CENTRO UNIVERSITARIO TECNOLÓGICO

CEUTEC

FACULTAD DE INGENIERÍA

PROYECTO DE GRADUACIÓN

SISTEMA DE DETECCIÓN DE TRANSACCIONES ATÍPICAS APOYADO POR INTELIGENCIA ARTIFICIAL.

SUSTENTADO POR:

JHORDY ALEXIS ROSADO FONSECA, 32121058

PREVIA INVESTIDURA AL TITULO DE LICENCIATURA EN INGENIERÍA EN INFORMÁTICA

TEGUCIGALPA **HONDURAS, C.A.**

OCTUBRE, 2025

CENTRO UNIVERSITARIO TECNOLÓGICO

CEUTEC

INGENIERÍA EN INFORMÁTICA

AUTORIDADES UNIVERSITARIAS

RECTOR

MARLON ANTONIO BREVÉ REYES

SECRETARIO GENERAL

ROGER MARTÍNEZ MIRALDA

VICERRECTORA ACADÉMICA CEUTEC

DINA ELIZABETH VENTURA DÍAZ

DIRECTORA ACADÉMICA CEUTEC

IRIS GABRIELA GONZALES ORTEGA

TEGUCIGALPA, M.D.C **HONDURAS, C.A.**

OCTUBRE, 2025

SISTEMA DE DETECCIÓN DE TRANSACCIONES ATIPICAS APOYADO POR INTELIGENCIA ARTIFICIAL.

TRABAJO PRESENTADO EN EL CUMPLIMIENTO DE LOS REQUISITOS EXIGIDOS PARA OPTAR AL TÍTULO DE:

INGENIERÍA EN INFORMÁTICA

ASESOR:

RAFAEL ARMANDO CERRATO CRUZ

TERNA EXAMINADORA:

NIDIA ARELY ROMERO OLIVA

DAVID EDUARDO NAVAS FLORES

TEGUCIGALPA, M.D.C. **HONDURAS, C.A.**

OCTUBRE, 2025

DEDICATORIA

Este proyecto de graduación va dedicado a mis padres, quienes con su amor, sacrificio y enseñanza me motivaron a nunca rendirme y a luchar con perseverancia y esmero por mis metas. Su apoyo incondicional, tanto emocional como económico, fue el pilar fundamental en este proceso.

Jhordy Alexis Rosado Fonseca.

AGRADECIMIENTOS

Agradezco a todas las personas que de una u otra forma me sirvieron de apoyo para poder continuar y culminar mi carrera universitaria con éxito: a mis padres, amigos y compañeros de trabajo. Que me ayudaron incondicionalmente, económica e intelectualmente en momentos claves de mi carrera.

Jhordy Alexis Rosado Fonseca.

RESUMEN EJECUTIVO

El presente proyecto de graduación se enfocó específicamente en el reciente incremento de transacciones de fraude con tarjetas de crédito en instituciones financieras medianas y pequeñas de Honduras. Este fenómeno ha afectado la salud laboral y operativa de los departamentos de riesgo transaccional, al verse sobrecargados por el monitoreo manual de alertas y la falta de herramientas tecnológicas adecuadas para identificar patrones sofisticados de fraude.

La metodología utilizada fue de enfoque mixto, combinando entrevistas cualitativas y encuestas aplicadas a especialistas de riesgo transaccional y oficiales de alerta de dos instituciones financieras representativas. Los resultados obtenidos revelan que, si bien el 100% de los encuestados utilizan herramientas tecnológicas, estas carecen de capacidades avanzadas de detección, lo que limita su capacidad de adaptación ante fraudes emergentes.

Ante este escenario, el proyecto propone el diseño de una herramienta antifraude parametrizable que utilice modelos de inteligencia artificial para detectar transacciones sospechosas en tiempo real. Esta solución está diseñada para ser operada por instituciones con recursos limitados, sin necesidad de contar con equipos especializados en IA. Mejorando de esta manera la productividad del área de riesgo transaccional, la cual se enfoca en mitigar el fraude con tarjetas de crédito en estas instituciones bancarias medianas o pequeñas del país.

Palabras clave: Productividad, salud laboral, herramienta antifraude.

ABSTRACT

This graduation project specifically focused on the recent increase in credit card fraud transactions in medium and small financial institutions in Honduras. This phenomenon has negatively impacted the operational and occupational well-being of transactional risk departments, which are overwhelmed by the manual monitoring of alerts and the lack of adequate technological tools to identify sophisticated fraud patterns.

The methodology used followed a mixed-methods approach, combining qualitative interviews and surveys applied to transactional risk specialists and alert officers from two representative financial institutions. The results revealed that although 100% of the respondents use technological tools, these lack advanced detection capabilities, limiting their ability to adapt to emerging fraud schemes.

In response to this scenario, the project proposes the design of a customizable anti-fraud tool that uses artificial intelligence models to detect suspicious transactions in real time. This solution is designed to be operated by institutions with limited resources, without the need for specialized AI teams. In doing so, it aims to enhance the productivity of transactional risk departments, which are focused on mitigating credit card fraud in these small and medium-sized financial institutions across the country.

Keywords: Productivity, occupational health, anti-fraud tool.

TABLA DE CONTENIDO

I. INTRODUCCIÓN 1
II. PLANTEAMIENTO DEL PROBLEMA 3
2.1 Antecedentes 3
2.2 Enunciado / Definición del Problema 4
2.3 Preguntas de Investigación 5
2.4 Hipótesis y/o Variables de Investigación 6
2.5 Justificación 7
III. OBJETIVOS 8
3.1 Objetivo General 8
3.2 Objetivos Específicos 8
IV. MARCO TEÓRICO 9
V. METODOLOGÍA / proceso 36
5.1 Enfoque y Métodos 36
5.2 Población y Muestra 37
5.2.1 Población 37
5.2.2 Muestra 37
5.3 Unidad de Análisis y Respuesta 38
5.4 Técnicas e Instrumentos Aplicados 40
5.4.1 La Entrevista 40
5.4.2 Encuesta 41
5.5 Fuentes de Información 41
5.5.1 Fuentes Primarias 41
5.5.2 Fuentes Secundarias 42
5.6 Cronología del Trabajo 44
VI. RESULTADOS Y ANÁLISIS 45
6.1 La Entrevista 45
VII. CONCLUSIONES 68
VIII. RECOMENDACIONES 70
IX. APLICABILIDAD 72
9.1 MANUAL TÉCNICO 72

9.1.1 Propósito....72
9.1.2 Alcance....72
9.1.3 Documentos de Referencia....72
9.1.4 Definiciones Importantes....75
9.1.4.1 Conceptos Generales....75
9.1.4.2 Procesos de Entrada y Salida....78
9.1.5 Descripción de Módulos....79
9.1.6 Diccionario de Datos....79
9.1.6.1 Modelo entidad-relación....84
9.1.6.2 Distribución física y lógica de base de datos....85
9.1.6.3 Tablas y vistas....86
9.1.6.4 Triggers....**Error! Bookmark not defined.**
9.1.6.5 Restricciones especiales....92
9.1.6.6 Funciones de usuario, Stored Procedures y paquetes A estos objetos debe especificarse:....94
9.1.6.7 Tareas programadas....113
9.1.7 Políticas de Respaldo....114
9.1.7.1 Archivos....**Error! Bookmark not defined.**
9.1.7.2 Base de datos....114
9.1.8 Descripción de Interfaces con Otros Sistemas....**Error! Bookmark not defined.**
9.1.9 Instalación y Configuración....115
9.1.9.1 Requisitos generales pre-instalación....120
9.1.9.2 Detalles del proceso de instalación....121
9.1.9.3 Detalles de configuración de la aplicación....**Error! Bookmark not defined.**
9.1.9.4 Lista de contactos técnicos....122
9.1.10 Diseño de la Arquitectura Física....123
9.1.11 Procesos de Continuidad y Contingencia....123
9.2 MANUAL DE USUARIO....131
BIBLIOGRAFÍA....174
ANEXOS....180

A.1. Instrumentos Utilizados en la Investigación.....180
A.2. Factibilidad del Proyecto.....188
A.2.1 Técnica.....188
A.2.2 Operativa.....190
A.2.3 Económica.....191
A.3. Lista de Requerimientos del Sistema.....193
A.4. OWASP.....199

ÍNDICE DE TABLAS

Tabla V.1 Encuesta aplicada a la muestra. 38

Tabla 2 Años de experiencia de los encuestados. 45

Tabla 3 Ubicación de la sede principal de la institución. 46

Tabla 4 Cargo desempeñado por el encuestado. 46

Tabla 5 ¿Su institución cuenta actualmente con alguna herramienta tecnológica para la detección de fraudes con tarjetas de crédito? 47

Tabla 6 ¿Esa herramienta dispone de inteligencia artificial para parametrizar sus reglas de monitoreo y detección de fraude? 48

Tabla 7 ¿Con qué frecuencia reciben reportes o reclamos relacionados con fraude en tarjetas de crédito? 49

Tabla 8 ¿Cuáles son los tipos de fraude más comunes que enfrentan en su institución? 50

Tabla 9 ¿Cuáles serían las características más valoradas en una herramienta de detección de fraude en tiempo real para su institución? 51

Tabla 10 ¿Preferiría una herramienta lista para usarse o una que permita ajustes y personalización interna? 52

Tabla 11 ¿Ha considerado su institución alianzas con universidades o terceros para desarrollar soluciones internas de bajo costo? 53

Tabla 12 En su opinión, ¿sería viable desarrollar una herramienta propia si se cuenta con apoyo externo y bajo presupuesto? 54

Tabla 13 ¿Se analizan patrones históricos de transacciones para detectar fraudes o alertas inusuales? 55

Tabla 14 ¿La institución tiene algún proceso para identificar y reducir falsos positivos en sus alertas de fraude? 56

Tabla 15 ¿El personal actual de su área tiene conocimientos sobre inteligencia artificial, análisis de datos o programación? 57

Tabla 16 ¿Cuáles serían las características más valoradas en una herramienta de detección de fraude en tiempo real para su institución? 58

ÍNDICE DE FIGURAS

Ilustración 1. Instituciones Supervisadas por la CNBS - Marzo 2025.....16

Ilustración 2 Posición del Sistema Bancos Comerciales.....18

Ilustración 3 inversión en capacidades de seguridad tecnológica de las instituciones financieras23

Ilustración 4 Medidas planeadas de control de ciberseguridad de las principales tendencias tecnológicas, entre ellas la IA aplicada. 24

Ilustración 5 Necesidad de talento especializado en la aplicación de IA al entorno de trabajo dentro de las instituciones financieras.....25

Ilustración 6 Gestión deficiente en el ciclo de vida de los datos dentro de las instituciones financieras.....26

Ilustración 7 Encuesta realizada por Gartner con respecto al uso de la inteligencia artificial por parte de los consumidores. Muestra un gráfico de barras con las razones por las que usarían esta tecnología. 33

Ilustración 8 Cronograma de trabajo.....44

Ilustración 9 Caso de uso Módulo de Autenticación. 79

Ilustración 10 Caso de uso Módulo de Bitácoras. 80

Ilustración 11 Caso de uso Módulo de Transacciones. 81

Ilustración 12 Caso de uso Módulo de Gestión de Casos. 82

Ilustración 13 Caso de uso Módulo de Gestión de Reglas 83

Ilustración 14 Modelo entidad-relación 84

Ilustración 15 Diseño de la arquitectura física. 123

Ilustración 16 Beneficios de implementación de recomendaciones para contingencia. 130

Ilustración 17 Vulnerabilidad Cabecera Content Security Policy (CSP) no configurada.....199

Ilustración 18 Vulnerabilidad Falta de cabecera Anti-Clickjacking.....200

Ilustración 19 Vulnerabilidad Librería JS Vulnerable 200

Ilustración 20 Vulnerabilidad El servidor filtra información de versión a través del campo "Server" del encabezado de respuesta HTTP 201

Ilustración 21 Falta encabezado X-Content-Type-Options.....201

Ilustración 22 Vulnerabilidad Strict-Transport-Security Header No Establecido.....202

GLOSARIO

A

Algoritmo: Conjunto ordenado y finito de operaciones que permite hallar la solución de un problema (Diccionario de la lengua española., s.f.).

Análisis de Comportamiento: El análisis del comportamiento es un subconjunto del análisis de datos que se centra específicamente en el comportamiento del cliente (What is Behavioral Analytics?, s.f.).

Atípico: Que se aparta de lo habitual (RAE, s.f.).

Análisis Forense: Es una actividad o profesión en la que se utiliza un conjunto de técnicas informáticas para extraer la información de los soportes en los que se ha cometido un delito informático con el fin de encontrar pruebas o evidencias del mismo. (Análisis Forense Ciberseguridad, 2024).

Aprendizaje Supervisado: Es una técnica de machine learning que utiliza conjuntos de datos de entrada y salida etiquetados por humanos para entrenar modelos de inteligencia artificial (¿Qué es el aprendizaje supervisado?, 2024).

C

Carga Computacional: Se refiere al trabajo que un sistema o dispositivo está realizando en un momento dado. Esto puede incluir la demanda en servidores (Carga: ¿qué significa en computación?, s.f.).

Ciberseguridad: Conjunto de elementos, medidas y equipos destinados a controlar la seguridad informática de una entidad o un espacio virtual (Diccionario de la lengua española., s.f.).

D

Deepfake: son archivos de vídeo, imagen o voz manipulados mediante un software de inteligencia artificial de modo que parezcan originales, auténticos y reales (Deepfakes: Qué es, tipos, riesgos y amenazas., s.f.).

Detección en Tiempo Real: es una técnica de vigilancia y control que permite observar y analizar la información que se produce en un sistema en tiempo real, con el objetivo de detectar y corregir posibles fallos o incidencias que puedan afectar a su correcto funcionamiento o al cumplimiento de sus objetivos (Monitoreo en tiempo real, s.f.).

E

Ecosistema Financiero: Se refiere a la red interconectada de varias entidades, sistemas y procesos que contribuyen al funcionamiento de la industria financiera. (Financial Ecosystem, 2023).

F

Falsos Positivos: se refiere a un caso en el que un sistema o algoritmo identifica incorrectamente contenido benigno o aceptable como dañino o inapropiado (False Positive Meaning & Definition., 2024).

Formjacking: es una técnica que consiste en el robo de credenciales bancarias a través de la inserción de código malicioso en las páginas web afectadas. Este ciberataque afecta principalmente a las páginas de comercio online (Sardanyés, s.f.).

H

Herramienta Antifraude: es una solución tecnológica diseñada para detectar y prevenir actividades fraudulentas, especialmente en transacciones electrónicas y plataformas de comercio digital (Sistema Antifraude: comprenda qué es y cómo funciona, 2025).

I

Ingeniería Social: es una técnica de manipulación que aprovecha el error humano para obtener información privada, acceso a sistemas u objetos de valor (¿Qué es la ingeniería social?, 2025).

Indicadores de Fraude: sirven como señales para las organizaciones o el equipo de supervisión del fraude, lo que les permite tomar medidas correctivas para evitar que se produzcan fraudes (¿Qué es un indicador de fraude?, 2025).

Instituciones Financieras: Se les llama así a las entidades cuya actividad principal es prestar servicios financieros a los agentes económicos de una comunidad, es decir a las personas económicamente productivas que requieren un servicio financiero. Sus prestaciones abarcan el área de la banca, valores y seguros (Instituciones financieras | BBVA México , s.f.).

Inteligencia Artificial (IA): es una tecnología que permite a las computadoras y máquinas simular el aprendizaje humano, la comprensión, la resolución de problemas, la toma de decisiones, la creatividad y la autonomía (Stryker, s.f.).

M

Machine Learning (ML): es una rama de la inteligencia artificial (IA) centrada en entrenar a computadoras y máquinas para imitar el modo en que aprenden los humanos, realizar tareas de forma autónoma y mejorar su rendimiento y precisión a través de la experiencia y la exposición a más datos (¿Qué es machine learning?, s.f.).

Modelo Predictivo: es una técnica estadística utilizada para predecir el resultado de eventos futuros basados en datos históricos. Implica la construcción de un modelo matemático que toma variables de entrada relevantes y genera una variable de salida predicha (What is Predictive Modeling? Types & Techniques, s.f.).

P

Parametrización: describir o estudiar algo mediante parámetros (Parametrizar , s.f.).

Phishing: es un tipo de ciberataque que utiliza correos electrónicos, mensajes de texto, llamadas telefónicas o sitios web fraudulentos para engañar a la gente y hacer que comparta datos confidenciales, descargue malware o se exponga a la ciberdelincuencia (¿Qué es el phishing?, s.f.).

Plataforma Digital: es el software y la tecnología que se utilizan para unificar y optimizar las operaciones de negocio y los sistemas de TI. Una plataforma digital funciona como la columna vertebral de una compañía para las operaciones y el engagement del cliente (Plataforma digital , s.f.).

Protección de Datos: se refiere a estrategias y procesos de seguridad que ayudan a proteger datos confidenciales frente a corrupción, vulneración y pérdida. Las amenazas a datos

confidenciales incluyen incidentes de vulneración y pérdida de datos (¿Qué es la protección de datos?, s.f.).

R

Reglas de Monitoreo: son las que forman la base de los sistemas efectivos de monitoreo de transacciones, guiando la identificación y detección de actividades sospechosas dentro de las instituciones financieras (Transaction monitoring – Everything you need to know, s.f.).

Reglas Estáticas: es la forma más básica de regla de fraude y tiende a seguir una lógica simple if/then. Se considera estática cuando el resultado de la regla es estricto e inflexible (Guía para la detección del fraude basada en reglas, s.f.).

Riesgo Transaccional: es el área de defensa esencial para las instituciones financieras, así como tecnologías y procesos que detectan, previenen y responden al fraude (Sistema antifraude: protección clave para el sector financiero en LATAM, s.f.).

S

Skimming: es una forma rápida e interactiva de obtener rápidamente datos de tarjetas de pago e información personal de cajeros automáticos y escáneres de caja. Los dispositivos de vigilancia, los correos electrónicos no solicitados y el código javascript malicioso utilizado en el robo cibernético capturan y transmiten en secreto los datos del titular de la tarjeta en tiempo real sin que la víctima se dé cuenta (What is skimming in cybersecurity? , s.f.).

T

Tarjeta de Crédito: es un instrumento que permite adquirir bienes, servicios y efectuar retiros de dinero en el momento que el titular lo desee, hasta el margen o límite de crédito pre acordado con la empresa emisora de la tarjeta (GEIFG - Educación Financiera, 2023).

Transacciones Digitales: son un proceso de intercambio de datos electrónicos a través de redes informáticas (Transacciones electrónicas: ¿Qué son y por qué son seguras?, 2022).

U

Umbrales Cuantitativos: consisten en cualquier información cuantificable que pueda utilizarse para realizar cálculos matemáticos y análisis estadísticos, de forma que puedan tomarse decisiones en la vida real basadas en estas derivaciones matemáticas (Datos cuantitativos, s.f.).

I. INTRODUCCIÓN

El presente trabajo está enfocado en la actual transformación digital acelerada, las instituciones financieras en el país, sobre todo las más pequeñas, se enfrentan a una creciente amenaza: el fraude con tarjetas de crédito, este fenómeno ha cobrado mayor relevancia debido al incremento de las transacciones digitales, las cuales crecieron más del 15% en los últimos años. Esta tendencia, aunque positiva desde el punto de vista financiero, ha venido acompañada de un aumento de delitos asociados al uso no autorizado de tarjetas de crédito.

Según datos de la Comisión Nacional de Bancos y Seguros (CNBS), en 2023 se reportaron 4,501 reclamos por fraude con tarjetas, reflejando un aumento del 50% respecto al año anterior. Esta realidad plantea serios desafíos para las instituciones del sistema financiero nacional, sobre todo para aquellas clasificadas como medianas o pequeñas, quienes enfrentan limitaciones técnicas, presupuestarias y operativas en la gestión eficaz de estos riesgos.

La presente investigación nació de la necesidad de atender esta problemática desde una perspectiva adaptada a la realidad nacional y se compone de un planteamiento del problema en donde se detalló el contexto específico de la problemática de fraude. Objetivos en donde se describió el objetivo general y los específicos que guiaron el camino de la investigación. Marco teórico en donde se abordó el contexto del fraude con tarjetas de crédito enfocado al panorama nacional. La metodología utilizada en la investigación tuvo un enfoque mixto, también se incluyeron los resultados derivados de la encuesta y entrevista dirigida a colaboradores clave del área de riesgo transaccional en bancos medianos y pequeños de Honduras,

En base a las conclusiones obtenidas en esta investigación se realizaron recomendaciones que constituyen un aporte valioso para el fortalecimiento de las capacidades antifraude en instituciones que, si bien son pequeñas en activos, juegan un papel fundamental en la dinamización de la economía y en el acceso a servicios financieros para miles de hondureños.

II. PLANTEAMIENTO DEL PROBLEMA

2.1 Antecedentes

El crecimiento acelerado de las transacciones digitales, impulsado principalmente por la adopción masiva de servicios financieros electrónicos tras la pandemia, ha incrementado significativamente los riesgos de fraude con tarjetas de crédito en Honduras. De acuerdo con Estrada (2024), el volumen de transacciones digitales en la región crece a una tasa anual del 15%, lo cual crea un entorno favorable para el fraude, especialmente en las instituciones financieras medianas y pequeñas que aún dependen de software básico y limitado para la detección de actividades fraudulentas.

El Reporte de Inclusión Financiera 2024 de la Comisión Nacional de Bancos y Seguros (CNBS) revela que los casos de fraude con tarjetas de crédito aumentaron en un 50% durante el año 2023, con un total de 4,501 reclamos, en comparación con los reportados el año anterior (Comisión Nacional de Bancos y Seguros, 2024). Esta estadística evidencia la urgencia de modernizar los mecanismos de detección de fraude, particularmente en aquellas instituciones que no cuentan con tecnología avanzada para monitorear transacciones en tiempo real.

A nivel internacional, empresas como MasterCard han desarrollado soluciones de vanguardia como Decision Intelligence, un sistema basado en inteligencia artificial (IA) y machine learning (ML) que permite detectar anomalías en tiempo real, identificar patrones complejos y reducir hasta en un 30% los falsos positivos (Decision Intelligence, s.f.). Sin embargo, el alto costo de implementación de estas soluciones representa una barrera significativa para las instituciones

financieras de menor tamaño en Honduras, que operan con presupuestos limitados y recursos tecnológicos reducidos.

En contraste con los sistemas tradicionales que dependen de reglas estáticas y requieren actualizaciones constantes por parte del especialista de riesgo transaccional, las herramientas basadas en IA ofrecen una adaptabilidad superior frente a las tácticas de fraude que evolucionan constantemente, como el phishing o las transacciones inusuales. Esta brecha tecnológica coloca a las instituciones pequeñas y medianas en una clara desventaja frente a los bancos grandes que ya han adoptado soluciones de detección inteligente como las ofrecidas por MasterCard.

Finalmente, en los talleres organizados por la Asociación Hondureña de Instituciones Bancarias (AHIBA) sobre modalidades de fraude recientes, se destacó que muchas instituciones financieras en el país aún enfrentan importantes limitaciones tecnológicas para detectar fraudes sofisticados. Este señalamiento refuerza la premisa de que los bancos medianos y pequeños en ciudades como Tegucigalpa todavía no cuentan con sistemas de detección de fraude de última tecnología, lo que los vuelve más vulnerables ante el creciente panorama de amenazas (Asociación Hondureña de Instituciones Bancarias).

2.2 Enunciado / Definición del Problema

El acelerado crecimiento de las transacciones digitales en Honduras, impulsado por la transformación digital posterior a la pandemia, ha venido acompañado de un aumento preocupante en los casos de fraude con tarjetas de crédito.

Esta situación representa un reto particular para las instituciones financieras, especialmente las de menor tamaño, que podrían estar enfrentando limitaciones en recursos tecnológicos y

humanos para hacer frente a este fenómeno. Si bien algunas entidades pueden contar con mecanismos de prevención, aún no está claro si las herramientas y capacidades actuales son suficientes para responder eficazmente a la creciente sofisticación de los fraudes digitales.

En este contexto, se vuelve necesario investigar cómo están gestionando las instituciones bancarias medianas y pequeñas la prevención del fraude con tarjetas de crédito, qué desafíos enfrentan y qué tipo de soluciones podrían ser viables y sostenibles para fortalecer sus capacidades de detección y respuesta.

2.3 Preguntas de Investigación

2.3.1 Pregunta General

¿Cómo están enfrentando las instituciones financieras medianas y pequeñas de Honduras el creciente problema del fraude con tarjetas de crédito, y cuáles son los principales desafíos que experimentan en sus estrategias de detección y prevención?

2.3.2 Preguntas Especificas

- ¿Cuál es el panorama actual del fraude con tarjetas de crédito en Honduras, y cómo está afectando específicamente a las instituciones financieras de menor escala?
- ¿Qué herramientas, procesos y capacidades están utilizando actualmente los departamentos antifraude de las instituciones bancarias medianas y pequeñas en Honduras para prevenir el fraude con tarjetas de crédito?
- ¿Qué limitaciones económicas, tecnológicas y de talento humano enfrentan estas instituciones en su labor de detección y respuesta ante fraudes?

- ¿Qué grado de efectividad perciben los responsables de prevención de fraude en relación con los métodos y sistemas que utilizan actualmente?
- ¿Qué tipos de datos, indicadores o señales utilizan estas instituciones para identificar actividades sospechosas relacionadas con fraude con tarjetas de crédito?
- ¿Qué conocimientos o perfiles técnicos posee el personal encargado de la prevención de fraude en estas instituciones, y cómo influye esto en su capacidad operativa?
- ¿Qué tipo de requerimientos regulatorios y de protección de datos están obligadas a cumplir este tipo de instituciones al implementar estrategias de prevención de fraude?

2.4 Hipótesis y/o Variables de Investigación

H1. La limitada capacidad económica de las instituciones financieras medianas y pequeñas impide la adopción de sistemas modernos de detección de fraude, lo que incrementa su exposición a fraudes modernos.

H2. La ausencia de personal capacitado en inteligencia artificial y análisis de datos en estas instituciones limita la posibilidad de implementar modelos propios de prevención de fraude.

H3. El uso de software tradicional con reglas predefinidas resulta insuficiente para detectar patrones complejos de fraude, lo que genera una mayor tasa de reclamos por parte de los clientes.

2.5 Justificación

El crecimiento acelerado de las transacciones digitales en Honduras ha venido acompañado de un aumento preocupante en los casos de fraude con tarjetas de crédito, lo que representa un riesgo significativo para la confianza en el sistema financiero. Este fenómeno afecta con mayor intensidad a las instituciones financieras medianas y pequeñas, las cuales enfrentan limitaciones económicas, tecnológicas y de personal especializado.

Ante esta situación, es necesario investigar las causas que hacen a estas instituciones más vulnerables frente al fraude, así como las condiciones que impiden una respuesta eficaz. Comprender estas limitaciones permitirá generar conocimiento útil para proponer soluciones viables, adaptadas a la realidad local y al contexto de transformación digital que atraviesa el país.

Esta investigación es relevante porque permitirá analizar el problema desde una perspectiva técnica y económica, aportando insumos clave para el fortalecimiento de la seguridad en las instituciones financieras que actualmente están en desventaja frente a amenazas cada vez más sofisticadas.

III. OBJETIVOS

3.1 Objetivo General

Desarrollar una propuesta de software de detección de fraude basado en inteligencia artificial (IA), accesible y adaptable, mediante el análisis de las limitaciones tecnológicas, económicas y operativas del departamento antifraude de las instituciones financieras medianas y pequeñas en el país, con el fin de reducir su vulnerabilidad frente al fraude con tarjetas de crédito.

3.2 Objetivos Específicos

- Identificar el panorama actual del fraude con tarjetas de crédito en Honduras, enfocándose en su impacto sobre las instituciones financieras pequeñas del país.
- Identificar las limitaciones tecnológicas, económicas y de talento humano que enfrentan estas instituciones para implementar soluciones avanzadas de detección de fraude como Decision Intelligence.
- Determinar los requerimientos técnicos, operativos y regulatorios necesarios para el desarrollo e implementación de un software de detección de fraude basado en IA, adaptado a entornos con recursos limitados.
- Proponer una alternativa tecnológica viable que permita detectar patrones de fraude en tiempo real, con bajo índice de falsos positivos, y que sea operable por instituciones con baja especialización técnica.

IV. MARCO TEÓRICO

4.1 GENERALIDADES DEL FRAUDE CON TARJETAS DE CRÉDITO

4.1.1 Definición de Fraude con Tarjetas de Crédito

Según el portal Fraud.com, el fraude con tarjetas de crédito ocurre cuando una persona utiliza una tarjeta de crédito o la información de una cuenta sin la autorización del titular. El dinero cargado a una tarjeta de crédito no pertenece directamente al usuario, sino que es prestado por una entidad financiera y debe ser devuelto con intereses. Los delincuentes emplean información robada para realizar compras no autorizadas, lo que genera cargos que recaen sobre el titular legítimo de la tarjeta (Credit card fraud – Ways to detect and prevent it, 2024).

El fraude con tarjetas de crédito también se considera una manifestación del delito más amplio de robo de identidad, en el cual un individuo sustrae y utiliza información personal de otra persona con el fin de obtener beneficios propios.

4.1.2 Principales Tipos de Fraude

4.1.2.1 Fraude con Tarjeta Presente

El fraude con tarjeta presente (en inglés, card-present fraud) se define como un tipo de fraude en el que el delincuente presenta físicamente una tarjeta de crédito robada o falsificada al comerciante para realizar una transacción. A diferencia de otros tipos de fraude con tarjetas de crédito que se ejecutan digitalmente sin la presencia física de la tarjeta, en este caso el acto fraudulento ocurre directamente en el punto de venta (Fernando & Rodriguez , 2024).

Adicionalmente el portal Investopedia identifica las siguientes características del fraude con tarjeta presente:

- Implica el uso físico de una tarjeta robada o falsificada.
- Aunque ha disminuido en frecuencia en los últimos años debido al aumento del fraude en línea, sigue siendo un problema significativo, especialmente en países como Estados Unidos.
- Los delincuentes suelen emplear tácticas como distraer al personal del comercio o realizar compras en momentos estratégicos (por ejemplo, justo al abrir o cerrar el local).
- En algunos casos, se utilizan tarjetas falsificadas con números de cuenta alterados o detalles visuales incorrectos, lo cual puede ser detectado por comerciantes capacitados.

4.1.2.2 Fraude con Tarjeta no Presente

Según Stripe el fraude con tarjeta no presente (por sus siglas en inglés, Card-Not-Present fraud) se refiere a un tipo de fraude que ocurre en transacciones donde no se requiere la presencia física de la tarjeta de crédito. Este tipo de fraude es común en compras realizadas a través de Internet, por teléfono o por correo, en las que el delincuente no necesita tener la tarjeta en su poder (¿Qué es el fraude de tarjeta no presente? | Stripe., 2024).

El portal Stripe también define las características del Fraude con Tarjeta no Presente:

- Este tipo de fraude ocurre principalmente en entornos digitales o remotos, como tiendas en línea, servicios de atención telefónica o pedidos por correspondencia.
- Los ciberdelincuentes utilizan datos de tarjetas robados, obtenidos mediante técnicas como phishing, filtraciones de bases de datos o malware. Les basta con tener el número de tarjeta,

la fecha de vencimiento y, en muchos casos, el código de seguridad (CVV) para completar transacciones fraudulentas.

- Resulta más difícil de detectar que el fraude con tarjeta presente, ya que no hay interacción física ni visual con el titular de la tarjeta. La validación de la transacción se basa en datos que pueden ser más fácilmente comprometidos.

Este tipo de fraude ha ido en aumento con el crecimiento del comercio electrónico y representa uno de los mayores desafíos para la seguridad de las transacciones digitales.

4.1.2.3 Skimming

Según el portal Stripe el skimming es un método de fraude en el que un estafador utiliza un dispositivo llamado skimmer para robar la información de la banda magnética de una tarjeta de crédito. Este dispositivo se conecta a lectores de tarjetas en cajeros automáticos o terminales de punto de venta, como surtidores de gasolina, carriles de autopago u otros puntos de pago. El skimmer captura los datos almacenados en la banda magnética, que posteriormente pueden ser usados para crear tarjetas falsificadas o realizar compras fraudulentas (Guía de prevención de fraude: reconoce y detén las estafas en los pagos | Stripe., 2022).

Además, los delincuentes pueden emplear pequeñas cámaras ocultas o superposiciones en el teclado del cajero o terminal para captar el PIN del usuario, información que se utiliza junto con los datos robados para efectuar transacciones no autorizadas o retiros.

4.1.2.4 Phishing

El phishing es un tipo de ataque de ingeniería social que consiste en engañar a las personas mediante manipulación psicológica para obtener información confidencial. Los estafadores envían correos electrónicos, mensajes de texto o crean sitios web fraudulentos que parecen provenir de fuentes confiables, como bancos o comercios en línea, con el objetivo de que las víctimas revelen datos sensibles, como credenciales de acceso o información de tarjetas de crédito (Guía de prevención de fraude: reconoce y detén las estafas en los pagos | Stripe., 2022).

Estos ataques suelen presentarse en correos que solicitan al usuario hacer clic en enlaces para actualizar información, verificar transacciones o reclamar premios, redirigiéndolo a páginas falsas que solicitan datos personales. También existen variantes como el smishing, que utiliza mensajes de texto, y el pharming, que manipula plataformas de redes sociales para robar datos o instalar malware.

4.1.2.5 Web skimming (Formjacking)

Según el portal Akamai el web skimming, también conocido como formjacking, es un tipo de ciberdelito que consiste en la sustracción de información sensible directamente desde sitios web. Esto se logra mediante la inyección de código malicioso o malware en el código del sitio web, el cual captura los datos que los usuarios ingresan en los formularios de la página, tales como números de tarjetas de crédito, información personal y credenciales de acceso.

Los atacantes aprovechan vulnerabilidades en el software del sitio web, especialmente en plataformas de comercio electrónico que utilizan software desactualizado o con fallas de seguridad. Una vez identificada la vulnerabilidad, insertan código malicioso habitualmente en

JavaScript que se integra con el código legítimo del sitio para evitar ser detectado. Este código malicioso recoge la información ingresada por los usuarios y la envía a servidores controlados por los ciberdelincuentes, quienes pueden utilizarla para realizar fraudes o robo de identidad (Akamai, s.f.).

4.2 PANORAMA DEL FRAUDE FINANCIERO EN HONDURAS

El fraude financiero es un fenómeno global que implica el uso deliberado de engaño para obtener un beneficio económico indebido. Puede manifestarse a través de múltiples formas, incluyendo el uso no autorizado de tarjetas bancarias, suplantación de identidad, phishing, web skimming, entre otros. En el entorno digital moderno, los fraudes financieros han migrado de canales tradicionales a plataformas digitales, aprovechando las vulnerabilidades tecnológicas y la falta de educación financiera entre los usuarios.

4.2.1 Evolución del Fraude Financiero en Honduras

En Honduras, el fenómeno del fraude financiero ha mostrado una tendencia al alza, especialmente a partir del año 2020. De acuerdo con la Comisión Nacional de Bancos y Seguros (CNBS), los reclamos de usuarios financieros han tenido un crecimiento significativo, pasando de 2,286 casos en 2020 a 4,501 en 2023, lo que representa un incremento del 96.9% en apenas tres años. Solo en el año 2023, los reclamos aumentaron un 50% respecto a 2022, según reportes de la Gerencia de Protección al Usuario Financiero (GPUF) (El Heraldo, 2024).

