al core bancario y estrategias para el manejo de errores transaccionales, durante el desarrollo el PO facilitó la resolución de bloqueos y gestionó la comunicación con el Equipo de Integración para validar requisitos técnicos con el core.

3.5.9.3 Revisión del Sprint 7

Durante la reunión de revisión del sprint, el equipo presentó las funcionalidades desarrolladas al Product Owner:

- Se mostró el flujo completo para las transacciones internas y externas.
- Se valido que cada una de las historias de usuario funcionen correctamente mediante el uso de datos de prueba o de casos específicos que los interesados solicitaron se usaran.
- Se valido que se cumplan con todos los criterios de aceptación de la épica de usuario.

Al finalizar la revisión, el Product Owner aprobó el avance y realizó observaciones menores del diseño visual con el objetivo de mejorar la navegación entre módulos.

3.5.9.4 Resultado del Sprint 7

Como resultado del trabajo colaborativo, se obtuvo un incremento funcional que incluye todas las historias de usuario descritas durante la fase de planificación y cuyas evidencias se describen en las siguientes Figuras.

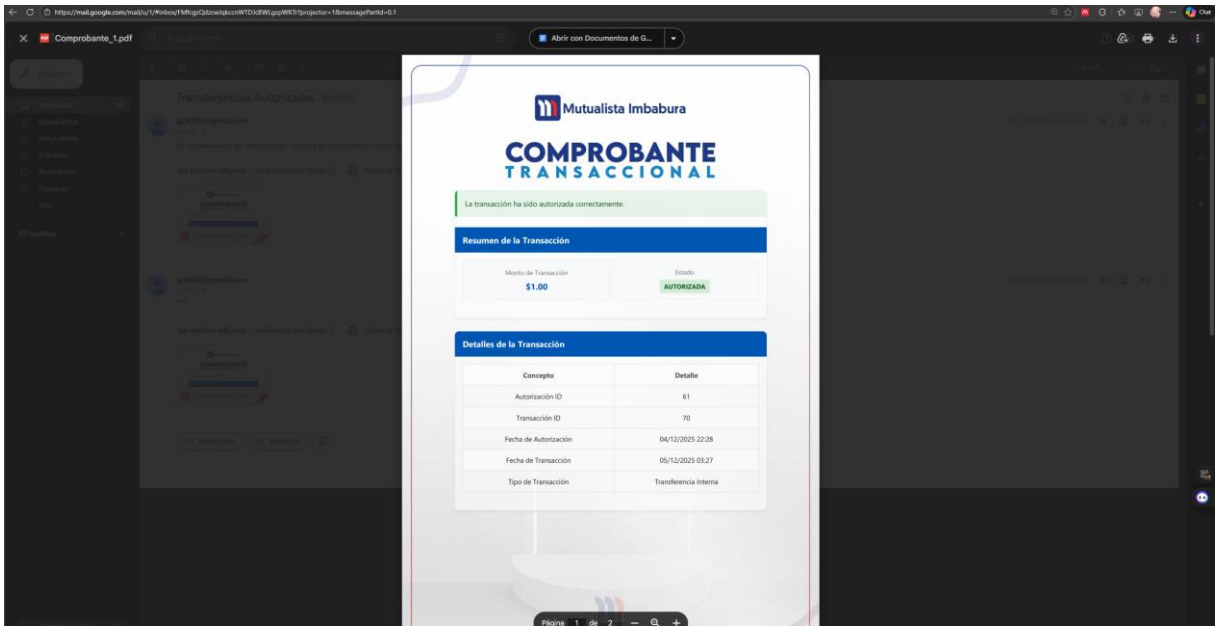


Figura 13: Generar comprobante de transferencia.

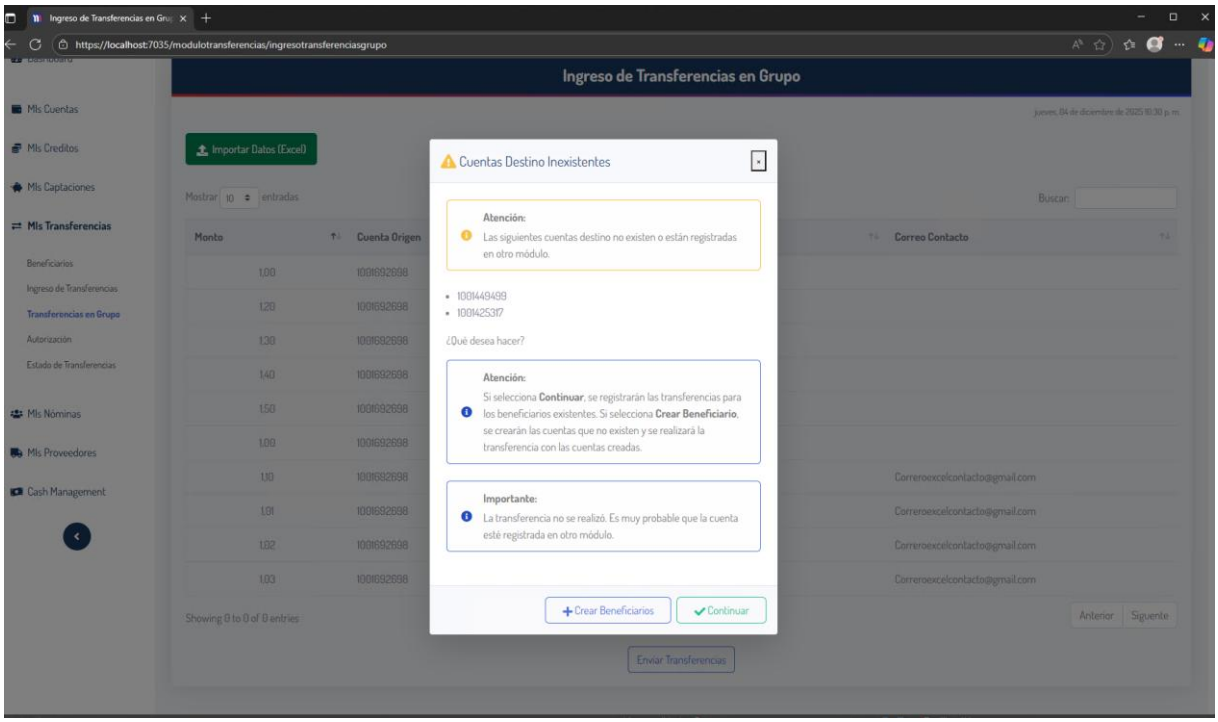


Figura 14: Ejecución de pagos masivos.

3.5.10 Desarrollo del Sprint 8

3.5.10.1 Planificación del Sprint 8

- *Objetivo:* Implementar el módulo de Aprobaciones y Control de Riesgo, incorporando flujos multinivel, límites transaccionales y reglas automáticas que mitiguen riesgos operativos y garanticen seguridad en las operaciones empresariales.
- *Duración estimada:* 2 semanas
- *Equipo involucrado:* Product Owner, Scrum Master, Desarrollador

La fase de planificación del Sprint 8 se centró en revisar y validar una a una las historias seleccionadas descritas en la Tabla 15.

Historia de Usuario	Descripción
HU-24 Flujo solicitante/aprobador	Como administrador empresarial, quiero flujo solicitante/aprobador, para implementar el principio de doble control para aprobar transacciones.
HU-25 Límites por monto	Como administrador empresarial, quiero límites por monto, para establecer umbrales monetarios que requieren aprobación adicional.

Historia de Usuario	Descripción
HU-26 Registro de evidencias	Como administrador empresarial, quiero registro de evidencias, para guardar trazas y comprobantes digitales de cada aprobación.
HU-61 Flujo de aprobación por niveles	Como usuario, quiero flujo de aprobación por niveles, para definir jerarquías para autorizar pagos según monto o tipo.
HU-62 Reglas por monto/día	Como administrador empresarial, quiero reglas por monto/día, para aplicar límites transaccionales diarios o por operación.
HU-63 Programación de pagos automáticos	Como usuario, quiero programación de pagos automáticos, para agendar pagos según calendario configurado.

Tabla 15: Planificación del Sprint 8.

3.5.10.2 Ejecución del Sprint 8

Se inició la ejecución con la implementación del flujo solicitante/aprobador (HU-24), que habilita el envío de operaciones a revisión antes de su ejecución; y el desarrollo del flujo de aprobación por niveles (HU-61), que establece jerarquías de aprobación basadas en montos, políticas corporativas o perfiles de riesgo.

Posteriormente, se trabajó en la implementación de controles preventivos, desarrollando la validación de límites por monto (HU-25) y las reglas por monto/día (HU-62), ambas orientadas a mitigar transacciones de alto riesgo mediante restricciones automáticas y la configuración de validadores monetarios, consultas al perfil del cliente y verificaciones del comportamiento histórico y límites permitidos.

Adicionalmente, se implementó el registro de evidencias (HU-26), que permite adjuntar y almacenar archivos, documentos o soportes digitales asociados a operaciones que requieren justificación o auditoría; para lo cual, se desarrolló la programación de pagos automáticos (HU-63), que permite al usuario configurar operaciones recurrentes dentro de parámetros de seguridad y validación, utilizando servicios temporizados y reglas predefinidas para su ejecución.

Durante las Daily Scrum, el equipo coordinó avances, discutió impedimentos y ajustó prioridades técnicas, se resolvieron desafíos relacionados con la integración del motor de reglas, la ejecución de múltiples niveles de aprobación y el almacenamiento seguro de evidencias digitales.

3.5.10.3 Revisión del Sprint 8

Durante la reunión de revisión del sprint, el equipo presentó las funcionalidades desarrolladas al Product Owner:

- Se mostró el flujo completo para la aprobación y control del riesgo.
- Se valido que cada una de las historias de usuario funcionen correctamente mediante el uso de datos de prueba o de casos específicos que los interesados solicitaron se usaran.
- Se valido que se cumplan con todos los criterios de aceptación de la épica de usuario.

Al finalizar la revisión, el Product Owner aprobó el avance y realizó observaciones menores del diseño visual con el objetivo de mejorar la navegación entre módulos.

3.5.10.4 Resultado del Sprint 8

Como resultado del trabajo colaborativo, se obtuvo un incremento funcional que incluye todas las historias de usuario descritas durante la fase de planificación y cuyas evidencias se describen en las siguientes Figuras.

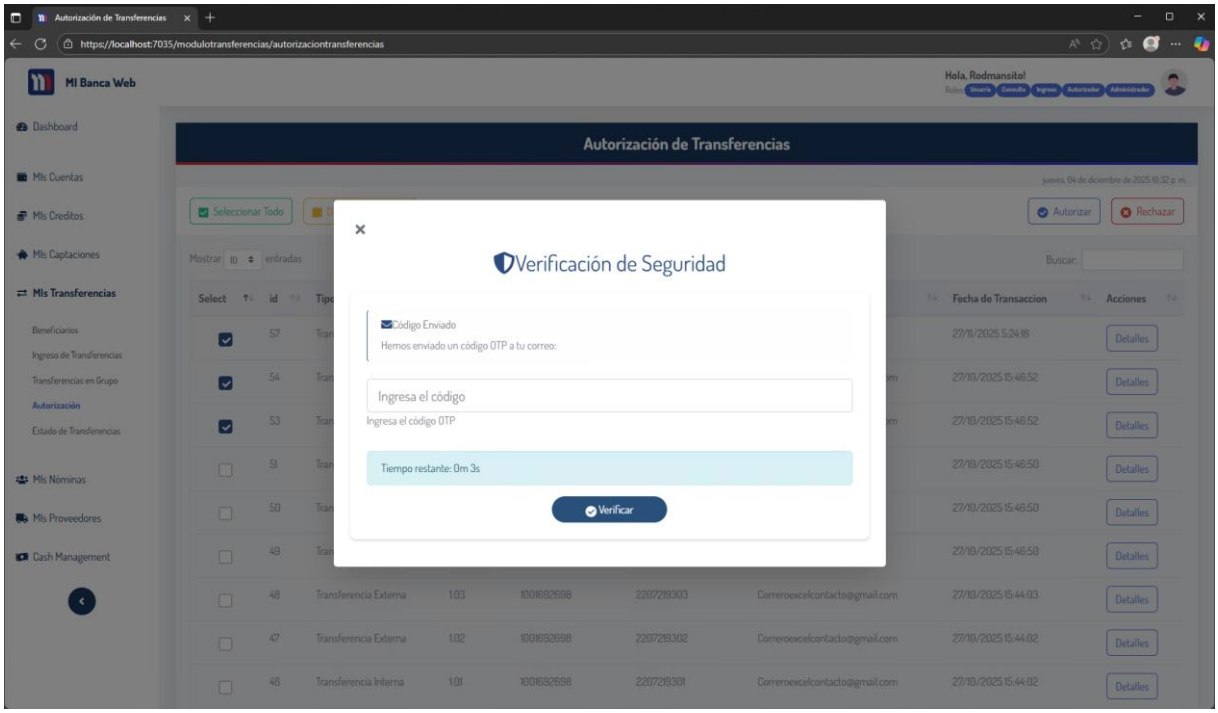


Figura 15: Flujo de aprobación por niveles.