El mayor incremento se produjo en la categoría de phishing, una técnica de fraude basada en la ingeniería social, que creció un 343.8%, al pasar de apenas 61 casos en 2020 a 1,318 en 2023. Este tipo de fraude consiste en engañar al usuario para que entregue sus credenciales bancarias u

otra información confidencial mediante mensajes falsos, enlaces fraudulentos o sitios web que imitan páginas legítimas. Según la CNBS, este aumento se atribuye al uso masivo de canales digitales, la falta de cultura de ciberseguridad entre los usuarios y deficiencias técnicas en las plataformas de las instituciones financieras (El Heraldo, 2024).

4.2.2 Modalidades más Frecuentes de Fraude en el Departamento de Francisco Morazán

Además del phishing, existen otras modalidades comunes de fraude financiero que no solo abarcan la región céntrica, sino que también el país entero:

- Fraude con tarjetas presente: En 2023, esta categoría concentró 1,440 reclamos, lo que representa el mayor volumen entre todos los tipos de reclamos financieros. En comparación con los 1,008 casos de 2020, se evidencia un crecimiento sostenido.
- Web skimming (Formjacking): Aunque menos reportado en medios nacionales, es una amenaza en crecimiento. Esta técnica consiste en la inyección de código malicioso en sitios web de comercio electrónico, que roba datos como números de tarjeta cuando los usuarios completan formularios en línea (Akamai, s.f.). Su éxito se basa en explotar vulnerabilidades en sitios web desactualizados o mal configurados.
- Fraudes por suplantación de identidad: Incluyen la apertura de cuentas bancarias o solicitudes de préstamos a nombre de otra persona.
- Operaciones no reconocidas: Transacciones realizadas sin autorización del usuario, especialmente en canales no presenciales (Internet y apps móviles).

4.2.3 Causas del Crecimiento del Fraude

El crecimiento sostenido del fraude financiero en Honduras puede explicarse por una combinación de factores tecnológicos, sociales e institucionales. Uno de los principales detonantes ha sido la acelerada digitalización de los servicios financieros y del comercio electrónico, un proceso que se intensificó especialmente después de la pandemia del COVID-19. Esta transición obligó a muchos usuarios a utilizar plataformas digitales sin contar con los conocimientos adecuados sobre ciberseguridad, lo que los dejó vulnerables a ataques como el phishing, el uso indebido de tarjetas y el robo de identidad.

Además, existe una baja cultura de ciberseguridad entre los usuarios hondureños. Muchas personas desconocen prácticas básicas de protección digital, como verificar la autenticidad de un sitio web, no compartir contraseñas ni códigos de verificación, y desconfiar de mensajes sospechosos que aparentan provenir de instituciones bancarias. Esta falta de conciencia ha sido aprovechada por los ciberdelincuentes, quienes utilizan técnicas de ingeniería social para engañar a sus víctimas de manera cada vez más sofisticada.

Otro factor determinante ha sido la existencia de debilidades tecnológicas en los sistemas de seguridad de algunas instituciones financieras. A pesar de que muchas han avanzado en la implementación de servicios en línea, no todas han invertido al mismo ritmo en mecanismos robustos de protección como la autenticación multifactorial, la detección temprana de fraudes o el monitoreo en tiempo real de operaciones sospechosas. Esta brecha técnica ha sido explotada por los atacantes para vulnerar cuentas y sistemas bancarios.

Por último, se debe mencionar que la respuesta institucional frente al fraude digital ha sido, en algunos casos, lenta o poco efectiva. Hasta fechas recientes, Honduras carecía de lineamientos regulatorios específicos que obligaran a las entidades financieras a adoptar medidas mínimas de protección frente a estas amenazas. Esta ausencia de regulación clara y obligatoria permitió que durante años las instituciones definieran sus propios criterios de seguridad, lo que resultó en prácticas desiguales y en una protección insuficiente para el usuario financiero (El Heraldo, 2024).

4.3 Lista de Bancos Comerciales Presentes en Honduras

A continuación, se detalla una lista de las instituciones presentes en Francisco Morazán:

No.	Institución	Nombre de Referencia
	Bancos Comerciales	
1	Banco de Honduras, S.A.	HONDURAS
2	Banco Atlántida, S.A.	BANCATLAN
3	Banco de Occidente, S.A.	BANCOCCI
4	Banco Cuscatlán Honduras, S.A.	CUSCATLÁN
5	Banco Financiera Centroamericana, S.A.	FICENSA
6	Banco Hondureño del Café, S.A.	BANHCAFE
7	Banco del País, S.A.	BANPAIS
8	Banco Financiera Comercial Hondureña, S.A.	FICOHSA
9	Banco Lafise (Honduras), Sociedad Anónima	LAFISE
10	Banco Davivienda Honduras, Sociedad Anónima	BANCO DAVIVIENDA
11	Banco Promerica, S.A.	PROMERICA
12	Banco de Desarrollo Rural Honduras, S.A.	BANRURAL
13	Banco Azteca de Honduras, S.A.	AZTECA
14	Banco Popular, S.A.	BANCO POPULAR
15	Banco de América Central Honduras, S. A.	BAC | CREDOMATIC

Ilustración 1. Instituciones Supervisadas por la CNBS - marzo 2025

Fuente: (Comisión Nacional de Bancos y Seguros, 2025)

Con base en el cuadro proporcionado por la Comisión Nacional de Bancos y Seguros (CNBS) al 31 de marzo de 2025, se identifican quince Bancos Comerciales supervisados que operan en Honduras, de los cuales catorce tienen su oficina principal ubicada en el departamento de Francisco Morazán, específicamente en Tegucigalpa. Estos son: Banco de Honduras, S.A. (HONDURAS); Banco Atlántida, S.A. (BANCATLÁN); Banco Cuscatlán Honduras, S.A. (CUSCATLÁN); Banco Financiera Centroamericana, S.A. (FICENSA); Banco Hondureño del Café, S.A. (BANHCAFE); Banco Financiera Comercial Hondureña, S.A. (FICOHSA); Banco Lafise (Honduras), S.A. (LAFISE); Banco Davivienda Honduras, S.A. (BANCO DAVIVIENDA); Banco Promerica, S.A. (PROMERICA); Banco de Desarrollo Rural Honduras, S.A. (BANRURAL); Banco Azteca de Honduras, S.A. (AZTECA); Banco Popular, S.A. (BANCO POPULAR); y Banco de América Central Honduras, S.A. (BAC | CREDOMATIC). Solo el Banco de Occidente, S.A. (con sede en Santa Rosa de Copán) y el Banco del País, S.A. (con sede en San Pedro Sula) tienen su oficina principal fuera de Francisco Morazán.

Esta información permitirá delimitar posteriormente qué bancos podrían considerarse medianos o pequeños con base a los activos totales de cada uno, para seleccionar adecuadamente la muestra y población de estudio.

4.4 Clasificación de Instituciones Financieras en Honduras

Para poder tener una noción clara de cuales de los 15 bancos comerciales presentes en el país son catalogados como medianos o pequeños es necesario utilizar a la Comisión Nacional de Bancos y Seguros (CNBS) como fuente principal de información este es el ente supervisor del sistema financiero hondureño, responsable de regular, autorizar, vigilar y sancionar a las

instituciones que prestan servicios financieros en el país. Entre sus funciones principales se encuentra garantizar la estabilidad, solidez y transparencia del sistema bancario, asegurando que las instituciones cumplen con las leyes, regulaciones y prácticas prudenciales establecidas.

La relevancia de la CNBS en la clasificación de los bancos radica en que esta entidad es la fuente oficial y más confiable de datos sobre los bancos comerciales, tales como el volumen de créditos otorgados, captación de depósitos, número de oficinas, agencias, empleados, así como su cobertura territorial y participación en el mercado. Además, la CNBS consolida la información financiera y de riesgo de cada institución, lo que permite realizar análisis comparativos y clasificaciones objetivas en función del tamaño operativo, solidez financiera y alcance de servicios.

Por esta razón, cualquier clasificación de bancos como la distinción entre grandes, medianos y pequeños debe basarse en los informes y estadísticas que la CNBS publica periódicamente, como el Reporte de Inclusión Financiera y los boletines de desempeño financiero, que ofrecen una visión integral y regulada del sistema bancario hondureño.

	Activos Totales		Cartera Crediticia		Depósitos		Capital y Reservas		Utilidades	
Institución	Saldo	Posición	Saldo	Posición	Saldo	Posición	Saldo	Posición	Saldo	Posición
BANCO FINANCIERA COMERCIAL HONDURENA, S.A.	206,728,647,436.8	1	123,944,857,257.7	2	108,124,206,277.3	3	11,021,136,214.6	4	417,921,526.8	4
BANCO ATLANTIDA, S.A.	203,393,906,801.8	2	139,513,494,366.5	1	143,056,105,231.5	1	15,093,058,231.2	1	337,878,268.6	5
BANCO DE AMERICA CENTRAL HONDURAS, S.A.	176,142,078,240.2	3	105,119,412,915.5	3	107,135,478,840.7	4	13,052,303,481.4	3	638,596,943.8	2
BANCO DE OCCIDENTE, S.A.	174,563,615,740.7	4	92,298,928,392.8	4	116,105,021,437.8	2	13,589,604,542.6	2	1,350,525,953.7	1
BANCO DEL PAIS, S.A.	135,623,341,342.4	5	92,162,449,699.1	5	75,811,146,773.5	5	9,209,791,564.1	5	546,092,868.7	3
BANCO DAVIVIENDA HONDURAS, SOCIEDAD ANONIMA	71,135,521,545.3	6	51,247,858,901.0	6	43,930,798,297.2	6	5,709,308,095.1	6	94,981,791.4	8
BANCO LAFISE, HONDURAS	32,161,084,743.0	7	19,238,910,705.8	7	20,038,640,041.8	7	1,672,315,105.0	8	68,664,897.5	9
BANCO PROMERICA, S.A.	25,124,352,304.7	8	13,900,480,467.0	8	15,472,428,704.9	8	1,349,178,450.2	10	7,308,154.5	12
BANCO DE DESARROLLO RURAL HONDURAS, S.A.	21,841,893,010.7	9	13,606,797,020.2	9	12,524,157,874.0	10	1,189,356,188.7	12	-220,418,700.3	15
BANCO FINANCIERA CENTROAMERICANA, S.A.	19,282,395,758.9	10	12,123,093,419.3	10	9,150,723,532.8	11	1,254,037,768.9	11	40,681,844.0	10
BANCO CUSCATLAN HONDURAS, S.A.	18,014,959,609.8	11	11,788,961,733.8	11	12,657,884,998.7	9	1,458,403,553.4	9	-80,540,137.0	13
BANCO DE HONDURAS, S.A.	10,681,928,065.0	12	1,901,602,008.6	15	6,728,992,986.7	12	1,103,839,186.4	13	211,716,308.8	6
BANCO HONDURENO DEL CAFE, S.A.	8,151,387,180.2	13	3,261,775,130.8	14	4,816,118,554.1	13	818,039,378.0	14	24,323,994.1	11
BANCO AZTECA DE HONDURAS, S.A.	7,291,716,691.5	14	3,697,230,443.5	13	3,783,032,368.8	14	1,981,655,082.6	7	114,015,052.4	7
BANCO POPULAR, S.A.	5,387,274,390.3	15	4,046,778,269.3	12	3,541,233,908.6	15	725,270,248.0	15	-124,817,553.1	14
TOTALES	1,115,524,102,861.4		687,852,630,730.8		682,875,969,828.4		79,227,297,090.3		3,426,931,214.1	

Ilustración 2 Posición del Sistema Bancos Comerciales

Fuente: (Comisión Nacional de Bancos y Seguros, 2025)

4.5 Clasificación de los Bancos según Tamaño Institucional

Con base en el Reporte de posición de sistema Bancos Comerciales de la CNBS, la clasificación de los bancos comerciales por tamaño (grandes, medianos o pequeños) puede fundamentarse en cinco indicadores principales:

1. Activos Totales
2. Cartera Crediticia
3. Depósitos
4. Capital y Reserva
5. Utilidades

Para identificar qué tan grande o pequeño es un banco, y especialmente para detectar cuáles podrían tener dificultades para adquirir herramientas de última tecnología en la gestión de riesgo, el mejor indicador suele ser:

Activos totales: la presente investigación establece una clasificación de las instituciones bancarias en función de sus activos totales, ya que estos constituyen una variable representativa del tamaño operativo y financiero de cada banco. Los activos totales reflejan la capacidad de una entidad para otorgar créditos, captar depósitos, invertir en infraestructura tecnológica, y gestionar el riesgo financiero. Por ende, su uso como criterio clasificatorio tiene un fuerte respaldo técnico y regulatorio.

4.5.1 Fundamento estadístico de la clasificación

La metodología empleada para la clasificación de bancos se basa en el uso de umbrales cuantitativos, definidos por rangos de activos totales. Con base en la información publicada por la Comisión Nacional de Bancos y Seguros (CNBS), se identificó que el sistema bancario hondureño presenta una distribución sesgada a la derecha, en la cual unos pocos bancos concentran la mayor parte de los activos del sistema. Esta dispersión natural de los datos justifica el uso de límites específicos para segmentar a las instituciones.

Los umbrales utilizados son los siguientes:

- **Bancos grandes**: activos totales superiores a L. 30,000,000,000
- **Bancos medianos**: activos entre L. 10,000,000,000 y L. 30,000,000,000
- **Bancos pequeños**: activos menores a L. 10,000,000,000

Estos cortes encuentran sustento en el comportamiento de los datos observados:

- El grupo de bancos con activos mayores a L. 30,000 millones coincide con el percentil 60 de la muestra, concentrando más del 70% del total de activos del sistema.
- El rango entre L. 10,000 y L. 30,000 millones se encuentra dentro del rango intercuartílico (IQR), representando la zona media donde se ubican instituciones de tamaño intermedio.

- Los bancos con activos menores a L. 10,000 millones conforman el grupo con menor participación relativa en el sistema y, generalmente, menor capacidad de inversión tecnológica.

Asimismo, esta metodología es consistente con las prácticas de organismos internacionales como el Fondo Monetario Internacional (FMI) y el Banco Mundial, que agrupan a las instituciones por nivel de activos para evaluar la exposición al riesgo sistémico y definir políticas de supervisión diferenciada.

Según los activos totales obtenemos la siguiente clasificación de bancos comerciales:

4.5.2 Bancos catalogados como grandes

(Activos Totales mayores a L. 30,000,000,000)

- Banco Financiera Comercial Hondureña, S.A.
- Banco Atlántida, S.A.
- Banco de América Central Honduras, S.A.
- Banco del País, S.A.
- Banco Davivienda Honduras, S.A.
- Banco LAFISE, Honduras

4.5.3 Bancos catalogados como medianos

(Activos Totales entre L. 30,000,000,000 y L. 10,000,000,000)

- Banco Promérica, S.A.
- Banco de Desarrollo Rural Honduras, S.A.
- Banco Financiera Centroamericana, S.A.
- Banco Cuscatlán Honduras, S.A.
- Banco de Honduras, S.A. (No ofrece producto de tarjeta de crédito)

4.5.4 Bancos catalogados como pequeños

(Activos Totales menores a L. 10,000,000,000)

- Banco Hondureño del Café, S.A.
- Banco Azteca de Honduras, S.A.
- Banco Popular, S.A.* (No ofrece producto de tarjeta de crédito)

4.6 Limitaciones de las Instituciones Financieras Medianas y Pequeñas

Las instituciones financieras medianas y pequeñas enfrentan una serie de limitaciones que obstaculizan su capacidad para adoptar tecnologías emergentes de forma segura y eficaz, especialmente en un entorno donde los riesgos cibernéticos y fraude con tarjetas de crédito crecen al ritmo de la innovación tecnológica.

Una de las principales restricciones es la capacidad limitada para invertir en tecnologías emergentes y ciberseguridad. Un estudio realizado por McKinsey revela que más del 70 % de las organizaciones encuestadas reconocen que no están invirtiendo lo suficiente en capacidades de seguridad tecnológica.

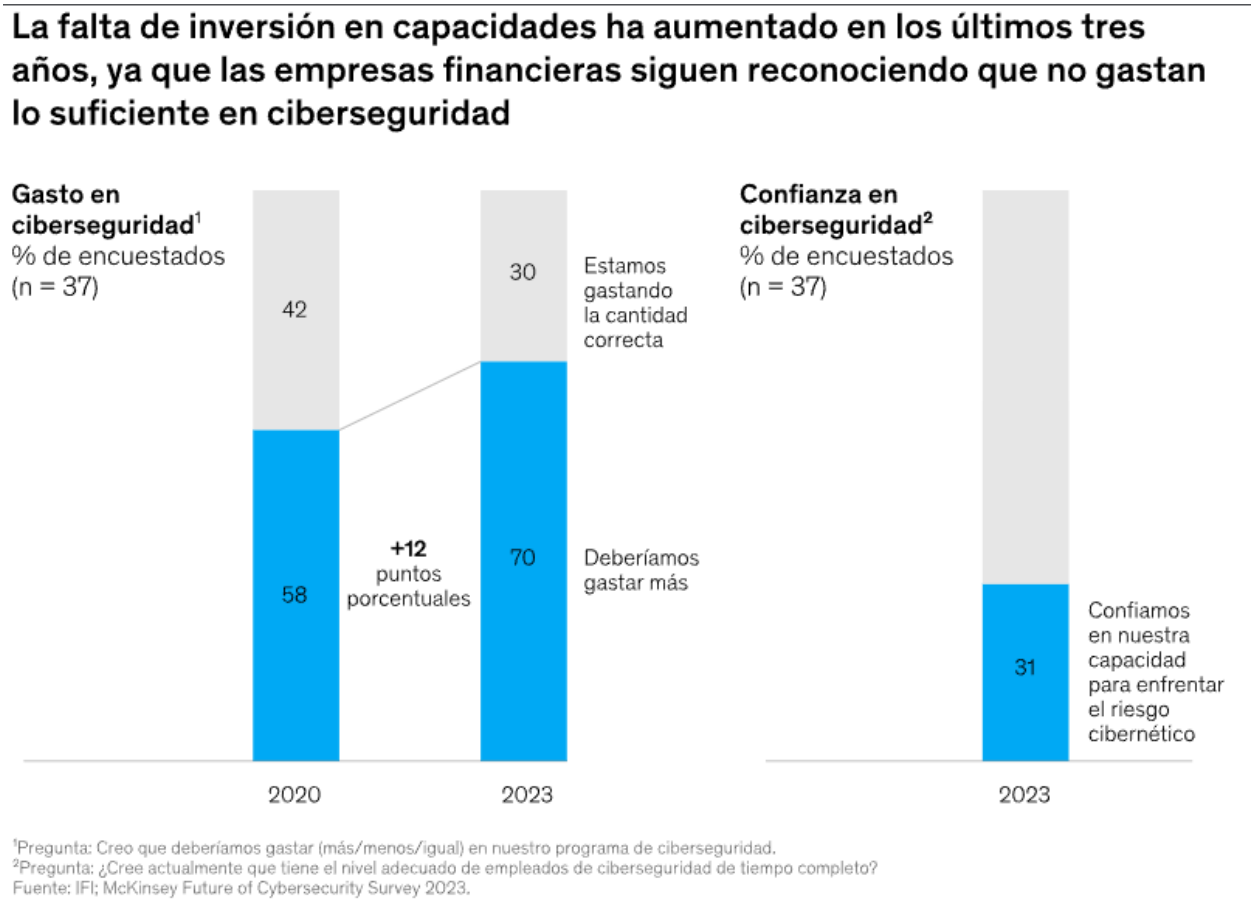


Ilustración 3 inversión en capacidades de seguridad tecnológica de las instituciones financieras

Fuente: (Atkins, y otros, 2024)

Aunque las organizaciones encuestadas comprenden la necesidad de proteger sus entornos digitales, el presupuesto destinado a ciberseguridad apenas representa en promedio el 13 % del total de TI, y esta proporción es aún menor en instituciones con menor volumen de capital (Atkins, y otros, 2024).

Otro punto débil es la falta de métricas e informes sólidos para evaluar y gestionar el riesgo cibernético. Solo el 55 % de las instituciones admiten que carecen de capacidades confiables en el control de la IA aplicada, lo que impide monitorear adecuadamente el desempeño en ciberseguridad y reportar a reguladores o directivos de forma precisa (Atkins, y otros, 2024).

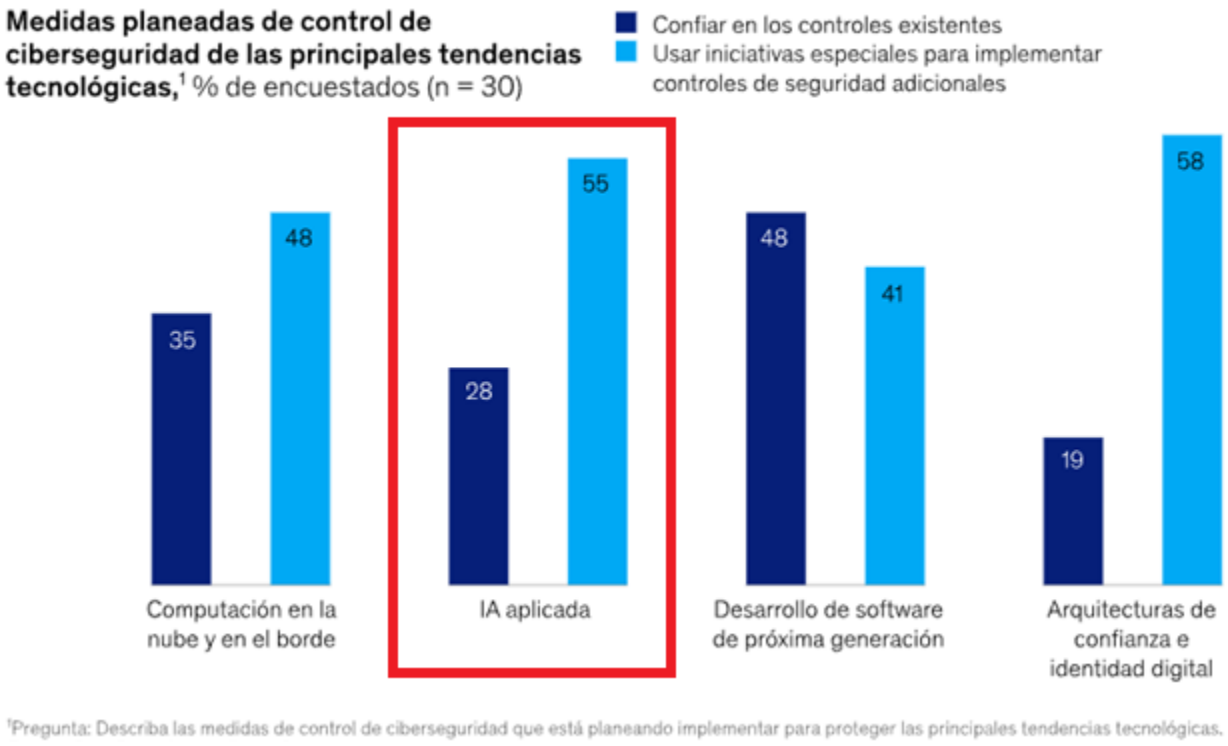


Ilustración 4 Medidas planeadas de control de ciberseguridad de las principales tendencias tecnológicas, entre ellas la IA aplicada.

Fuente: (Atkins, y otros, 2024)

Esta limitación también genera dificultades para anticiparse a incidentes de seguridad y tomar decisiones informadas en materia de inversión y mitigación de riesgos como los existentes en el tema de fraude con tarjetas de crédito.

El déficit de talento especializado en ciberseguridad y tecnologías emergentes también representa un reto estructural. El 71 % de las organizaciones expresó su preocupación por la escasez de profesionales capacitados en la IA aplicada. Este problema es aún más crítico en bancos pequeños o medianos que no pueden competir salarialmente con grandes corporaciones para atraer o retener talento técnico de alto nivel (Atkins, y otros, 2024).

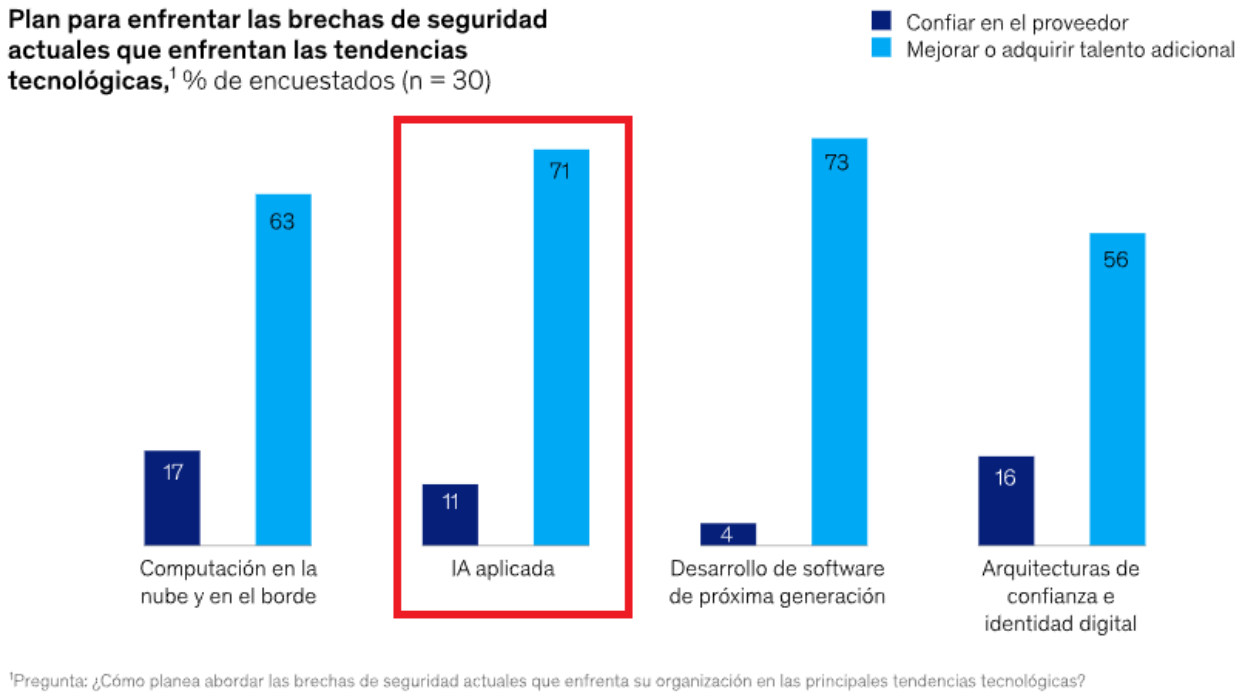


Ilustración 5 Necesidad de talento especializado en la aplicación de IA al entorno de trabajo dentro de las instituciones financieras.

Fuente: (Atkins, y otros, 2024)

A esto se suma una gestión deficiente del ciclo de vida de los datos, donde un 30 % de los encuestados señala deficiencias. En un contexto donde se trabaja con inteligencia artificial, es fundamental proteger los datos desde su generación hasta su destrucción, garantizando su integridad, privacidad y trazabilidad. Sin estas garantías, las ventajas que ofrece la tecnología no pueden materializarse completamente y, por el contrario, se convierten en fuentes de vulnerabilidad (Atkins, y otros, 2024).

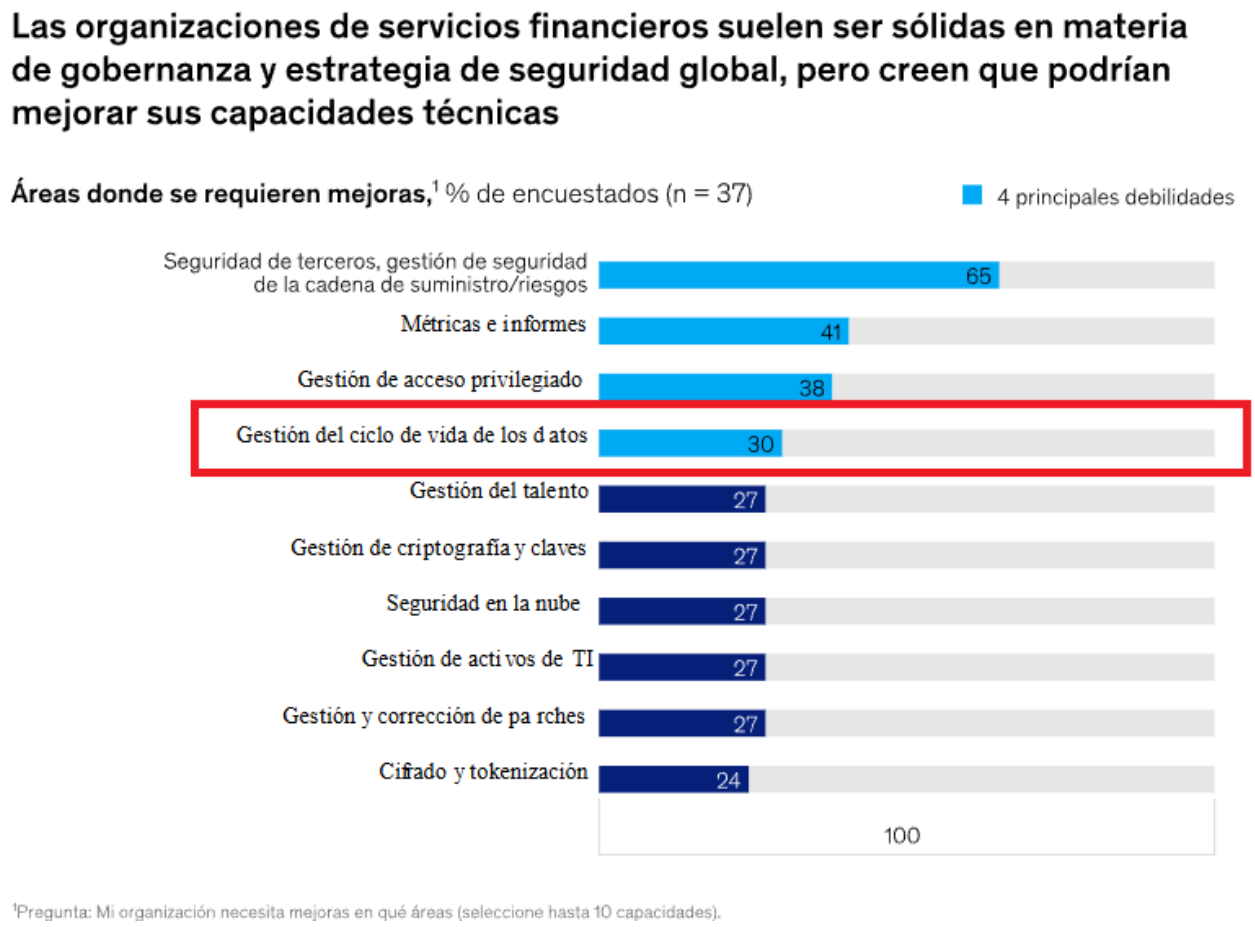


Ilustración 6 Gestión deficiente en el ciclo de vida de los datos dentro de las instituciones financieras.

Fuente: (Atkins, y otros, 2024)

Por último, se observa una brecha entre la velocidad de adopción tecnológica y la madurez de las capacidades de seguridad, lo cual genera tensiones operativas. A pesar del entusiasmo por migrar a la nube o implementar IA, muchas instituciones lo hacen sin haber fortalecido previamente su infraestructura de protección digital. Esto las deja expuestas a configuraciones erróneas, fugas de información, y cumplimiento deficiente de las normativas emergentes, como las relacionadas con el uso responsable de la IA (Atkins, y otros, 2024).

Tomando en consideración lo antes expuesto, las instituciones financieras medianas y pequeñas se enfrentan a una tormenta perfecta: limitaciones presupuestarias, carencias de talento

y la presión creciente por transformarse digitalmente sin contar con capacidades de ciberseguridad robustas. Estas barreras no solo limitan su competitividad, sino que incrementan significativamente su exposición a fraudes, ataques cibernéticos y sanciones regulatorias.

Aunque el estudio de McKinsey fue realizado a instituciones financieras de diversas regiones del mundo, sus hallazgos resultan altamente extrapolables al contexto de Honduras, especialmente en lo que respecta a las instituciones bancarias medianas y pequeñas. Estas entidades comparten características similares con sus pares internacionales, como limitaciones presupuestarias, falta de talento especializado en ciberseguridad, y dificultades para adoptar tecnologías emergentes de forma segura. Por tanto, los desafíos identificados en el estudio reflejan de manera precisa la situación actual del sistema bancario hondureño, donde la transformación digital avanza con rapidez, pero muchas veces sin el acompañamiento de una infraestructura de protección adecuada.

4.7 Avances en Tecnología de Detección de Fraude

En el panorama financiero contemporáneo, la velocidad con la que evolucionan las transacciones digitales obliga a las organizaciones a adoptar herramientas analíticas de última generación que permitan anticipar, detectar y mitigar actividades fraudulentas en tiempo real. A continuación, se desarrolla, de manera integral, el cuerpo conceptual y técnico que describe los avances más relevantes en la materia.

La Inteligencia Artificial (IA) se define, en el contexto de la detección de fraude, como el uso de algoritmos y modelos capaces de aprender de datos históricos para identificar patrones o

anomalías que indiquen posibles ilícitos. Estos sistemas se nutren principalmente de técnicas de machine learning, lo que les permite actualizar sus criterios conforme reciben nueva información, adaptándose a tipologías de fraude emergentes. Entre sus ventajas destacan la capacidad de procesar grandes volúmenes de datos en milisegundos y la rápida identificación de irregularidades que pasarían inadvertidas para los analistas humanos (Fraud.com International, 2023).

Las plataformas modernas de detección de fraudes con IA han superado el enfoque tradicional basado únicamente en reglas predefinidas y revisiones manuales. En su lugar, estas soluciones emplean tecnologías avanzadas como redes neuronales profundas y aprendizaje supervisado para analizar grandes volúmenes de datos de transacciones, huellas digitales de dispositivos, señales de red y comportamiento del usuario. Esto les permite detectar con mayor precisión comportamientos sospechosos que serían difíciles de identificar por analistas humanos o sistemas convencionales. A medida que los fraudes digitales evolucionan en complejidad, los procesos manuales han demostrado ser insuficientes frente a la velocidad y sofisticación de los ataques modernos (Datadome, 2025).

Una característica destacable de estos sistemas es su enfoque en la intención más que en la identidad. Esto implica que ya no basta con diferenciar entre un humano y un bot, sino que se analiza el propósito subyacente de la actividad. Esta orientación permite detectar fraudes que no necesariamente dependen de credenciales robadas, sino de interacciones sospechosas dentro de la plataforma, elevando la eficacia preventiva.

Según el portal Datadome, la detección de fraude basada en IA ha experimentado tres fases de maduración tecnológica:

1. Reglas estáticas y revisiones manuales, propias de los sistemas tradicionales.
2. Aprendizaje automático y análisis del comportamiento, donde se comenzó a identificar patrones adaptativos.
3. Prevención en tiempo real con IA avanzada, que analiza cientos de variables de manera simultánea y aprende de cada intento de fraude detectado para mejorar su capacidad predictiva.

Un avance clave en los últimos años ha sido la IA generativa, la cual representa tanto una amenaza como una solución. Por un lado, los estafadores utilizan modelos generativos para perfeccionar sus ataques: desde correos de phishing indistinguibles de comunicaciones legítimas hasta deepfakes con clonación de voz o rostro para cometer fraudes por suplantación de identidad. Por otro lado, los defensores pueden aprovechar esta misma tecnología para crear modelos de comportamiento de referencia, generar datos sintéticos para entrenar sistemas más robustos o incluso apoyar a los analistas mediante asistentes virtuales impulsados por IA (Datadome, 2025).

Según el portal Datadome entre los beneficios tangibles de la detección de fraudes con IA destacan:

1. **Detección y respuesta en tiempo real**: los sistemas identifican y bloquean actividades fraudulentas en milisegundos, lo que permite actuar antes de que el ataque se concrete.
2. **Escalabilidad**: estas soluciones pueden procesar millones de transacciones diarias sin comprometer el rendimiento, adaptándose al crecimiento del negocio.

3. **Reducción de costos**: al automatizar la detección, se minimiza la necesidad de equipos extensos de revisión manual y se disminuyen pérdidas financieras, cargos por contracargos y daños a la reputación.

4. **Mayor precisión**: los algoritmos de IA reducen drásticamente los falsos positivos, mejorando la experiencia del cliente al evitar bloqueos innecesarios.

5. **Confianza y satisfacción del cliente**: una protección eficaz, pero sin fricción, refuerza la percepción positiva del usuario sobre la seguridad del sistema.

En conclusión, los avances en tecnologías de detección de fraude, encabezados por la inteligencia artificial, han redefinido la forma en que las empresas enfrentan las amenazas digitales. Frente a un panorama de fraudes cada vez más automatizados y sofisticados, el uso estratégico de IA no solo permite adelantarse a las tácticas delictivas, sino que también establece un estándar de eficiencia, precisión y resiliencia para la protección del entorno financiero digital, esto puede representar una ventaja sustancial en instituciones financieras de menor escala quienes pueden ahorrar una parte de su presupuesto destinado en personal especializado y utilizarlo en una gestión semi automática de detección de fraude con tarjetas.

4.8 Beneficios de la Implementación de IA en la Detección de Fraude

La implementación de la inteligencia artificial (IA) en los sistemas de detección de fraude ha traído consigo una transformación significativa en la forma en que las organizaciones previenen y responden a las amenazas digitales. La IA, entendida como la capacidad de las máquinas para aprender y actuar de manera autónoma a partir de grandes volúmenes de datos, no solo automatiza procesos, sino que también mejora su precisión, velocidad y capacidad de adaptación a nuevas

amenazas. Estos beneficios son especialmente relevantes en el ámbito financiero, donde los fraudes evolucionan constantemente y demandan una respuesta rápida y eficaz.

Uno de los beneficios más destacados de la IA en este contexto es la automatización inteligente de procesos que anteriormente requerían intervención humana constante. Gracias al aprendizaje automático y al análisis de comportamiento, los sistemas pueden identificar patrones sospechosos de forma autónoma, reduciendo así el tiempo de respuesta ante un posible intento de fraude y liberando a los analistas para que se concentren en tareas estratégicas. Esta automatización también ayuda a disminuir significativamente los errores humanos, que, en procesos repetitivos como la verificación de datos o validación de transacciones, pueden ser fuente de vulnerabilidades.

La precisión analítica es otra de las fortalezas de la IA. Mediante el procesamiento simultáneo de millones de datos transaccionales, señales de red, comportamientos históricos y huellas digitales de los dispositivos, los algoritmos pueden detectar anomalías mínimas que podrían pasar desapercibidas para los sistemas tradicionales o los analistas humanos. Este nivel de exactitud contribuye no solo a evitar fraudes reales, sino también a reducir los falsos positivos, mejorando la experiencia del cliente al evitar bloqueos innecesarios.

Además, la velocidad en la toma de decisiones representa una ventaja clave. En milisegundos, los sistemas de IA pueden determinar si una transacción representa un riesgo, lo que es crucial en entornos digitales donde una demora mínima puede significar una pérdida millonaria. Esta capacidad de análisis inmediato no solo frena los intentos de fraude, sino que permite diseñar estrategias reactivas más efectivas a partir de datos actualizados en tiempo real.

La capacidad de personalización que ofrece la IA también juega un papel relevante en la gestión del riesgo de fraude. Al analizar las conductas y características individuales de cada usuario, estos sistemas pueden adaptar sus respuestas de seguridad y controles según el perfil y comportamiento habitual del cliente. Esto permite, por ejemplo, exigir múltiples factores de autenticación solo cuando una acción parece inusual, evitando incomodidades innecesarias para los usuarios legítimos.

Desde una perspectiva más amplia, la IA contribuye a fortalecer la cultura de seguridad organizacional. Su aplicación en la detección de fraude no solo implica beneficios técnicos, sino que también promueve la adopción de prácticas preventivas en toda la empresa. La posibilidad de anticiparse a las amenazas, detectar brechas y simular ataques permite establecer medidas de seguridad más sólidas y generar confianza tanto interna como externamente.

También se puede destacar que la IA reduce costos operativos de forma significativa. Al automatizar la revisión de alertas y la clasificación de riesgos, disminuye la necesidad de grandes equipos de análisis manual. Asimismo, al prevenir fraudes exitosos, se evitan pérdidas económicas directas, penalizaciones legales y daños reputacionales que, de otra forma, podrían comprometer la continuidad del negocio.

Además, en una encuesta realizada por la consultora Gartner se destaca que el 58% de los colaboradores encuestados están dispuestos a utilizar la IA si esta les ayuda a ahorrar tiempo y dinero.

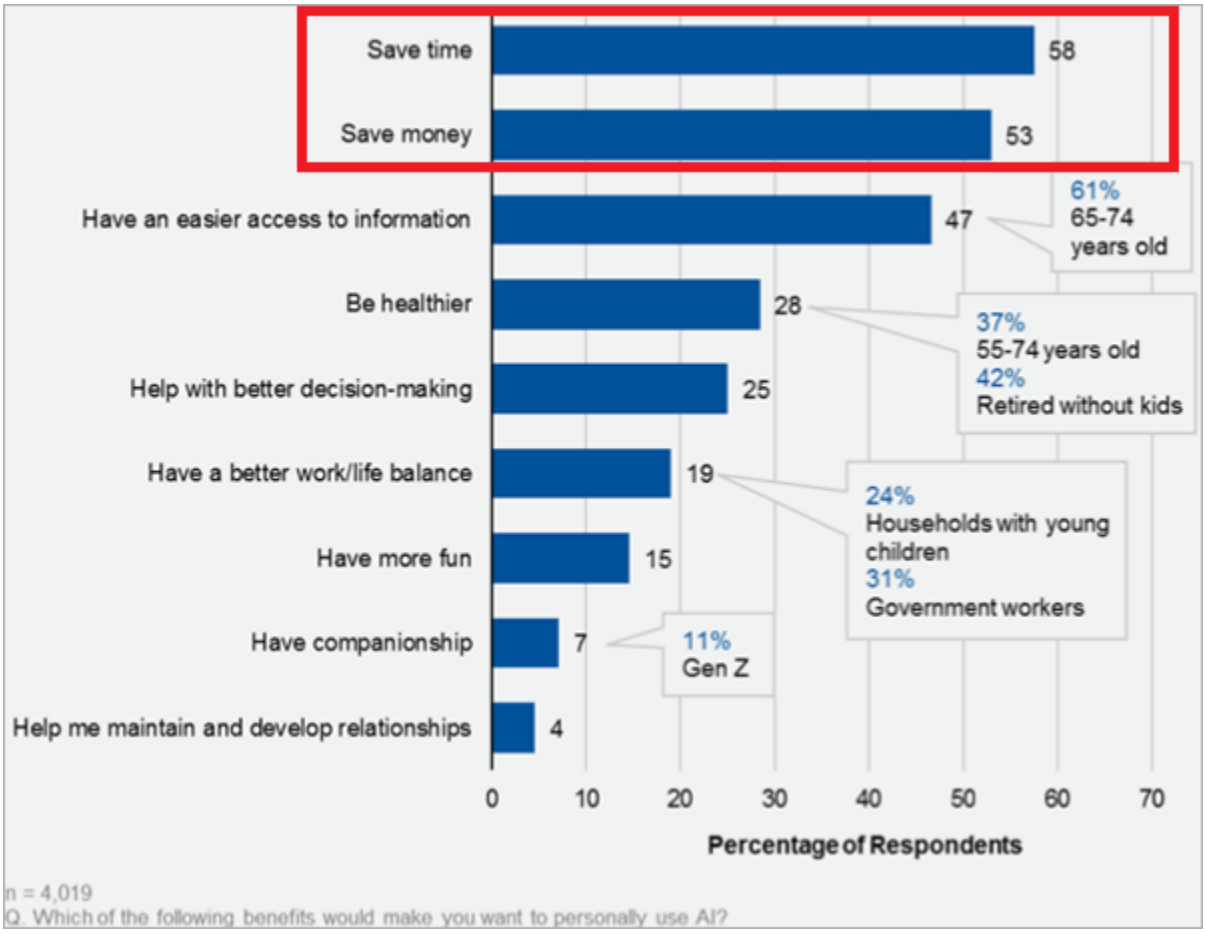


Ilustración 7 Encuesta realizada por Gartner con respecto al uso de la inteligencia artificial por parte de los consumidores. Muestra un gráfico de barras con las razones por las que usarían esta tecnología.

Fuente: (Esmartcity, 2018)

En conclusión, la implementación de la inteligencia artificial en la detección de fraude representa una herramienta de alto valor estratégico para las instituciones. No solo mejora la eficiencia, precisión y velocidad del proceso, sino que también permite escalar la protección sin afectar la experiencia del cliente, fomenta la resiliencia tecnológica, y abre nuevas posibilidades para la innovación y personalización de servicios seguros. Todo ello convierte a la IA no solo en una herramienta tecnológica, sino en un pilar clave para el fortalecimiento de la confianza digital en el entorno financiero moderno (Herrero, Bajuelos, & Lava, 2024).

4.9 Necesidad de Soluciones Adaptadas a Instituciones con Recursos Limitados

En el contexto financiero latinoamericano, y especialmente en economías en vías de desarrollo como Honduras, las instituciones financieras de tamaño mediano y pequeño enfrentan múltiples desafíos para hacer frente al creciente riesgo de fraude electrónico. Si bien las grandes instituciones cuentan con capacidades tecnológicas, presupuestarias y humanas que les permiten implementar soluciones sofisticadas, no ocurre lo mismo con entidades de menor escala que representan un importante porcentaje del ecosistema financiero nacional.

Según un informe de La Organización de los Estados Americanos (OEA) y el Banco Interamericano de Desarrollo (BID), las microfinancieras y cooperativas en la región suelen operar con presupuestos ajustados, dependencias tecnológicas heredadas y bajos niveles de inversión en ciberseguridad. Estas limitaciones estructurales dificultan la adopción de tecnologías emergentes como la inteligencia artificial (IA) aplicada a la detección de fraudes, lo que amplía la brecha de protección frente a actores maliciosos que cada vez emplean técnicas más complejas y automatizadas (Banco Interamericano de Desarrollo, & Organización de los Estados Americanos., 2020).

Según el PwC Global Economic Crime and Fraud Survey 2022, las organizaciones de menor tamaño enfrentan serias limitaciones en cuanto a recursos financieros, capital humano especializado y acceso a tecnologías analíticas avanzadas. Estas condiciones reducen significativamente su capacidad para implementar sistemas de detección proactiva de fraudes, en comparación con grandes empresas que cuentan con unidades de análisis forense robustas y

modelos automatizados de vigilancia. Esta brecha tecnológica no solo incrementa la vulnerabilidad de las organizaciones más pequeñas frente a esquemas de fraude sofisticado, sino que también deteriora la percepción de seguridad entre los usuarios finales. En consecuencia, podría producirse una disminución en la confianza del consumidor y una menor adopción de los canales digitales como plataformas confiables para la gestión de servicios financieros (Global Economic Crime Survey 2024).

Por lo tanto, existe necesidad de soluciones adaptadas a este tipo de organizaciones, no es solamente una necesidad técnica sino estructural. Estas soluciones deben considerar una arquitectura tecnológica ligera, facilidad de integración con sistemas existentes, interfaces intuitivas que no requieran personal altamente especializado, y modelos económicos escalables que permitan su adopción progresiva.

Tomando en cuenta lo anterior expuesto se puede decir que existe una clara demanda por soluciones que no solo ofrezcan eficiencia tecnológica, sino que respondan a las limitaciones estructurales y contextuales de las instituciones financieras pequeñas y medianas. El desarrollo de alternativas que se adapten a estas realidades es clave para cerrar la brecha de ciberseguridad financiera en países como Honduras, y avanzar hacia una inclusión digital segura y sostenible.

V. METODOLOGÍA / PROCESO

5.1 Enfoque y Métodos

5.1.1 Enfoque

Al hacer una investigación mixta se utilizan diversos métodos y fuentes de datos para examinar un mismo fenómeno. La triangulación permite identificar aspectos de un fenómeno con mayor precisión al abordarlo desde distintos puntos de vista (Ortega, 2025).

El enfoque seleccionado para esta investigación fue un enfoque mixto ya que es el que abre una mayor posibilidad de éxito en la recolección de información útil para el análisis y conclusión de la investigación. En el contexto de esta investigación fue necesario recolectar datos cuantitativos como ser: estadísticas de fraude (número de reclamos, tipo de fraude, montos) como también datos cualitativos como ser: experiencias y percepciones sobre la efectividad de los sistemas actuales.

5.1.2 Método

Los diseños no experimentales son usados para describir, diferenciar o examinar asociaciones, en vez de buscar relaciones directas entre variables, grupos o situaciones. No existen tareas aleatorias, grupos control, o manipulación de variables, ya que este modelo utiliza apenas la observación (SousaI, Driessnack, & Costa Mendes, 2007).

El diseño metodológico de esta investigación fue un diseño no experimental porque no se manipularon variables directamente, sino que se observó y analizó un fenómeno ya existente.

5.2 Población y Muestra.

5.2.1 Población

La población se define como el conjunto de todos los casos que concuerdan con ciertas especificaciones. En una investigación, la población representa el universo sobre el que se desea obtener información y realizar inferencias (Sampieri, 2014, pág. 174).

En el presente estudio, la población está conformada por colaboradores de instituciones financieras clasificadas como medianas o pequeñas en Honduras que ofrecen productos de tarjeta de crédito, tengan su sede central en algún municipio de Francisco Morazán y que tienen experiencia directa en el uso o gestión de herramientas de prevención de fraude.

De las quince instituciones financieras registradas en el país, catorce ofrecen al menos un producto de tarjeta de crédito. De estas, seis se categorizan como instituciones medianas o pequeñas. En cada una de estas seis instituciones se identificaron dos puestos clave en el área de Riesgo Transaccional: el Especialista de Riesgo y el Oficial de Alertas, quienes manipulan directamente las herramientas antifraude. Por lo tanto, la población total considerada para este estudio está compuesta por 14 colaboradores (2 por institución).

5.2.2 Muestra

"¿Cómo seleccionar la muestra? La muestra representa un grupo de elementos extraídos de la población que se estudiará. Su correcta selección es clave para la validez de los resultados de la investigación." (Sampieri, 2014, pág. 175).

Para este estudio, se logró obtener acceso a dos de las seis instituciones financieras medianas o pequeñas identificadas, lo cual permitió entrevistar a un total de cuatro colaboradores (dos por institución) pertenecientes a las áreas encargadas de la prevención de fraude transaccional. Esta muestra fue seleccionada de forma intencional, con base en su experiencia directa en la operación de herramientas de detección de fraude con tarjetas de crédito.

5.3 Unidad de Análisis y Respuesta

Tabla V.1 Encuesta aplicada a la muestra.

Unidad de Análisis	Respuesta
¿Su institución cuenta actualmente con alguna herramienta tecnológica para la detección de fraudes con tarjetas de crédito?	Especialista de Riesgo Transaccional
Si su respuesta anterior es sí. ¿Esa herramienta dispone de inteligencia artificial para parametrizar sus reglas de monitoreo y detección de fraude?	Especialista de Riesgo Transaccional
¿Con qué frecuencia reciben reportes o reclamos relacionados con fraude en tarjetas de crédito?	Especialista de Riesgo Transaccional
¿Cuáles son los tipos de fraude más comunes que enfrentan en su institución?	Especialista de Riesgo Transaccional
¿Considera que el número de fraudes ha aumentado, disminuido o se ha mantenido en los últimos años? ¿A qué cree que se debe?	Especialista de Riesgo Transaccional

¿Cuáles son los principales desafíos que enfrenta su institución en relación con la detección o prevención de fraudes?	Especialista de Riesgo Transaccional
¿La institución ha considerado implementar soluciones avanzadas de detección de fraude como las ofrecidas por grandes proveedores (por ejemplo, Decision Intelligence de Mastercard)?	Especialista de Riesgo Transaccional
¿Qué factores limitan la posibilidad de adquirir este tipo de soluciones en su institución?	Especialista de Riesgo Transaccional
En su experiencia, ¿qué funcionalidades considera indispensables en un software de detección de fraude?	Oficial de alertas
¿Cuáles serían las características más valoradas en una herramienta de detección de fraude en tiempo real para su institución?	Oficial de alertas
¿Preferiría una herramienta lista para usarse o una que permita ajustes y personalización interna?	Especialista de Riesgo Transaccional
¿Ha considerado su institución alianzas con universidades o terceros para desarrollar soluciones internas de bajo costo?	Especialista de Riesgo Transaccional
En su opinión, ¿sería viable desarrollar una herramienta propia si se cuenta con apoyo externo y bajo presupuesto?	Especialista de Riesgo Transaccional

¿Qué tipo de datos recopilan actualmente durante las transacciones con tarjeta de crédito?	Especialista de Riesgo Transaccional
¿Se analizan patrones históricos de transacciones para detectar fraudes o alertas inusuales?	Especialista de Riesgo Transaccional
¿La institución tiene algún proceso para identificar y reducir falsos positivos en sus alertas de fraude?	Especialista de Riesgo Transaccional
¿El personal actual de su área tiene conocimientos sobre inteligencia artificial, análisis de datos o programación?	Especialista de Riesgo Transaccional
¿Qué requisitos regulatorios en materia de seguridad de la información debe cumplir su institución al tratar con datos de tarjetas de crédito?	Especialista de Riesgo Transaccional
¿La institución cuenta con políticas específicas para la protección de datos personales de los clientes?	Especialista de Riesgo Transaccional

Encuesta aplicada a la muestra de estudio.

Fuente: Elaboración propia

5.4 Técnicas e Instrumentos Aplicados

5.4.1 La Entrevista

Según la Universidad Europea la entrevista es un método de recolección de datos y tiene un carácter cualitativo, ya que se centra en la experiencia personal de la parte entrevistada. y se utilizó el método de entrevista asistida, que, según la misma fuente, el entrevistado responde a una

serie de preguntas de manera digital por computadora u otro medio electrónico. Suele ser un tipo de entrevista rápida y directa (Universidad Europea, 2023).

En esta investigación dado el enfoque exploratorio que se definió, fue importante recabar información cualitativa que los colaboradores que manipulan el software de alertar antifraude pudieron brindar, esto ayudó a identificar puntos de mejora a la vez de identificar necesidades presentes.

5.4.2 Encuesta

La encuesta es un método utilizado para recabar información entre la población. Íntimamente relacionado con el enfoque cuantitativo, se utiliza para obtener datos en gran escala de una población determinada. Antes de meternos de lleno al tema, les presentaremos algunas definiciones que son importantes para partir de bases sólidas (Universidad Veracruzana, s.f.).

Esta herramienta permitió estandarizar las respuestas de los colaboradores, facilitando la comparación de datos entre diferentes instituciones y la identificación de patrones comunes en cuanto a limitaciones tecnológicas, uso de software, y nivel de conocimiento en inteligencia artificial.

5.5 Fuentes de Información

5.5.1 Fuentes Primarias

Son todos aquellos usuarios y acompañantes a quienes se les aplicó un instrumento de investigación. En este caso, los datos provienen directamente de la población o una muestra de la misma (E, Soberón, & Acosta E , 2008).

En este caso las fuentes primarias de la investigación fueron:

1. Entrevistas aplicadas a:
    - Especialistas de Riesgo Transaccional
    - Oficiales de Alerta
2. Encuestas aplicadas a:
    - Especialistas de Riesgo Transaccional
    - Oficiales de Alerta
3. Reporte de Inclusión Financiera – CNBS (2024 y 2025)
4. Clasificación de bancos según activos totales – CNBS (2025)
5. Taller organizado por la AHIBA

5.5.2 Fuentes Secundarias

Son las que contienen información primaria, sintetizada y reorganizada. Están especialmente diseñadas para facilitar y maximizar el acceso a las fuentes primarias o a sus contenidos. Parten de datos preelaborados, como pueden ser datos obtenidos de anuarios estadísticos, de Internet, de medios de comunicación, de bases de datos procesadas con otros fines, artículos y documentos relacionados con la enfermedad, libros, tesis, informes oficiales, etc. (E, Soberón, & Acosta E , 2008).

En el contexto de esta investigación las fuentes secundarias fueron:

1. Artículos especializados
    - Fraud.com (2024). Credit card fraud – Ways to detect and prevent it
    - Datadome (2025). Detección de fraude con IA

- Investopedia (2024). Card-present fraud
- Stripe (2022–2024). Fraude con tarjeta no presente, skimming

2. Estudios y reportes
    - McKinsey (2024). Reporte sobre inversión en ciberseguridad financiera
    - PwC (2022–2024). Global Economic Crime and Fraud Survey
    - BID & OEA (2020). Estado de ciberseguridad en Latinoamérica
3. Normativas y organismos nacionales
    - Boletines del Banco Central de Honduras
    - Comisión Nacional de Bancos y Seguros (CNBS)
    - Asociación Hondureña de Instituciones Bancarias (AHIBA)
4. Noticias y medios de comunicación
    - El Heraldo (2024). Incremento de fraudes bancarios y phishing
5. Libros y recursos metodológicos
    - Sampieri, R. (2014). Metodología de la Investigación
    - Sousa, Driessnack & Costa Mendes (2007). Diseños no experimentales
6. Documentos académicos y educativos
    - Universidad Europea (2023). Método de entrevista asistida
    - Universidad Veracruzana. Técnicas de encuesta

5.6 Cronología del Trabajo

Nombre de tarea	Duración	Comienzo	Fin
Formulación de idea de proyecto	3 días	lun 21/4/25	mié 23/4/25
Planteamiento del problema	7 días	jue 24/4/25	vie 2/5/25
Recopilación de información general de fraude y sistemas de detección	9 días	jue 24/4/25	mar 6/5/25
Desarrollo de Objetivos	3 días	mié 7/5/25	vie 9/5/25
Desarrollo de Marco Teórico	18 días	lun 12/5/25	mié 4/6/25
Definicíon de la metodología utilizada	3 días	lun 12/5/25	mié 14/5/25
Contacto con las intituciones bancarias para la muestra	5 días	jue 15/5/25	mié 21/5/25
Aplicación de encuesta y entrevista	4 días	jue 22/5/25	mar 27/5/25
Definición de fuentes de información	1 día	jue 15/5/25	jue 15/5/25
Correcciones sugeridas por el asesor	4 días	jue 5/6/25	mar 10/6/25
Interpretacion de los resultados de la encuesta y entrevista	5 días	mié 11/6/25	mar 17/6/25
Elaboración de conclusiones	2 días	mié 18/6/25	jue 19/6/25
Elaboración de recomendaciones	2 días	vie 20/6/25	lun 23/6/25

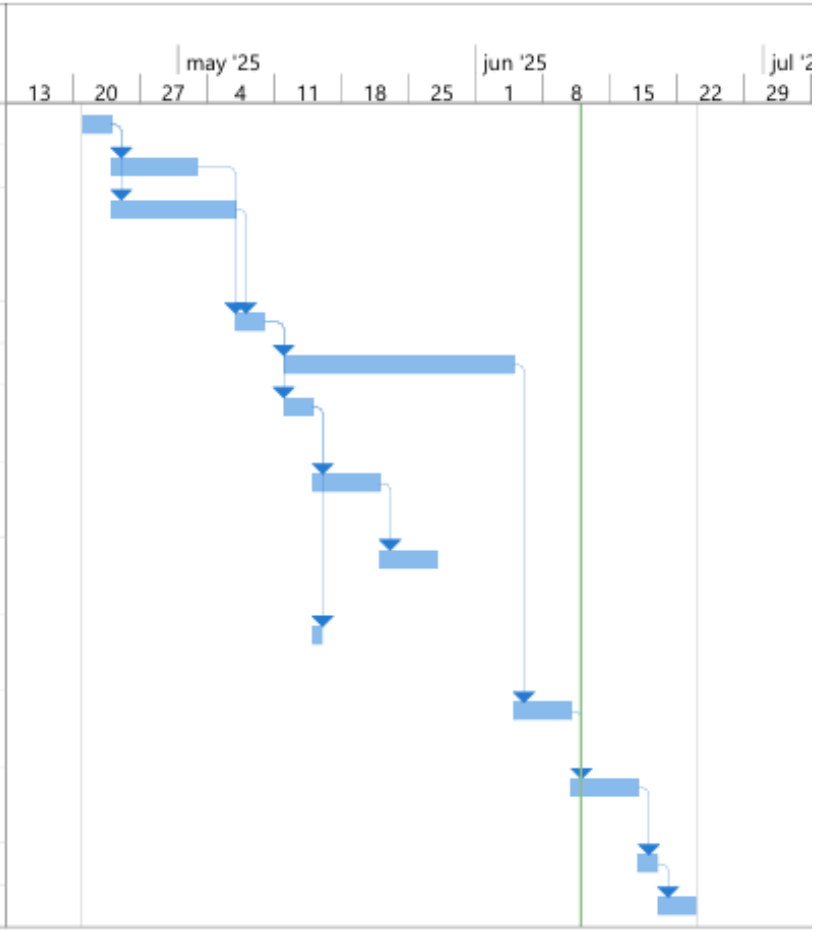


Ilustración 8 Cronograma de trabajo

Fuente: Elaboración propia.

VI. RESULTADOS Y ANÁLISIS

6.1 La Encuesta

6.1.1 Presentación de los resultados de la encuesta

Tabla 2 Años de experiencia de los encuestados.

Descripción	No. de casos	Porcentaje
Menos de 1 año	0	0
1 a 3 años	3	75%
4 a 6 años	1	25%
Más de 6 años	0	0
Total	**4**	**100%**

Fuente: Elaboración propia.

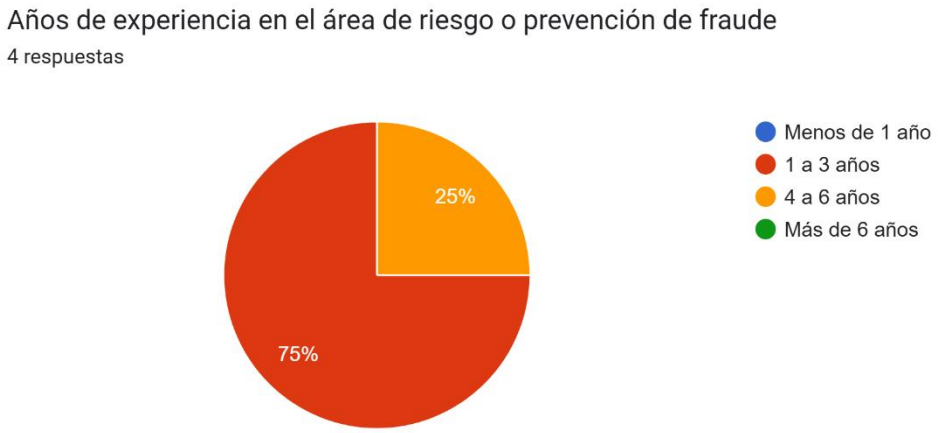


Gráfico 1 Años de experiencia de los encuestados.

Descripción de resultado:

El 75% de los encuestados tiene entre 1 a 3 años de experiencia en el sector de prevención de fraude, mientras que el otro 25% tiene de 4 a 6 años de experiencia, tiempo suficiente para tener un criterio solido sobre las siguientes preguntas de investigación relacionadas con la prevención de fraude con tarjetas de crédito.

Tabla 3 Ubicación de la sede principal de la institución.

Descripción	No. de casos	Porcentaje
Tegucigalpa	4	100%
San Pedro sula	0	0
Total	**4**	**100%**

Fuente: Elaboración propia.

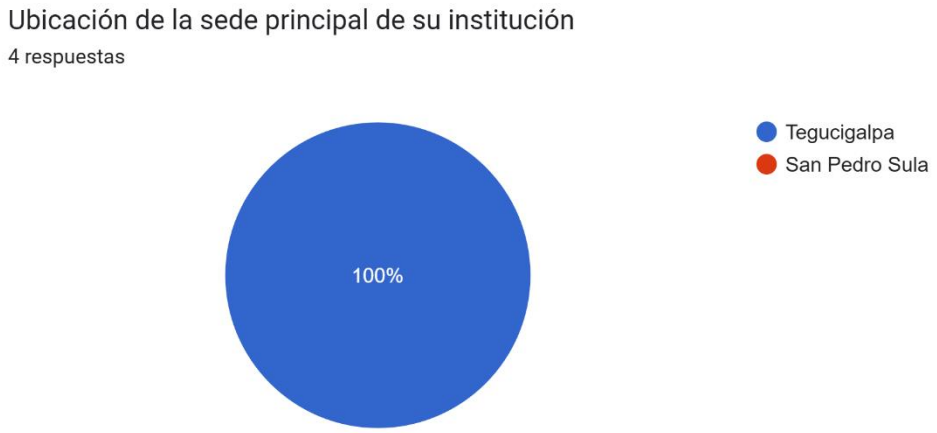


Gráfico 2 Ubicación de la sede principal de la institución

Descripción de resultado:

El 100% de los encuestados laboran en la sede principal de la institución bancaria, la cual en este caso según lo esperado está ubicada en Tegucigalpa, tal como se definió en la muestra.

Tabla 4 Cargo desempeñado por el encuestado.

Descripción	No. de casos	Porcentaje
Especialista en Riesgo Transaccional o equivalente en su institución.	2	50%
Oficial de revisión de Alertas o equivalente en su institución.	2	50%
Total	**4**	**100%**

Fuente: Elaboración propia.

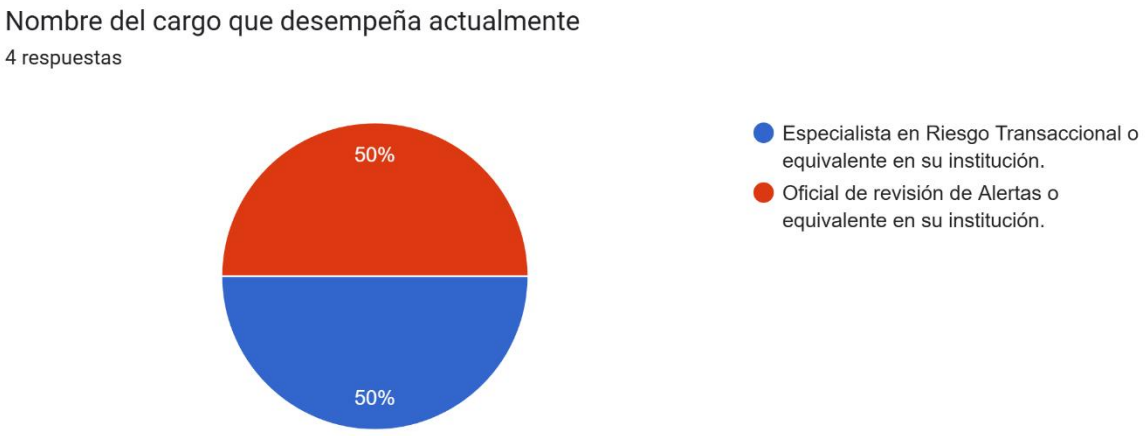


Gráfico 3 Cargo desempeñado por el encuestado.

Descripción de resultado:

Para la muestra se contempló elegir un especialista y un oficial de revisión de alertas por cada institución bancaria, lo que determinó un resultado de 50% por cada cargo desempeñado.

Tabla 5 ¿Su institución cuenta actualmente con alguna herramienta tecnológica para la detección de fraudes con tarjetas de crédito?

Descripción	No. de casos	Porcentaje
Si	2	100%
No	0	0
Total	**2**	**100%**

Fuente: Elaboración propia.

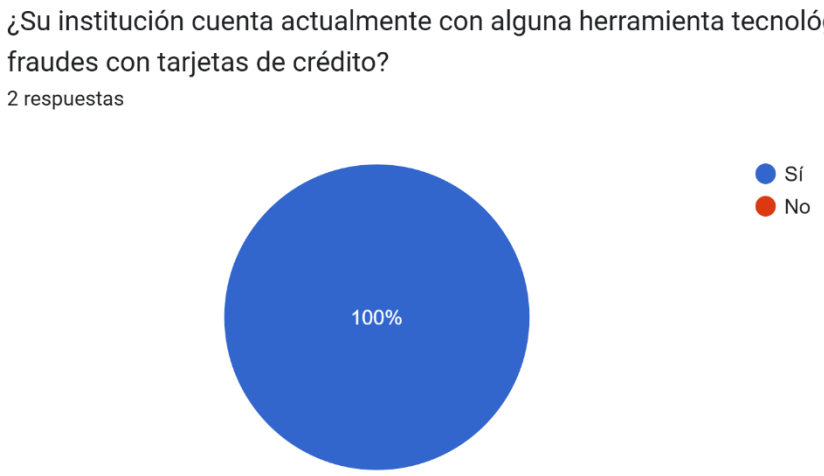


Gráfico 4 ¿Su institución cuenta actualmente con alguna herramienta tecnológica para la detección de fraudes con tarjetas de crédito?

Descripción de resultado:

En este caso la pregunta fue dirigida específicamente para los especialistas de riesgo transaccional por lo que se tiene un total de dos respuestas, de las cuales el 100% de los encuestados indicaron que su institución si cuentan con una herramienta tecnológica que ayude a mitigar el fraude con tarjetas de crédito.

Tabla 6 ¿Esa herramienta dispone de inteligencia artificial para parametrizar sus reglas de monitoreo y detección de fraude?

Descripción	No. de casos	Porcentaje
Si	0	0
No	2	100%
Total	**2**	**100%**

Fuente: Elaboración propia.

Gráfico 5 ¿Esa herramienta dispone de inteligencia artificial para parametrizar sus reglas de monitoreo y detección de fraude?

Descripción de resultado:

En este caso la pregunta fue dirigida específicamente para los especialistas de riesgo transaccional por lo que se tiene un total de dos respuestas, de las cuales el 100% de los encuestados indicaron que la herramienta que utilizan para mitigar el fraude no dispone de ayuda adicional proporcionada por inteligencia artificial en la gestión y parametrización de las reglas de monitoreo y detección de fraude.

Tabla 7 ¿Con qué frecuencia reciben reportes o reclamos relacionados con fraude en tarjetas de crédito?

Descripción	No. de casos	Porcentaje
Diariamente	2	100%
Semanalmente	0	0
Mensualmente	0	0
Total	**2**	**100%**

Fuente: Elaboración propia.

Gráfico 6 ¿Con qué frecuencia reciben reportes o reclamos relacionados con fraude en tarjetas de crédito?

Descripción de resultado:

En este caso la pregunta fue dirigida específicamente para los especialistas de riesgo transaccional por lo que se tiene un total de dos respuestas, de las cuales el 100% de los encuestados indicaron que reciben diariamente reportes o reclamos de fraude realizado con tarjetas de crédito, lo que indica una alta incidencia y que los controles o herramientas implementadas pueden no ser suficientes en la mitigación del fraude.

Tabla 8 ¿Cuáles son los tipos de fraude más comunes que enfrentan en su institución?

Descripción	No. de casos	Porcentaje
Fraude con Tarjeta Presente	0	0
Fraude con Tarjeta no Presente	2	100%
Skimming	0	0
Total	**2**	**100%**

Fuente: Elaboración propia.

Gráfico 7 ¿Cuáles son los tipos de fraude más comunes que enfrentan en su institución?

Descripción de resultado:

En este caso la pregunta fue dirigida específicamente para los especialistas de riesgo transaccional por lo que se tiene un total de dos respuestas, de las cuales el 100% de los encuestados indicaron que el tipo de fraude más común al que se enfrentan es el fraude con tarjeta no presente (transacciones en comercio electrónico), este tipo de fraude tiene la particularidad de que su tendencia es variable por lo que las reglas estáticas son poco efectivas y que la inteligencia artificial puede desempeñar un mejor papel en la detección de esta tipología de fraude con tarjeta de crédito.