3.5.7 Desarrollo del Sprint 9

3.5.7.1 Planificación del Sprint 9

- *Objetivo:* Implementar el módulo de Documentación Digital, incorporando la generación de PDFs contractuales, la firma/verificación OTP y el envío seguro de documentos electrónicos.
- *Duración estimada:* 2 semanas
- *Equipo involucrado:* Product Owner, Scrum Master, Desarrollador

La fase de planificación del Sprint 9 se centró en revisar y validar una a una las historias seleccionadas descritas en la Tabla 16.

Historia de Usuario	Descripción
HU-31 Generar PDF contractual	Como usuario, quiero generar pdf contractual, para crear documentos contractuales en pdf a partir de plantillas html.
HU-32 Firma y verificación OTP en documentos	Como usuario, quiero firma y verificación otp en documentos, para asociar una firma o verificación de seguridad mediante otp.
HU-33 Enviar documentos por correo	Como usuario, quiero enviar documentos por correo, para enviar automáticamente los documentos firmados al correo del cliente.

Tabla 16: Planificación del Sprint 9.

3.5.7.2 Ejecución del Sprint 9

Durante esta fase se trasladaron las historias de usuario al tablero Scrum, donde se dividieron en tareas técnicas específicas que permitieron la generación de documento en formato PDF contractual con su respectiva firma y verificación OTP para finalmente poder ser compartidos mediante correo electrónico de manera segura.

Durante las Daily Scrum, el equipo revisó su progreso, ajustó prioridades técnicas y resolvió impedimentos relacionados con la compatibilidad de plantillas, validación de firmas y seguridad en el transporte de documentos; para lo cual, el PO facilitó la comunicación con el Área Legal y el Equipo de Seguridad para garantizar el cumplimiento normativo y la integridad documental.

3.5.7.3 Revisión del Sprint 9

Durante la reunión de revisión del sprint, el equipo presentó las funcionalidades desarrolladas al Product Owner:

- Se mostró el flujo completo para la documentación digital.

- Se valido que cada una de las historias de usuario funcionen correctamente mediante el uso de datos de prueba o de casos específicos que los interesados solicitaron se usaran.
- Se valido que se cumplan con todos los criterios de aceptación de la épica de usuario.

Al finalizar la revisión, el Product Owner aprobó el avance y realizó observaciones menores del diseño visual con el objetivo de mejorar la navegación entre módulos.

3.5.7.4 Resultado del Sprint 9

Como resultado del trabajo colaborativo, se obtuvo un incremento funcional que incluye todas las historias de usuario descritas durante la fase de planificación y cuyas evidencias se describen en las siguientes Figuras.

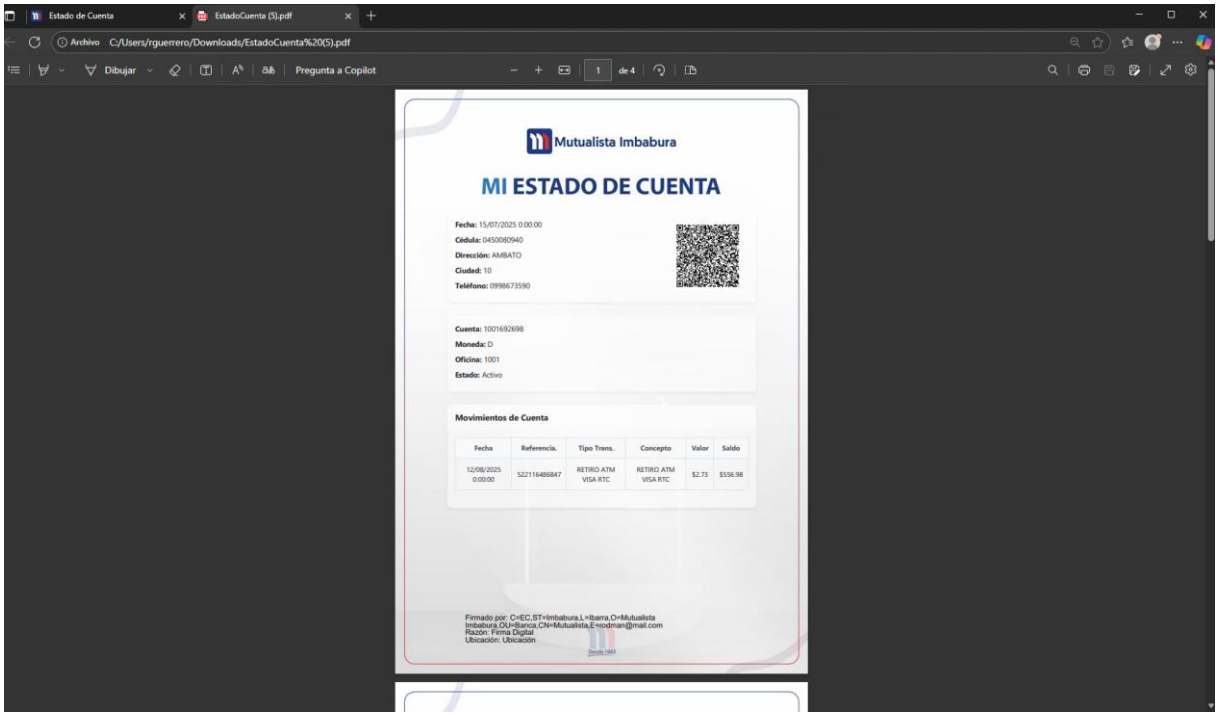


Figura 16: Generar el PDF contractual.

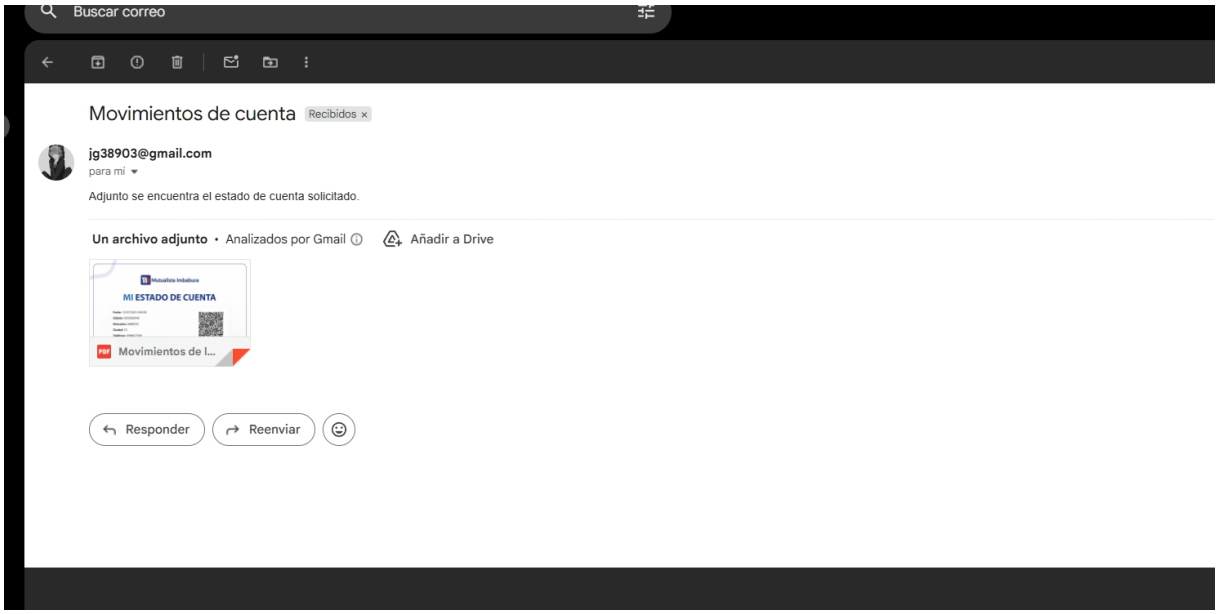


Figura 17: Envío de documentos por correo.

3.5.7 Desarrollo del Sprint 10

3.5.7.1 Planificación del Sprint 10

- *Objetivo:* Implementar el módulo de Nómina y Proveedores, garantizando la validación previa de nómina, la gestión de proveedores, la verificación de cuentas bancarias y la ejecución segura y documentada de pagos individuales.
- *Duración estimada:* 2 semanas
- *Equipo involucrado:* Product Owner, Scrum Master, Desarrollador

La fase de planificación del Sprint 10 se centró en revisar y validar una a una las historias seleccionadas descritas en la Tabla 17.

Historia de Usuario	Descripción
HU-52 Validación previa de nómina	Como usuario, quiero validación previa de nómina, para comprobar estructura y consistencia de los archivos de nómina.
HU-53 Totales por banco/cuenta	Como usuario, quiero totales por banco/cuenta, para calcular los montos totales por institución o cuenta destino.
HU-54 Detección de cuentas inválidas	Como usuario, quiero detección de cuentas inválidas, para identificar cuentas inexistentes o erróneas antes del pago.
HU-55 Generar orden de pago individual	Como usuario, quiero generar orden de pago individual, para crear la instrucción de pago para cada empleado o proveedor.

Historia de Usuario	Descripción
HU-56 Emitir comprobante PDF de pago	Como usuario, quiero emitir comprobante pdf de pago, para generar recibos individuales en formato pdf.
HU-57 Reversos controlados	Como usuario, quiero reversos controlados, para permitir revertir operaciones de nómina con registro de motivo.
HU-58 Alta/edición de proveedores	Como usuario, quiero alta/edición de proveedores, para registrar y actualizar información de proveedores.
HU-59 Validación de cuenta bancaria	Como usuario, quiero validación de cuenta bancaria, para comprobar la validez de la cuenta registrada del proveedor.
HU-60 Bloqueo de pagos no verificados	Como usuario, quiero bloqueo de pagos no verificados, para impedir realizar pagos a cuentas sin verificación.

Tabla 17: Planificación del Sprint 10.

Todas las historias fueron descompuestas en tareas técnicas específicas, tales como: construcción de servicios para lectura y validación de archivos de nómina, integración con validadores bancarios del core, desarrollo de cálculos agregados, generación de documentos PDF, creación de flujos de reversos, implementación de formularios para administración de proveedores y reglas de seguridad para bloquear pagos no verificados.

3.5.7.2 Ejecución del Sprint 10

La fase de ejecución del Sprint 10 corresponde al periodo en el cual el Equipo de Desarrollo transforma las historias priorizadas en funcionalidades operativas, integradas y verificadas para la implementación del módulo Nómina y Proveedores, el cual gestiona procesos sensibles como la validación de nóminas, pagos individuales, administración de proveedores y controles antifraude asociados.

- Para la HU-52 – Validación previa de nómina, se implementaron servicios para la lectura, análisis y validación automática de archivos de nómina, identificando inconsistencias como montos incorrectos, duplicados o cuentas inactivas.
- Se desarrolló la HU-53 – Totales por banco/cuenta, creando cálculos automáticos de agrupación que permiten generar totales por institución financiera o cuenta, facilitando conciliaciones posteriores.
- Con la HU-54 – Detección de cuentas inválidas, el equipo integró validadores contra el core bancario y sistemas externos, asegurando que todas las cuentas incluidas en un archivo sean válidas, activas y correspondan al beneficiario indicado.