Tabla 9 ¿Cuáles serían las características más valoradas en una herramienta de detección de fraude en tiempo real para su institución?

Descripción	No. de casos	Porcentaje
Parametrización apoyada por Inteligencia Artificial	2	50%
Reportes en base a gráficos	1	25%
Bloqueos automáticos de tarjeta con sospecha de fraude	0	0
Facilidad de uso	1	25%
Total	**4**	**100%**

Fuente: Elaboración propia.

Gráfico 8 ¿Cuáles serían las características más valoradas en una herramienta de detección de fraude en tiempo real para su institución?

Descripción de resultado:

En este caso la pregunta fue dirigida específicamente para los especialistas de riesgo transaccional por lo que se tiene un total de dos respuestas, de las cuales el 100 % indicó que quisieran tener la característica de parametrización apoyada por inteligencia artificial, también se obtuvo una división del 50% entre las características de reportes en base a gráficos y facilidad de uso. Lo que demuestra una necesidad de una herramienta fácil de utilizar y con funciones adicionales que ayuden a detectar mejor el fraude, como es el caso de la parametrización en base a IA.

Tabla 10 ¿Preferiría una herramienta lista para usarse o una que permita ajustes y personalización interna?

Descripción	No. de casos	Porcentaje
Lista para usarse	0	0
Que permita ajustes y personalización	2	100%

interna		
Total	**2**	**100%**

Fuente: Elaboración propia.

Gráfico 9 ¿Preferiría una herramienta lista para usarse o una que permita ajustes y personalización interna?

Descripción de resultado:

En este caso la pregunta fue dirigida específicamente para los especialistas de riesgo transaccional por lo que se tiene un total de dos respuestas, de las cuales el 100 % indicó que prefieren utilizar una herramienta que permita ajustes y personalización interna antes que una herramienta lista para usarse. Lo que sugiere que los especialistas en riesgo transaccional desean un apoyo adicional en base a inteligencia artificial sin embargo no desean perder el control total de la herramienta lo que sugiere la implementación de una herramienta con parametrización mixta, tanto manual como apoyada con IA.

Tabla 11 ¿Ha considerado su institución alianzas con universidades o terceros para desarrollar soluciones internas de bajo costo?

Descripción	No. de casos	Porcentaje
Si	0	0
No	2	100%
Total	**2**	**100%**

Fuente: Elaboración propia.

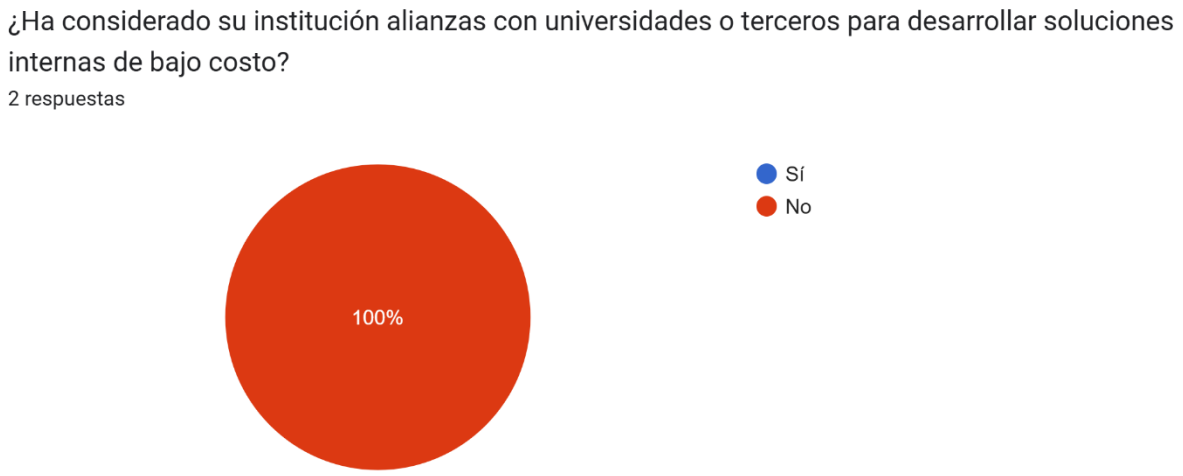


Gráfico 10 ¿Ha considerado su institución alianzas con universidades o terceros para desarrollar soluciones internas de bajo costo?

Descripción de resultado:

En este caso la pregunta fue dirigida específicamente para los especialistas de riesgo transaccional por lo que se tiene un total de dos respuestas, de las cuales el 100 % indicó que no han considerado el desarrollo de una herramienta con el apoyo de alguna universidad u otro ente que ofrezca un producto con un presupuesto y capacidad técnica al alcance de su institución.

Tabla 12 En su opinión, ¿sería viable desarrollar una herramienta propia si se cuenta con apoyo externo y bajo presupuesto?

Descripción	No. de casos	Porcentaje
Si	2	100%
No	0	0
Total	**2**	**100%**

Fuente: Elaboración propia.

Gráfico 11 En su opinión, ¿sería viable desarrollar una herramienta propia si se cuenta con apoyo externo y bajo presupuesto?

Descripción de resultado:

En este caso la pregunta fue dirigida específicamente para los especialistas de riesgo transaccional por lo que se tiene un total de dos respuestas, de las cuales el 100 % indicó que si creen que es viable el desarrollo de una herramienta propia y adaptada a las necesidades de la institución en caso de contar con un apoyo adicional que les ofrezca una herramienta a bajo costo.

Tabla 13 ¿Se analizan patrones históricos de transacciones para detectar fraudes o alertas inusuales?

Descripción	**No. de casos**	**Porcentaje**
Si	2	100%
No	0	0
Total	**2**	**100%**

Fuente: Elaboración propia.

Gráfico 12 ¿Se analizan patrones históricos de transacciones para detectar fraudes o alertas inusuales?

Descripción de resultado:

En este caso la pregunta fue dirigida específicamente para los especialistas de riesgo transaccional por lo que se tiene un total de dos respuestas, de las cuales el 100 % indicó que, si realizan un análisis manual de patrones históricos de transacciones, lo que sugiere que dedican una parte de su tiempo en identificar patrones de fraude, función que con el apoyo de la inteligencia artificial no fuese necesario.

Tabla 14 ¿La institución tiene algún proceso para identificar y reducir falsos positivos en sus alertas de fraude?

Descripción	**No. de casos**	**Porcentaje**
Si	0	0
No	2	100%
Total	**2**	**100%**

Fuente: Elaboración propia.

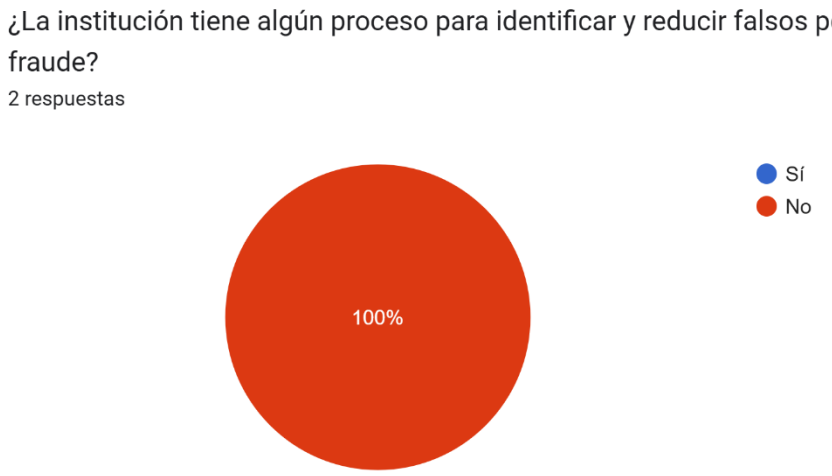


Gráfico 13 ¿La institución tiene algún proceso para identificar y reducir falsos positivos en sus alertas de fraude?

Descripción de resultado:

En este caso la pregunta fue dirigida específicamente para los especialistas de riesgo transaccional por lo que se tiene un total de dos respuestas, de las cuales el 100 % indicó que no tienen ningún proceso para identificar y reducir la cantidad de falsos positivos en las alertas. Lo que sugiere que los oficiales de atención de alertas tienen una alta carga operativa atendiendo alertas que no representan peligro real y que podrían ser reducidas con la implementación de parametrización en base a inteligencia artificial.

Tabla 15 ¿El personal actual de su área tiene conocimientos sobre inteligencia artificial, análisis de datos o programación?

Descripción	No. de casos	Porcentaje
Si	0	0
No	2	100%
Total	**2**	**100%**

Fuente: Elaboración propia.

Gráfico 14 ¿El personal actual de su área tiene conocimientos sobre inteligencia artificial, análisis de datos o programación?

Descripción de resultado:

En este caso la pregunta fue dirigida específicamente para los especialistas de riesgo transaccional por lo que se tiene un total de dos respuestas, de las cuales el 100 % indicó que su personal a cargo no posee conocimientos profundos sobre inteligencia artificial, programación o machine learning (análisis de datos). Lo que sugiere que en caso de implementarse una herramienta adaptada a las necesidades de estas instituciones bancarias debe ser una herramienta intuitiva y sin necesidad de que el usuario final tenga conocimientos profundos sobre IA.

Tabla 16 ¿Cuáles serían las características más valoradas en una herramienta de detección de fraude en tiempo real para su institución?

Descripción	No. de casos	Porcentaje
Facilidad de uso	3	37.5%
Bitácora de acciones tomadas en cada caso de fraude	3	37.5%
Gestión de casos amigable	2	25%
Reporte de casos automático por correo electrónico	0	0

Total	**8**	**100%**

Fuente: Elaboración propia.

Gráfico 15 ¿Cuáles serían las características más valoradas en una herramienta de detección de fraude en tiempo real para su institución?

Descripción de resultado:

En este caso la pregunta fue dirigida a toda la muestra obteniendo un total de cuatro respuestas, de las cuales el 75 % indicó que la característica que más valorarían al implementar una nueva herramienta de detección de fraude es la facilidad de uso, de igual manera el 75% indicó que sería útil implementar una bitácora de acciones tomadas por cada caso de fraude, el 50% indicó que desean una gestión amigable de casos. Esto sugiere que el desarrollo del sistema de detección de fraude basado en inteligencia artificial debe tener una interfaz amigable, de fácil interpretación y no dejar de lado la bitácora de acciones tomadas en cada caso de fraude, por lo que se descarta la implementación de una herramienta avanzada que requiera expertos en desarrollo en base a IA.

6.2 La Entrevista

6.2.1 Resultados de la entrevista aplicada tanto a los especialistas como a los oficiales de riesgo transaccional de cada institución.

A continuación, se desglosa una serie de preguntas abiertas tanto a los tomadores de decisiones que en este caso son los especialistas de riesgo transaccional como a los que utilizan la herramienta de monitoreo que en este caso son los oficiales de atención de alertas (en cada pregunta se especifica a cuál colaborador fue dirigida).

1. **¿Considera que el número de fraudes ha aumentado, disminuido o se ha mantenido en los últimos años? ¿A qué cree que se debe?**

Especialista de Riesgo Transaccional #1:

He observado que el número de fraudes ha aumentado en los últimos años. Esto se ve reflejado en la frecuencia diaria con la que recibimos reportes de clientes afectados. En mi opinión, esto se debe principalmente a que los métodos de fraude han evolucionado más rápido en los últimos años. Usamos sistemas de detección que dependen de reglas estáticas y requieren mucho ajuste manual, lo que no nos permite responder con agilidad ante fraudes nuevos. Además, la falta de conciencia en ciberseguridad por parte de los usuarios hace que muchas veces entreguen sus datos sin darse cuenta, lo que complica la situación.

Especialista de Riesgo Transaccional #2:

He notado que, si ha habido un aumento de casos de fraude con tarjetas en la institución, sobre todo desde el crecimiento del comercio digital. A diario atendemos casos, y muchos tienen que ver con transacciones en línea no autorizadas, que son difíciles de prevenir con las herramientas que actualmente poseemos. Considero que una parte del problema es que las instituciones pequeñas como la nuestra no tienen acceso a tecnologías avanzadas de detección, y eso nos pone en desventaja frente a los ciberdelincuentes. Quizás la alta gerencia no le ha dado la suficiente importancia al tema de inversión en herramientas avanzada,

Conclusión:

Ambos especialistas coincidieron en que el número de fraudes con tarjetas de crédito ha aumentado considerablemente en los últimos años. Se identificó como causa principal la evolución de los métodos de fraude digital (fraude con tarjeta no presente), frente a la incapacidad de las instituciones de actualizar sus herramientas de detección. Este hallazgo evidencia una desventaja tecnológica en las instituciones bancarias medianas y pequeñas, incapaces de responder ágilmente al creciente entorno de amenazas digitales.

2. **¿Cuáles son los principales desafíos que enfrenta su institución en relación con la detección o prevención de fraudes?**

Especialista de Riesgo Transaccional #1:

Uno de los principales desafíos es que nuestra herramienta de monitoreo no se actualiza automáticamente. Cada cambio en las reglas de detección tiene que hacerse manualmente, lo cual toma tiempo y puede generar retrasos críticos. Además, no tenemos un sistema que analice patrones históricos de forma inteligente, por lo que muchas veces dependemos del conocimiento

empírico del equipo para identificar fraudes. Otro desafío es la sobrecarga de alertas que luego del análisis de los oficiales de alertas resultan ser compras legitimas de los clientes, porque no contamos con una solución que ayude a filtrar los falsos positivos de forma eficaz.

Especialista de Riesgo Transaccional #2:

Desde mi perspectiva, el mayor reto es la limitación tecnológica general de la institución. Prácticamente todo lo haceos de una manera manual, no tenemos acceso a una personalización avanzada. También enfrentamos una falta de integración entre sistemas, lo que hace que parte del trabajo se desarrolle de una manera muy lenta, lo que reduce nuestra capacidad de respuesta ante incidentes.

Conclusión:

Las respuestas de los especialistas reflejan una coincidencia en los principales desafíos institucionales: herramientas tecnológicas desactualizadas, procesos manuales y falta de talento humano capacitado en tecnologías emergentes. Estas debilidades se traducen en una carga operativa elevada, un sistema de alertas ineficiente y una alta exposición al riesgo. Se confirma que estas instituciones requieren urgentemente una solución tecnológica adaptada a sus capacidades y contexto operativo.

3. **¿La institución ha considerado implementar soluciones avanzadas de detección de fraude como las ofrecidas por grandes proveedores (por ejemplo, Decision Intelligence de Mastercard)?**

Especialista de Riesgo Transaccional #1:

Sí se ha considerado, al menos en términos generales. Sabemos que existen plataformas como la de Mastercard, que usan inteligencia artificial y tienen una alta capacidad de detección. Sin embargo, el costo de estas herramientas es demasiado alto para nuestra institución, y eso ha frenado cualquier intento serio de adopción.

Especialista de Riesgo Transaccional #2:

Hemos tenido conocimiento de estas herramientas a través de talleres y capacitaciones, pero no ha habido una intención real de adquirirlas porque no se ajustan a nuestro presupuesto ni a nuestra infraestructura tecnológica. Son soluciones más apropiadas para bancos grandes, con equipos de TI amplios y capacidad para implementar integraciones complejas.

Conclusión:

Si bien ambas instituciones conocen y reconocen el valor de herramientas avanzadas como Decision Intelligence de Mastercard, ninguna ha iniciado su implementación debido al alto costo económico y la complejidad técnica. Este hallazgo revela que existe interés, pero no viabilidad práctica de adoptar soluciones comerciales de gran escala, reforzando la necesidad de una herramienta propia, económica y contextualizada.

4. **¿Qué factores limitan la posibilidad de adquirir este tipo de soluciones en su institución?**

Especialista de Riesgo Transaccional #1:

Los factores principales son el presupuesto limitado. Tampoco tenemos la infraestructura tecnológica adecuada, y muchas veces dependemos de proveedores externos para tareas básicas.

Especialista de Riesgo Transaccional #2:

Además del tema económico, creo que un factor importante es la estructura organizativa. La toma de decisiones es lenta y muchas veces se priorizan temas operativos sobre la innovación tecnológica. También nos hace falta conciencia institucional sobre el retorno de inversión que implicaría mejorar nuestras herramientas antifraude.

Conclusión:

Se identificaron factores comunes que limitan la adquisición de soluciones tecnológicas avanzadas: restricciones presupuestarias, falta de personal técnico, incompatibilidad con sistemas actuales y estructuras organizativas conservadoras. Este hallazgo reafirma que las soluciones disponibles en el mercado no se adaptan a las condiciones operativas de estas instituciones, lo que refuerza la viabilidad de desarrollar una herramienta propia con enfoque modular y parametrizable.

5. **En su experiencia, ¿qué funcionalidades considera indispensables en un software de detección de fraude?**

Oficial de atención de alertas #1:

Lo más importante sería contar con parametrización dinámica, porque permitiría que las reglas evolucionen sin intervención constante. También considero clave que tenga una interfaz simple y amigable, ya que no todos tenemos formación técnica avanzada. Por último, me gustaría contar con bitácoras de seguimiento de casos y reportes visuales que faciliten la gestión operativa.

Oficial de atención de alertas #2:

Para mí es vital que la herramienta pueda aprender del comportamiento del cliente y generar alertas en función de cambios en sus hábitos de consumo. También valoro mucho la posibilidad de hacer ajustes internos según las particularidades que se detecten en su momento. Un panel de control con gráficos claros y gestión de alertas por prioridad sería de gran ayuda.

Conclusión:

Ambos oficiales de alertas coincidieron en que una herramienta de detección de fraude debe ofrecer: facilidad de uso, capacidad de aprendizaje del comportamiento del cliente (sugiere implementación de IA), bitácoras de casos y reportes visuales. Este hallazgo demuestra que hay claridad sobre las necesidades funcionales de un sistema antifraude moderno.

6. **¿Qué tipo de datos recopilan actualmente durante las transacciones con tarjeta de crédito?**

Especialista de Riesgo Transaccional #1:

Recopilamos datos básicos como monto, códigos de respuesta, modo de entrada, ubicación y rubro del comercio, fecha y número de tarjeta. Sin embargo, no analizamos estos datos en tiempo real, ni tampoco los usamos para hacer predicciones o detectar anomalías automáticamente. Todo el análisis es posterior al fraude, no preventivo.

Especialista de Riesgo Transaccional #2:

Además de los datos de la transacción en sí, revisamos de forma manual el historial del cliente, pero esto consume mucho tiempo. Actualmente no tenemos herramientas que hagan esto automáticamente. Una IA podría usar estos mismos datos para detectar patrones sospechosos más rápido que nosotros.

Conclusión:

Las instituciones encuestadas recopilan únicamente datos básicos de las transacciones, sin aplicar análisis predictivo ni monitoreo inteligente en tiempo real. Se identificó que existe una infraestructura mínima de datos, pero que esta no está siendo aprovechada para prevenir fraudes de manera anticipada. Esto confirma una oportunidad crítica de mejora mediante herramientas que procesen estos datos con IA.

7. **¿Qué requisitos regulatorios en materia de seguridad de la información debe cumplir su institución al tratar con datos de tarjetas de crédito?**

Especialista de Riesgo Transaccional #1:

Cumplimos con las normativas de la CNBS, especialmente en temas de protección de datos y también ellos especifican en la normativa la manera correcta de realizar la gestión de respuesta a los clientes afectados por algún fraude con tarjetas.

Especialista de Riesgo Transaccional #2:

Manejamos los datos siguiendo políticas internas y por mandato también debemos cumplir con la CNBS.

Conclusión:

Ambas instituciones cumplen con los requisitos regulatorios mínimos exigidos por la CNBS, como el cifrado de datos y políticas de acceso restringido. Normativa que debe ser implementada en el desarrollo del sistema de detección de fraude.

8. **¿La institución cuenta con políticas específicas para la protección de datos personales de los clientes?**

Especialista de Riesgo Transaccional #1:

Sí, tenemos una política de protección de datos, firmada por todos los colaboradores, y protocolos de acceso restringido. A nivel de sistemas también se cuenta con una serie de políticas que aseguran el manejo correcto de la información almacenada en dichos sistemas.

Especialista de Riesgo Transaccional #2:

Si contamos con políticas internas que están enfocadas en el manejo correcto de la información almacenada en los servidores o cualquier otro medio de la institución.

Conclusión:

Ambas instituciones dijeron tener políticas internas de protección de la información, respuesta que resulta clave en el desarrollo del sistema, tomando en cuenta siempre priorizar la confidencialidad, integridad y disponibilidad de la información.

VII. CONCLUSIONES

- La conclusión es que el desarrollo del sistema generador de alertas antifraude con parametrización apoyada con inteligencia artificial con enfoque en transacciones de tarjetas de crédito no solo es viable, sino también necesario para abordar el creciente riesgo de fraude con tarjetas de crédito entre las pequeñas y medianas instituciones financieras de Honduras. El análisis reveló que estas instituciones enfrentan limitaciones operativas y de presupuesto que las hacen particularmente vulnerables a los ataques especialmente en la modalidad de fraude con tarjeta no presente. La propuesta va enfocada en atacar estas deficiencias con una herramienta personalizable y accesible destinada a mejorar su capacidad de detección y respuesta en tiempo real.

- Un análisis de la situación actual mostró que el fraude con tarjetas de crédito ha aumentado significativamente en Honduras. Esto afecta especialmente a las instituciones más pequeñas, que cuentan con menos recursos para implementar soluciones robustas de monitoreo de transacciones. El tipo de fraude más común es el llamado fraude de tarjeta no presente, que representa un mayor desafío porque requiere un monitoreo avanzado en tiempo real, con el que la mayoría de estas instituciones aún no cuentan.

- La investigación identificó limitaciones que afectan directamente la implementación de tecnologías avanzadas de prevención del fraude como las que ofrecen las empresas de gran magnitud como MasterCard. Entre ellas, destacan los presupuestos limitados, la falta de personal especializado en IA o análisis de datos, y la dependencia de software con reglas

estáticas. Estos factores limitan drásticamente la capacidad de las instituciones bancarias para detectar transacciones fraudulentas con tarjetas de crédito.

- Se determinaron requerimientos clave para garantizar la implementación efectiva de una herramienta antifraude con IA en instituciones con recursos limitados. Estos incluyen una interfaz amigable y baja dependencia de personal especializado, de igual manera se priorizó el cumplimiento de normativas sobre protección de datos y ciberseguridad. El cumplimiento de estos requisitos posibilita que la solución propuesta sea operativa incluso en instituciones con infraestructura básica.

- La propuesta logra cumplir con los criterios de viabilidad tecnológica, operativa y económica. Al combinar algoritmos de inteligencia artificial con opciones de parametrización manual, la herramienta ofrece un sistema híbrido capaz de adaptarse a diferentes niveles de madurez tecnológica. Además, la detección en tiempo real y la reducción de falsos positivos mejoran significativamente la eficiencia operativa y la salud laboral de los equipos antifraude de las instituciones financieras de menor escala en el país.

VIII. RECOMENDACIONES

- Para fortalecer la capacidad de respuesta contra el fraude con tarjetas de crédito, se recomienda implementar una herramienta que proporcione soporte adicional basado en IA para detectar casos de fraude complejos, como el fraude con tarjeta no presente. Esto permitirá mejorar la efectividad en la reducción de riesgos y mejora de la salud laboral en los equipos de riesgo transaccional de las instituciones financieras de menor escala en el país.

- Se recomienda a las instituciones financieras de menor escala (medianas y pequeñas) mantener un monitoreo constante del panorama nacional de fraude con tarjetas de crédito, especialmente respecto a nuevas modalidades como el fraude con tarjeta no presente. Este conocimiento debe integrarse como insumo fundamental para actualizar periódicamente los parámetros y algoritmos de sus sistemas de detección.

- Se sugiere a las instituciones del sector financiero y a los entes reguladores como la CNBS fomentar espacios de formación y alianzas estratégicas que permitan reducir las barreras económicas, tecnológicas y de talento humano identificadas. Esto incluye promover la colaboración con universidades como ser UNITEC/CEUTEC, para promover soluciones más económicas o de código abierto especializadas en inteligencia artificial aplicada a la prevención del fraude.

- Se recomienda definir una guía técnica que establezca los requerimientos mínimos para desarrollar e implementar soluciones antifraude en estas instituciones financieras. Esta guía debe contener aspectos como arquitectura ligera, cumplimiento normativo, integración con

sistemas existentes, protección de datos personales, facilidad de uso y soporte a mediano o largo plazo.

- Se sugiere a las instituciones financieras de menor escala priorizar el uso de herramientas híbridas que combinen parametrización manual y aprendizaje automático, permitiendo un equilibrio entre control humano y automatización. Este enfoque facilitará la adopción progresiva de tecnologías avanzadas sin sacrificar la operatividad ni aumentar la cantidad de falsos positivos que cargan de trabajo al personal.

IX. APLICABILIDAD

9.1 MANUAL TÉCNICO

9.1.1 Propósito

El presente manual técnico tiene como finalidad servir como guía integral para la instalación, configuración y operación del Antifraud System, una solución web desarrollada con tecnologías ya conocidas desde hace años como ser HTML, CSS y JavaScript, así como también tecnologías de vanguardia como ser Python con FastAPI que han venido a revolucionar y simplificar la programación.

Este documento proporciona la información necesaria para comprender la arquitectura, los módulos principales, el diseño de base de datos, las interfaces de usuario y los procesos internos que permiten el funcionamiento del sistema. Su propósito es garantizar que los administradores, desarrolladores y personal técnico dispongan de una referencia clara para implementar el sistema dentro del entorno de su banco.

En conjunto, este manual asegura la disponibilidad de lineamientos técnicos que contribuyen al uso eficiente del Antifraud System, alineado con los objetivos del proyecto que tiene como enfoque la detección temprana de transacciones atípicas con un apoyo adicional de la inteligencia artificial.

9.1.2 Alcance

El presente manual técnico abarca la descripción, uso y administración del Antifraud System, delimitando el contenido a los aspectos técnicos para la correcta implementación y operación.

Este documento va dirigido a clientes tanto internos como externos del área de Tecnología como ser:

- **Administradores de sistemas**: responsables de la instalación y configuración del software.
- **Desarrolladores y personal técnico**: quienes están encargados de extender o adaptar las funcionalidades del sistema.
- **Oficiales y Especialistas de Riesgo Transaccional**: quienes utilizarán el Antifraud System como herramienta de apoyo en la detección del fraude transaccional.

Para la adecuada comprensión de este manual se recomienda que los lectores posean conocimientos básicos en:

- Sistemas operativos (Windows) para la instalación de dependencias.
- Bases de datos relacionales, específicamente SQL, para la administración de la información almacenada.
- Conceptos de redes y seguridad informática, en lo referente a autenticación, permisos y protección de datos sensibles.
- Conocimientos en HTML y lenguajes de programación web (CSS, JavaScript y Python) para la comprensión del código de los módulos descritos.

En cuanto al software en sí, el alcance del documento se limita a describir las funcionalidades principales del sistema:

- Gestión de usuarios y roles, con controles de acceso diferenciados según privilegios.
- Monitoreo de transacciones en tiempo real, identificando operaciones atípicas según parámetros establecidos.
- Visualización de reportes y alertas, mediante una interfaz web adaptable y de fácil uso.
- Integración con bases de datos y módulos internos, garantizando la consistencia de la información.
- Procesos de respaldo y seguridad, orientados a la protección de datos y continuidad operativa.

Quedan fuera del alcance de este documento aspectos como el entrenamiento avanzado de modelos de inteligencia artificial, la modificación profunda de la arquitectura del sistema y la personalización total de interfaces.

9.1.3 Documentos de Referencia

- Circular CNBS No.018/2024
- Reporte de Inclusión Financiera 2025
- Tendencias de fraude con tarjeta no presente y formas de gestionar el riesgo (MasterCard).

9.1.4 Definiciones Importantes

9.1.4.1 Hardware y Software Requerido

En este apartado se describen las plataformas y componentes técnicos indispensables para ejecutar el sistema.

9.1.4.2 Hardware mínimo:

- Servidor o equipo con procesador de al menos 4 núcleos.
- Memoria RAM de 16 GB o superior.
- Almacenamiento de 200 GB disponible.
- Conexión de red estable (mínimo 10 Mbps).

9.1.4.3 Software necesario:

- Backend: Python 3.11+, FastAPI, SQLAlchemy.
- Frontend: HTML5, CSS3, JavaScript (ES6+).
- Base de datos: MySQL o PostgreSQL.
- Dependencias adicionales: librerías de seguridad (JWT, bcrypt), frameworks de validación de datos (Pydantic).

9.1.4.4 Herramientas de apoyo:

- Git para control de versiones.
- Docker (opcional) para despliegue.
- Postman o cURL para pruebas de API.

9.1.4.5 Conceptos Generales

API REST: es una interfaz de programación de aplicaciones (API) que se ajusta a los principios de diseño del estilo arquitectónico de transferencia de estado representacional (REST),

un estilo utilizado para conectar sistemas de hipermedia distribuidos. Las API REST a veces se denominan API RESTful o API web RESTful (¿Qué es una API REST?, s.f.).

Base de datos relacional: es un tipo de base de datos que almacena y proporciona acceso a puntos de datos relacionados entre sí. Las bases de datos relacionales se basan en el modelo relacional, una forma intuitiva y directa de representar datos en tablas. En una base de datos relacional, cada fila en una tabla es un registro con una ID única, llamada clave. Las columnas de la tabla contienen los atributos de los datos y cada registro suele tener un valor para cada atributo, lo que simplifica la creación de relaciones entre los puntos de datos (What is a Relational Database (RDBMS)?, 2021).

CSS: es un lenguaje de programación que sirve para determinar el diseño de los documentos electrónicos. Con la ayuda de unas sencillas instrucciones -presentadas en forma de código fuente claro-, los elementos del sitio web, como el diseño, el color y la tipografía, pueden adaptarse como se desee (¿Qué es CSS? Explicamos el Cascading Style Sheets, 2021).

FastAPI: es un framework web moderno, rápido (de alto rendimiento), para construir APIs con Python basado en las anotaciones de tipos estándar de Python (FastAPI, s.f.).

HTML: se conoce como Hyper Text Markuo Languaje o Lenguaje de Marcado de Hipertexto. Es el fundamento o lenguaje sobre el que se construye toda página web, se utiliza para estructurar el contenido de forma sencilla para que cualquier usuario pueda acceder a la información de forma sencilla y útil (Qué es HTML y cuáles son sus aplicaciones, 2024).

JavaScript: es un lenguaje de programación que los desarrolladores utilizan para hacer páginas web interactivas. Desde actualizar fuentes de redes sociales a mostrar animaciones y

mapas interactivos, las funciones de JavaScript pueden mejorar la experiencia del usuario de un sitio web (¿Qué es JavaScript (JS)?, s.f.).

JWT (JSON Web Token): es un estándar abierto (RFC 7519) que define una forma compacta y autónoma de transmitir información de forma segura entre partes como un objeto JSON. Esta información se puede verificar y confiar porque está firmada digitalmente. Los JWT se pueden firmar mediante un secreto (con el algoritmo HMAC) o un par de claves pública/privada mediante RSA o ECDSA (JSON Web Token Introduction, 2024).

NumPy: es una librería de Python especializada en el cálculo numérico y el análisis de datos, especialmente para un gran volumen de datos. Incorpora una nueva clase de objetos llamados arrays que permite representar colecciones de datos de un mismo tipo en varias dimensiones, y funciones muy eficientes para su manipulación (Alberca, La librería Numpy, 2022).

Pandas: es una librería de Python especializada en el manejo y análisis de estructuras de datos (Alberca, La librería Pandas, 2022)

Python: es un lenguaje de programación orientado a objetos fácil de interpretar y de alto nivel con una sintaxis fácil de leer. Ideal para la creación de prototipos y tareas ad-hoc, Python tiene un amplio uso en computación científica, desarrollo web y automatización. Como lenguaje de programación de propósito general y fácil de usar para principiantes, Python es compatible con muchos de los mejores científicos informáticos y desarrolladores de aplicaciones a nivel mundial (¿Qué es Python?, s.f.).

SQLAlchemy: es una herramienta basada en el principio de mapeo relacional de objetos (ORM). ORM es una técnica informática que mapea el esquema de una base de datos relacional (comúnmente conocida como bases de datos SQL) y las clases de un lenguaje de programación orientado a objetos (en este caso, Python) (What is it? What's it for? DataScientest, 2023).

9.1.4.6 Procesos de Entrada y Salida

9.1.4.6.1 Entradas principales:

- Credenciales de usuario (usuario y contraseña) para autenticación.
- Datos de transacciones (monto, hora, número de tarjeta, fecha de vencimiento, comercio, país, MCC, etc.).
- Parámetros configurables de reglas antifraude (umbrales, montos límites, cantidad de transacciones).

9.1.4.6.2 Procesos internos:

- Validación de credenciales y asignación de roles.
- Registro de transacciones en la base de datos.
- Evaluación de transacciones en tiempo real con reglas predefinidas y modelos de IA.
- Generación de alertas cuando se detectan anomalías.

9.1.4.6.3 Salidas principales:

- Alertas de transacciones sospechosas (en la interfaz web).

- Reportes históricos de actividad (consultas por fecha, usuario, estado de alerta).
- Confirmación de acciones administrativas (crear usuario, modificar parámetros, etc.).

9.1.5 Descripción de Módulos

9.1.5.1 Módulo de login / autenticación

- Funcionalidad/Propósito: validar que las credenciales que el usuario ingresa en el sistema coincidan con las registradas en la base de datos de usuarios, de ser así el sistema permite el ingreso del usuario.

- Dependencias funcionales: Usuarios(pk id, fk rol_id) bitacora_login(pk id, fk usuario_id)

- Diagramas de Casos de uso:

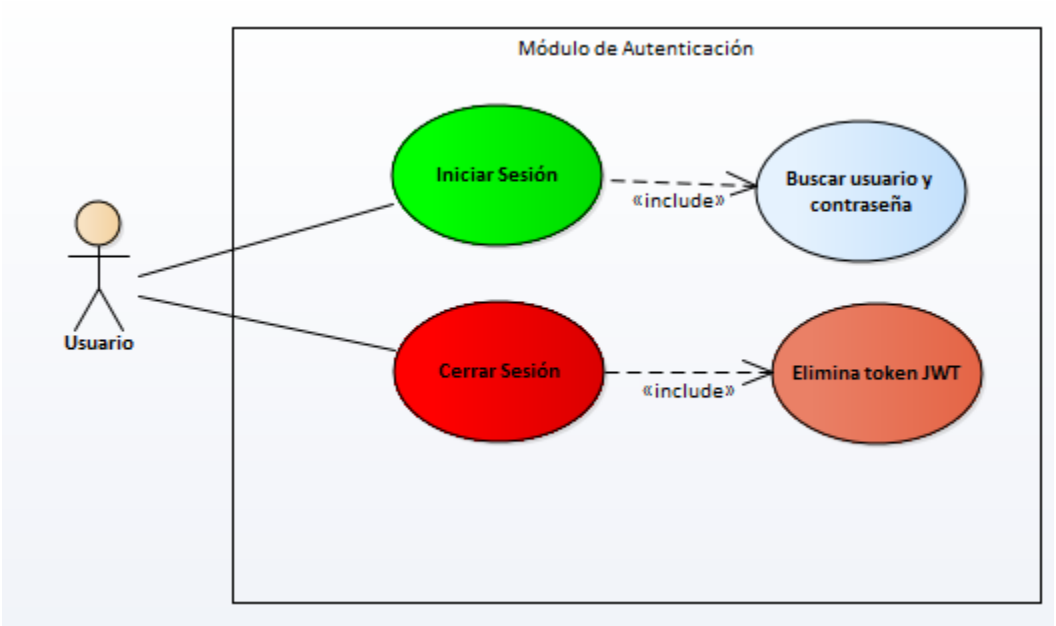


Ilustración 9 Caso de uso Módulo de Autenticación.

Fuente: elaboración propia.

9.1.5.2 Módulo de Bitácoras

Funcionalidad/Propósito: llevar un registro con fecha, hora y usuario que realizó alguna inserción, actualización o eliminación de algún registro de la base de datos a través de la interfaz del sistema.

- Dependencias funcionales: : Usuarios(pk id, fk rol_id), bitacora_login(pk id, fk usuario_id), tarjetas(pk id_tc, fk id_cuenta), transacciones(pk id_transaccion, fk id_tc).
- Diagramas de Casos de uso:

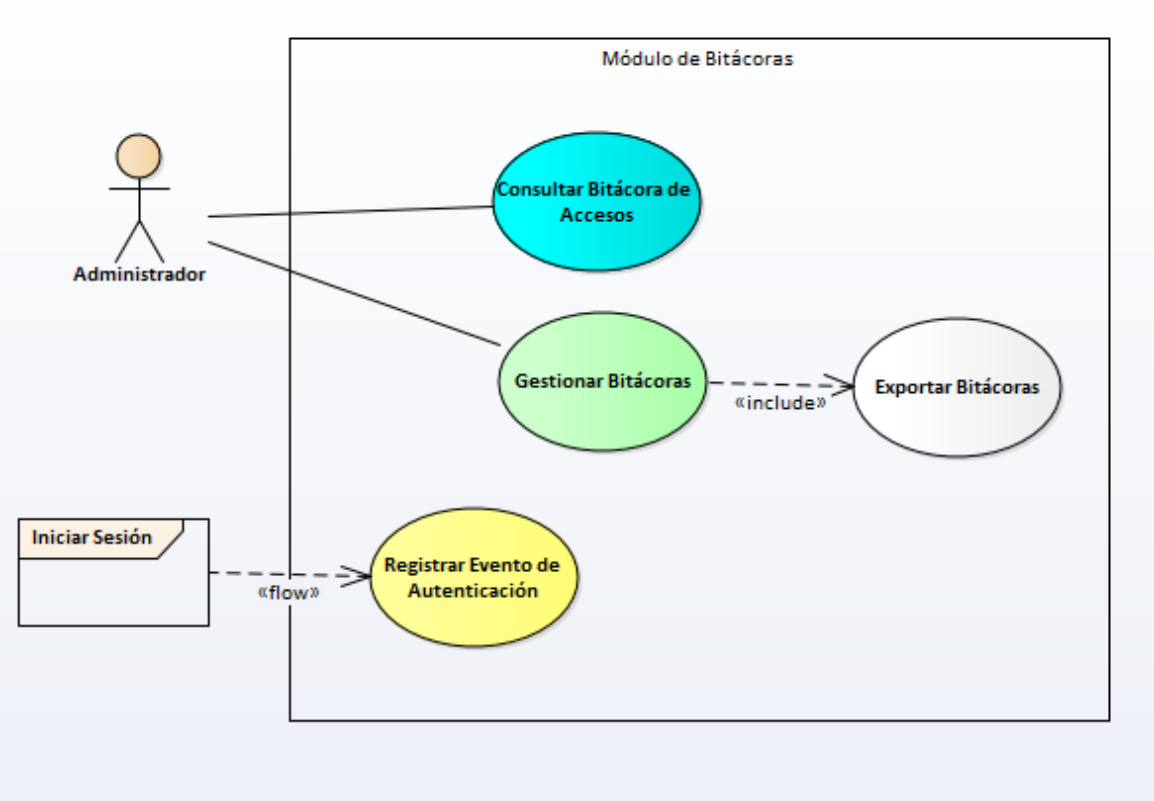


Ilustración 10 Caso de uso Módulo de Bitácoras.

Fuente: elaboración propia.

9.1.5.3 Módulo de Transacciones

Funcionalidad/Propósito: módulo principal del sistema en donde se pueden observar todas las transacciones con tarjetas de crédito registradas en el sistema, se puede filtrar según tipo de transacción como ser: descartada, sospechosa, fraude o "todas" que son las transacciones que no fueron detectadas como sospechosas por las reglas del sistema. También desde este módulo se pueden abrir casos de investigación, bloquear tarjetas o filtrar las transacciones en un rango de fecha y hora.

- Dependencias funcionales: tarjetas(pk id_tc, fk id_cuenta), transacciones(pk id_transaccion, fk id_tc), casos(pk id_caso, fk id_transaccion), Tbreglas(pk id_regla, fk id_usuario_creacion).

- Diagramas de Casos de uso:

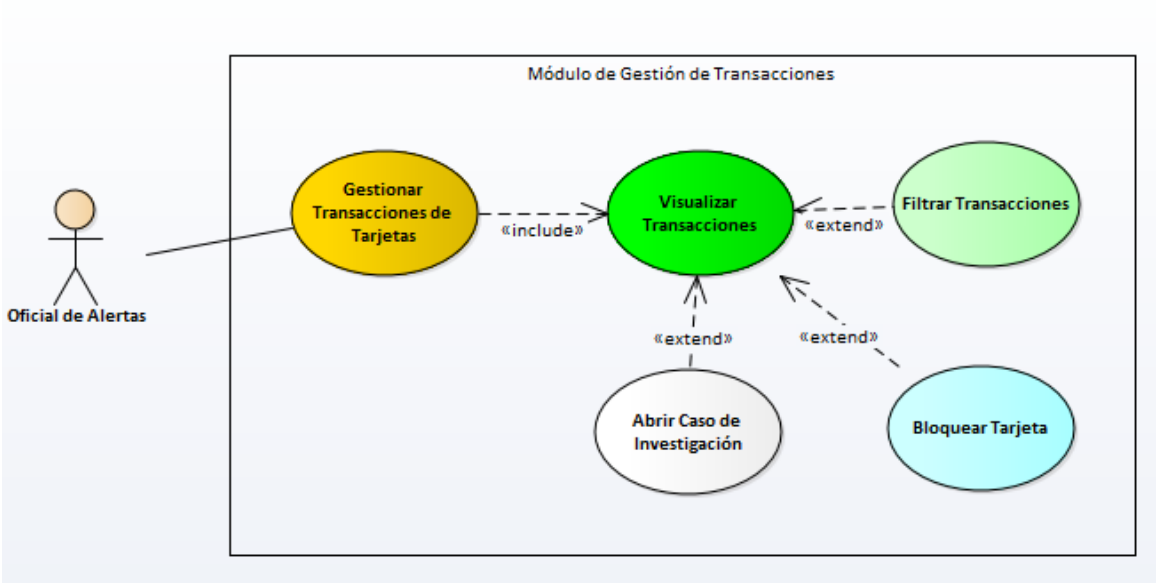


Ilustración 11 Caso de uso Módulo de Transacciones.

Fuente: elaboración propia.

9.1.5.4 Módulo de Casos

Funcionalidad/Propósito: aquí es donde se hace toda la gestión de los casos de investigación, una vez que el usuario ha abierto el caso desde el módulo de transacciones, se puede hacer gestión de él desde este módulo, el oficial de alertas puede darle seguimiento mediante un historial de acciones realizadas, por ejemplo: llamada telefónica, SMS, mensaje de WhatsApp, email. Así como también se puede dar una resolución al caso como: descartado o fraude.

- Dependencias funcionales: transacciones(pk id_transaccion, fk id_tc).
- Diagramas de Casos de uso:

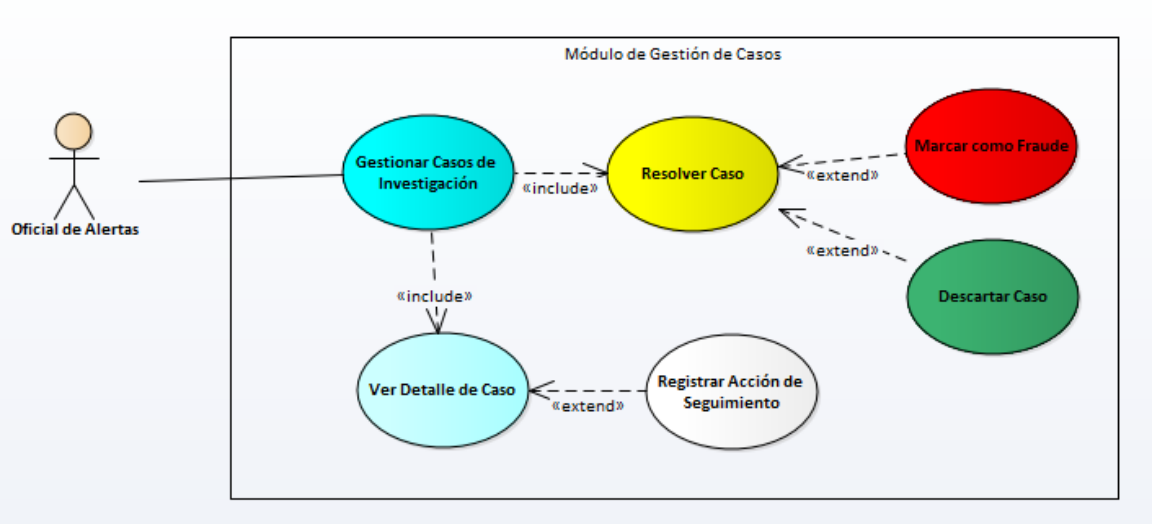


Ilustración 12 Caso de uso Módulo de Gestión de Casos.

Fuente: elaboración propia.

9.1.5.5 Módulo de Reglas

Funcionalidad/Propósito: en este módulo se hace la administración general de las reglas de detección de fraude, se puede crear, modificar, activar o inactivar las reglas. Tanto las reglas estáticas como las generadas con inteligencia artificial.

- Dependencias funcionales: transacciones(pk id_transaccion, fk id_tc), Tbreglas(pk id_regla, fk id_usuario_creacion).

- Diagramas de Casos de uso:

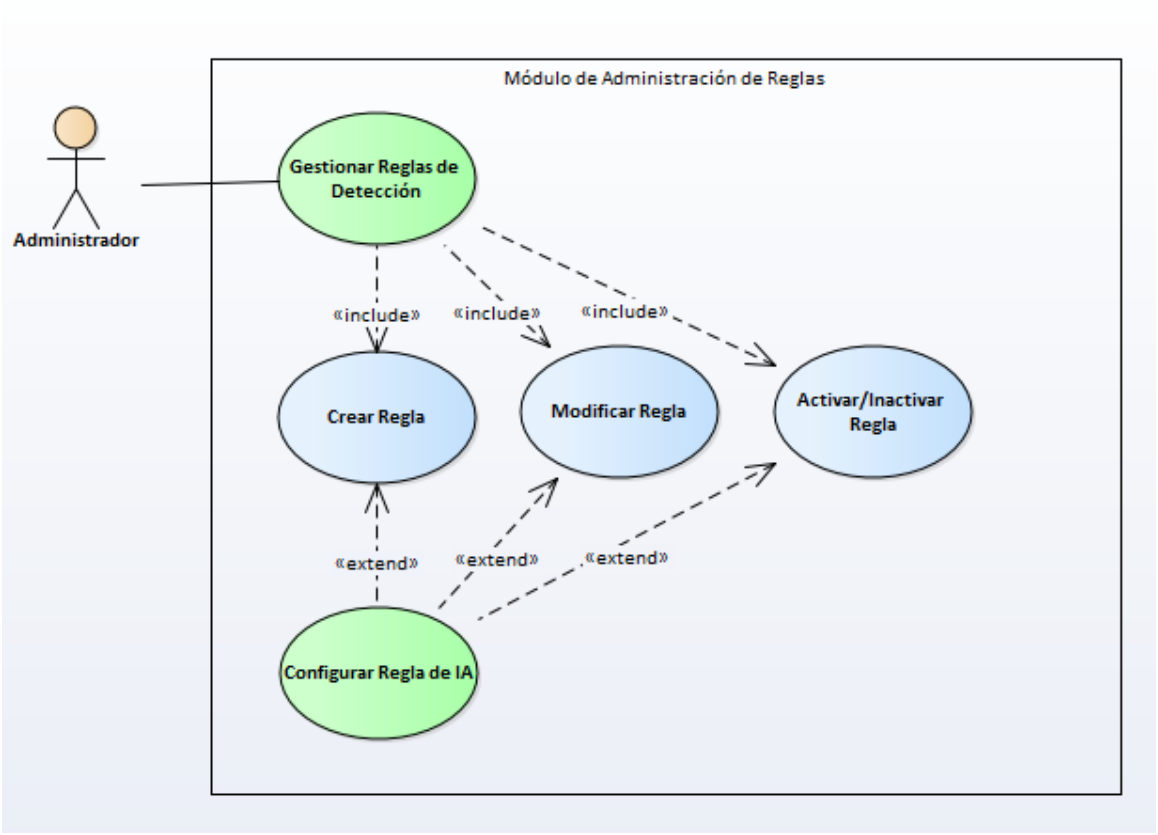


Ilustración 13 Caso de uso Módulo de Gestión de Reglas

Fuente: elaboración propia.

9.1.6 Diccionario de Datos

9.1.6.1 Modelo entidad-relación

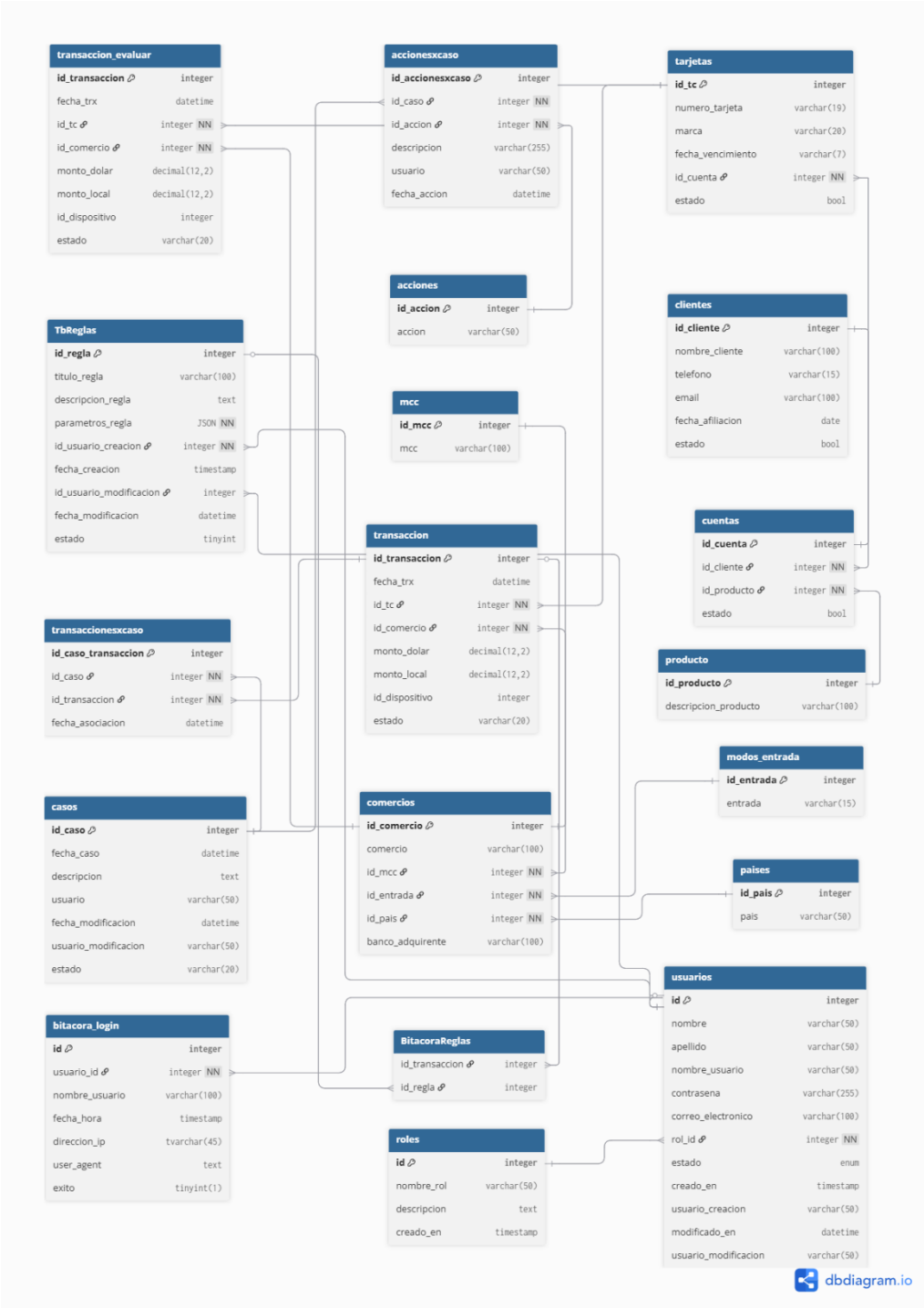


Ilustración 14 Modelo entidad-relación

Fuente: elaboración propia mediante la herramienta dbdiagram.io

9.1.6.2 Distribución física y lógica de base de datos

Distribución Física:

La base de datos del sistema de gestión de fraudes se implementará en un servidor MySQL/MariaDB. La ubicación de los archivos de datos, índices y bitácora de transacciones seguirá la estructura predeterminada del motor de base de datos, la cual puede variar según el sistema operativo:

- Linux: /var/lib/mysql/
- Windows: C:\ProgramData\MySQL\MySQL Server X.X\Data\

Se recomienda configurar los siguientes parámetros de almacenamiento:

Tabla 17 Parámetros de almacenamiento.

Fuente: elaboración propia.

Tipo de archivo	Ubicación sugerida	Tamaño inicial	Crecimiento	Tipo de crecimiento
Archivos de datos (.ibd)	Por defecto del motor	500MB	100MB	Automático
Archivos de Índices	Mismo tablespace	Incluido en datos	-	Automático
Archivo de log de transacciones (ib_logfile)	Por defecto	50 MB C/U	Fijo	Manual (requiere un reinicio)

Distribución Lógica:

La base de datos se organizará en los siguientes tablespaces para optimizar el rendimiento y la administración:

- **Tablespace por defecto (innodb_file_per_table = ON**): cada tabla tendrá su propio archivo de tablespace (.ibd), lo que facilita la gestión independiente de almacenamiento y la optimización de operaciones de mantenimiento.

- **Tablespace para tablas transaccionales**: tablas como transaccion, transaccion_evaluar, bitacora_login, y BitacoraReglas se agruparán lógicamente en un tablespace dedicado a operaciones de alta frecuencia.

- **Tablespace para tablas maestras o de parámetros**: tablas como roles, usuarios, clientes, tarjetas, comercios, mcc, paises, modos_entrada, producto, acciones, y TbReglas se ubicarán en un tablespace separado para facilitar respaldos y administración.

- **Tablespace para índices:** los índices de las tablas transaccionales se almacenarán en un tablespace independiente para mejorar el rendimiento de las consultas.

9.1.6.3 Tablas y vistas

A continuación, se describen las tablas utilizadas por el sistema de gestión de fraudes:

1. **usuarios**
    a. Descripción: Almacena la información de los usuarios del sistema.
    b. Propietario/Esquema: Esquema principal (Proyecto_Graduacion).
    c. Atributos:
        i. id (integer, PK): Identificador único del usuario.
        ii. nombre (varchar(50)): Nombre del usuario.
        iii. apellido (varchar(50)): Apellido del usuario.
        iv. nombre_usuario (varchar(50)): Nombre de usuario para login.
        v. contrasena (varchar(255)): Contraseña encriptada.
        vi. correo_electronico (varchar(100)): Correo electrónico.
        vii. rol_id (integer, NN): Referencia al rol del usuario.

viii. estado (enum): Estado del usuario (activo/inactivo).
ix. creado_en (timestamp): Fecha de creación.
x. usuario_creacion (varchar(50)): Usuario que creó el registro.
xi. modificado_en (datetime): Fecha de modificación.
xii. usuario_modificacion (varchar(50)): Usuario que modificó el registro.

d. Llaves:
i. PK: id
ii. FK: rol_id → roles(id)

2. Roles
a. Descripción: Define los roles de los usuarios en el sistema.
b. Atributos:
i. id (integer, PK): Identificador único del rol.
ii. nombre_rol (varchar(50)): Nombre del rol.
iii. descripcion (text): Descripción del rol.
iv. creado_en (timestamp): Fecha de creación.
c. Llaves:
i. PK: id

3. bitacora_login
a. Descripción: Registra los intentos de login de los usuarios.
b. Atributos:
i. id (integer, PK, AUTO_INCREMENT): Identificador único.
ii. usuario_id (integer, NN): ID del usuario.
iii. nombre_usuario (varchar(100)): Nombre de usuario.
iv. fecha_hora (timestamp): Fecha y hora del intento.
v. direccion_ip (tvarchar(45)): Dirección IP del cliente.
vi. user_agent (text): Agente de usuario del navegador.
vii. exito (tinyint(1)): 1 si fue exitoso, 0 si falló.
c. Llaves:
i. PK: id
ii. FK: usuario_id → usuarios(id)

4. Tarjetas
a. Descripción: Almacena información de tarjetas de crédito/débito.
b. Atributos:
i. id_tc (integer, PK): Identificador único de la tarjeta.
ii. numero_tarjeta (varchar(19)): Número de tarjeta.
iii. marca (varchar(20)): Marca de la tarjeta (Visa, MasterCard, etc.).
iv. fecha_vencimiento (varchar(7)): Fecha de vencimiento (MM/YYYY).
v. id_cuenta (integer, NN): Cuenta asociada.
vi. estado (bool): Estado de la tarjeta (activa/inactiva).

   c. Llaves:
      i. PK: id_tc
      ii. FK: id_cuenta → cuentas(id_cuenta)
5. Clientes
   a. Descripción: Información de clientes del sistema.
   b. Atributos:
      i. id_cliente (integer, PK): Identificador único del cliente.
      ii. nombre_cliente (varchar(100)): Nombre completo.
      iii. telefono (varchar(15)): Teléfono de contacto.
      iv. email (varchar(100)): Correo electrónico.
      v. fecha_afiliacion (date): Fecha de afiliación.
      vi. estado (bool): Estado del cliente (activo/inactivo).
   c. Llaves:
      i. PK: id_cliente
6. Cuentas
   a. Descripción: Cuentas bancarias asociadas a clientes.
   b. Atributos:
      i. id_cuenta (integer, PK): Identificador único de la cuenta.
      ii. id_cliente (integer, NN): Cliente asociado.
      iii. id_producto (integer, NN): Producto asociado.
      iv. estado (bool): Estado de la cuenta.
   c. Llaves:
      i. PK: id_cuenta
      ii. FK: id_cliente → clientes(id_cliente)
      iii. FK: id_producto → producto(id_producto)
7. Producto
   a. Descripción: Catálogo de productos bancarios.
   b. Atributos:
      i. id_producto (integer, PK): Identificador único del producto.
      ii. descripcion_producto (varchar(100)): Descripción del producto.
   c. Llaves:
      i. PK: id_producto
8. modos_entrada
   a. Descripción: Modos de entrada de transacciones (POS, Web, etc.).
   b. Atributos:
      i. id_entrada (integer, PK): Identificador único.
      ii. entrada (varchar(15)): Descripción del modo.
   c. Llaves:
      i. PK: id_entrada

9. paises
    a. Descripción: Catálogo de países.
    b. Atributos:
        i. id_pais (integer, PK): Identificador único.
        ii. pais (varchar(50)): Nombre del país.
    c. Llaves:
        i. PK: id_pais
10. mcc
    a. Descripción: Códigos MCC (Merchant Category Code) para categorizar comercios.
    b. Atributos:
        i. id_mcc (integer, PK): Identificador único.
        ii. mcc (varchar(100)): Descripción del código MCC.
    c. Llaves:
        i. PK: id_mcc
11. comercios
    a. Descripción: Información de comercios donde se realizan transacciones.
    b. Atributos:
        i. id_comercio (integer, PK): Identificador único.
        ii. comercio (varchar(100)): Nombre del comercio.
        iii. id_mcc (integer, NN): Categoría MCC.
        iv. id_entrada (integer, NN): Modo de entrada.
        v. id_pais (integer, NN): País del comercio.
        vi. banco_adquirente (varchar(100)): Banco adquirente.
    c. Llaves:
        i. PK: id_comercio
        ii. FK: id_mcc → mcc(id_mcc)
        iii. FK: id_entrada → modos_entrada(id_entrada)
        iv. FK: id_pais → paises(id_pais)
12. transaccion
    a. Descripción: Registro de transacciones financieras.
    b. Atributos:
        i. id_transaccion (integer, PK): Identificador único.
        ii. fecha_trx (datetime, DEFAULT NOW()): Fecha de la transacción.
        iii. id_tc (integer, NN): Tarjeta utilizada.
        iv. id_comercio (integer, NN): Comercio donde se realizó.
        v. monto_dolar (decimal(12,2)): Monto en dólares.
        vi. monto_local (decimal(12,2)): Monto en moneda local.
        vii. id_dispositivo (integer): Dispositivo utilizado (opcional).

viii. estado (varchar(20)): Estado de la transacción.

c. Llaves:
   i. PK: id_transaccion
   ii. FK: id_tc → tarjetas(id_tc)
   iii. FK: id_comercio → comercios(id_comercio)

13. casos
    a. Descripción: Casos de fraude investigados.
    b. Atributos:
       i. id_caso (integer, PK, AUTO_INCREMENT): Identificador único.
       ii. fecha_caso (datetime, DEFAULT NOW()): Fecha de creación del caso.
       iii. descripcion (text): Descripción del caso.
       iv. usuario (varchar(50)): Usuario que creó el caso.
       v. fecha_modificacion (datetime): Fecha de modificación.
       vi. usuario_modificacion (varchar(50)): Usuario que modificó el caso.
       vii. estado (varchar(20)): Estado del caso.
    c. Llaves:
       i. PK: id_caso
14. transaccionesxcaso
    a. Descripción: Relación entre casos y transacciones asociadas.
    b. Atributos:
       i. id_caso_transaccion (integer, PK, AUTO_INCREMENT): Identificador único.
       ii. id_caso (integer, NN): Caso asociado.
       iii. id_transaccion (integer, NN): Transacción asociada.
       iv. fecha_asociacion (datetime, DEFAULT NOW()): Fecha de asociación.
    c. Llaves:
       i. PK: id_caso_transaccion
       ii. FK: id_caso → casos(id_caso)
       iii. FK: id_transaccion → transaccion(id_transaccion)
15. accionesxcaso
    a. Descripción: Acciones tomadas en cada caso.
    b. Atributos:
       i. id_accionesxcaso (integer, PK, AUTO_INCREMENT): Identificador único.
       ii. id_caso (integer, NN): Caso asociado.
       iii. id_accion (integer, NN): Acción realizada.
       iv. descripcion (varchar(255)): Descripción de la acción.
       v. usuario (varchar(50)): Usuario que realizó la acción.
       vi. fecha_accion (datetime, DEFAULT NOW()): Fecha de la acción.

c. Llaves:
    i. PK: id_accionesxcaso
    ii. FK: id_caso → casos(id_caso)
    iii. FK: id_accion → acciones(id_accion)

16. acciones
    a. Descripción: Catálogo de acciones disponibles para casos.
    b. Atributos:
        i. id_accion (integer, PK, AUTO_INCREMENT): Identificador único.
        ii. accion (varchar(50)): Descripción de la acción.
    c. Llaves:
        i. PK: id_accion
17. transaccion_evaluar
    a. Descripción: Transacciones pendientes de evaluación por el sistema de reglas.
    b. Atributos:
        i. id_transaccion (integer, PK): Identificador único.
        ii. fecha_trx (datetime, DEFAULT NOW()): Fecha de la transacción.
        iii. id_tc (integer, NN): Tarjeta utilizada.
        iv. id_comercio (integer, NN): Comercio donde se realizó.
        v. monto_dolar (decimal(12,2)): Monto en dólares.
        vi. monto_local (decimal(12,2)): Monto en moneda local.
        vii. id_dispositivo (integer): Dispositivo utilizado.
        viii. estado (varchar(20)): Estado de la transacción.
    c. Llaves:
        i. PK: id_transaccion
        ii. FK: id_tc → tarjetas(id_tc)
        iii. FK: id_comercio → comercios(id_comercio)
18. TbReglas
    a. Descripción: Reglas de detección de fraude configuradas en el sistema.
    b. Atributos:
        i. id_regla (integer, PK, AUTO_INCREMENT): Identificador único.
        ii. titulo_regla (varchar(100)): Título de la regla.
        iii. descripcion_regla (text): Descripción de la regla.
        iv. parametros_regla (JSON, NN): Parámetros de la regla en formato JSON.
        v. id_usuario_creacion (integer, NN): Usuario que creó la regla.
        vi. fecha_creacion (timestamp): Fecha de creación.
        vii. id_usuario_modificacion (integer): Usuario que modificó la regla.
        viii. fecha_modificacion (datetime): Fecha de modificación.
        ix. estado (tinyint, DEFAULT 1): Estado (1: activa, 0: inactiva).
    c. Llaves:

i. PK: id_regla
ii. FK: id_usuario_creacion → usuarios(id)
iii. FK: id_usuario_modificacion → usuarios(id)

19. BitacoraReglas
    a. Descripción: Bitácora de reglas aplicadas a transacciones.
    b. Atributos:
        i. id_transaccion (integer): Transacción evaluada.
        ii. id_regla (integer): Regla aplicada.
    c. Llaves:
        i. FK: id_transaccion → transaccion(id_transaccion)
        ii. FK: id_regla → TbReglas(id_regla)

9.1.6.4 Restricciones especiales

1. Restricción de Integridad Referencial
    a. Descripción: Todas las tablas relacionadas mantienen integridad referencial mediante llaves foráneas (foreign keys) que garantizan la consistencia de los datos.
    b. Tablas afectadas: Todas las tablas con relaciones definidas.
    c. Comportamiento: Las operaciones de DELETE y UPDATE siguen el comportamiento por defecto de MySQL (RESTRICT para eliminaciones).
2. Restricción de Unicidad en Usuarios
    a. Descripción: El campo nombre_usuario en la tabla usuarios debe ser único para evitar duplicados.
3. Restricción de Unicidad en Tarjetas
    a. Descripción: El campo numero_tarjeta en la tabla tarjetas debe ser único.
4. Restricción de Unicidad en Correos Electrónicos
    a. Descripción: El campo correo_electronico en la tabla usuarios debe ser único.
5. Restricciones a Nivel de Campo

a. Restricción ENUM en Estado de Usuarios
    i. Tabla: usuarios
    ii. Campo: estado
    iii. Valores permitidos: 'activo', 'inactivo'
    iv. Propósito: Limitar los valores posibles para el estado del usuario.
b. Restricción de Formato de Fecha de Vencimiento
    i. Tabla: tarjetas
    ii. Campo: fecha_vencimiento
    iii. Formato: MM/YYYY (7 caracteres)
    iv. Implementación: Se validará mediante triggers o aplicación para mantener el formato consistente.
c. Restricción de Longitud en Número de Tarjeta
    i. Tabla: tarjetas
    ii. Campo: numero_tarjeta
    iii. Longitud máxima: 19 caracteres (standard para tarjetas de crédito)
    iv. Propósito: Cumplir con estándares internacionales de numeración de tarjetas.
d. Restricción de Precisión en Montos
    i. Tablas: transaccion, transaccion_evaluar
    ii. Campos: monto_dolar, monto_local
    iii. Tipo: DECIMAL(12,2)
    iv. Propósito: Permitir montos hasta 999,999,999,999.99 con precisión de centavos.

e. Restricción de Direcciones IP

i. Tabla: bitacora_login

ii. Campo: direccion_ip

iii. Longitud: 45 caracteres (soporta IPv6)

iv. Propósito: Almacenar direcciones IP completas incluyendo IPv6.

9.1.6.5 Funciones de usuario, Stored Procedures y paquetes A estos objetos debe especificarse:

A continuación, se describen los procedimientos almacenados utilizados por el sistema:

1. sp_obtener_transacciones_completas

a. Descripción: Obtiene información detallada de todas las transacciones con datos relacionados (tarjeta, comercio, MCC, modo de entrada, país).

b. Propietario/Esquema: Esquema principal (Proyecto_Graduacion).

c. Código:

```
DELIMITER //

CREATE PROCEDURE sp_obtener_transacciones_completas()
BEGIN
   SELECT
      t.id_transaccion,
      t.fecha_trx,
      tc.numero_tarjeta,
      tc.marca,
```

```
    tc.fecha_vencimiento,
    tc.id_cuenta,
    t.monto_dolar,
    t.monto_local,
    t.id_comercio,
    c.comercio,
    c.id_mcc,
    m.mcc,
    c.id_entrada,
    me.entrada,
    c.id_pais,
    p.pais,
    c.banco_adquirente,
    t.id_dispositivo,
    tc.estado AS estado_tarjeta,
    t.estado AS estado_transaccion
FROM
    transaccion t
INNER JOIN
    tarjetas tc ON t.id_tc = tc.id_tc
INNER JOIN
    comercios c ON t.id_comercio = c.id_comercio
INNER JOIN
```

```
        mcc m ON c.id_mcc = m.id_mcc
    INNER JOIN
        modos_entrada me ON c.id_entrada = me.id_entrada
    INNER JOIN
        paises p ON c.id_pais = p.id_pais
    ORDER BY
        t.fecha_trx DESC;
END //

DELIMITER ;
```

d. Parámetros: Ninguno.

e. Comentarios: Creado para facilitar la visualización completa de transacciones. Ordena por fecha descendente.

2. sp_obtener_usuarios_sin_password

a. Descripción: Retorna información de usuarios sin incluir la contraseña por seguridad.

b. Código:

```
DELIMITER //

CREATE PROCEDURE sp_obtener_usuarios_sin_password()
BEGIN
    SELECT
        u.id,
```

```
        u.nombre,
        u.apellido,
        u.nombre_usuario,
        u.correo_electronico,
        u.rol_id,
        r.nombre_rol AS nombre_rol,
        r.descripcion AS descripcion_rol,
        u.estado,
        u.creado_en
    FROM
        usuarios u
    LEFT JOIN
        roles r ON u.rol_id = r.id
    ORDER BY
        u.creado_en DESC;
END //

DELIMITER ;
```

c. Parámetros: Ninguno.

d. Comentarios: Diseñado para reportes administrativos donde no se debe exponer información sensible.

3. ObtenerInformacionUsuario

a. Descripción: Obtiene información básica de un usuario específico por su nombre de usuario.

b. Código:

```
ELIMITER //

CREATE PROCEDURE ObtenerInformacionUsuario(IN
p_nombre_usuario VARCHAR(50))
BEGIN
  SELECT
    CONCAT(u.nombre, ' ', u.apellido) AS nombre_completo,
    u.nombre_usuario,
    u.correo_electronico,
    r.nombre_rol AS rol,
    u.creado_en
  FROM
    usuarios u
  INNER JOIN
    roles r ON u.rol_id = r.id
  WHERE
    u.nombre_usuario = p_nombre_usuario;
END //

DELIMITER ;
```

c. Parámetros:

i. p_nombre_usuario (VARCHAR(50)): Nombre de usuario a consultar.

d. Comentarios: Utilizado para perfiles de usuario y verificación de datos.

4. ActualizarUsuario

a. Descripción: Actualiza la información de un usuario existente.

b. Código:

```
DELIMITER //

CREATE PROCEDURE ActualizarUsuario(
    IN p_id INT,
    IN p_nombre VARCHAR(50),
    IN p_apellido VARCHAR(50),
    IN p_correo_electronico VARCHAR(100),
    IN p_rol_id INT,
    IN p_usuario_modificacion VARCHAR(50)
)
BEGIN
    UPDATE usuarios
    SET
        nombre = p_nombre,
        apellido = p_apellido,
        correo_electronico = p_correo_electronico,
        rol_id = p_rol_id,
```

```
        usuario_modificacion = p_usuario_modificacion,
        modificado_en = NOW()
    WHERE
        id = p_id;
END //

DELIMITER ;
```

c. Parámetros:
    i. p_id: ID del usuario a actualizar.
    ii. p_nombre: Nuevo nombre.
    iii. p_apellido: Nuevo apellido.
    iv. p_correo_electronico: Nuevo correo.
    v. p_rol_id: Nuevo rol.
    vi. p_usuario_modificacion: Usuario que realiza la modificación.
d. Comentarios: Registra automáticamente la fecha de modificación.