- Para la HU-55 – Generar orden de pago individual, se construyeron los flujos necesarios para emitir pagos unitarios, integrando verificaciones previas y generando estructuras formales de pago.
- Esta funcionalidad se complementó con la HU-56 – Emitir comprobante PDF de pago, la cual implicó generar documentos PDF con folio único, sello temporal, metadatos financieros y registro en auditoría.
- Se implementó la HU-57 – Reversos controlados, habilitando la reversión de pagos bajo condiciones estrictas, validaciones adicionales y trazabilidad completa.
- Para la administración de proveedores, se desarrolló la HU-58 – Alta/edición de proveedores, incluyendo formularios, controles de integridad y auditoría de cambios.
- También se implementó la HU-59 – Validación de cuenta bancaria, que verifica en tiempo real que la cuenta registrada por un proveedor esté activa y pertenezca al titular indicado.
- Finalmente, se construyó la HU-60 – Bloqueo de pagos no verificados, un mecanismo de seguridad que impide ejecutar pagos a proveedores cuya verificación bancaria o documental esté incompleta.

Durante las Daily Scrum, el equipo sincronizó avances, resolvió impedimentos técnicos y priorizó tareas relacionadas con validaciones complejas, integración con el core bancario y controles antifraude; para lo cual, el PO facilitó la comunicación con el Equipo Contable y el Área de Seguridad para asegurar que las reglas financieras y medidas de protección se aplicaran correctamente.

Cada historia fue marcada como completada únicamente cuando cumplió con la Definition of Done (DoD), incluyendo pruebas superadas, documentación actualizada, revisión de código, auditoría registrada y despliegue en el entorno de pruebas del sprint.

3.5.7.3 Revisión del Sprint 10

Durante la reunión de revisión del sprint, el equipo presentó las funcionalidades desarrolladas al Product Owner:

- Se mostró el flujo completo para la nómina y proveedores.
- Se valido que cada una de las historias de usuario funcionen correctamente mediante el uso de datos de prueba o de casos específicos que los interesados solicitaron se usaran.
- Se valido que se cumplan con todos los criterios de aceptación de la épica de usuario.

Al finalizar la revisión, el Product Owner aprobó el avance y realizó observaciones menores del diseño visual con el objetivo de mejorar la navegación entre módulos.

3.5.7.4 Resultado del Sprint 10

Como resultado del trabajo colaborativo, se obtuvo un incremento funcional que incluye todas las historias de usuario descritas durante la fase de planificación y cuyas evidencias se describen en las siguientes Figuras.

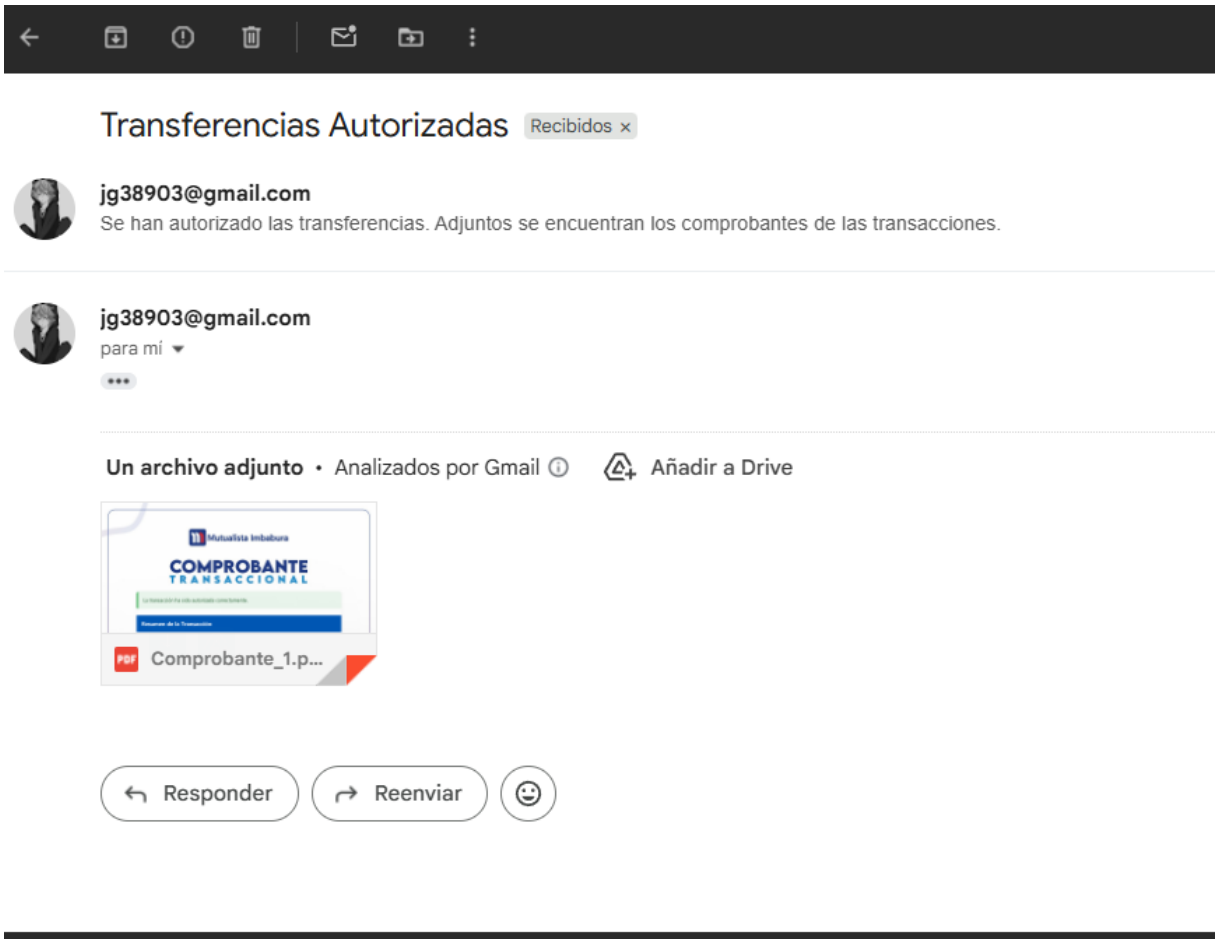


Figura 18: Comprobante PDF de pago.

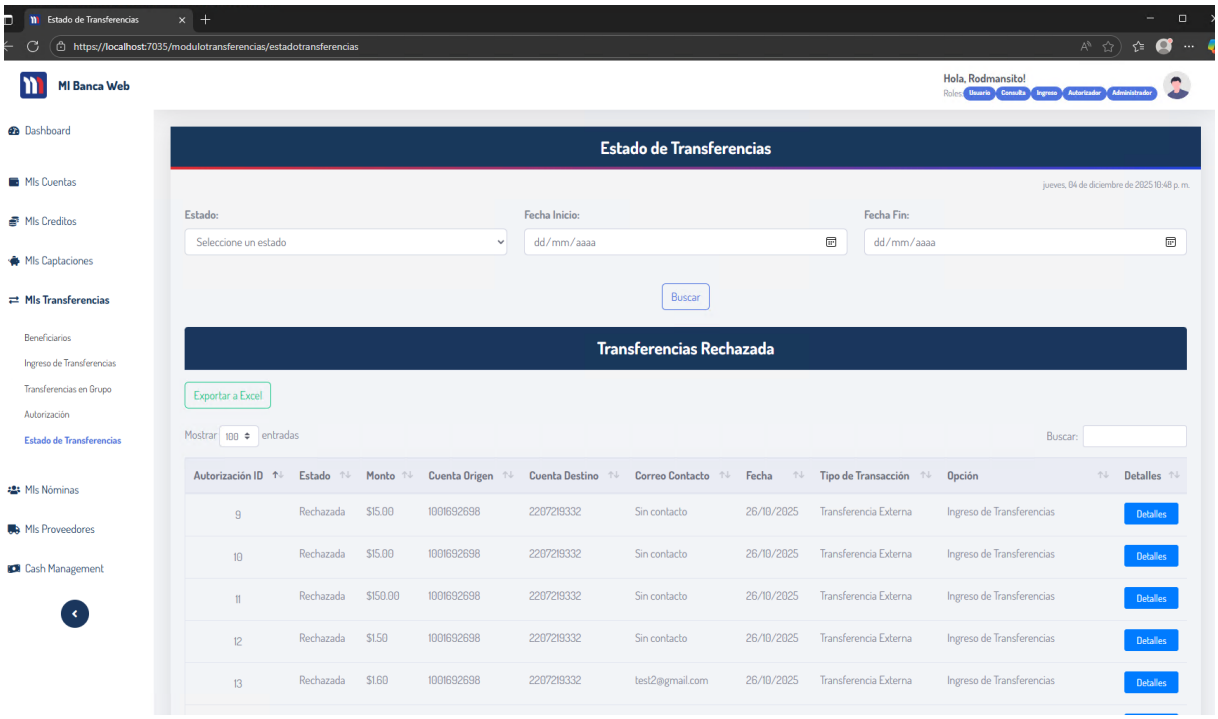


Figura 19: Bloqueo de pagos no verificados.

3.5.7 Desarrollo del Sprint 11

3.5.7.1 Planificación del Sprint 11

- *Objetivo:* Implementar funcionalidades clave para la gestión de cartera y productos financieros, incluyendo alertas de mora, mecanismos de riesgo y herramientas de simulación, cálculo y renovación de CDP.
- *Duración estimada:* 2 semanas
- *Equipo involucrado:* Product Owner, Scrum Master, Desarrollador.

La fase de planificación del Sprint 11 se centró en revisar y validar una a una las historias seleccionadas descritas en la Tabla 18.

Historia de Usuario	Descripción
HU-64 Alertas por días de mora	Como administrador del sistema, quiero alertas por días de mora, para notificar al usuario sobre obligaciones vencidas.
HU-65 Semáforo de riesgo	Como usuario, quiero semáforo de riesgo, para clasificar deudores por nivel de riesgo visualmente.
HU-66 Recordatorios automáticos	Como usuario, quiero recordatorios automáticos, para enviar notificaciones periódicas de vencimiento.

Historia de Usuario	Descripción
HU-67 Simulación de tasa/plazo CDP	Como usuario, quiero simulación de tasa/plazo cdp, para calcular proyecciones de intereses para depósitos a plazo.
HU-68 Cálculo de intereses CDP	Como usuario, quiero cálculo de intereses cdp, para determinar el valor de intereses según tasa y plazo.
HU-69 Renovación de CDP	Como usuario, quiero renovación de cdp, para permitir renovar automáticamente el depósito vencido.

Tabla 18: Planificación del Sprint 11.

Finalmente, se descompuso cada historia en tareas técnicas específicas: integración con motores de riesgo, diseño de reglas de alerta, construcción de microservicios de cálculo financiero, definición de plantillas de notificaciones, creación de simuladores dinámicos y validaciones automáticas para procesos de renovación.

3.5.7.2 Ejecución del Sprint 11

Durante la fase de ejecución del Sprint 11, se trabajó en transformar las historias priorizadas del módulo Cartera y Productos Financieros en funcionalidades completas, verificadas y listas para integración:

- Para la HU-64 – Alertas por días de mora, se implementaron servicios que consultan automáticamente el estado de cartera de cada cliente, calculan días de atraso y disparan alertas cuando se cumplen los umbrales establecidos.
- En la HU-65 – Semáforo de riesgo, el equipo desarrolló un motor de reglas que clasifica a los clientes en niveles bajo, medio o alto riesgo, basado en indicadores como historial de pago, comportamiento crediticio y montos pendientes, integrando la visualización del semáforo en el panel administrativo.
- Se construyó la HU-66 – Recordatorios automáticos, que generó un sistema de notificaciones programadas que envía recordatorios preventivos a los clientes antes de incurrir en mora.
- Se desarrolló la HU-67 – Simulación de tasa/plazo CDP, implementando un simulador dinámico que permite proyectar intereses según diferentes montos, tasas y períodos definidos.
- De forma complementaria, la HU-68 – Cálculo de intereses CDP incorporó fórmulas financieras validadas por el área de captaciones, considerando tasas vigentes, días exactos de capitalización y reglas internas del producto.

- La HU-69 – Renovación de CDP habilitó un flujo automatizado que permite renovar certificados al vencimiento, ya sea con las mismas condiciones o con parámetros actualizados, integrando validaciones, registros de auditoría y comunicación al cliente.