5. ObtenerBitacoraUsuarios
    a. Descripción: Obtiene el historial de creación y modificación de usuarios en un rango de fechas.
    b. Código:

```
DELIMITER //

CREATE PROCEDURE ObtenerBitacoraUsuarios(
    IN p_fecha_inicial DATETIME,
```

```
    IN p_fecha_final DATETIME
)
BEGIN
    -- Registros de creación (usando creado_en)
    SELECT
        'Creación' AS Accion,
        u.nombre_usuario AS 'Usuario_afectado',
        u.usuario_creacion AS 'Usuario_accion', -- En creación, el usuario se
crea a sí mismo
        u.creado_en AS 'Fecha_Hora'
    FROM
        usuarios u
    WHERE
        u.creado_en BETWEEN p_fecha_inicial AND p_fecha_final

    UNION ALL

    -- Registros de modificación (usando modificado_en)
    SELECT
        'Modificación' AS Accion,
        u.nombre_usuario AS 'Usuario_afectado',
        u.usuario_modificacion AS 'Usuario_accion', -- Usuario que realizó
la modificación
```

```
    u.modificado_en AS 'Fecha_Hora'
  FROM
    usuarios u
  WHERE
    u.modificado_en BETWEEN p_fecha_inicial AND p_fecha_final
    AND u.modificado_en IS NOT NULL -- Solo registros que han sido
modificados

  ORDER BY
    Fecha_Hora DESC; -- Orden descendente (más reciente primero)
END //

DELIMITER ;
```

c. Parámetros:
    i. p_fecha_inicial: Fecha inicial del rango.
    ii. p_fecha_final: Fecha final del rango.
d. Comentarios: Útil para auditoría de cambios en usuarios.

6. ObtenerBitacoraCasos
    a. Descripción: Obtiene el historial de creación y modificación de casos en un rango de fechas.
    b. Código:

```
DELIMITER //
```

```
CREATE PROCEDURE ObtenerBitacoraCasos(
    IN p_fecha_inicial DATETIME,
    IN p_fecha_final DATETIME
)
BEGIN
    -- Registros de creación de casos (usando fecha_caso y usuario)
    SELECT
        'Creación' AS Accion,
        c.id_caso AS 'Id_caso',
        c.descripcion AS 'Caso_afectado',
        c.usuario AS 'Usuario_accion', -- Usuario que creó el caso
        c.fecha_caso AS 'Fecha_Hora'
    FROM
        casos c
    WHERE
        c.fecha_caso BETWEEN p_fecha_inicial AND p_fecha_final

    UNION ALL

    -- Registros de modificación de casos (usando fecha_modificacion y
usuario_modificacion)
    SELECT
        'Modificación' AS Accion,
```

```
        c.id_caso AS 'Id_caso',
        c.descripcion AS 'Caso_afectado',
        c.usuario_modificacion AS 'Usuario_accion', -- Usuario que modificó
el caso
        c.fecha_modificacion AS 'Fecha_Hora'
    FROM
        casos c
    WHERE
        c.fecha_modificacion BETWEEN p_fecha_inicial AND
p_fecha_final
        AND c.fecha_modificacion IS NOT NULL -- Solo registros que han
sido modificados
        AND c.usuario_modificacion IS NOT NULL -- Solo registros con
usuario de modificación

    ORDER BY
        Fecha_Hora DESC; -- Orden descendente (más reciente primero)
END //

DELIMITER ;
```

c. Parámetros:

   i. p_fecha_inicial: Fecha inicial del rango.

   ii. p_fecha_final: Fecha final del rango.

d. Comentarios: Diseñado para seguimiento de actividades en casos de fraude.

7. ObtenerReglasCompletas

a. Descripción: Obtiene información completa de todas las reglas incluyendo usuarios creadores y modificadores.

b. Código:

```
DELIMITER //

CREATE PROCEDURE ObtenerReglasCompletas()
BEGIN
  SELECT
    r.id_regla,
    r.titulo_regla,
    r.descripcion_regla,
    r.parametros_regla,
    r.estado,
    -- Información del usuario que creó la regla
    uc.nombre_usuario AS usuario_creacion,
    r.fecha_creacion,
    -- Información del usuario que modificó la regla
    um.nombre_usuario AS usuario_modificacion,
    r.fecha_modificacion
  FROM
    TbReglas r
```

```
    LEFT JOIN
        usuarios uc ON r.id_usuario_creacion = uc.id
    LEFT JOIN
        usuarios um ON r.id_usuario_modificacion = um.id
    ORDER BY
        r.fecha_creacion DESC;
END //

DELIMITER ;
```

c. Parámetros: Ninguno.

d. Comentarios: Incluye joins con la tabla de usuarios para obtener nombres en lugar de IDs.

8. ModificarReglaCompleta

a. Descripción: Modifica todos los campos de una regla existente.

b. Código:

```
DELIMITER //

CREATE PROCEDURE ModificarReglaCompleta(
    IN p_id_regla INT,
    IN p_titulo_regla VARCHAR(100),
    IN p_descripcion_regla TEXT,
    IN p_parametros_regla JSON,
    IN p_estado TINYINT,
```

```
    IN p_id_usuario_modificacion INT,
    IN p_fecha_modificacion DATETIME
)
BEGIN
    UPDATE TbReglas
    SET
        titulo_regla = p_titulo_regla,
        descripcion_regla = p_descripcion_regla,
        parametros_regla = p_parametros_regla,
        estado = p_estado,
        id_usuario_modificacion = p_id_usuario_modificacion,
        fecha_modificacion = NOW()
    WHERE
        id_regla = p_id_regla;
END //

DELIMITER ;
```

c. Parámetros:

   i. p_id_regla: ID de la regla a modificar.

   ii. p_titulo_regla: Nuevo título.

   iii. p_descripcion_regla: Nueva descripción.

   iv. p_parametros_regla: Nuevos parámetros en JSON.

   v. p_estado: Nuevo estado.

vi. p_id_usuario_modificacion: ID del usuario que modifica.

vii. p_fecha_modificacion: Fecha de modificación (se usa NOW() automáticamente).

d. Comentarios: Actualiza automáticamente la fecha de modificación.

9. RegistrarNuevoUsuario

a. Descripción: Registra un nuevo usuario en el sistema.

b. Código:

```
DELIMITER //

CREATE PROCEDURE RegistrarNuevoUsuario(
    IN p_nombre VARCHAR(50),
    IN p_apellido VARCHAR(50),
    IN p_nombre_usuario VARCHAR(50),
    IN p_contrasena VARCHAR(255),
    IN p_correo_electronico VARCHAR(100),
    IN p_rol_id INT,
    IN p_estado ENUM('activo', 'inactivo'),
    IN p_usuario_creacion VARCHAR(50)
)
BEGIN
    INSERT INTO usuarios (
        nombre,
        apellido,
```

```
        nombre_usuario,
        contrasena,
        correo_electronico,
        rol_id,
        estado,
        usuario_creacion,
        creado_en
    ) VALUES (
        p_nombre,
        p_apellido,
        p_nombre_usuario,
        p_contrasena,
        p_correo_electronico,
        p_rol_id,
        COALESCE(p_estado, 'activo'),
        p_usuario_creacion,
        NOW()
    );
END //

DELIMITER ;
```

c. Parámetros: Todos los campos necesarios para crear un usuario.

d. Comentarios: Usa COALESCE para establecer estado por defecto como 'activo'.

10. ActualizarEstadoTarjetaPorTransaccion

    a. Descripción: Actualiza el estado de una tarjeta basado en una transacción.

    b. Código:

```
DELIMITER //

CREATE PROCEDURE ActualizarEstadoTarjetaPorTransaccion(
   IN p_id_transaccion INT,
   IN p_nuevo_estado BOOL
)
BEGIN
   DECLARE v_id_tc INT;

   -- Obtener el id_tc de la transacción
   SELECT id_tc INTO v_id_tc
   FROM transaccion
   WHERE id_transaccion = p_id_transaccion;

   -- Verificar si se encontró la transacción
   IF v_id_tc IS NOT NULL THEN
      -- Actualizar el estado de la tarjeta
      UPDATE tarjetas
      SET estado = p_nuevo_estado
      WHERE id_tc = v_id_tc;
```

```
        SELECT 'Éxito: Estado de tarjeta actualizado' AS resultado;
    ELSE
        SELECT 'Error: Transacción no encontrada' AS resultado;
    END IF;
END //

DELIMITER ;
```

c. Parámetros:
    i. p_id_transaccion: ID de la transacción.
    ii. p_nuevo_estado: Nuevo estado de la tarjeta.
d. Comentarios: Incluye manejo de errores para transacciones no encontradas.

11. ObtenerEfectividadReglasPorFecha
    a. Descripción: Calcula la efectividad de las reglas en detectar fraudes dentro de un rango de fechas.
    b. Código:

```
DELIMITER //

CREATE PROCEDURE ObtenerEfectividadReglasPorFecha(
    IN p_fecha_inicio DATE,
    IN p_fecha_fin DATE
)
BEGIN
```

```
SELECT
    CONCAT(br.id_regla, ' - ', r.titulo_regla) AS regla_info,
    COUNT(br.id_transaccion) AS total_transacciones,
    SUM(CASE WHEN t.estado = 'Fraude ' THEN 1 ELSE 0 END) AS
transacciones_fraude,
    ROUND(
        (SUM(CASE WHEN t.estado = 'Fraude ' THEN 1 ELSE 0 END) /
COUNT(br.id_transaccion)) * 100,
        2
    ) AS efectividad_porcentaje
FROM
    BitacoraReglas br
INNER JOIN
    TbReglas r ON br.id_regla = r.id_regla
INNER JOIN
    transaccion t ON br.id_transaccion = t.id_transaccion
WHERE
    r.estado = 1
    AND t.fecha_trx BETWEEN p_fecha_inicio AND p_fecha_fin
GROUP BY
    br.id_regla, r.titulo_regla
ORDER BY
    efectividad_porcentaje DESC;
```

```
END //


DELIMITER ;
```

c. Parámetros:

   i. p_fecha_inicio: Fecha inicial del análisis.

   ii. p_fecha_fin: Fecha final del análisis.

d. Comentarios: Calcula porcentaje de efectividad y ordena de mayor a menor.

9.1.6.6 Tareas programadas

1. Limpieza de Bitácora de Login

   a. Nombre: cleanup_bitacora_login

   b. Descripción/Propósito: Elimina registros antiguos de la tabla bitacora_login para mantener el tamaño de la base de datos manejable y mejorar el rendimiento de las consultas.

   c. Frecuencia: Mensual (primer día del mes a las 02:00 AM).

   d. Consideraciones antes de ejecución manual:

      i. Verificar que se haya realizado un backup completo de la base de datos.

      ii. Confirmar que no haya procesos activos que estén consultando la bitácora.

      iii. Validar el espacio en disco disponible para operaciones de limpieza.

   e. Query de implementación:

```
DELETE FROM bitacora_login
WHERE fecha_hora < DATE_SUB(NOW(), INTERVAL 90 DAY);
```

f. Comentarios: Conserva solo los registros de los últimos 90 días. Se recomienda ajustar el intervalo según políticas de retención.

2. Tarea: Archivo de Transacciones Antiguas
    a. Nombre: archive_old_transactions
    b. Descripción/Propósito: Mueve transacciones mayores a 2 años a una tabla de archivado para mejorar el rendimiento de las consultas activas.
    c. Frecuencia: Trimestral (primer día del trimestre a 03:00 AM).
    d. Consideraciones antes de ejecución manual:
        i. Verificar la integridad de los datos a archivar.
        ii. Confirmar que el proceso de archivado no afecte las relaciones referenciales.
        iii. Asegurar espacio suficiente en el tablespace de archivado.
    e. Comentarios: Mantiene el rendimiento del sistema mientras preserva datos históricos para auditoría.

9.1.7 Políticas de Respaldo

9.1.7.1 Base de datos

Base de Datos Principal: Proyecto_Graduacion

- Justificación: Contiene toda la información crítica del sistema de gestión de fraudes, incluyendo:
    - Transacciones financieras en tiempo real
    - Información de clientes y tarjetas

- Reglas de detección de fraude configuradas
- Casos de investigación y bitácoras de auditoría
- Usuarios del sistema y permisos de acceso

- Estrategia de Respaldo
  - Respaldos Completos (Full Backups)
  - Periodicidad: Diaria
  - Horario: 01:00 AM (ventana de baja actividad)
  - Retención: 7 días
  - Justificación: Garantiza la disponibilidad de una base consistente para recuperación completa.

9.1.8 Instalación y Configuración

9.1.8.1 Servidor de Aplicaciones (Backend – FastAPI/Python)

Requisitos de Hardware Recomendados

- Procesador: 8 núcleos o más (para manejar 25,000 transacciones/día y procesamiento de IA).
- Memoria RAM: 32 GB (16 GB para la aplicación + 16 GB para modelos de IA).
- Almacenamiento: 500 GB SSD (para sistema operativo, aplicaciones y logs).
- Sistema operativo: Ubuntu Server 22.04 LTS o Windows Server 2022.

Software Requerido

- Python 3.11 o superior
- FastAPI

- Uvicorn (servidor ASGI)
- Librerías de IA: pandas y numpy.
- MySQL Connector/Python
- JWT para autenticación
- Otras dependencias listadas en requirements.txt

9.1.8.2 Proceso de Instalación en Windows Server

9.1.8.2.1 Instalar Python 3.11+

```
# Descargar e instalar Python 3.11 desde python.org
# Durante la instalación, marcar "Add Python to PATH"
# Verificar instalación
python --version
pip --version
```

9.1.8.2.2 Instalar Git para Windows

```
# Descargar desde git-scm.com y instalar con opciones por defecto
# Verificar instalación
git --version
```

9.1.8.2.3 Clonar o copiar el proyecto

```
# Crear directorio de aplicación
mkdir C:\AntifraudSystem
cd C:\AntifraudSystem
copiar manualmente los archivos del proyecto
```

9.1.8.2.4 Crear entorno virtual e instalar dependencias

```
# Crear entorno virtual
python -m venv venv
# Activar entorno virtual
.\venv\Scripts\activate
# Instalar dependencias
pip install -r requirements.txt
# Instalar dependencias específicas del proyecto
pip install fastapi uvicorn python-multipart sqlalchemy pymysql pandas scikit-learn
numpy jwt cryptography
```

9.1.8.2.5 Configurar como servicio de Windows usando NSSM

```
# Descargar NSSM desde https://nssm.cc/download
# Extraer nssm.exe en C:\Windows\System32 o en una carpeta del PATH
# Crear servicio
nssm install AntifraudAPI
# Configurar servicio
nssm set AntifraudAPI Application C:\AntifraudSystem\venv\Scripts\python.exe
nssm set AntifraudAPI AppParameters -m uvicorn main:app --host 0.0.0.0 --port
8000 --workers 4
nssm set AntifraudAPI AppDirectory C:\AntifraudSystem
nssm set AntifraudAPI DisplayName "Antifraud System API"
```

```
nssm set AntifraudAPI Description "Sistema de detección de transacciones atípicas
con IA"
nssm set AntifraudAPI Start SERVICE_AUTO_START
nssm set AntifraudAPI AppStdout C:\AntifraudSystem\logs\api.log
nssm set AntifraudAPI AppStderr C:\AntifraudSystem\logs\api-error.log
# Crear directorio de logs
mkdir C:\AntifraudSystem\logs
# Iniciar servicio
nssm start AntifraudAPI
```

9.1.8.3 Servidor de Base de Datos (MySQL)

Requisitos de Hardware

- Procesador: 4 núcleos
- RAM: 16 GB
- Almacenamiento: 200 GB SSD (para transacciones y logs de auditoría)

Software Requerido

- MySQL Server 8.0+
- MySQL Workbench (opcional, para administración)

9.1.8.4 Servidor Web (Frontend – HTML/CSS/JS)

Requisitos de Hardware

- Procesador: 2 núcleos

- RAM: 4 GB
- Almacenamiento: 50 GB

Software Requerido

- Nginx o Apache HTTP Server
- Certificado SSL (opcional pero recomendado)

9.1.8.5 Estaciones de Cliente (Usuarios Finales)

Requisitos Mínimos por Equipo

- Sistema operativo: Windows 10/11 o Ubuntu 20.04+
- Navegador: Chrome 90+, Firefox 88+, Edge 90+
- RAM: 8 GB
- Almacenamiento: 100 GB
- Conexión de red: 10 Mbps estable

Configuración Recomendada

- Acceso vía navegador web a la URL del frontend.
- No se requiere instalación local de software adicional.

9.1.8.6 Consideraciones de Red y Seguridad

- Firewall: permitir puertos 80 (HTTP), 443 (HTTPS), 8000 (API backend interno).
- VPN: acceso remoto seguro si los usuarios no están en la red local.
- Certificado SSL: usar Let's Encrypt o certificado comercial para HTTPS.

9.1.8.7 Requisitos generales pre-instalación

9.1.8.7.1 Requisitos de Hardware Mínimos y Recomendados

Tabla 18 Servidor Principal (Aplicación + Base de Datos)

Componente	Mínimo	Recomendado	Justificación
Procesador	4 núcleos	8 núcleos	Procesamiento de modelo de IA y 25,000 transacciones/día
Memoria RAM	16 GB	32 GB	Carga de modelos de ML + transacciones en memoria
Almacenamiento	200 GB SSD	500 GB NVMe SSD + 1 TB HDD (backups)	Para transacciones y logs
Red	1 Gbps	1 Gbps	Concurrencia de 4 usuarios + comunicación API
UPS	15 minutos	30-60 minutos	Prevención de pérdida de datos por cortes

Fuente: Elaboración propia.

Tabla 19 Estaciones de Cliente (4 usuarios concurrentes)

Componente	Mínimo	Recomendado
Procesador	Intel i3 8va gen	Intel i5 10ma gen o superior
Memoria RAM	8 GB	16 GB
Almacenamiento	256 GB SSD	512 GB SSD
Navegador	Chrome 90+ / Firefox 88+	Chrome 90+ / Firefox 88+
Conexión	10 Mbps	50 Mbps estables

Fuente: Elaboración propia.

Tabla 20 Sistema Operativo - Servidor Principal

Componente	Versión	Observaciones
Windows server	2022 Standard/Datacenter	Requisito obligatorio - Versión 64-bit
Actualizaciones	Ultima actualización	Instalar antes de la implementación
.NET Framework	4.8 o superior	Incluido en Windows Server 2022

Fuente: Elaboración propia.

Tabla 21 Software de Base de Datos

Componente	Versión	Tipo
MySQL Server	8.0.30 o superior	Community o Enterprise Edition

Fuente: Elaboración propia.

9.1.8.8 Orden de Instalación

1. Instalar Windows Server 2022
    - Seleccionar instalación limpia
    - Configurar partición del sistema (C:) con mínimo 100 GB
    - Habilitar .NET Framework 3.5 y 4.8 durante instalación
2. Aplicar actualizaciones de Windows
3. Configurar red estática
4. Instalar MySQL Server 8.0
5. Instalar Python 3.11+
6. Instalar Git
7. Configurar Windows Firewall
8. Configurar políticas de seguridad
9. Preparar entorno de aplicación
10. Instalar dependencias Python

9.1.8.9 Detalles del proceso de instalación

9.1.8.9.1 Estructura de Discos Recomendada

C:\ (SSD/NVMe) - Sistema operativo y aplicación (100 GB mínimo)

D:\ (SSD) - Base de datos MySQL (200 GB mínimo)

E:\ (HDD/SSD) - Backups y logs (500 GB recomendado)

9.1.8.9.2 Instalación de Dependencias

Link de descarga: https://www.python.org/ftp/python/3.11.4/python-3.11.4-amd64.exe

Opciones de instalación (CRÍTICAS):

1. Add Python 3.11 to PATH
2. Install for all users
3. Customize installation
4. Install pip
5. Add Python to environment variables
6. Documentation (opcional)
7. tcl/tk and IDLE (opcional)

9.1.8.9.3 Instalación de MySQL Server 8.0.33

Link de descarga: https://dev.mysql.com/get/MySQLInstaller8.0.33.msi

Selección de componentes:

1. MySQL Server 8.0.33
2. MySQL Workbench 8.0.33
3. MySQL Shell 8.0.33
4. Connector/Python 8.0.33
5. Samples and Examples (opcional)

9.1.8.10 Lista de contactos técnicos.

Tabla 22 Lista de contactos técnicos.

Nombre completo	**Empresa/Unidad Ejecutora**	**Módulo que atiende**	**Teléfonos/Correo electrónico**

Jhordy Alexis Rosado Fonseca	N/A	Sistema completo	• 95903841 • jhordyfonseca@gmail.com

Fuente: Elaboración propia.

9.1.9 Diseño de la Arquitectura Física

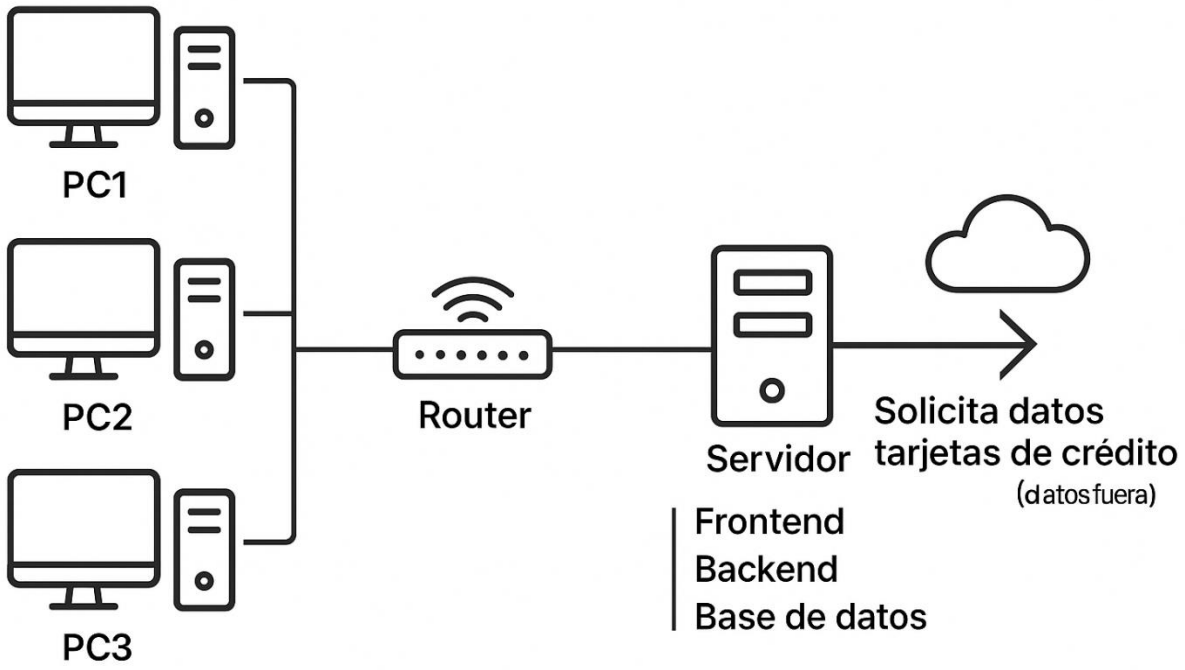


Ilustración 15 Diseño de la arquitectura física.

Fuente: elaboración propia.

9.1.10 Procesos de Continuidad y Contingencia

El sistema implementa un proceso de backup manual de MySQL que permite backup completo de la base de datos, Backup de solo esquema y verificación de integridad.

El proceso de contingencia permite una recuperación completa de base de datos desde backup, Reinstalación rápida del sistema aplicativo y una migración a servidor alterno en caso de falla del principal.

9.1.10.1 Script Principal de Backup:

```
# backup-manual.ps1 - Script de backup manual MySQL

param(

    [string]$BackupType = "full",  # full, schema, incremental

    [string]$BackupPath = "E:\Backups\Antifraud",

    [string]$MySQLUser = "antifraud_user",

    [string]$MySQLPassword = "TuPasswordSeguro123!",

    [switch]$VerifyIntegrity = $true

)



# Crear directorio de backup con timestamp

$Timestamp = Get-Date -Format "yyyyMMdd_HHmmss"

$BackupDir = "$BackupPath\$BackupType`_$Timestamp"

New-Item -ItemType Directory -Path $BackupDir -Force
```

```
try {
    switch ($BackupType) {
        "full" {
            # Backup completo de la base de datos
            $BackupFile = "$BackupDir\antifraud_full_$Timestamp.sql"
            & "C:\Program Files\MySQL\MySQL Server 8.0\bin\mysqldump.exe" `
                -u $MySQLUser -p$MySQLPassword `
                --single-transaction `
                --routines `
                --events `
                --triggers `
                --complete-insert `
                antifraud_db > $BackupFile

            Write-Host "Backup completo creado: $BackupFile" -ForegroundColor Green
        }
```

```
"schema" {
    # Backup solo del esquema (estructura)
    $BackupFile = "$BackupDir\antifraud_schema_$Timestamp.sql"
    & "C:\Program Files\MySQL\MySQL Server 8.0\bin\mysqldump.exe" `
        -u $MySQLUser -p$MySQLPassword `
        --no-data `
        --routines `
        --events `
        --triggers `
        antifraud_db > $BackupFile

    Write-Host "Backup de esquema creado: $BackupFile" -ForegroundColor Green
}

"incremental" {
    # Backup incremental de tablas transaccionales
```

```
        $BackupFile = "$BackupDir\antifraud_incremental_$Timestamp.sql"
        & "C:\Program Files\MySQL\MySQL Server 8.0\bin\mysqldump.exe" `
            -u $MySQLUser -p$MySQLPassword `
            --single-transaction `
            --where="fecha_trx > DATE_SUB(NOW(), INTERVAL 24 HOUR)" `
            antifraud_db transaccion transaccion_evaluar casos > $BackupFile

        Write-Host "Backup incremental creado: $BackupFile" -ForegroundColor Green
    }
}

# Verificar integridad del backup
if ($VerifyIntegrity) {
    $FileSize = (Get-Item $BackupFile).Length
    if ($FileSize -gt 1024) {  # Mayor a 1KB
        Write-Host "✓ Integridad del backup verificada ($([math]::Round($FileSize/1MB,2)) MB)" -ForegroundColor Green
```

```
        } else {
            Write-Host "✗ El archivo de backup parece estar vacío o corrupto" -ForegroundColor
Red
        }
    }

    # Registrar en log de operaciones
    $LogEntry = "$(Get-Date -Format 'yyyy-MM-dd HH:mm:ss') - Backup $BackupType
completado: $BackupFile"
    Add-Content -Path "C:\AntifraudSystem\logs\backup.log" -Value $LogEntry

} catch {
    Write-Host "Error durante el backup: $($_.Exception.Message)" -ForegroundColor Red
    Add-Content -Path "C:\AntifraudSystem\logs\backup-error.log" -Value "$(Get-Date -Format
'yyyy-MM-dd HH:mm:ss') - ERROR: $($_.Exception.Message)"
}
```

9.1.10.2 Ejecución de Backup Manual

```
# Ejemplos de uso:

# Backup completo (recomendado para fines de semana)

.\backup-manual.ps1 -BackupType full -BackupPath "E:\Backups\Antifraud"



# Backup de esquema (rápido, para desarrollo)

.\backup-manual.ps1 -BackupType schema -BackupPath "E:\Backups\Antifraud"



# Backup incremental (diario, solo transacciones recientes)

.\backup-manual.ps1 -BackupType incremental -BackupPath "E:\Backups\Antifraud"
```

9.1.10.3 Proceso de recuperación:

```
# 1. Identificar el backup más reciente

Get-ChildItem "E:\Backups\Antifraud" -Filter "*.sql" | Sort-Object LastWriteTime -Descending |

Select-Object -First 5

# 2. Ejecutar recuperación
```

.\restore-database.ps1 -BackupFile

"E:\Backups\Antifraud\full_20241215_143022\antifraud_full_20241215_143022.sql"

9.1.10.4 Beneficios de esta implementación

Nivel	Beneficio
Integridad de los datos	Backup consistente transaccional.
Disponibilidad	Recuperación menor a 30 minutos.
Confidencialidad	Backups en ubicación segura.
Auditoria	Mantiene trazabilidad de las operaciones.

Ilustración 16 Beneficios de implementación de recomendaciones para contingencia.

Fuente: Elaboración propia.

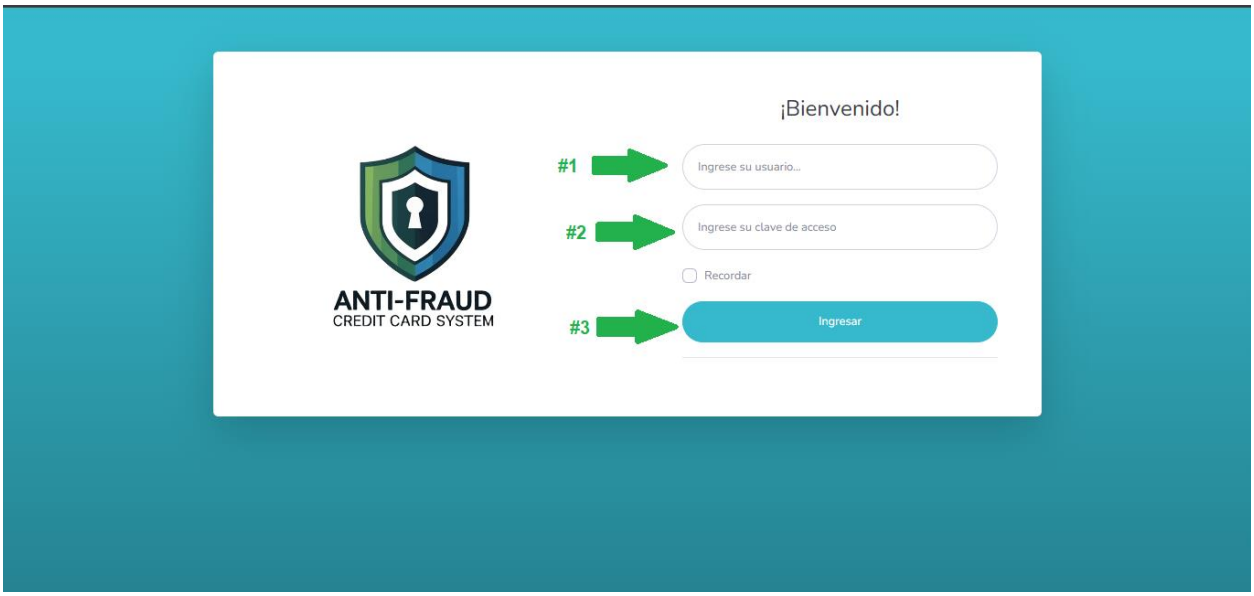
9.1.10.5 Consecuencias de la omisión de este plan de contingencia

De omitirse este plan de contingencia se está expuesto a la perdida de datos, tiempos de inactividad largos durante la recuperación, lo que provoca tiempos de inactividad mientras finaliza el proceso de recuperación. La consecuencia de esto puede incurrir en fraude concretado con tarjeta de crédito mientras el sistema no está en funcionamiento.

9.2 MANUAL DE USUARIO

9.2.1 MANUAL DE USUARIO PARA ADMINISTRADORES

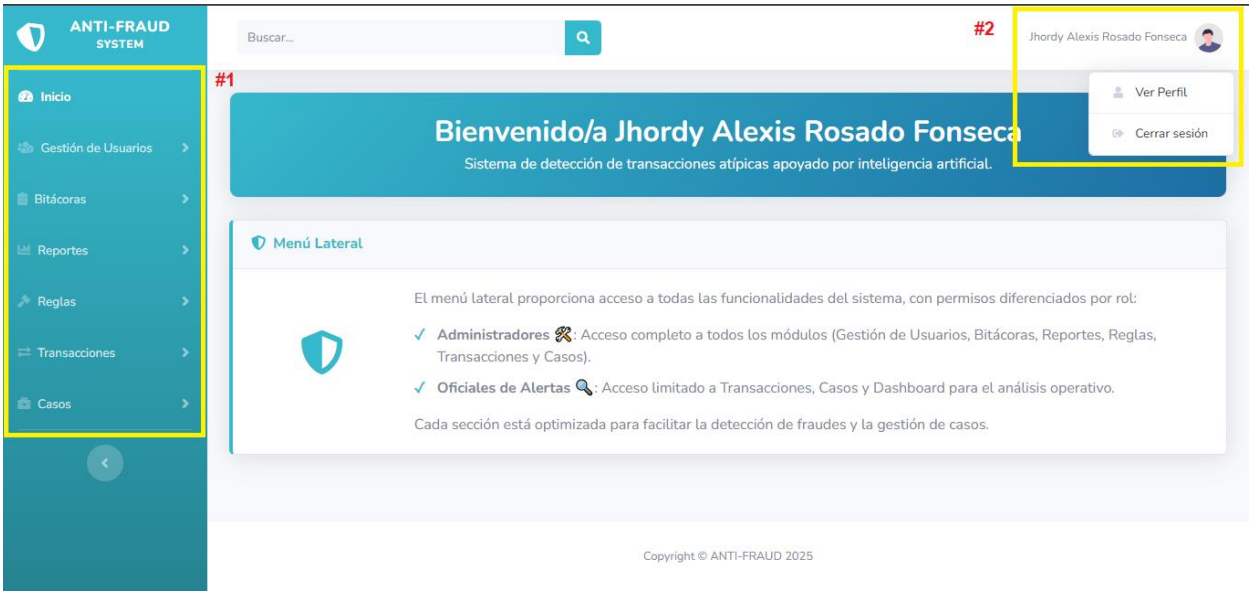
9.2.1.1 Inicio de sesión



Para poder ingresar debe contar con un usuario y contraseña válidos y activos registrados previamente en la base de datos por el proveedor del sistema o por otro usuario administrador.

1. Campo donde debe ingresar su usuario.
2. Campo donde debe ingresar su contraseña.
3. Una vez ingresado su usuario y contraseña debe dar clic en el botón “Ingresar” para poder acceder al sistema (tiene la posibilidad de recordad sus credenciales dando clic en “Recordar” justo arriba del botón “Ingresar”).

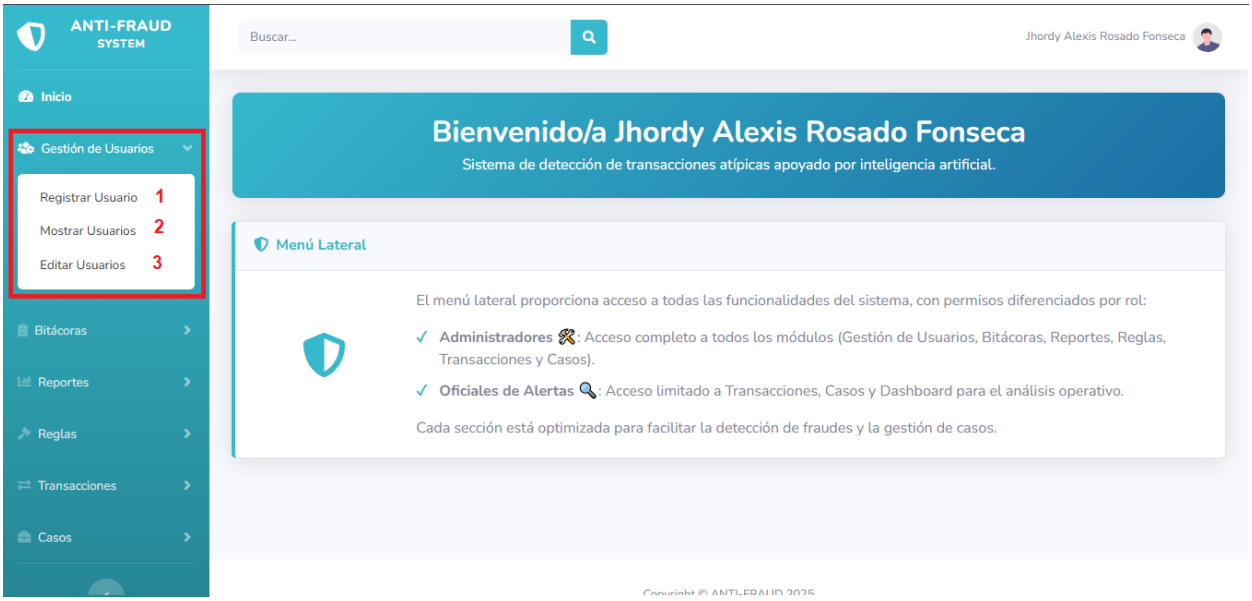
9.2.1.2 Pantalla Principal



Esta es la primera pantalla que observará al ingresar al sistema, cuenta con un mensaje de bienvenida al sistema, así como una pequeña explicación del menú lateral izquierdo.

1. Menú lateral: este es el menú principal que sirve para acceder a todas las funcionalidades del sistema, organizadas por similitudes entre funcionalidades para facilitar el uso.
2. Perfil: desde esta sección puede acceder a ver la información de su perfil desde la opción “Ver Perfil” o en su defecto salir del sistema dando clic en “Cerrar sesión”.

9.2.1.3 Gestión de Usuarios

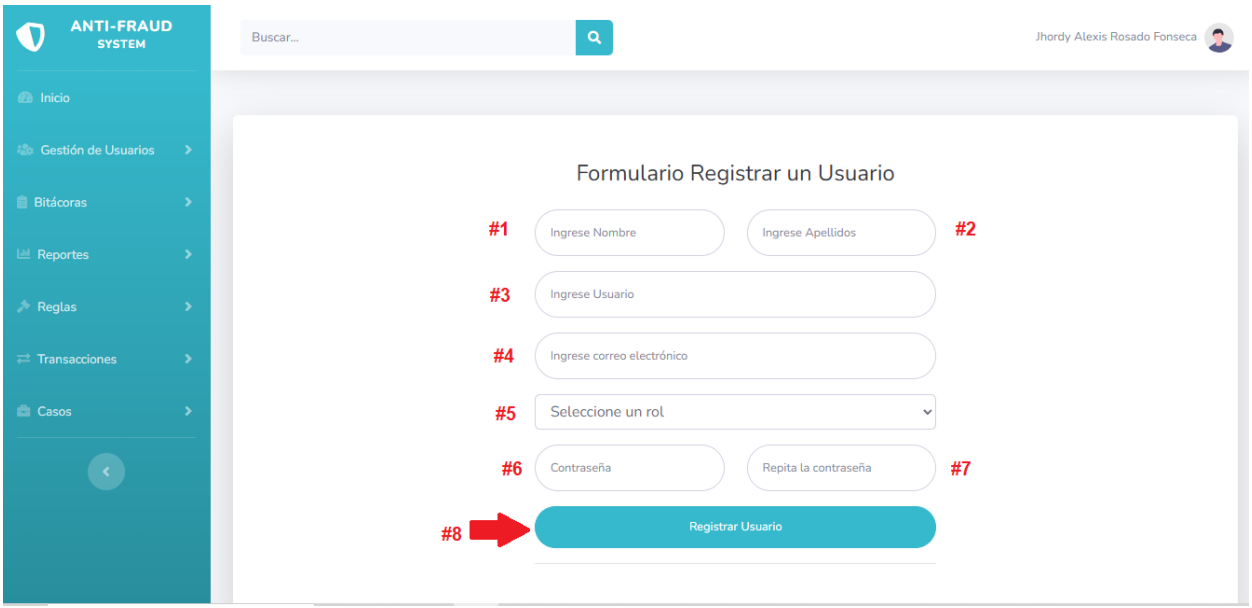


Dando clic en la opción del menú lateral “Gestión de Usuarios” tiene la posibilidad de ingresar a tres módulos:

1. Registra Usuario
2. Mostrar Usuarios
3. Editar Usuarios

A continuación, en la siguiente sección se explica cada uno de ellos.

9.2.1.4 Registrar Usuario

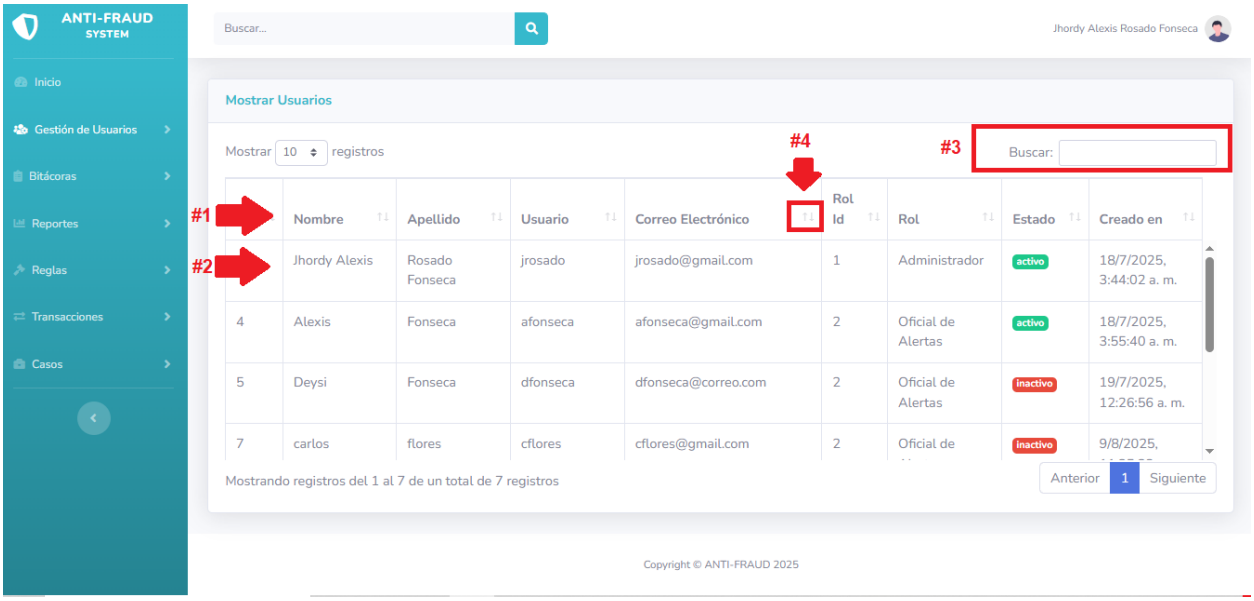


Una vez haya ingresado al módulo de "Registrar Usuario" debe llenar los siguientes campos:

1. Nombre(s) del nuevo usuario del sistema.
2. Apellido(s) del nuevo usuario del sistema.
3. Un usuario que no haya sido registrado en el sistema, ya que con este se podrá ingresar al posteriormente (si coloca un usuario ya registrado el formulario no le permitirá volver a registrarlo).
4. Correo electrónico del nuevo usuario.
5. Aquí se le despliegan dos opciones para los roles que tendrá el nuevo usuario, puede elegir entre administrador (con todos los privilegios del sistema) u oficial de alertas (con acceso limitado a la atención de alertas y atención de casos).
6. Espacio para la contraseña del usuario.
7. Espacio para repetir la contraseña y así evitar errores al escribirla.

8. Una vez ingresados todos los campos obligatorios pueda dar clic en el botón “Registrar Usuario” para completar el proceso y el nuevo usuario quede registrado en el sistema.

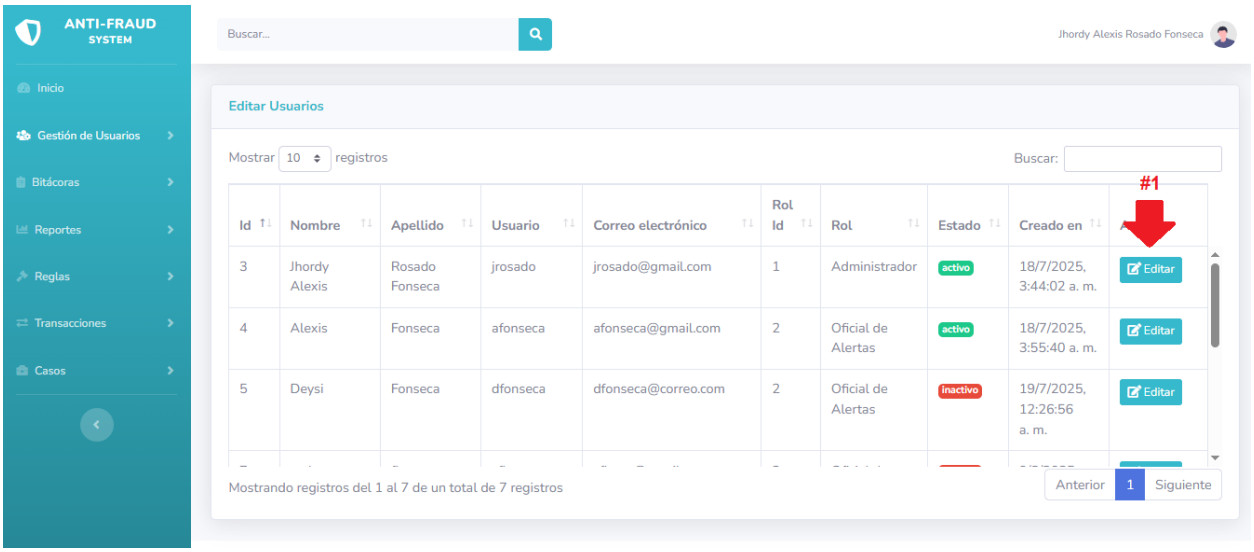
9.2.1.5 Mostrar Usuarios



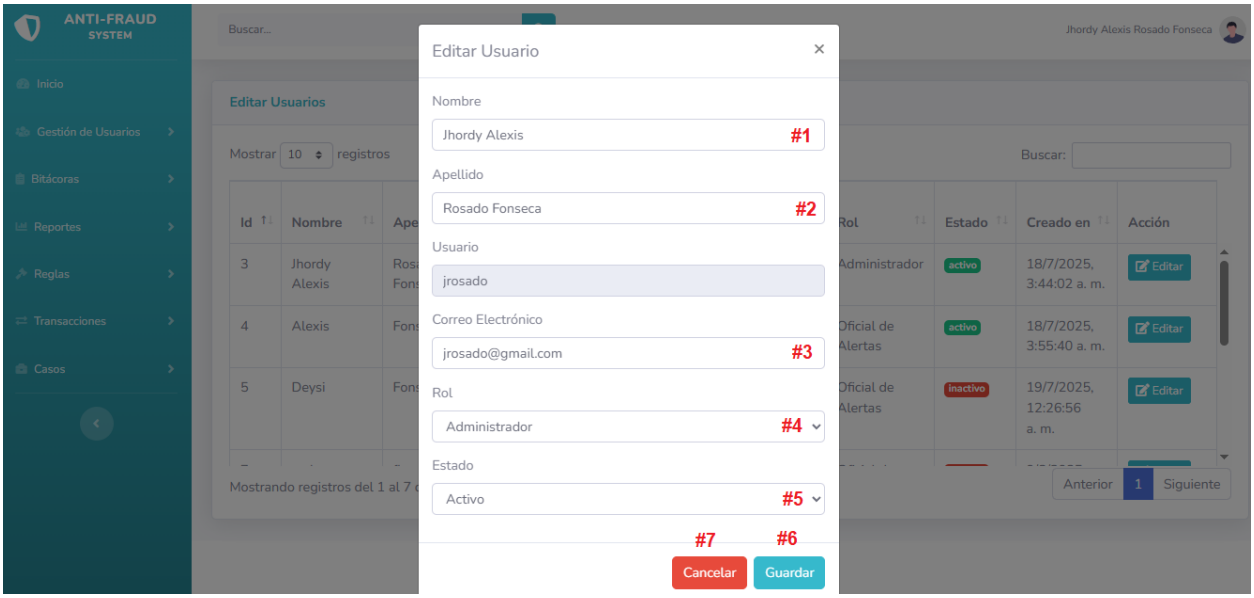
En este módulo se puede observar toda la información de los usuarios registrados en el sistema.

1. Estos son los encabezados o columnas de la información de los usuarios, por ejemplo: Id, nombre, apellido, correo electrónico, rol, estado y fecha de creación.
2. Registros: información de cada uno de los usuarios ordenada en filas.
3. Espacio para buscar, donde puede escribir una búsqueda personalizada de la información en la tabla de usuarios.
4. Mediante este icono tiene la posibilidad de ordenar cada encabezado o columna de manera descendente o ascendente.

9.2.1.6 Editar Usuarios



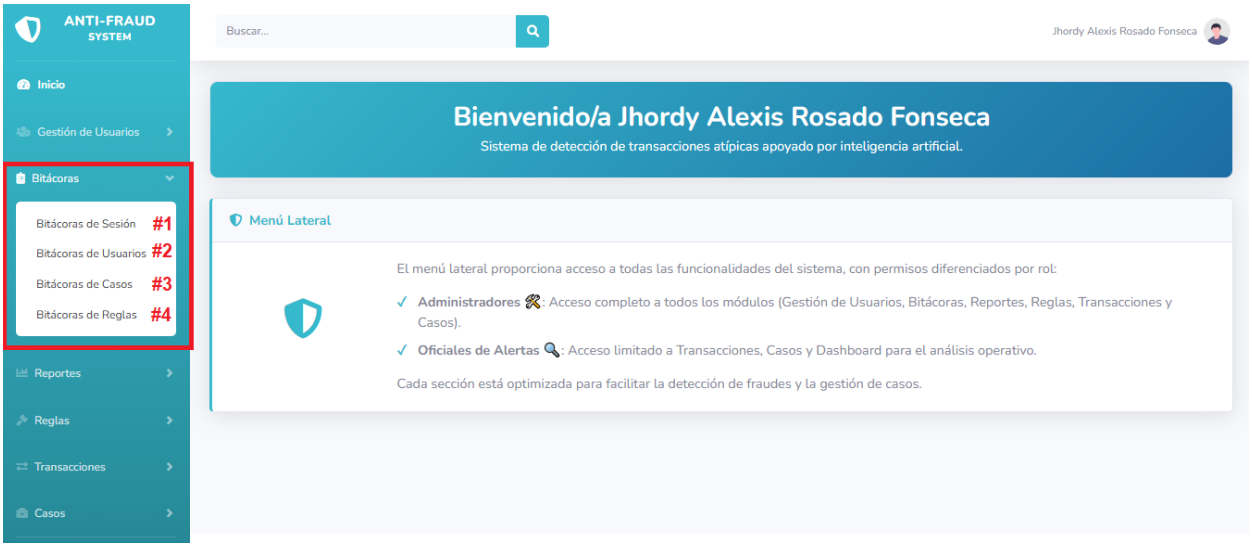
En este módulo tiene la misma posibilidad de ver y organizar la tabla de usuarios tal y como lo hace el módulo de “Mostrar Usuarios”, pero un nuevo botón (#1) llamado “Editar” que le permite modificar la información de cada usuario.



Una vez se da clic en el botón “Editar” se le despliega este formulario donde tiene la posibilidad de modificar los siguientes campos de cada usuario.

1. Modificar nombre(s) de usuario.
2. Modificar apellido(s) de usuario.
3. Modificar correo electrónico del usuario.
4. Modificar el rol del usuario opciones entre administrador y oficial de alertas.
5. Modificar el estado del usuario activo o inactivo (si lo modifica a “inactivo” ese usuario ya no podrá acceder al sistema).
6. Una vez realizadas todas las modificaciones que el administrador estime conveniente puede guardar los cambios dando clic en “Guardar”.
7. Si decide volver atrás y no aplicar los cambios puede hacer clic en el botón “Cancelar”

9.2.1.7 Bitácoras



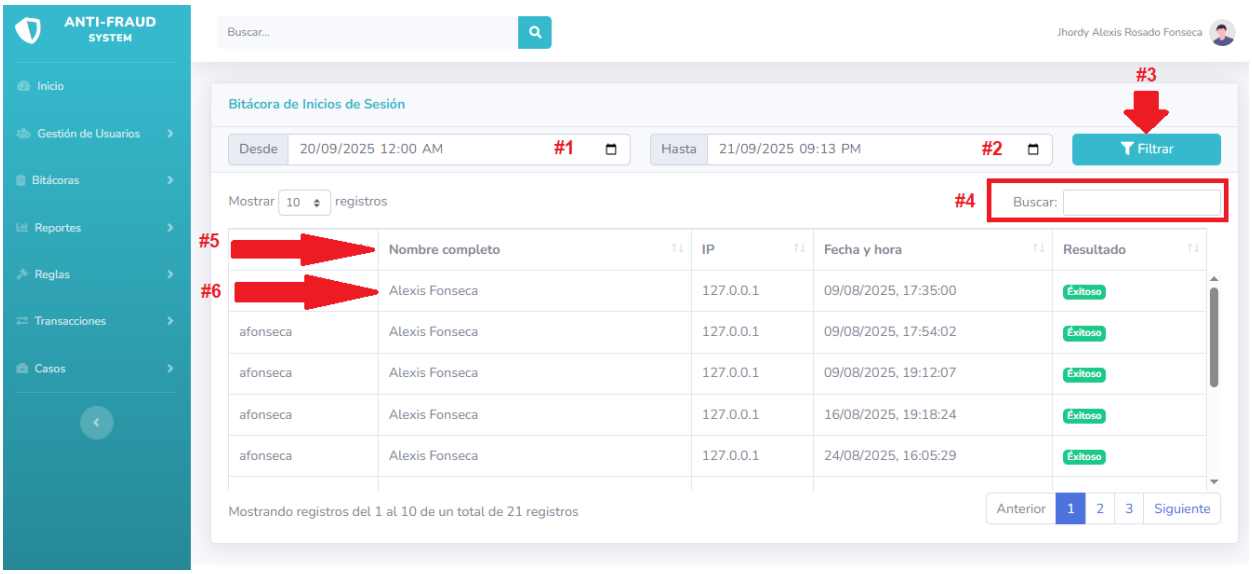
Dando clic en la opción del menú lateral “Bitácoras” tiene la posibilidad de ingresar a cuatro módulos:

1. Bitácoras de Sesión
2. Bitácoras de Usuarios

3. Bitácoras de Casos
4. Bitácoras de Reglas

A continuación, en la siguiente sección se explica cada uno de ellos.

9.2.1.8 Bitácoras de Sesión

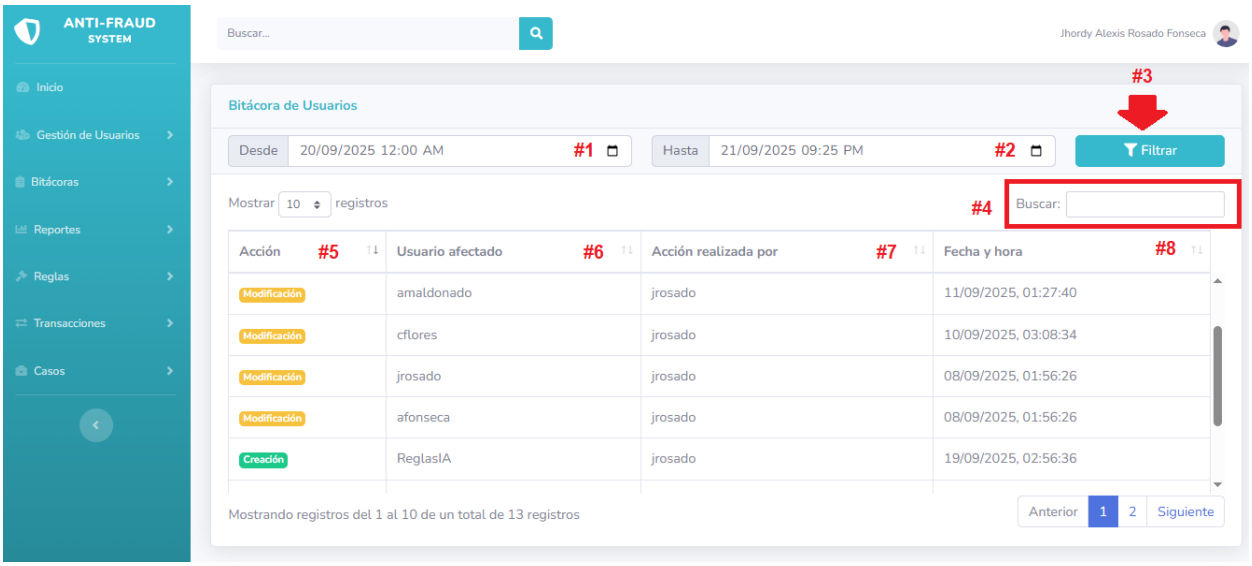


Este módulo tiene el objetivo de registrar todos los inicios de sesión, tanto los exitosos como los intentos fallidos, a continuación, se desglosan sus funcionalidades:

1. Espacio donde puede colocar una fecha y hora de inicio a filtrar.
2. Espacio donde puede colocar una fecha y hora final a filtrar.
3. Una vez haya seleccionado tanto una fecha y hora inicial como una fecha y hora final usted tiene la posibilidad de dar clic en el botón “Filtrar” para mostrar los inicios de sesión que ocurrieron en el rango de fecha y hora que usted seleccionó.
4. Espacio para una búsqueda personalizada entre todos los registros de la tabla.

5. Columnas donde se muestra la información referente a los inicios de sesión, por ejemplo, usuario que ingresó, nombre completo, dirección IP, fecha y hora del inicio de sesión y el resultado el cual puede ser exitoso o fallido.
6. Filas donde se muestran los registros del inicio de sesión.

9.2.1.9 Bitácoras de Usuarios

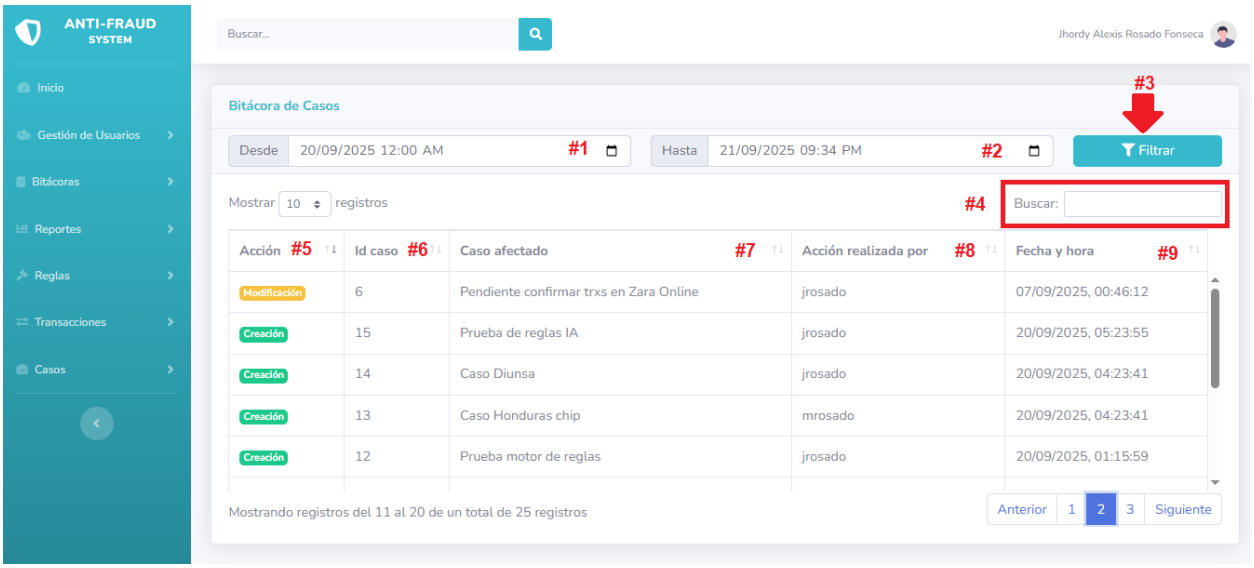


En este módulo puede observar una bitácora de todos los cambios realizados a los usuarios del sistema, se registran tanto creaciones de usuarios como modificaciones, se desglosa de la siguiente manera:

1. Misma funcionalidad que en el módulo de “Bitácoras de Sesión”
2. Misma funcionalidad que en el módulo de “Bitácoras de Sesión”
3. Misma funcionalidad que en el módulo de “Bitácoras de Sesión”
4. Misma funcionalidad que en el módulo de “Bitácoras de Sesión”
5. Columna de “Acción” aquí se registra el cambio realizado en el usuario de la fila seleccionada, se registran las creaciones o modificaciones de los usuarios del sistema.

6. Usuario afectado: se registra el nombre de usuario que fue afectado.
7. Acción realizada por: se registra el usuario del sistema que hizo la modificación al "usuario afectado".
8. Fecha y hora: para registrar el momento exacto de la creación o modificación del usuario.

9.2.1.10 Bitácoras de Casos

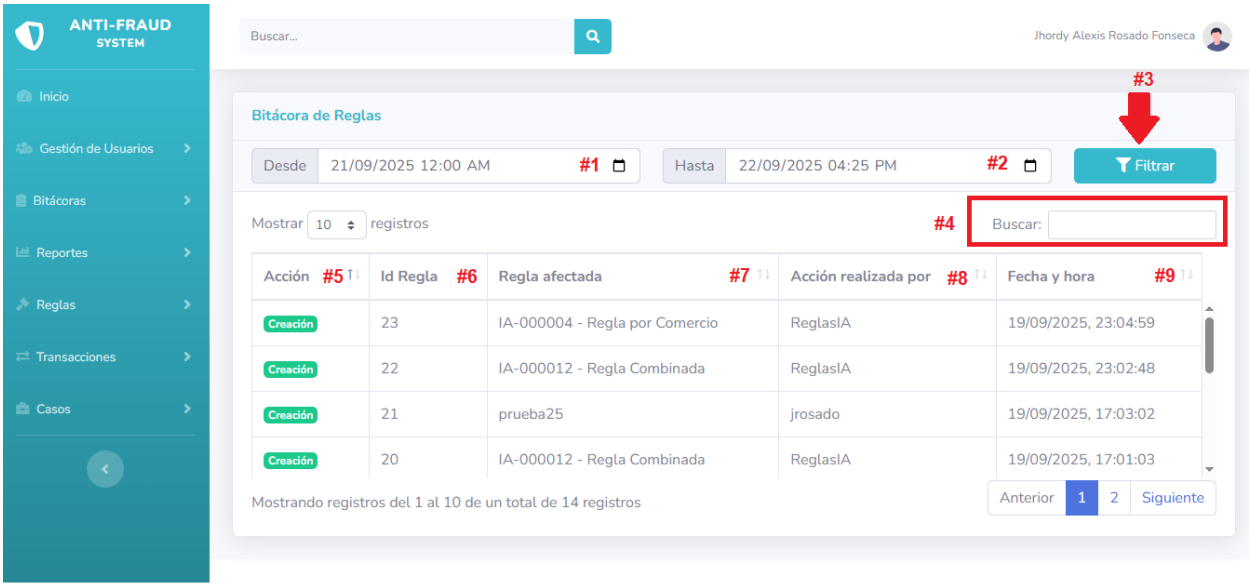


En este módulo puede observar una bitácora de todos los cambios realizados a los casos registrados en el sistema, se registran tanto creaciones como modificaciones de casos, se desglosa de la siguiente manera:

1. Misma funcionalidad que en el módulo de "Bitácoras de Sesión"
2. Misma funcionalidad que en el módulo de "Bitácoras de Sesión"
3. Misma funcionalidad que en el módulo de "Bitácoras de Sesión"
4. Misma funcionalidad que en el módulo de "Bitácoras de Sesión"

5. Columna de “Acción” aquí se registra el cambio realizado en los casos de la fila seleccionada, se registran las creaciones o modificaciones de los casos registrados en el sistema.
6. Id caso: se muestra el identificador único del caso que fue creado o modificado.
7. Caso afectado: registra el nombre del caso que fue creado o modificado.
8. Acción realizada por: muestra el usuario del sistema que realizó la creación o modificación del caso.
9. Fecha y hora: para registrar el momento exacto de la creación o modificación del caso.

9.2.1.11 Bitácora de Reglas

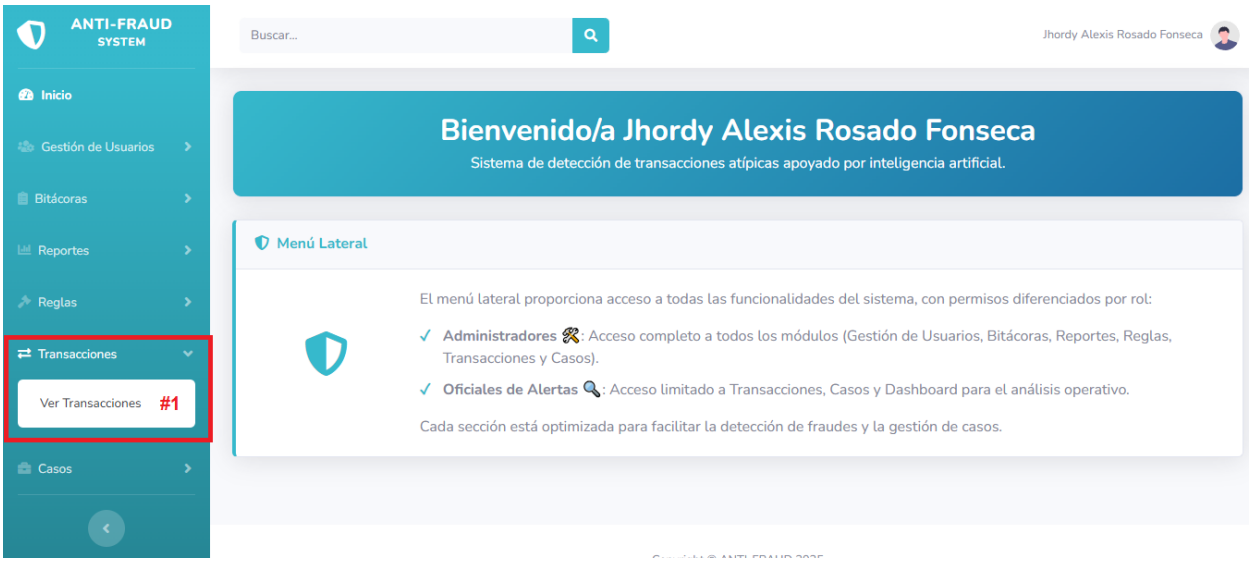


En este módulo puede observar una bitácora de todos los cambios realizados a las reglas registradas en el sistema, se registran tanto creaciones como modificaciones de reglas, se desglosa de la siguiente manera:

1. Misma funcionalidad que en el módulo de “Bitácoras de Sesión”

2. Misma funcionalidad que en el módulo de “Bitácoras de Sesión”
3. Misma funcionalidad que en el módulo de “Bitácoras de Sesión”
4. Misma funcionalidad que en el módulo de “Bitácoras de Sesión”
5. Columna de “Acción” aquí se registra el cambio realizado en la regla de la fila seleccionada, se registran las creaciones o modificaciones de las reglas registradas en el sistema.
6. Id Regla: identificador único de la regla que fue afectada.
7. Regla afectada: registra el nombre de la regla que fue creada o modificada.
8. Acción realizada por: muestra el usuario del sistema que realizó la creación o modificación de la regla.
9. Fecha y hora: para registrar el momento exacto de la creación o modificación de la regla.

9.2.1.12 Transacciones

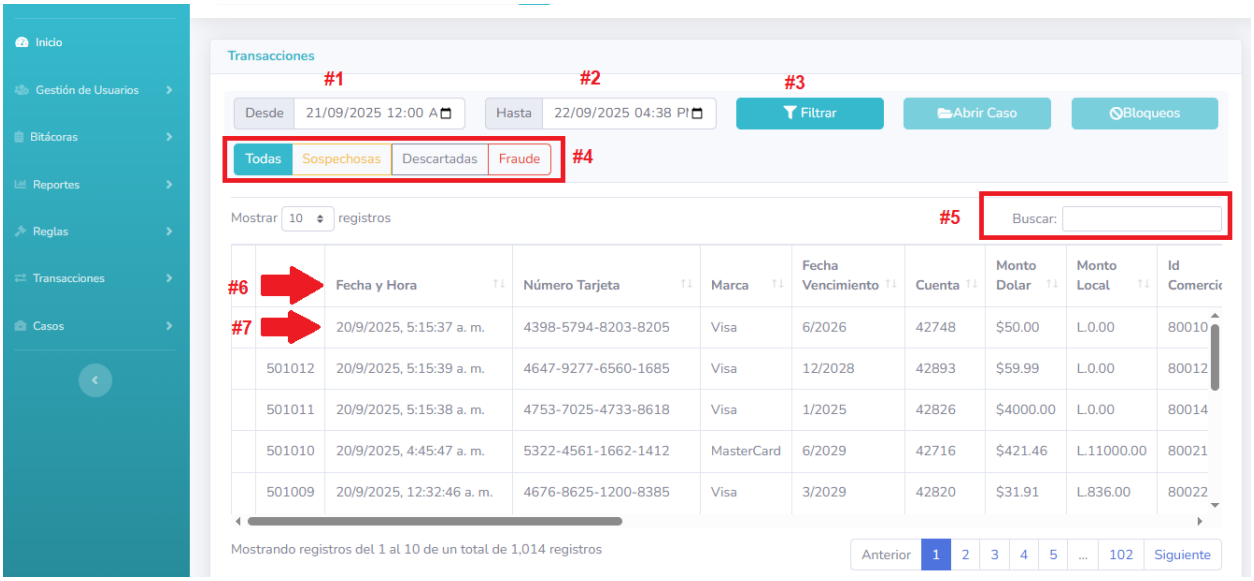


Dando clic en la opción del menú lateral “Transacciones” tiene la posibilidad de ingresar a un módulo:

1. Ver Transacciones

A continuación, en la siguiente sección se explica el funcionamiento del módulo.

9.2.1.13 Ver Transacciones



El módulo “Ver Transacciones” funciona como el apartado principal donde se registran todas las transacciones con tarjetas de crédito procesadas por la institución bancaria, aquí se registran las transacciones sospechosas, descartadas y fraude. Aquí se puede observar toda la información referente a la transacción, así como aplicar otras gestiones como abrir un caso de investigación o aplicar un bloqueo o desbloqueo a la tarjeta.