Durante las Daily Scrum, el equipo coordinó avances, resolvió impedimentos relacionados con el motor de riesgo y cálculos financieros, y ajustó tareas en función de dependencias técnicas; para lo cual, el PO facilitó la comunicación con áreas de negocio, especialmente Riesgos y Créditos, para validar los criterios financieros y las reglas operativas.

3.5.7.3 Revisión del Sprint 11

Durante la reunión de revisión del sprint, el equipo presentó las funcionalidades desarrolladas al Product Owner:

- Se mostró el flujo completo para la cartera y productos financieros.
- Se valido que cada una de las historias de usuario funcionen correctamente mediante el uso de datos de prueba o de casos específicos que los interesados solicitaron se usaran.
- Se valido que se cumplan con todos los criterios de aceptación de la épica de usuario.

Al finalizar la revisión, el Product Owner aprobó el avance y realizó observaciones menores del diseño visual con el objetivo de mejorar la navegación entre módulos.

3.5.7.4 Resultado del Sprint 11

Como resultado del trabajo colaborativo, se obtuvo un incremento funcional que incluye todas las historias de usuario descritas durante la fase de planificación y cuyas evidencias se describen en las siguientes Figuras.

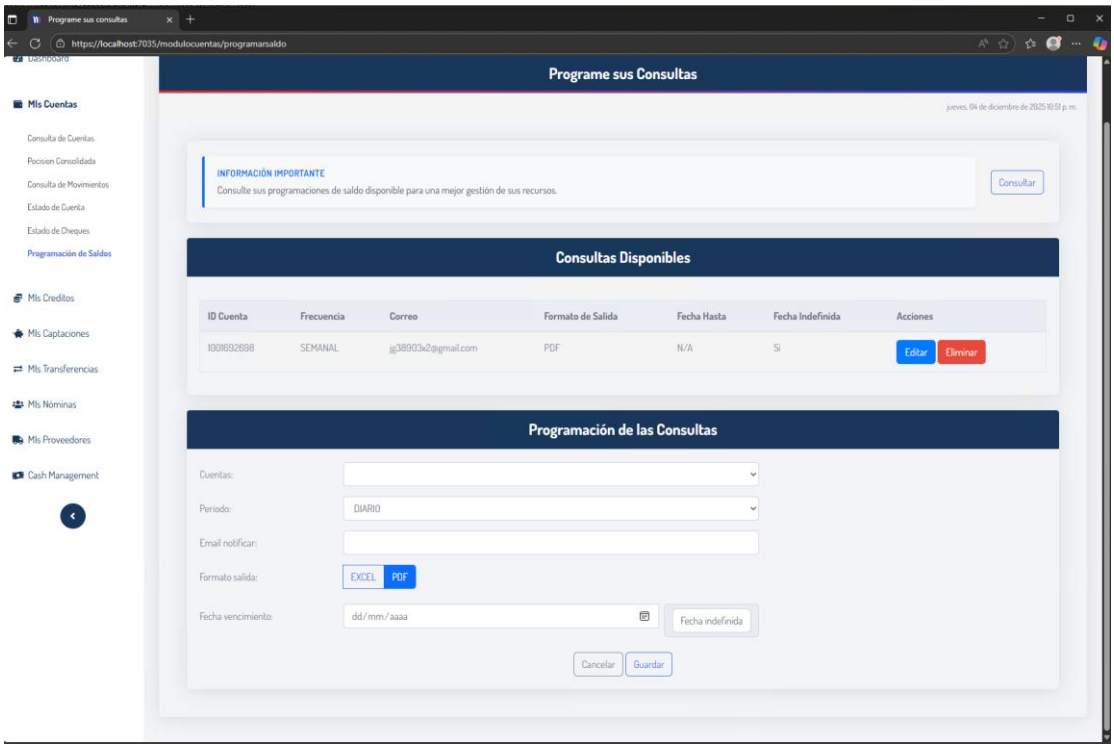


Figura 20: notificaciones periódicas.

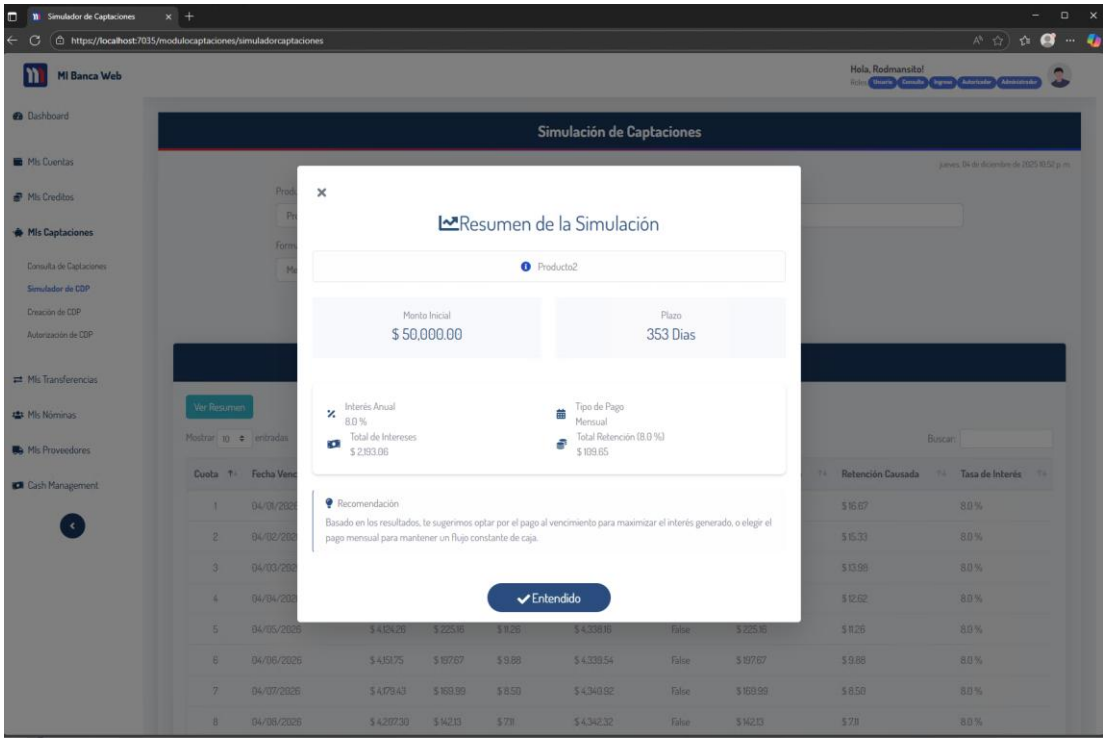


Figura 21: Cálculo de intereses CDP.

3.5.8 Pruebas de funcionamiento

Con el propósito de garantizar que el sistema de banca electrónica empresarial cumpla con los requisitos normativos y de seguridad establecidos por la Superintendencia de Economía Popular y Solidaria y las mejores prácticas internacionales definidas por OWASP, se ejecutó un conjunto estructurado de pruebas de funcionamiento orientadas a validar la correcta implementación de los controles exigidos en la resolución SEPS-009 y de los mecanismos de protección frente a las vulnerabilidades descritas en el marco OWASP Top 10.

Las pruebas abarcaron aspectos críticos como autenticación, control de acceso, trazabilidad, límites transaccionales, validación de datos, manejo de sesiones, protección contra inyección y exposición de datos sensibles, entre otros, cuyos resultados se encuentran descritos en dos tablas (Tabla y Tabla), que evidencian que todas las funcionalidades evaluadas cumplen de manera satisfactoria con los criterios de seguridad, integridad y confiabilidad requeridos, demostrando que el sistema implementado es estable, seguro y alineado a los estándares regulatorios y de ciberseguridad vigentes.

ID	Funcionalidad	Descripción de la Prueba	Resultado Esperado	Resultado Obtenido	Estado
SEPS-01	Autenticación segura	Probar acceso con credenciales válidas y bloqueo tras múltiples intentos fallidos.	Solo usuarios válidos acceden; la cuenta se bloquea al exceder intentos permitidos y se registra el evento.	El usuario válido accede; la cuenta se bloquea tras intentos fallidos y queda registrado en bitácora.	Aprobado
SEPS-02	Gestión de sesiones	Verificar expiración automática y cierre seguro de sesión.	La sesión expira según el tiempo configurado y el cierre manual invalida el token.	La sesión expira correctamente e invalida el token, requiriendo autenticación al reingresar.	Aprobado
SEPS-03	Control de acceso (RBAC)	Validar acceso a funciones según rol: administrador, aprobador, operador, auditor.	Cada rol accede solo a sus funciones; accesos no autorizados se rechazan y auditan.	Los usuarios solo acceden a funciones permitidas y los accesos restringidos se registran.	Aprobado
SEPS-04	Trazabilidad y auditoría	Verificar registro de eventos (login, operaciones, aprobaciones, pagos, bloqueos).	Todos los eventos críticos se registran con usuario, fecha, hora, IP y detalle.	La auditoría registra todos los eventos probados con detalle completo.	Aprobado

ID	Funcionalidad	Descripción de la Prueba	Resultado Esperado	Resultado Obtenido	Estado
SEPS-05	Límites transaccionales	Ejecutar transacciones dentro del límite, en el límite y fuera del mismo.	Las operaciones válidas se ejecutan; las que superan límites se bloquean o requieren aprobación.	El sistema ejecuta o bloquea según la regla configurada y registra el evento.	Aprobado
SEPS-06	Flujos de aprobación	Ejecutar operaciones que requieren uno o varios aprobadores según monto.	Las operaciones quedan pendientes hasta completarse el flujo; cada aprobación se registra.	El sistema exige aprobaciones según la regla, registra el flujo completo y libera la operación.	Aprobado
SEPS-07	Integridad documental	Generar comprobantes (transferencias, barridos, nómina) y validar su folio único.	Cada comprobante genera folio único, sello temporal y datos verificables en el sistema.	Los comprobantes se generan correctamente, con folio y validación en el sistema.	Aprobado
SEPS-08	Gestión de datos de beneficiarios / proveedores	Validar alta, edición y bloqueo por falta de verificación.	Solo datos completos y verificados se aceptan; proveedores no verificados se bloquean.	Los registros incompletos se rechazan; proveedores no verificados no pueden recibir pagos.	Aprobado
SEPS-09	Continuidad del servicio	Simular carga moderada y validar disponibilidad del canal.	El sistema mantiene operación estable sin caídas ni pérdida de integridad.	La aplicación mantuvo tiempos de respuesta adecuados bajo carga simulada.	Aprobado
SEPS-10	Integración con core bancario	Forzar fallos de comunicación durante transacciones.	El sistema marca la operación como pendiente/error y registra el evento.	Los fallos no generan duplicados; la operación queda en estado controlado y auditado.	Aprobado

Tabla 19: Resultados de las pruebas de funcionamiento sobre la base de la Resolución SEPS-009.

ID	Funcionalidad	Descripción de la Prueba	Resultado Esperado	Resultado Obtenido	Estado
OWASP-01	Protección contra Inyección	Probar SQL/NoSQL injection en formularios (login, búsqueda, alta de datos).	Las entradas son saneadas; no se ejecutan comandos maliciosos.	Todas las entradas maliciosas fueron rechazadas o ignoradas sin afectar el sistema.	Aprobado
OWASP-02	Control de acceso	Intentar acceder a funciones restringidas mediante URL o manipulación del frontend.	El acceso es denegado y auditado; no se exponen datos sensibles.	El acceso no autorizado fue bloqueado y registrado.	Aprobado
OWASP-03	Gestión de autenticación	Probar OTP inválidos, expirados, y múltiples intentos fallidos.	El sistema rechaza OTP inválidos/ expirados y registra los eventos.	Los OTP inválidos fueron rechazados y los correctos aceptados dentro del tiempo permitido.	Aprobado
OWASP-04	Seguridad de sesiones	Manipular cookies/tokens para intentar reutilizarlos tras logout o expiración.	Los tokens caducan y no pueden reutilizarse; la sesión no puede reabrirse sin login.	Los tokens expirados fueron invalidados y no permitieron reuso.	Aprobado
OWASP-05	Validación de entrada	Probar formularios con datos inválidos, vacíos o mal formados.	Los campos obligatorios deben validarse; no se acepta información incorrecta.	Todos los formularios aplicaron validaciones de integridad y formato.	Aprobado
OWASP-06	Manejo seguro de errores	Probar URLs inválidas y operaciones incorrectas para capturar mensajes del sistema.	Se muestran errores genéricos sin revelar detalles internos.	Los errores mostrados no exponen información del servidor ni stack trace.	Aprobado
OWASP-07	Exposición de datos sensibles	Revisar logs y respuestas del sistema para verificar enmascaramiento y cifrado.	No se debe mostrar información sensible en texto claro.	Logs y pantallas enmascaran cuentas y cifran credenciales.	Aprobado

ID	Funcionalidad	Descripción de la Prueba	Resultado Esperado	Resultado Obtenido	Estado
OWASP-08	Protección contra XSS	Intentar inyectar scripts en campos de entrada.	El sistema escapa o rechaza scripts; no se ejecuta código en el navegador.	Los scripts fueron mostrados como texto literal o rechazados.	Aprobado
OWASP-09	Registro y monitoreo	Generar eventos anómalos (OTP fallido, intentos de acceso, errores).	Todos los eventos deben registrarse y ser visibles para auditoría.	Los eventos fueron capturados con usuario, fecha y detalle.	Aprobado
OWASP-10	Disponibilidad (DoS básico)	Simular múltiples solicitudes rápidas e intensas.	El sistema mantiene estabilidad y limita impactos sin caída del servicio.	La aplicación respondió correctamente bajo el escenario de estrés controlado.	Aprobado

Tabla 20: Resultados de las pruebas de funcionamiento sobre la base de OWASP Top 10.

3.5.9 Pruebas de Integración

Con el objetivo de verificar la correcta interacción entre los distintos módulos del sistema de banca electrónica empresarial y asegurar que su funcionamiento integral cumple con los lineamientos establecidos por la resolución SEPS-009 y con los controles de seguridad definidos en el estándar OWASP Top 10, se desarrolló un conjunto de pruebas de integración orientadas a evaluar flujos completos, dependencias entre componentes, comunicación con servicios externos y coherencia de los mecanismos de seguridad implementados.

Estas pruebas permitieron validar procesos críticos como autenticación, gestión de sesiones, límites transaccionales, aprobación multinivel, generación de comprobantes, integración con el core bancario, validación de datos, sanitización de entradas, manejo seguro de errores y monitoreo de eventos, los resultados obtenidos se presentan en la Tabla y Tabla , evidenciando que el sistema integra adecuadamente todas sus funcionalidades, mantiene la trazabilidad requerida, protege la información en cada capa y opera de manera segura, estable y conforme a las disposiciones regulatorias y de ciberseguridad vigentes.

ID	Funcionalidad Integrada	Descripción de la Prueba	Resultado Esperado	Resultado Obtenido	Estado
SEPS-INT-01	Autenticación + Gestión de Sesiones	Validar login, generación de token y expiración conforme a	El token se genera, expira según el tiempo configurado y no permite reutilización.	El token vence correctamente y no se puede reutilizar tras logout o expiración.	Aprobado

ID	Funcionalidad Integrada	Descripción de la Prueba	Resultado Esperado	Resultado Obtenido	Estado
		políticas SEPS-009.			
SEPS-INT-02	Autenticación + Auditoría	Verificar que login y logout registren trazabilidad completa.	Se registran usuario, IP, fecha, hora y estado del evento en bitácora.	Los eventos se registran con detalle y pueden consultarse/exportarse.	Aprobado
SEPS-INT-03	Roles + Control de Acceso	Validar que los roles definidos limiten el acceso en toda la plataforma.	Cada usuario accede solo a sus funciones; el acceso no autorizado se registra.	El control funciona correctamente y los accesos indebidos quedan auditados.	Aprobado
SEPS-INT-04	Límites + Transferencias	Ejecutar transferencias dentro, en y fuera de los límites.	Se procesan solo operaciones dentro del límite; las demás se bloquean o requieren aprobación.	Las transacciones fueron gestionadas según reglas y auditadas correctamente.	Aprobado
SEPS-INT-05	Transferencias + Flujo de Aprobación	Validar integración entre montos altos y aprobaciones multinivel.	Operaciones sobre el umbral quedan “Pendientes de aprobación”.	Las aprobaciones multinivel funcionaron y las operaciones se liberaron tras aprobación.	Aprobado
SEPS-INT-06	Beneficiarios/Proveedores + Core Bancario	Validar cuentas consultando bases externas.	La cuenta debe validarse contra datos del core antes de usarse.	Las cuentas se validaron correctamente y las inválidas fueron rechazadas.	Aprobado
SEPS-INT-07	Nómina + Auditoría	Procesar una nómina completa y validar su registro en bitácora.	Los pagos, validaciones y rechazos deben registrar eventos.	Todos los eventos quedaron auditados con detalle.	Aprobado
SEPS-INT-08	Documentación + Operaciones	Generar comprobantes PDF y registrar operación.	Cada comprobante incluye folio único y queda registrado.	Todos los comprobantes se generaron con folio y se registraron en el log.	Aprobado
SEPS-INT-09	Barridos Programados + Core Bancario	Ejecutar barridos automáticos basados en reglas.	Los barridos deben ejecutarse en horario	Los barridos se ejecutaron automáticamente,	Aprobado

ID	Funcionalidad Integrada	Descripción de la Prueba	Resultado Esperado	Resultado Obtenido	Estado
			definido y registrar la operación.	generando documentos y auditoría.	
SEPS-INT-10	KPIs + Módulos Financieros	Validar actualización de KPIs tras operaciones.	Las métricas deben actualizarse sin inconsistencias y reflejar la actividad real.	Los KPIs se actualizaron correcta y oportunamente.	Aprobado

Tabla 21: Resultados de las pruebas de funcionamiento sobre la base de Resolución SEPS-009.

ID	Funcionalidad Integrada	Descripción de la Prueba	Resultado Esperado	Resultado Obtenido	Estado
OWASP-INT-01	Frontend + API + BD (Inyección)	Enviar cadenas maliciosas para probar SQL/NoSQL injection.	Los datos se validan en todas las capas; la inyección no se ejecuta.	Las cadenas fueron neutralizadas y no afectaron la BD.	Aprobado
OWASP-INT-02	Roles + URLs Protegidas	Intentar acceso a funcionalidad restringida mediante manipulación de URLs.	El acceso es denegado y auditado.	El sistema rechazó el acceso y registró el evento.	Aprobado
OWASP-INT-03	OTP + Flujo Transaccional	Validar OTP en operaciones críticas y su registro.	OTP correcto permite avanzar; fallos quedan registrados.	OTP válido funcionó y OTP incorrectos fueron rechazados.	Aprobado
OWASP-INT-04	Sesiones + Tokens	Manipular el token tras logout para intentar reutilizar la sesión.	El token debe invalidarse en backend y no ser reutilizable.	El token no pudo ser reutilizado.	Aprobado
OWASP-INT-05	Formularios + Validaciones	Probar integraciones completas de validación de campos.	Se bloquean datos inválidos en frontend y backend.	Las validaciones funcionaron integralmente.	Aprobado
OWASP-INT-06	Manejo de Errores + API	Forzar errores en API para evaluar exposición de información.	El sistema muestra mensajes genéricos sin	No se expuso información sensible ni stack traces.	Aprobado

ID	Funcionalidad Integrada	Descripción de la Prueba	Resultado Esperado	Resultado Obtenido	Estado
			detalles del servidor.		
OWASP-INT-07	Logs + Sistema Completo	Generar operaciones anómalas para evaluar monitoreo.	Todos los eventos deben aparecer en logs y bitácora.	Todos los eventos fueron registrados con integridad.	Aprobado
OWASP-INT-08	XSS + Formularios	Inyectar código JavaScript en campos de texto.	Las entradas deben escapar/limpiar código y no ejecutarlo.	Ningún script se ejecutó; la entrada fue sanitizada.	Aprobado
OWASP-INT-09	APIs + Seguridad	Probar llamadas repetitivas con el fin de evaluar disponibilidad.	El sistema controla carga y no cae ante múltiples solicitudes.	La aplicación se mantuvo estable y operativa.	Aprobado
OWASP-INT-10	Exportes + Seguridad	Validar exportes CSV/XLSX sin exponer datos sensibles.	Los datos sensibles deben enmascararse antes de exportar.	Los exportes muestran datos cifrados/ enmascarados.	Aprobado

Tabla 22: Resultados de las pruebas de integración sobre la base de OWASP Top 10.

3.5.10 Pruebas de Auditoría de Seguridad

Con el fin de evaluar el cumplimiento de los lineamientos regulatorios y de seguridad aplicables al sistema de banca electrónica empresarial, se ejecutó un conjunto integral de pruebas de auditoría de seguridad, orientadas a comprobar la efectiva incorporación de los controles establecidos en la Resolución SEPS-009 y las buenas prácticas definidas en el marco OWASP Top 10.

Los resultados obtenidos, presentados la Tabla y Tabla, demuestran que el sistema registra adecuadamente cada evento relevante, protege la integridad de la información auditada y responde de manera segura ante acciones indebidas o riesgosas, cumpliendo así con los estándares regulatorios y de ciberseguridad requeridos para su operación confiable en un entorno financiero.

ID	Funcionalidad	Descripción de la Prueba	Resultado Esperado	Resultado Obtenido	Estado
SEPS -	Bitácora de eventos críticos	Auditar registro de	Todos los eventos deben registrar	Todos los eventos se	Aprobad o

ID	Funcionalidad	Descripción de la Prueba	Resultado Esperado	Resultado Obtenido	Estado
AUD-01		login, logout, cambios de contraseña, bloqueos y eventos relevantes.	usuario, IP, fecha, hora, módulo y resultado.	registraron con trazabilidad completa y exportable.	
SEPS-AUD-02	Auditoría de transacciones	Validar registro de transferencias internas, externas y pagos masivos.	Cada transacción debe registrar monto, cuentas, usuario, estado, aprobaciones y comprobante.	El historial de transacciones fue registrado sin inconsistencias.	Aprobado
SEPS-AUD-03	Auditoría de reglas y configuraciones	Auditar cambios en límites, roles, permisos y reglas de flujo.	Registrar usuario responsable, valores anteriores, nuevos y fecha/hora.	Todos los cambios quedaron registrados con detalle completo.	Aprobado
SEPS-AUD-04	Integridad de la bitácora	Intentar alterar o eliminar registros desde la interfaz.	No debe permitirse manipulación y el intento debe quedar registrado.	Los registros no pudieron modificarse y el intento quedó auditado.	Aprobado
SEPS-AUD-05	Auditoría de beneficiarios/proveedores	Auditar creación, modificación y bloqueo de beneficiarios y proveedores.	Registrar datos del cambio, usuario y motivo.	Todos los eventos quedaron registrados correctamente.	Aprobado
SEPS-AUD-06	Auditoría de OTP	Verificar registro de envío, validaciones, fallos y expiración de OTP.	Registrar todos los intentos con resultado y marca de tiempo.	Todos los eventos fueron registrados sin omisiones.	Aprobado
SEPS-AUD-07	Auditoría de errores operativos	Forzar errores de negocio y	Registrar tipo de error, módulo y usuario involucrado.	Los errores fueron registrados con	Aprobado

ID	Funcionalidad	Descripción de la Prueba	Resultado Esperado	Resultado Obtenido	Estado
		validar registro.		clasificación adecuada.	
SEPS-AUD-08	Auditoría de accesos a información sensible	Consultar cartera, CDP y nómina con distintos roles.	Registrar accesos permitidos/denegados.	La auditoría capturó cada acceso y denegación.	Aprobado
SEPS-AUD-09	Auditoría de exportaciones	Validar registro de exportes de CSV/XLSX.	Registrar quién, cuándo y qué datos fueron exportados.	Todos los exportes quedaron auditados correctamente.	Aprobado
SEPS-AUD-10	Auditoría de barridos automáticos	Validar registro de ejecuciones programadas.	Registrar ejecución, reglas aplicadas, monto y comprobante.	Todas las ejecuciones quedaron auditadas con datos completos.	Aprobado

Tabla 23: Resultados de Auditoría de Seguridad (SEPS-009).

ID	Funcionalidad	Descripción de la Prueba	Resultado Esperado	Resultado Obtenido	Estado
OWASP-AUD-01	Control de acceso	Intentar acceder a funcionalidades restringidas mediante URL o manipulación de parámetros.	Acceso denegado y registro del intento (OWASP: Broken Access Control).	El acceso fue bloqueado y registrado como incidente.	Aprobado
OWASP-AUD-02	Inyección	Enviar cadenas maliciosas en distintas capas (frontend, API, BD).	Las entradas son sanitizadas; se registra el intento.	Todas las cadenas fueron rechazadas y auditadas.	Aprobado
OWASP-AUD-03	Gestión de sesiones	Forzar reutilización de tokens o uso de cookies manipuladas.	Token inválido debe registrarse como intento sospechoso.	Cada intento quedó registrado en auditoría como actividad anómala.	Aprobado
OWASP-AUD-04	Manejo de errores	Forzar errores internos y validar el registro sin exponer detalles.	Debe registrarse el error con	Los errores quedaron registrados y sin	Aprobado

ID	Funcionalidad	Descripción de la Prueba	Resultado Esperado	Resultado Obtenido	Estado
			código, tipo y módulo.	exposición de datos sensibles.	
OWASP-AUD-05	Validación y saneamiento	Registrar intentos fallidos de carga de datos inválidos.	Registrar el fallo y bloqueo de la solicitud.	Todos los intentos se registraron con detalle.	Aprobado
OWASP-AUD-06	Registro y monitoreo	Generar eventos anómalos (OTP fallidos, intentos repetidos de login, cambios masivos).	Cada evento debe clasificarse como incidente de seguridad.	Los eventos fueron registrados y clasificados como riesgo medio/alto.	Aprobado
OWASP-AUD-07	XSS	Injectar scripts en formularios y validar auditoría.	El sistema debe bloquear el script y registrar el intento.	Los scripts fueron rechazados y auditados correctamente.	Aprobado
OWASP-AUD-08	Configuración de seguridad	Cambiar configuraciones desde usuario no autorizado.	La acción debe ser bloqueada y registrada.	Los intentos fueron denegados y auditados.	Aprobado
OWASP-AUD-09	Integración con APIs	Probar accesos no autorizados a endpoints.	Denegar acceso y registrar anomalía.	El sistema bloqueó e integró el evento en la auditoría.	Aprobado
OWASP-AUD-10	Actividad sospechosa	Simular patrones de fraude (transacciones rápidas, cambios repetidos).	Registrar el incidente y activar alertas.	Todos los patrones fueron detectados y registrados como actividad sospechosa.	Aprobado

Tabla 24: Resultados de las pruebas de Auditoría de Seguridad sobre la base de OWASP Top 10.

CAPÍTULO IV
RESULTADOS Y ANÁLISIS

4.1 Resultados

Los resultados de la investigación evidencian que el análisis de artículos científicos, normas técnicas, manuales de seguridad, lineamientos regulatorios y documentos de arquitectura permitieron identificar las mejores prácticas para la autenticación, protección de datos, modelos de integración, diseño de APIs, observabilidad, gestión de sesiones y manejo seguro de errores, cuya comprensión aportó claridad sobre los estándares necesarios para asegurar la confiabilidad del sistema, garantizando que los componentes diseñados respondieran a criterios de calidad ampliamente validados en entornos bancarios.

Asimismo, la investigación bibliográfica permitió comprender a profundidad el contenido, alcance y exigencias de la Resolución SEPS-009, la cual establece disposiciones obligatorias para la seguridad de canales electrónicos y la operación de sistemas financieros en entidades reguladas por la Superintendencia de Economía Popular y Solidaria, lo que permitió que la modelación del sistema se fundamentara en un marco normativo sólido, asegurando que cada módulo y cada funcionalidad cumplan con las obligaciones regulatorias vigentes.

Adicionalmente, la revisión de literatura técnica sobre OWASP Top 10 y marcos de ciberseguridad permitió realizar el análisis de vulnerabilidades como inyección, control de acceso deficiente, exposición de datos sensibles, fallas criptográficas y deficiencias en registros y monitoreo lo que contribuyó directamente a la definición de requisitos funcionales y no funcionales orientados a fortalecer la seguridad desde el diseño (security by design) posibilitando que la arquitectura del sistema incorporara controles preventivos, detectivos y correctivos.

Complementariamente, las entrevistas aplicadas a personal clave de la Mutualista Imbabura brindaron información contextual indispensable para adaptar el sistema a las necesidades reales de la entidad permitieron identificar procesos internos, limitaciones actuales, necesidades de automatización, flujos de aprobación, tiempos de respuesta, problemáticas reales y oportunidades de mejora, lo cual fue decisivo para definir un conjunto de funcionalidades orientadas a la operación diaria.

Los datos recolectados a través de las entrevistas también permitieron validar y complementar la información obtenida en la bibliografía, logrando una triangulación metodológica que

fortaleció la definición del product backlog y la priorización de los módulos del sistema; así también, las percepciones de los usuarios sobre los riesgos operativos, la necesidad de controles adicionales, la importancia de los flujos de aprobación y la gestión documental digital influyeron directamente en el diseño de los Sprint y en la definición de historias de usuario más precisas y alineadas a los procesos internos.

En base a lo antes descrito, los resultados muestran que la integración de la investigación bibliográfica y las entrevistas fue clave para construir un sistema de banca electrónica empresarial robusto, seguro y funcional, alineado tanto a los estándares regulatorios (SEPS-009) como a las mejores prácticas de seguridad (OWASP Top 10), con una arquitectura modular, altos niveles de seguridad y capacidad de auditoría, que aseguran que el sistema no solo satisfaga necesidades tecnológicas, sino que también mejore la eficiencia operativa, reduzca riesgos y fortalezca la gestión financiera digital de la Mutualista Imbabura.

4.2 Análisis

Los estudios de Luo et al. [1] y Gaol et al. [2] muestran cómo la modernización de la banca empresarial depende de arquitecturas escalables, desacopladas y orientadas a servicios, lo cual se alinea con el enfoque adoptado en esta investigación al diseñar un sistema modular basado en N-capas y principios DDD, es importante destacar que las investigaciones antes nombradas se enfocan en la optimización de consultas y gobernanza de reglas de negocio, subrayando que el valor del procesamiento eficiente y la autonomía funcional son elementos clave que justifican la elección de tecnologías de Microsoft.

Asimismo, los estudios de Ibarra-Fiallos et al. [3], Aljabri et al. [4] y de Kellezi et al. [9] constituyen un eje crítico al demostrar que la seguridad no puede concebirse como un componente accesorio, sino como un elemento transversal que debe integrarse desde la arquitectura, el desarrollo y la operación, lo que respaldó la necesidad de incorporar controles alineados a OWASP Top 10, tales como validación estricta, protección criptográfica, monitoreo y segregación de privilegios.

En cuanto a la banca electrónica y su digitalización, los estudios revisados señalan que la banca corporativa exige mayores controles, trazabilidad y flexibilidad que la banca personal, lo cual, críticamente, sustenta la necesidad de módulos especializados como aprobaciones por niveles, control de riesgo, cash management y generación automática de documentos contractuales; además, las evidencias sobre debilidades detectadas en certificados digitales y prácticas de

seguridad en Ecuador justifican la incorporación obligatoria de MFA, TLS 1.3, cifrado AES-256 y auditorías continuas, alineando el diseño del sistema con riesgos reales del entorno local.

El análisis de cifrado, autenticación multifactor y protección de datos permite vincular la teoría con la práctica del desarrollo del sistema al establecer que las vulnerabilidades más frecuentes como inyección, autenticación débil y manejo inseguro de datos coinciden con los riesgos regulados por SEPS-009 y OWASP, lo que demuestra que el sistema no solo cumple con lineamientos normativos, sino que responde a riesgos ampliamente documentados en la literatura científica; no obstante, se reconoce que la mayor parte de los estudios sobre criptografía expuestos en el marco teórico tienen un enfoque conceptual, y no operativo, por lo que esta investigación aporta al transferir dichos principios a un contexto aplicado específico.

En lo referente a la metodología Scrum, la literatura citada destaca su capacidad para generar entregables incrementales y gestionar la complejidad en entornos regulados, lo que resulta coherente con la división por Sprints adoptada en el proyecto con el objetivo de facilitar la mitigación temprana de riesgos y la incorporación continua de requisitos normativos, lo que resulta clave para sistemas financieros en constante actualización.

Los resultados obtenidos de las distintas pruebas realizadas (incluyendo pruebas de funcionamiento, integración y auditoría de seguridad) evidencian que el sistema de banca electrónica empresarial opera de manera completa, coherente y confiable en todos sus módulos, lo que confirma que las funcionalidades implementadas responden adecuadamente a los requerimientos normativos de la resolución SEPS-009 y a los controles de seguridad establecidos por OWASP Top 10, garantizando autenticación robusta, trazabilidad íntegra, control de accesos, protección de datos sensibles, manejo seguro de errores y operación estable en escenarios reales.

Conclusiones y recomendaciones

Conclusiones

Los resultados de esta investigación permiten concluir que el desarrollo e implementación del sistema de Banca Electrónica Empresarial para la Mutualista Imbabura cumple de manera efectiva con el objetivo general planteado, al integrar una arquitectura robusta, funcional y segura, diseñada conforme a los lineamientos regulatorios de la resolución SEPS-009 y a los controles de ciberseguridad establecidos en OWASP Top 10.

En relación con el primer objetivo específico, la revisión sistemática de literatura realizada aportó una base conceptual sólida para el diseño del sistema, permitiendo comprender de forma integral los requerimientos técnicos, normativos y de seguridad aplicables a plataformas de banca electrónica garantizando una estructura del sistema fundamentada en estándares internacionales.

Respecto al segundo objetivo específico, se concluye que la implementación del sistema fue exitosa, logrando construir módulos operativos para consulta de saldos, movimientos, transferencias internas y externas, pagos masivos, administración de cuentas, flujo de aprobaciones, cash management, generación de comprobantes digitales, incorporación de un módulo de seguridad basado en MFA, cifrado de datos, manejo seguro de sesiones, validación de integridad y trazabilidad de auditoría que aseguró un funcionamiento orientado a la prevención de fraudes y al cumplimiento normativo.

Finalmente, en relación con el tercer objetivo específico, la validación del sistema mediante pruebas técnicas basadas en los controles SEPS-009 verificaron el cumplimiento de políticas de seguridad, límites transaccionales, segregación de funciones y trazabilidad detallada; mientras que las pruebas OWASP Top 10 confirmaron la resistencia del sistema frente a vulnerabilidades como inyección, exposición de datos sensibles, control de acceso deficiente y fallas de gestión de sesiones.

Recomendaciones

A continuación, se presentan las recomendaciones de la investigación orientadas tanto a la continuidad del proyecto como al fortalecimiento del sistema de Banca Electrónica Empresarial en la Mutualista Imbabura:

- **Fortalecer la mejora continua del sistema mediante actualizaciones periódicas de seguridad:** Se recomienda que la Mutualista Imbabura mantenga un ciclo permanente de revisión y actualización del sistema, especialmente en lo referente a la incorporación de nuevas versiones de OWASP Top 10, actualización de algoritmos criptográficos, mejoras en los métodos de autenticación y nuevas disposiciones emitidas por la SEPS con el objetivo de asegurar que el sistema continúe alineado a los estándares actuales y responda adecuadamente a la evolución de amenazas cibernéticas.
- **Implementar un programa interno de capacitación técnica y operativa:** Debido a la naturaleza crítica del sistema, es recomendable que el personal administrativo, operativo, de riesgos y de TI reciba capacitaciones regulares sobre el uso del sistema, los flujos de aprobación, la gestión de incidentes y las políticas de seguridad, esto garantizará un uso adecuado de la plataforma y minimizará errores operativos que puedan comprometer la seguridad o trazabilidad de las transacciones.
- **Establecer un plan de auditorías periódicas internas y externas:** Se sugiere programar auditorías técnicas y de cumplimiento al menos una vez al año, con el objetivo de validar el funcionamiento del sistema, verificar la integridad de la información, evaluar el cumplimiento continuo de la resolución SEPS-009 y asegurar que no existan vulnerabilidades emergentes.
- **Ampliar gradualmente la arquitectura del sistema para integrar nuevos servicios financieros:** Dado que el sistema fue diseñado bajo principios de modularidad y escalabilidad, se recomienda agregar progresivamente nuevas funcionalidades como inversiones empresariales, confirmación electrónica de pagos, conciliación avanzada, conexión con sistemas tributarios y automatización inteligente mediante IA con el objetivo de que la Mutualista expanda su portafolio digital de manera ordenada y sostenible.
- **Fortalecer los mecanismos de monitoreo y respuesta a incidentes:** Se recomienda implementar o ampliar un SOC (Centro de Operaciones de Seguridad) que supervise en tiempo real los eventos del sistema, alertas de auditoría, patrones anómalos de transacción y posibles incidentes de seguridad cuya correlación contribuirá a una detección temprana y mitigación más eficiente de riesgos.

- **Desarrollar pruebas continuas de calidad y de seguridad en ambientes controlados:** Se sugiere mantener un entorno de pruebas separado del ambiente de producción para ejecutar pruebas de regresión, pruebas automáticas, pruebas de carga y ejercicios de ethical hacking de forma rutinaria. Esto permitirá detectar problemas antes de que afecten a los usuarios finales y asegurar la consistencia funcional del sistema.
- **Fortalecer la gobernanza tecnológica mediante políticas internas actualizadas:** Se recomienda actualizar y formalizar políticas de seguridad, gestión de contraseñas, administración de usuarios, auditoría y retención de datos, basadas en los controles implementados y en mejores prácticas regulatorias, esto garantizará la alineación del sistema con los principios de gestión de riesgos y buen gobierno corporativo.

-

Referencias Bibliográficas

[1] V. Stefanelli, F. Manta, and P. Toma, “Digital financial services and open banking innovation: are banks becoming invisible?” Accessed: Apr. 29, 2025. [Online]. Available: https://arxiv.org/pdf/2210.01109

[2] T. Abbasi and H. Weigand, “The Impact of Digital Financial Services on Firm’s Performance: a Literature Review,” May 2017, [Online]. Available: http://arxiv.org/abs/1705.10294

[3] A. M. Ocampo Alvarado, “Efectos de la transformación digital en el sector contable y financiero en Ecuador,” *ACADEMO Revista de Investigación en Ciencias Sociales y Humanidades*, vol. 11, no. 3, pp. 233–241, Aug. 2024, doi: 10.30545/academo.2024.set-dic.2.

[4] Dino. Esposito and Andrea. Saltarello, *Microsoft .NET : architecting applications for the enterprise*. Microsoft Press, 2014. Accessed: Apr. 29, 2025. [Online]. Available: https://ptgmedia.pearsoncmg.com/images/9780735685352/samplepages/9780735685352.pdf

[5] J. Luo, J. Xu, O. Aldosari, S. A. Althubiti, and W. Deebani, “Design and Implementation of an Efficient Electronic Bank Management Information System Based Data Warehouse and Data Mining Processing,” *Inf Process Manag*, vol. 59, no. 6, p. 103086, Nov. 2022, doi: 10.1016/J.IPM.2022.103086.

[6] F. L. Gaol, G. D. Nugraha, and T. Matsuo, “Decision as a Service for Transaction Banking Using Service-Oriented Modeling Architecture Methodology,” *IEEE Access*, vol. 11, pp. 41455–41466, 2023, doi: 10.1109/ACCESS.2023.3268284.

[7] S. Ibarra-Fiallos, J. B. Higuera, M. Intriago-Pazmino, J. R. B. Higuera, J. A. S. Montalvo, and J. Cubo, “Effective Filter for Common Injection Attacks in Online Web Applications,” *IEEE Access*, vol. 9, pp. 10378–10391, 2021, doi: 10.1109/ACCESS.2021.3050566.

[8] M. Aljabri *et al.*, *Testing and Exploiting Tools to Improve OWASP Top Ten Security Vulnerabilities Detection*. IEEE, 2022. doi: 10.1109/cicn.2022.137.

[9] D. Kellezi, C. Boegelund, and W. Meng, “Securing Open Banking with Model-View-Controller Architecture and OWASP,” *Wirel Commun Mob Comput*, vol. 2021, 2021, doi: 10.1155/2021/8028073.

[10] G. Luo, W. Li, and Y. Peng, “Overview of Intelligent Online Banking System Based on HERCULES Architecture,” *IEEE Access*, vol. 8, pp. 107685–107699, 2020, doi: 10.1109/ACCESS.2020.2997079.

[11] A. Kumar and A. Gandhi, “A Study Using OWASP on Secure Open Banking Architecture,” in *2023 3rd International Conference on Advance Computing and Innovative Technologies in Engineering, ICACITE 2023*, Institute of Electrical and Electronics Engineers Inc., 2023, pp. 2062–2067. doi: 10.1109/ICACITE57410.2023.10182656.

[12] G. R. Acosta Palomeque, “RESPONSABILIDAD SOCIAL EMPRESARIAL: INCLUSIÓN FINANCIERA EN EL SISTEMA BANCARIO PRIVADO ECUATORIANO.” Accessed: Jun. 07, 2025. [Online]. Available: https://www.redalyc.org/journal/3579/357959548007/html/

[13] C. Cuesta, M. Ruesta, D. Tuesta, and P. Urbiola, “La transformación digital de la banca,” 2015, Accessed: Jun. 07, 2025. [Online]. Available: https://www.bbvaresearch.com/wp-content/uploads/2015/08/Observatorio_Banca_Digital_vf.pdf

[14] D. Peñarrieta, M. Navia, E. Garcia, and D. Zambrano, “Evaluación de la Seguridad de Certificados Digitales en las Plataformas Financieras de Ecuador,” *Revista Tecnológica - ESPOL*, vol. 36, no. 2, pp. 174–189, Dec. 2024, doi: 10.37815/RTE.V36N2.1222.

[15] M. Campuzano and L. Mendoza, “Análisis en la evolución de los beneficios del E-Banking en el sector financiero en la ciudad de Machala en el periodo 2023”, Accessed: Jun. 07, 2025. [Online]. Available: https://repositorio.utmachala.edu.ec/bitstream/48000/23230/1/Trabajo_Titulacion_3195.pdf

[16] C. Toloba, J. Miguel, and J. Miguel Del Río, “La perspectiva de la digitalización de la banca española: riesgos y oportunidades”, Accessed: Jun. 07, 2025. [Online]. Available: https://www.bde.es/f/webbde/GAP/Secciones/Publicaciones/InformesBoletinesRevistas/RevistaEstabilidadFinanciera/20/mayo/es/Digitalizacion.pdf

[17] C. M. Merchán, B. M. González, and J. M. M. Largacha, “El big data y su impacto en los servicios financieros en Ecuador,” *Revista Científica FIPCAEC (Fomento de la investigación y publicación científico-técnica multidisciplinaria). ISSN : 2588-090X . Polo de Capacitación, Investigación y Publicación (POCAIP)*, vol. 8, no. 3, pp. 3–19, Jul. 2023, doi: 10.23857/fipcaec.v8i3.

[18] J. A. Moncayo Lara, “RESOLUCIÓN Nro. SEPS-IGT-IGS-INSESF-INR-INGINT-INSEPS-009 .” Accessed: Jun. 07, 2025. [Online]. Available: https://www.seps.gob.ec/wp-content/uploads/Resol-SEPS-IGT-IGS-INSESF-INR-INGINT-INSEPS-009-NORMA_DE_CANALES_ELECTRONICOS.pdf

[19] “USO DE CANALES ELECTRÓNICOS PARA ENTIDADES CONTROLADAS POR LA SEPS”, Accessed: Jun. 07, 2025. [Online]. Available: https://www.zonalegal.net/uploads/documento/USO%20DE%20CANALES%20ELECTRONICOS%20PARA%20ENTIDADES%20CONTROLADAS%20POR%20LA%20SEPS.pdf

[20] “Guía del Desarrollador OWASP | Fundamentos de Seguridad | OWASP Foundation.” Accessed: Jun. 07, 2025. [Online]. Available: https://owasp.org/www-project-developer-guide/release-es/fundamentos/fundamentos_seguridad/

[21] C. Fernández, “The OWASP Foundation OWASP Introducción a OWASP,” 2004, Accessed: Jun. 07, 2025. [Online]. Available: https://wiki.owasp.org/images/2/21/Introduccion_a_la_OWASP.pdf

[22] “OWASP Top 10:2021.” Accessed: Jun. 07, 2025. [Online]. Available: https://owasp.org/Top10/es/

[23] A. Technologies, “White paper sobre las 10 principales vulnerabilidades según OWASP,” Oct. 2022, Accessed: Jun. 07, 2025. [Online]. Available: https://www.akamai.com/site/es/documents/white-paper/2022/akamai-how-to-mitigate-the-owasp-top-10-risks.pdf

[24] “Guía del Desarrollador OWASP | OWASP Top Ten | OWASP Foundation.” Accessed: Jun. 07, 2025. [Online]. Available: https://owasp.org/www-project-developer-guide/release-es/fundamentos/owasp_top_ten/

[25] “OWASP Top 10 2021 mitigation options on Google Cloud | Cloud Architecture Center.” Accessed: Jun. 07, 2025. [Online]. Available: https://cloud.google.com/architecture/security/owasp-top-ten-mitigation

[26] C. Romero Romero, Y. Alvarado Salinas, and N. Paladines Enriquez, “Criptografía y seguridad en M-COMMERCE,” *Revista Científica Ciencia y Tecnología*, vol. 17, no. 13, Jan. 2017, doi: 10.47189/RCCT.V17I13.100.

[27] J. C. Mendoza T., “Demostración de cifrado simétrico y asimétrico,” *Ingenius*, no. 3, pp. 46–53, Dec. 2008, doi: 10.17163/INGS.N3.2008.06.

[28] I. Cristhian, R. Romero, I. Yasser, A. Salinas, I. Nixon, and P. Enríquez, “Criptografía y seguridad en M-COMMERCE,” *Revista Científica Ciencia y Tecnología*, vol. 17, no. 13, pp. 75–91, Jan. 2017, doi: 10.47189/RCCT.V17I13.100.

[29] A. J. Reyes Riveros, E. Salinas, and A. C. Mendoza de los Santos, “Modelo de Autentificación de Doble Factor,” *Revista Innovación y Software, ISSN 2708-0935, ISSN-e 2708-0927, Vol. 4, No. 1, 2023 (Ejemplar dedicado a: March - August), págs. 82-95*, vol. 4, no. 1, pp. 82–95, 2023, Accessed: Jun. 08, 2025. [Online]. Available: https://dialnet.unirioja.es/servlet/articulo?codigo=8978689&info=resumen&idioma=ENG

[30] I. V. M. Corona, G. A. S. Manzano, F. A. B. Aguilar, and Y. F. S. Gonzalez, “Seguridad en Sistemas de Autenticación: Análisis de Vulnerabilidades y Estrategias de Mitigación: Importancia y mejores prácticas para proteger la autenticación en línea,” *XIKUA Boletín Científico de la Escuela Superior de Tlahuelilpan*, vol. 11, no. 22, pp. 39–43, Jul. 2023, doi: 10.29057/XIKUA.V11I22.10802.

[31] I. De Transformación, D. Sistema Bancario, and M. C. Mediomundo, “El ecosistema fintech (tecnología financiera) como instrumento de transformación del sistema bancario tradicional en beneficio del cliente,” *Revista Gestión I+D, ISSN-e 2542-3142, Vol. 7, No. 1, 2022, págs. 12-39*, vol. 7, no. 1, pp. 12–39, 2022, Accessed: Jun. 08, 2025. [Online]. Available: https://dialnet.unirioja.es/servlet/articulo?codigo=8255368&info=resumen&idioma=FRE

[32] A. N. Cadavid, J. Daniel Fernández Martínez, and J. Morales Vélez, “Revisión de metodologías ágiles para el desarrollo de software A review of agile methodologies for software development”, Accessed: Jun. 08, 2025. [Online]. Available: https://www.redalyc.org/pdf/4962/496250736004.pdf

[33] K. Schwaber, J. Sutherland, and L. G. Definitiva, “La Guía Scrum,” 2020, Accessed: Jun. 08, 2025. [Online]. Available: https://scrumguides.org/docs/scrumguide/v2020/2020-Scrum-Guide-Spanish-European.pdf

[34] “¿Qué es Scrum? - Azure DevOps | Microsoft Learn.” Accessed: Jun. 08, 2025. [Online]. Available: https://learn.microsoft.com/es-es/devops/plan/what-is-scrum

[35] N. Tymkiw, J. Manuel Bournissen, and M. Cecilia Tumino, “SCRUM como Herramienta Metodológica para el Aprendizaje de la Programación,” *Revista Iberoamericana de Tecnología en Educación y Educación en Tecnología*, no. 26, pp. 81–89, 2020, doi: 10.24215/18509959.26.e9.

[36] C. De la Torre Llorente, U. Zorrilla Castro, M. Á. Ramos Barros, and J. Calvarro Nelson, “Guia Arquitectura N-Capas DDD NET 4 (Borrador Marzo 2010),” 2010, Accessed: Jun. 08, 2025. [Online]. Available: https://download.microsoft.com/download/2/2/1/221AD022-E701-488F-B070-7A0B87DFE789/Guia_Arquitectura_N-Capas_DDD_NET_4_(Borrador_Marzo_2010).pdf

[37] “Arquitecturas de aplicaciones web comunes - .NET | Microsoft Learn.” Accessed: Jun. 08, 2025. [Online]. Available: https://learn.microsoft.com/es-es/dotnet/architecture/modern-web-apps-azure/common-web-application-architectures

[38] S. Domingo, M. Henríquez, H. Vega Huerta, and L. Guerra Grados, “Programación en N capas,” 2010. Accessed: Jun. 08, 2025. [Online]. Available: https://sisbib.unmsm.edu.pe/BibVirtual/Publicaciones/risi/2010_n2/v7n2/a07v7n2.pdf

[39] “Propiedades de ACID en SQL Server.” Accessed: Jun. 10, 2025. [Online]. Available: https://ichi.pro/es/propiedades-de-acid-en-sql-server-236475841317774

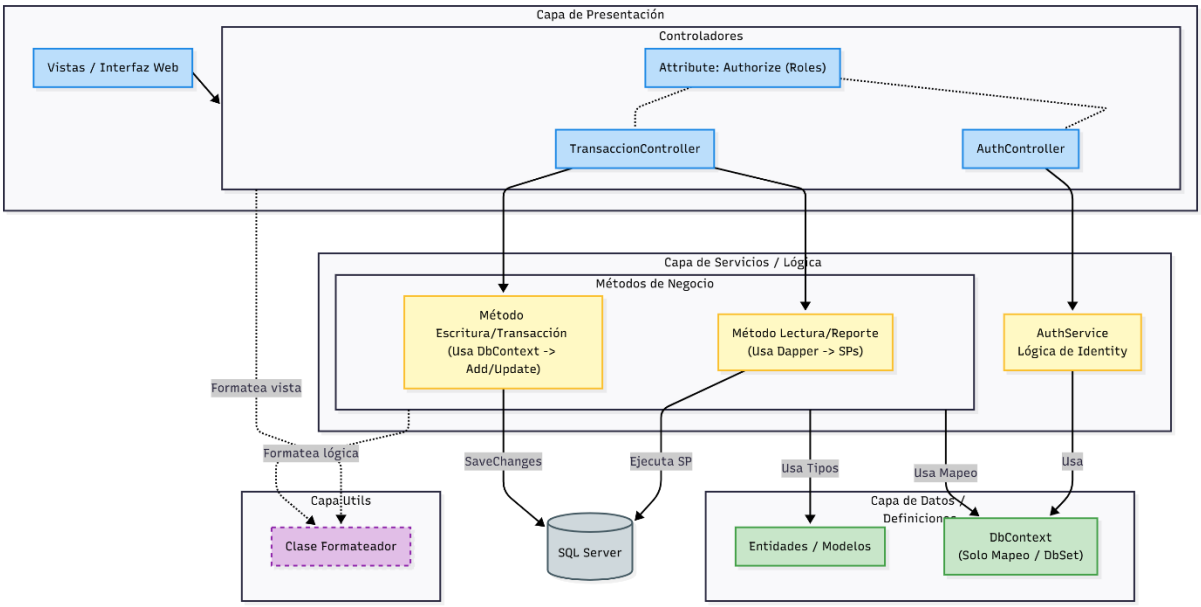
[40] “Prácticas recomendadas de seguridad para SQL Server - SQL Server | Microsoft Learn.” Accessed: Jun. 10, 2025. [Online]. Available: https://learn.microsoft.com/es-es/sql/relational-databases/security/sql-server-security-best-practices?view=sql-server-ver17

[41] “Herramientas de Auditoría de SQL Server por Microsoft y DataSunrise.” Accessed: Jun. 10, 2025. [Online]. Available: https://www.datasunrise.com/es/centro-de-conocimiento/herramientas-de-auditoria-para-microsoft-sql-server/

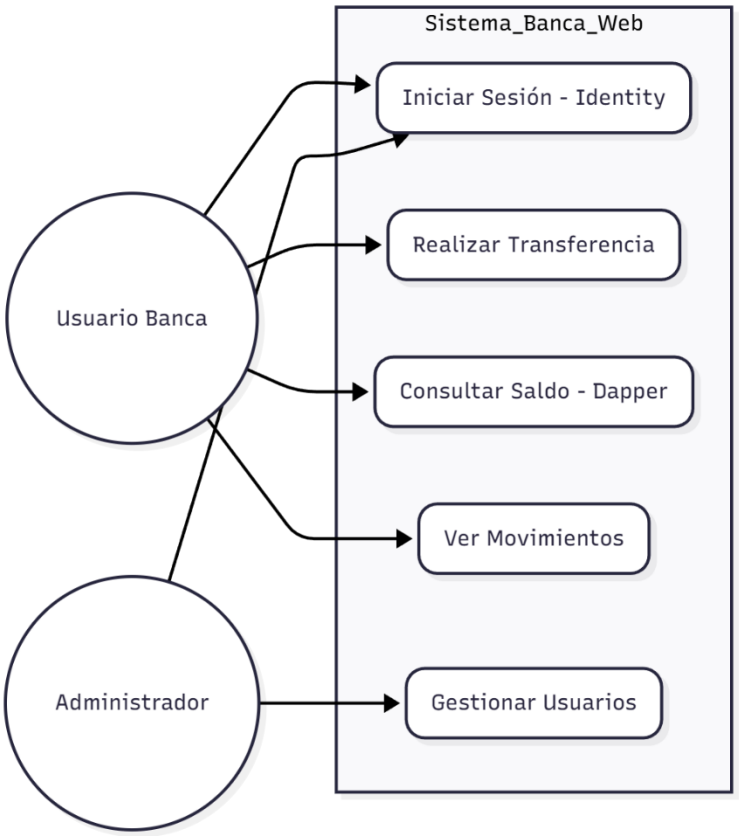
[42] M. Nesha, “Varias técnicas para auditar bases de datos de SQL Server.” Accessed: Jun. 10, 2025. [Online]. Available: https://www.sqlshack.com/es/varias-tecnicas-para-auditar-bases-de-datos-de-sql-server/

[43] “SQL Server Audit (motor de base de datos) - SQL Server | Microsoft Learn.” Accessed: Jun. 10, 2025. [Online]. Available: https://learn.microsoft.com/es-es/sql/relational-databases/security/auditing/sql-server-audit-database-engine?view=sql-server-ver16

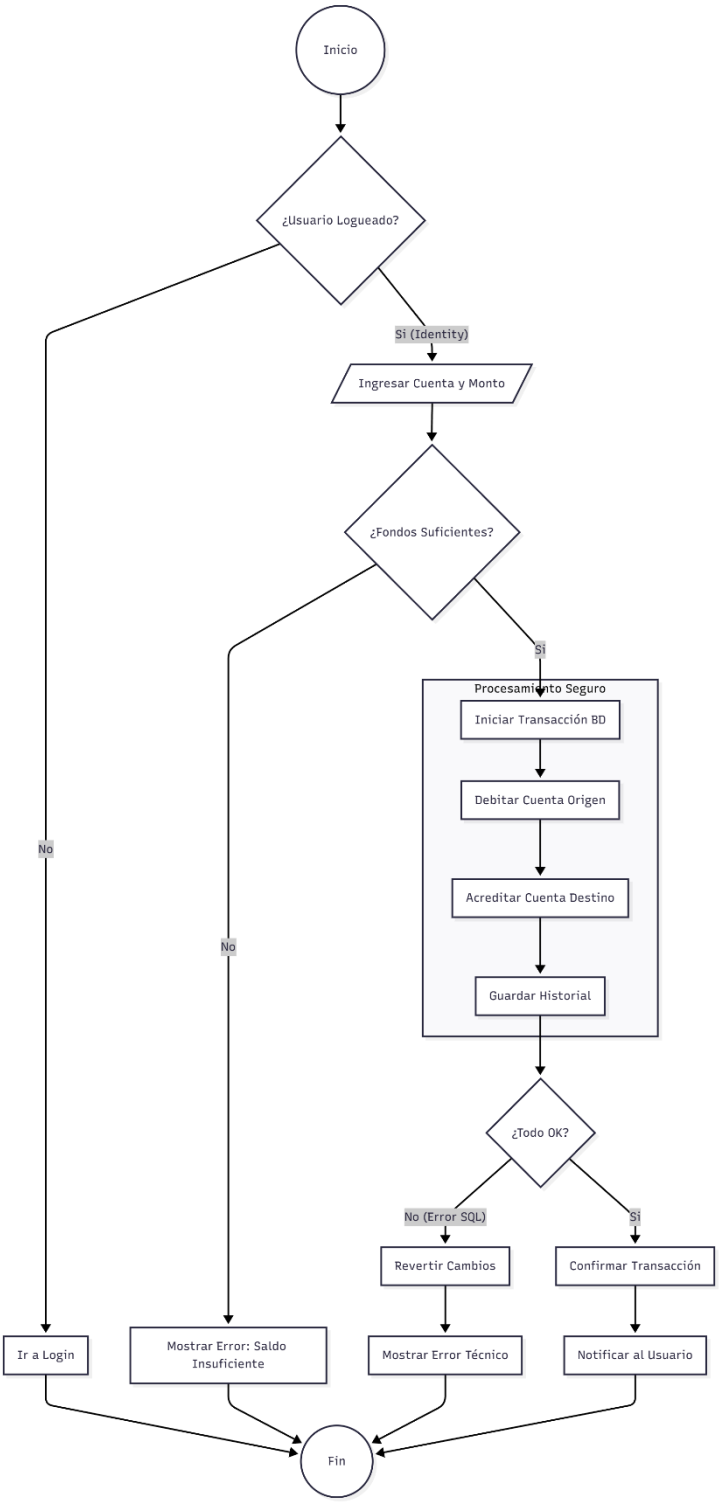
Anexos


Capa de Presentación
Controladores
Vistas / Interfaz Web
Attribute: Authorize (Roles)
TransaccionController
AuthController
Capa de Servicios / Lógica
Métodos de Negocio
Método
Escritura/Transacción
(Usa DbContext ->
Add/Update)
Método Lectura/Reporte
(Usa Dapper -> SPs)
AuthService
Lógica de Identity
Formatea vista
Formatea lógica
SaveChanges
Ejecuta SP
Usa Tipos
Usa Mapeo
Usa
Capa Utils
Clase Formateador
SQL Server
Capa de Datos /
Definiciones
Entidades / Modelos
DbContext
(Solo Mapeo / DbSet)

Anexo 1


Sistema_Banca_Web
Iniciar Sesión - Identity
Realizar Transferencia
Usuario Banca
Consultar Saldo - Dapper
Ver Movimientos
Administrador
Gestionar Usuarios

Anexo 2


Inicio
¿Usuario Logueado?
Si (Identity)
Ingresar Cuenta y Monto
¿Fondos Suficientes?
Si
Procesamiento Seguro
Iniciar Transacción BD
Debitar Cuenta Origen
Acreditar Cuenta Destino
Guardar Historial
¿Todo OK?
No (Error SQL)
Si
Revertir Cambios
Confirmar Transacción
No
No
Ir a Login
Mostrar Error: Saldo Insuficiente
Mostrar Error Técnico
Notificar al Usuario
Fin

Anexo 3