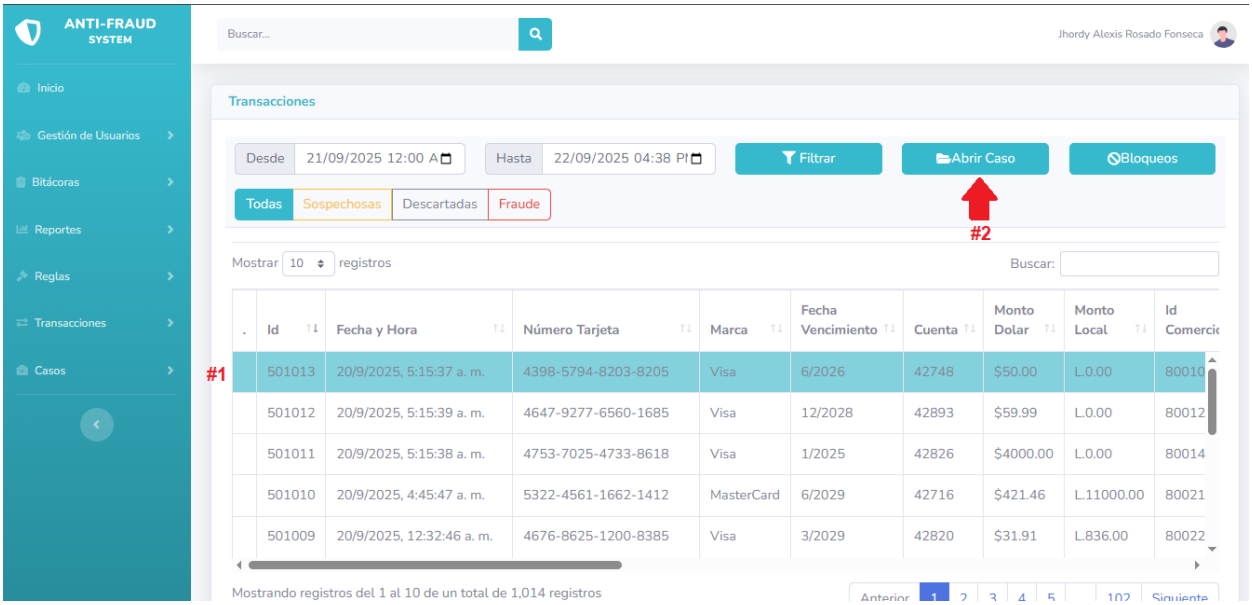
Este módulo se compone de los siguientes elementos:

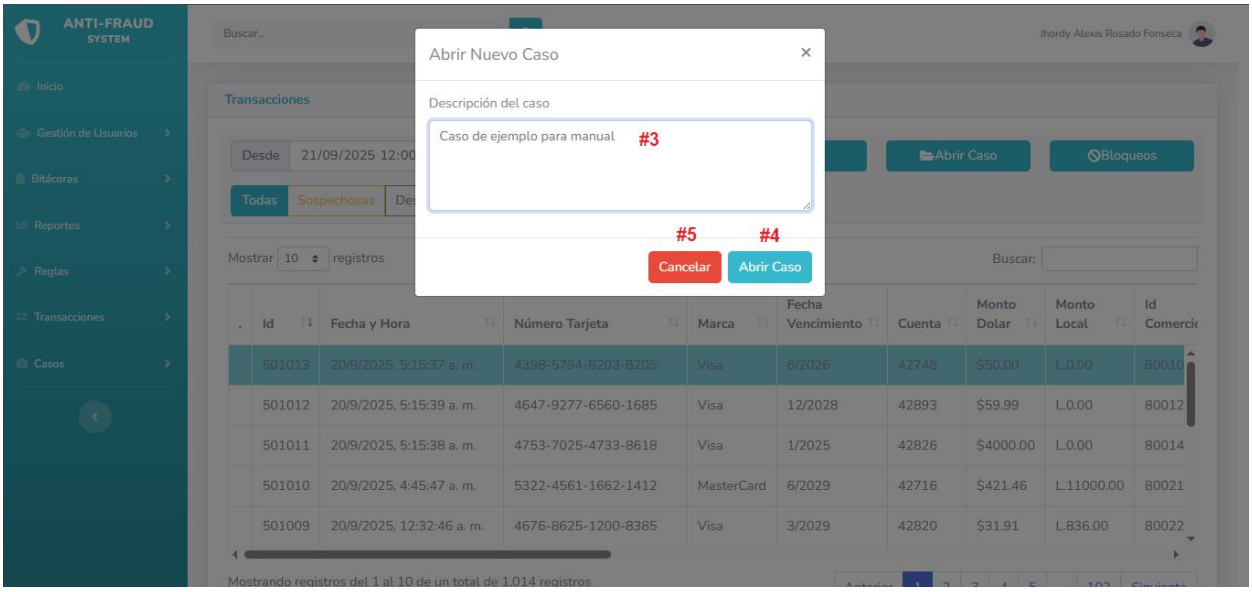
1. Misma funcionalidad que en el módulo de “Bitácoras de Sesión”
2. Misma funcionalidad que en el módulo de “Bitácoras de Sesión”
3. Misma funcionalidad que en el módulo de “Bitácoras de Sesión”

4. Filtro de transacciones por estado: los botones “Todas”, “Sospechosas”, “Descartadas” y “Fraude” permite mostrar en la tabla solo las transacciones que tengan el estado que el usuario seleccionó.
5. Misma funcionalidad que en el módulo de “Bitácoras de Sesión”
6. Columnas de la tabla transacciones: todos los campos relevantes de una transacción, se encuentran elementos como: número de tarjeta, fecha de vencimiento, comercio, país, monto dólar, monto local, cuenta, estado de la tarjeta de crédito, estado de la transacción, etc.
7. Filas de la tabla transacciones: donde se registra la información de cada transacción.

A continuación, se muestras más funcionalidades de este módulo de ver transacciones.

9.2.1.13.1 Abrir un caso de investigación

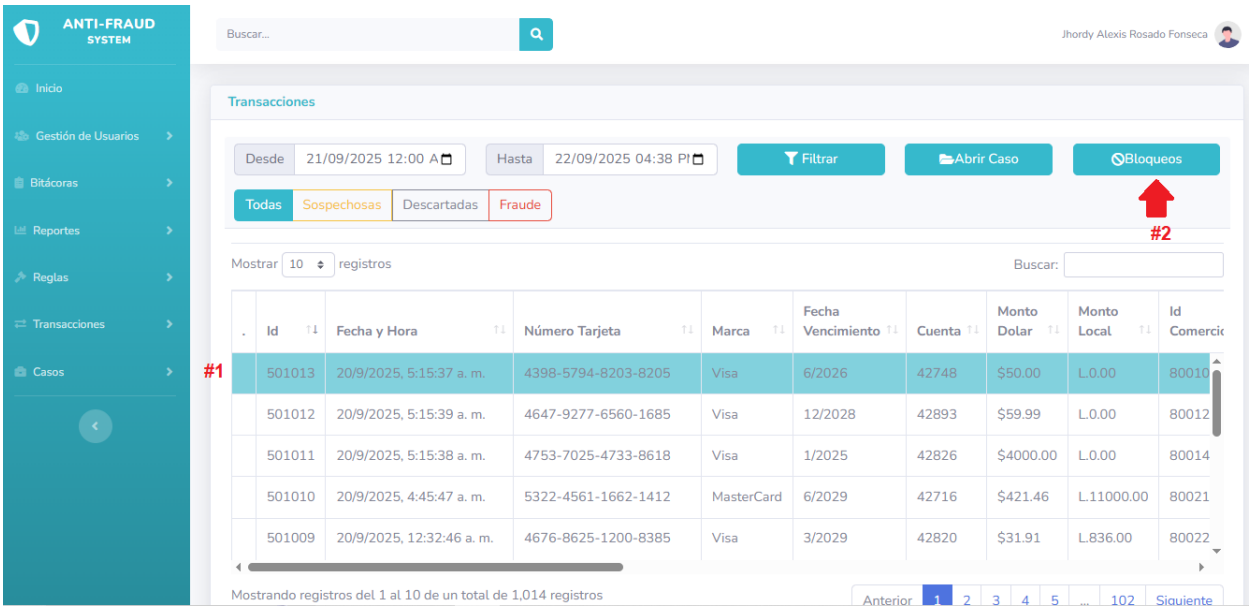


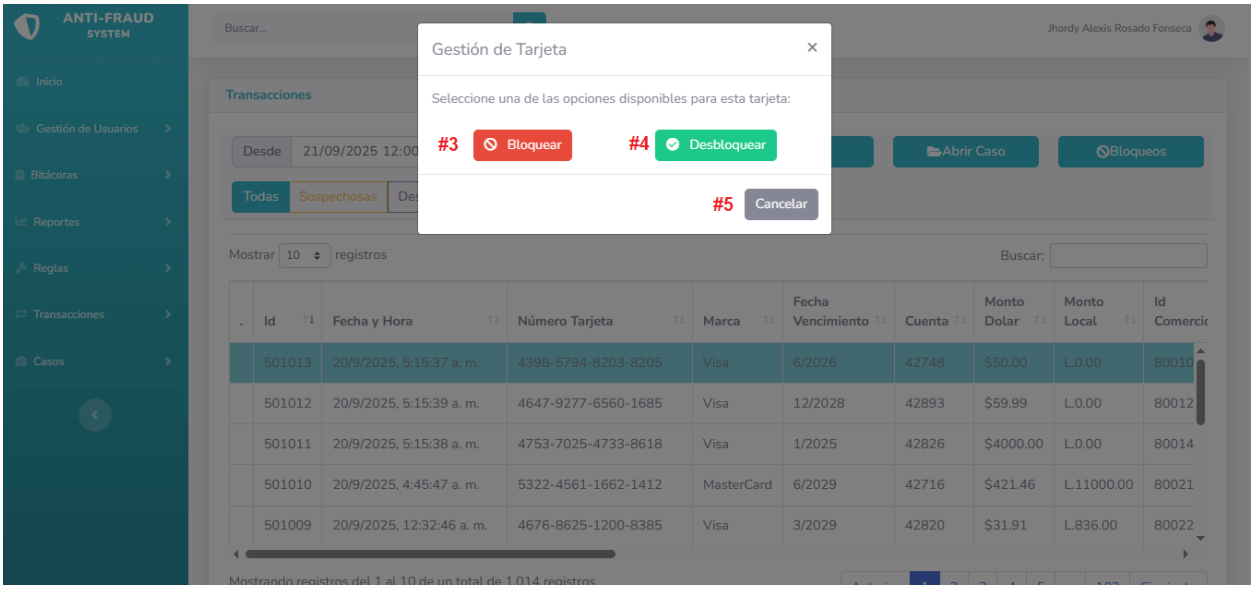


Para abrir un caso de investigación se necesita seguir los siguientes pasos:

1. Se debe seleccionar una o más transacciones que el usuario del sistema estime que necesiten ser investigadas, en general se abren casos de investigación por transacciones que tienen un estado “Sospechosa”.
2. Una vez seleccionada(s) la(s) transacción(es) se puede abrir un caso de investigación y poder gestionar de mejor manera esa investigación, para ello se da clic en el botón “Abrir Caso”.
3. En este punto se debe desplegar un apartado para colocarle un texto descriptivo al caso, ese texto debe describir características relevantes del caso, por ejemplo: “Caso de investigación por compras en Panamá en comercio Apple”.
4. Una vez tengamos la descripción del caso procedemos a guardarlo dando clic en “Abrir Caso”.
5. Botón para cancelar el proceso.

9.2.1.13.2 Bloqueos de tarjetas

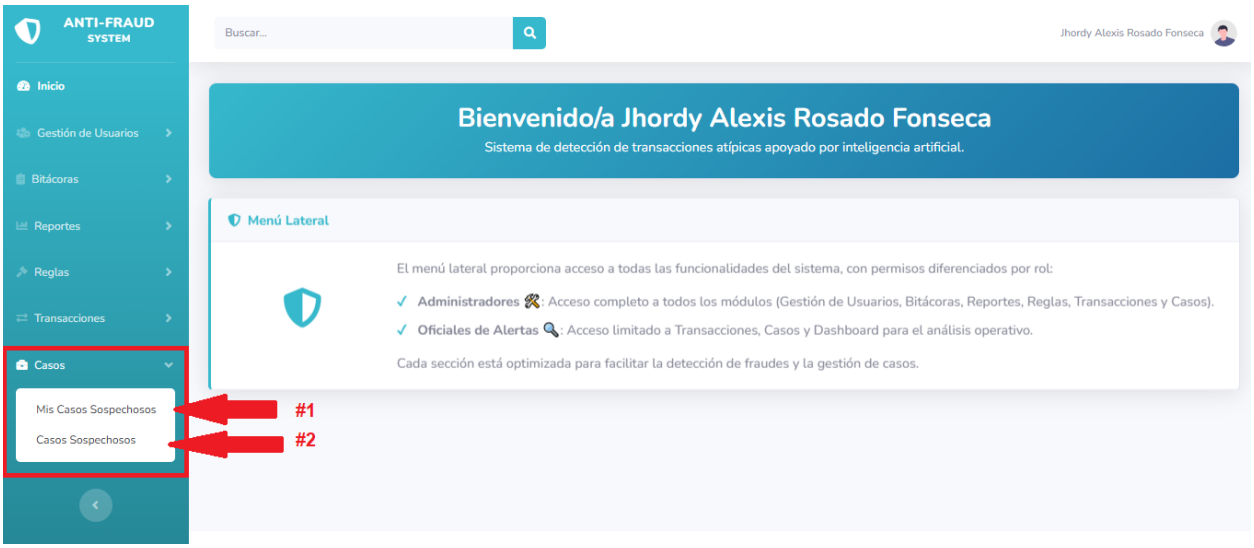




1. Para aplicar un bloqueo o desbloqueo de tarjeta de crédito primero se debe seleccionar una transacción dando clic en la fila correspondiente a la misma.
2. Posteriormente se da clic en el botón “Bloqueos”

3. En este punto se despliega un submenú que permite seleccionar una opción para la tarjeta seleccionada, si da clic en “Bloquear” a la tarjeta se le aplicaría un bloqueo preventivo lo que es útil cuando se tiene un caso de investigación por transacciones sospechosas.
4. Este botón sirve para desbloquear la tarjeta de crédito seleccionada, útil cuando el oficial de alertas ya contactó al tarjetahabiente y confirmó que las transacciones sospechosas fueron realizadas por él.
5. Cancela todo el proceso de bloqueo o desbloqueo.

9.2.1.14 Casos



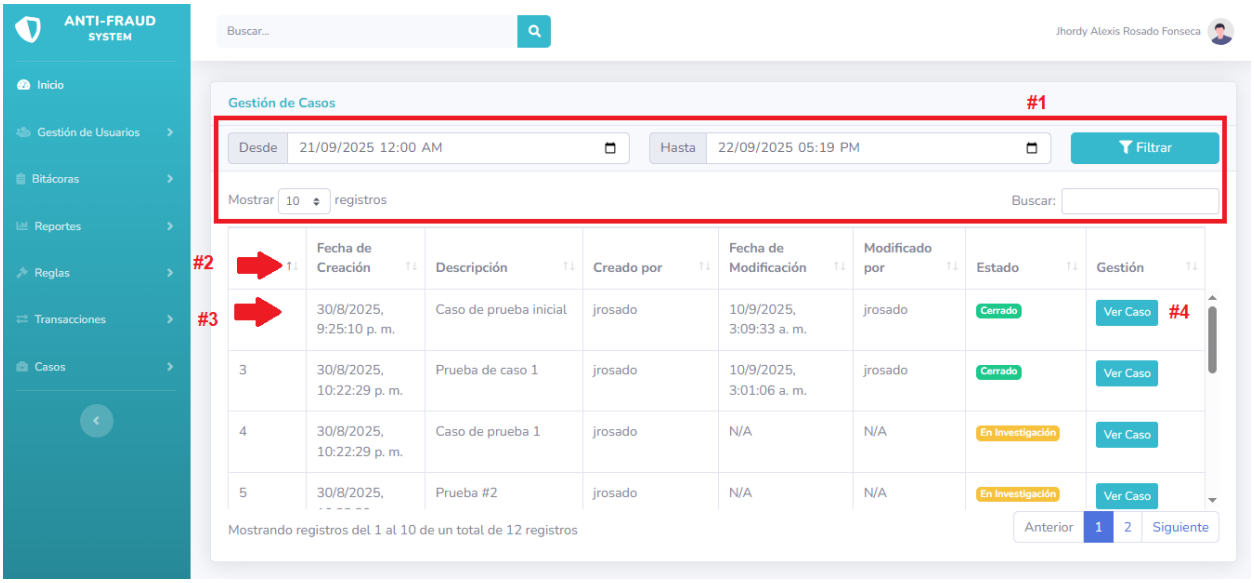
Dando clic en la opción del menú lateral “Casos” tiene la posibilidad de ingresar a dos módulos:

1. Mis casos Sospechosos
2. Casos Sospechosos

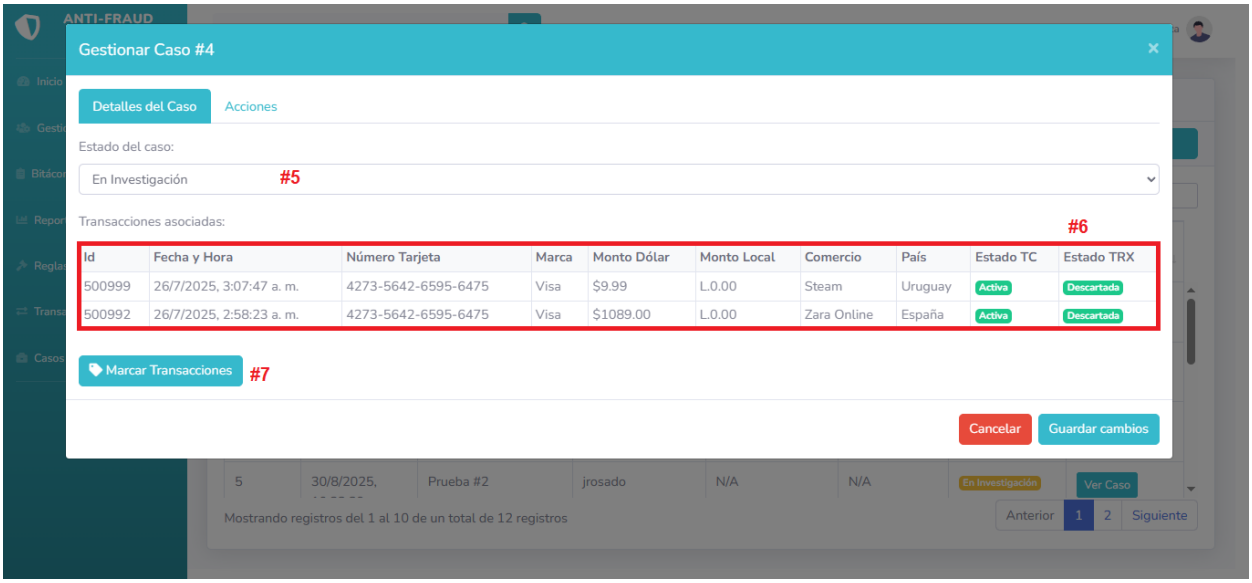
A continuación, en la siguiente sección se explica el funcionamiento de cada uno de ellos.

9.2.1.15 Mis Casos Sospechosos

Este es el módulo principal para gestionar todos los casos de investigación que se abrieron previamente desde el módulo de “Ver Transacciones”, se especifica que en este módulo solo se observan los casos que el usuario conectado al sistema ha creado, para ver todos los casos registrados incluyendo lo de los demás usuarios se puede utilizar el módulo de “Casos Sospechoso”.

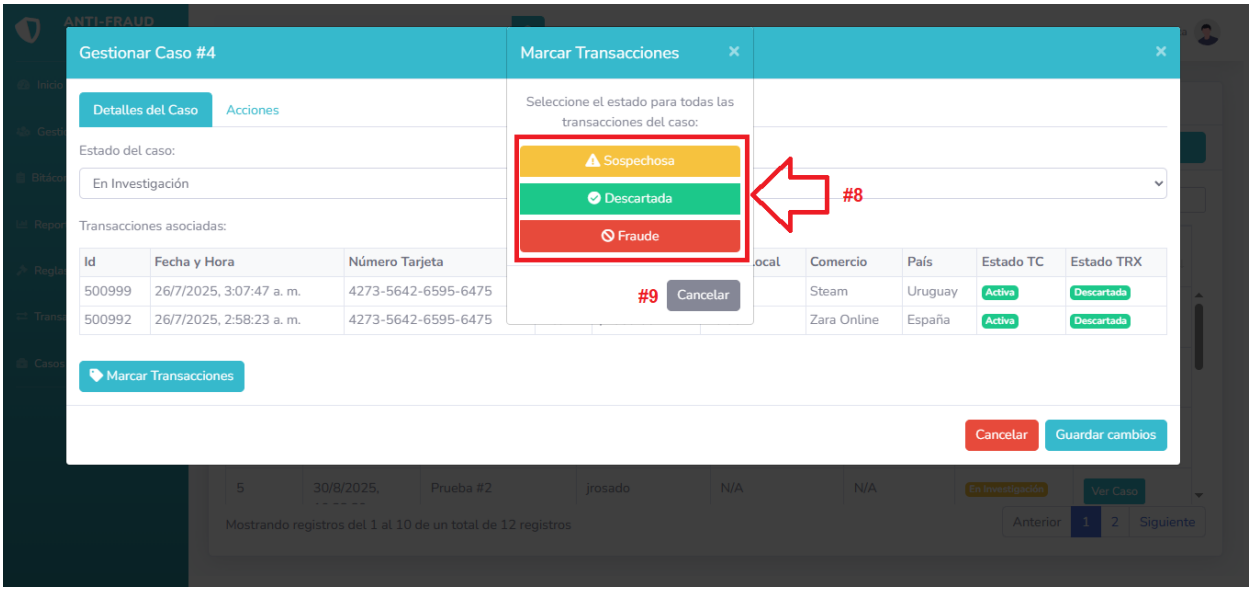


1. Opciones de filtrado que han sido explicado en módulos anteriores, puede dirigirse a la explicación del módulo “Bitácoras” para más detalles.
2. Columnas de la tabla Casos: aquí se observan columnas relevantes de los casos registrados en el sistema, por ejemplo: identificador del caso, fecha de creación, usuario de creación, fecha de modificación y usuario de modificación, así como también el estado del caso que puede ser “En investigación” o “Cerrado”.
3. Filas donde se puede ver la información de cada caso.
4. Botón de “Ver Caso” que sirve para ver todos los detalles del caso de investigación.

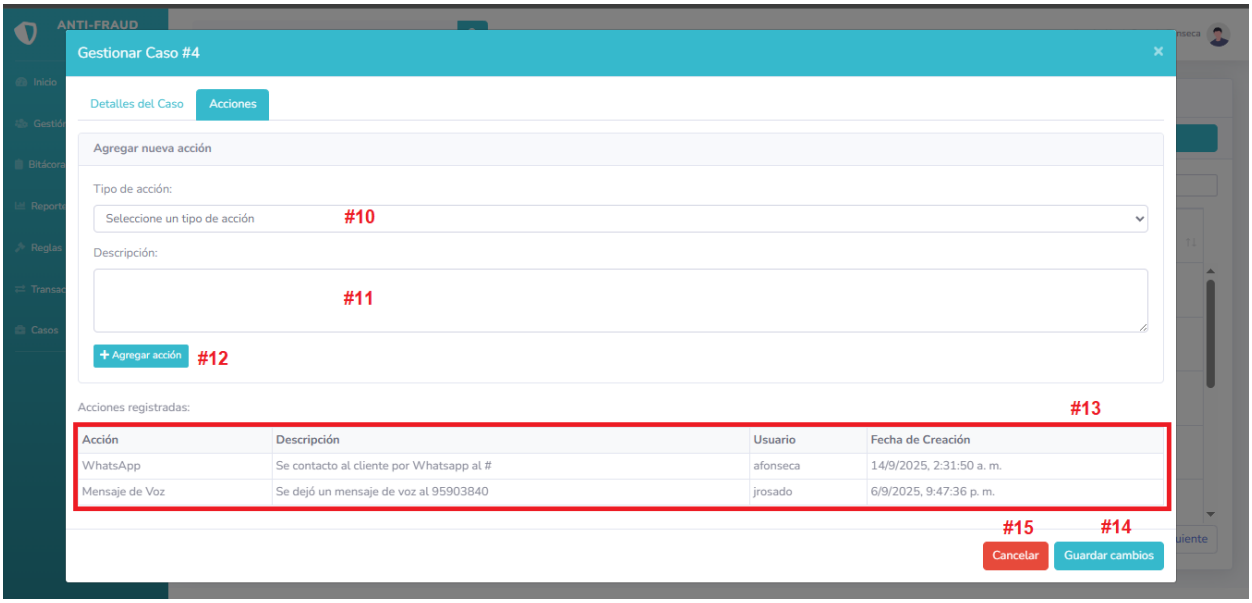


Una vez que haya dado clic en “Ver Caso” se despliega la siguiente pantalla con dos pestañas: “Detalles del caso” y “Acciones”

5. Menú desplegable de opciones que permite cambiar el estado del caso, puede ser “En investigación” o “Cerrado”.
6. Tabla donde se muestran todas las transacciones asociadas al caso en investigación.
7. Botón que sirve para cambiar el estado de las transacciones.



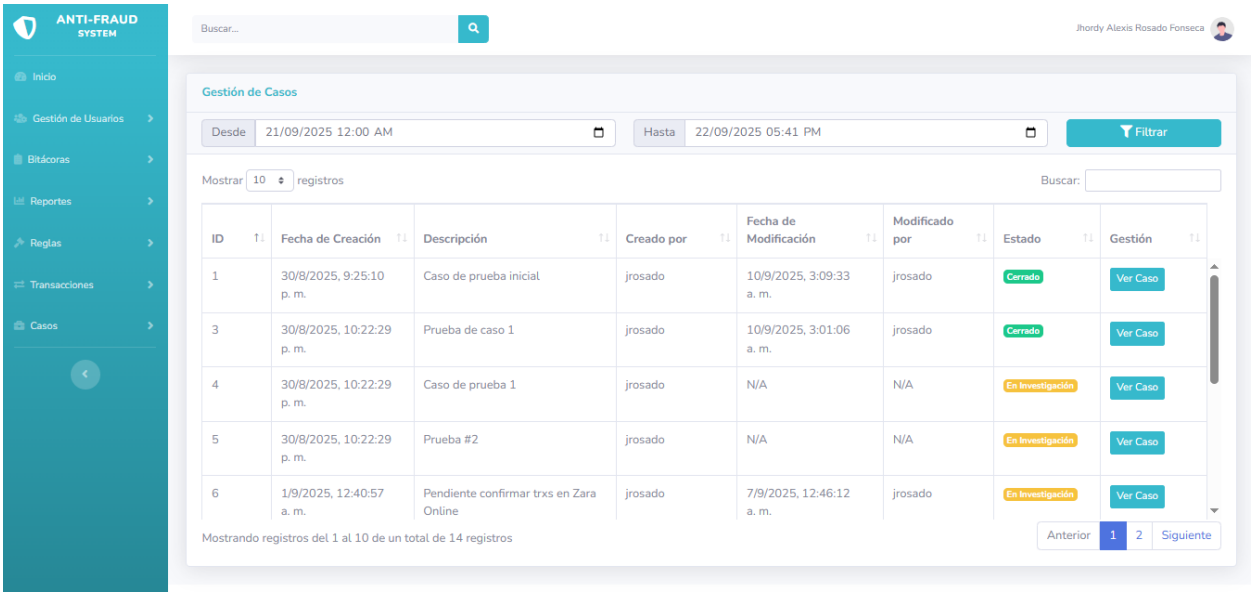
8. Una vez que haya dado clic en “Marcar Transacciones” se despliega una pequeña pantalla donde puede seleccionar el nuevo estado de la transacción, puede elegir entre: sospechosa, descartada y fraude, este estado dependerá de la resolución que el oficial de alertas le dio al caso.
9. Botón para cancelar todo el proceso.



Si vamos a la pestaña de “Acciones” tenemos la posibilidad de registrar una pequeña bitácora de acciones realizadas por el oficial de alertas, aquí se puede registrar el seguimiento que se le dio al caso, por ejemplo, llamadas realizadas, SMS, mensajes de WhatsApp, etc. Así como también puede servir como una sección de notas recordatorias para el oficial de alertas.

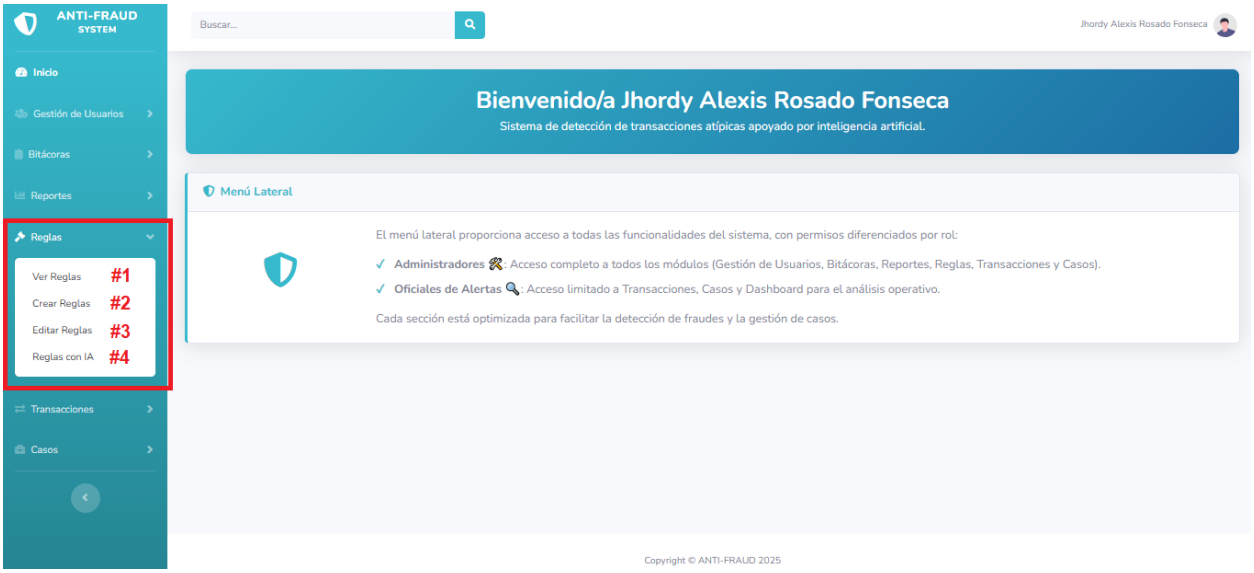
10. Menú desplegable que permite seleccionar una acción, por ejemplo: llamadas realizadas, SMS, mensajes de WhatsApp, etc.
11. Espacio donde el oficial puede escribir en esa acción, por ejemplo: registrar el número de teléfono del cliente u otra nota útil para el seguimiento del caso.
12. Botón “Agregar acción” para guardar los cambios realizados en esa acción en específico.
13. Pequeña tabla de todas las acciones registradas en el caso de investigación.
14. Botón de “Guardar” para registrar todos los cambios realizados en el caso.
15. Cancelar todo el proceso.

9.2.1.16 Casos Sospechosos



Este es el módulo principal para gestionar todos los casos de investigación que se abrieron previamente desde el módulo de “Ver Transacciones”, se conservan todas las funcionalidades de “Mis Casos Sospechosos”, en este módulo a diferencia del módulo de “Mis Casos Sospechoso” se pueden ver todos los casos registrados en el sistema, incluyendo los creados por los demás usuarios.

9.2.1.17 Reglas

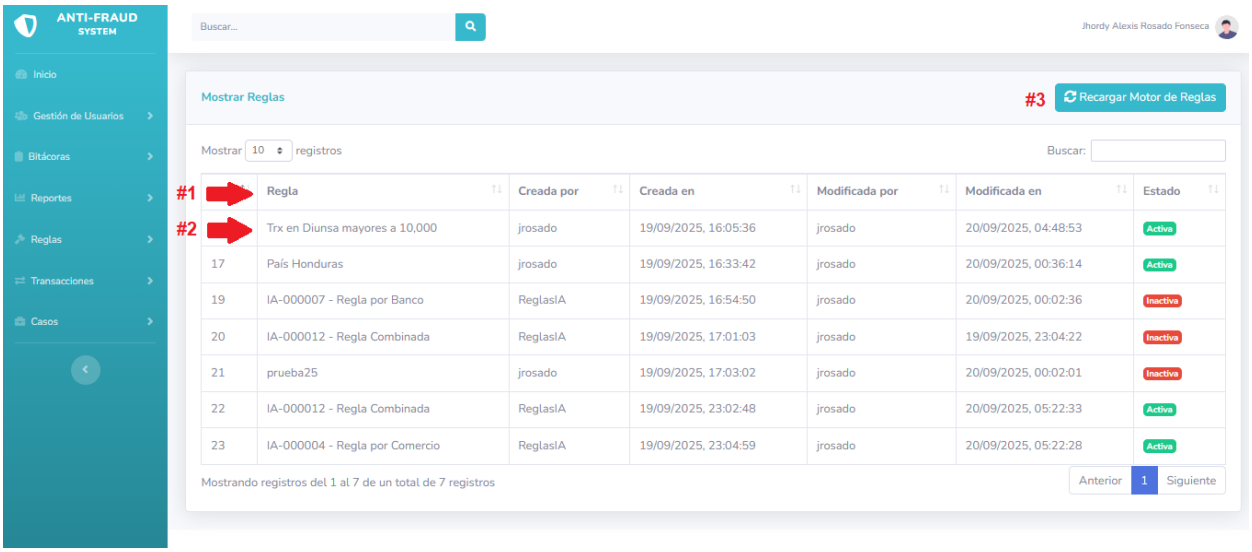


Dando clic en la opción del menú lateral “Reglas” tiene la posibilidad de ingresar a cuatro módulos:

1. Ver Reglas
2. Crear Reglas
3. Editar Reglas
4. Reglas con IA

A continuación, en la siguiente sección se explica el funcionamiento de cada uno de ellos.

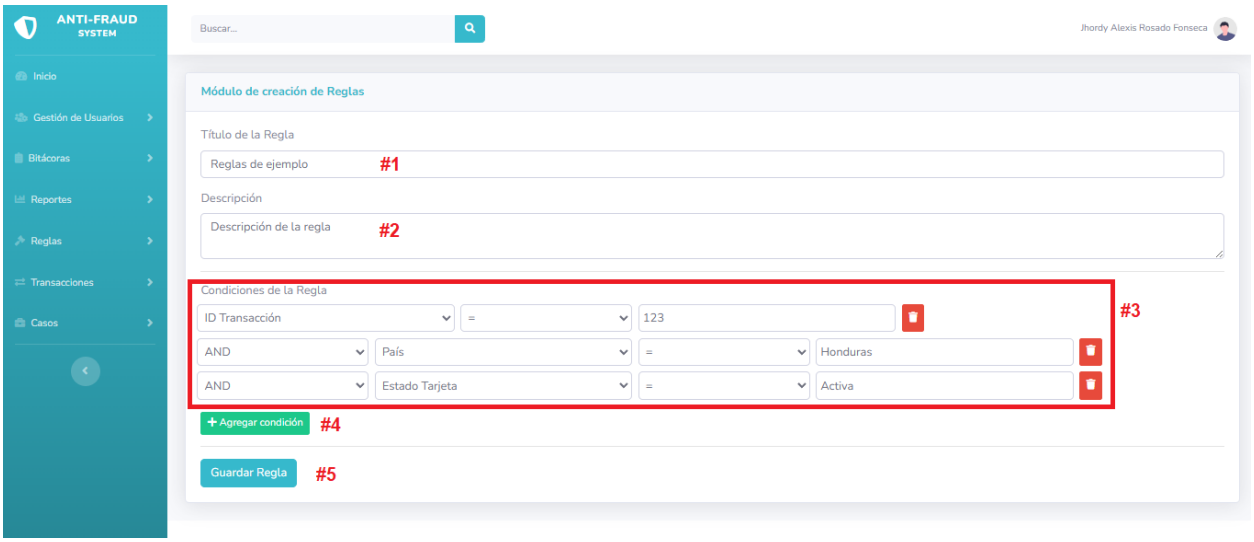
9.2.1.18 Ver Reglas



En este módulo se pueden observar todas las reglas registradas en el sistema tanto las activas como inactivas. Una regla en palabras sencillas es un filtro de transacciones que permite seleccionar cuales transacciones en base a un análisis previo pueden tener tendencia de fraude, todas las transacciones que pasan por este "filtro" van a registrarse como transacciones sospechosas.

1. Columnas de la tabla reglas: aquí se desglosan todos los campos importantes de las reglas registradas en el sistema, por ejemplo: identificador único de la regla, nombre de la regla, descripción, quien la creó o modificó y su fecha y hora correspondiente, así como el estado de esta.
2. Filas correspondientes a las reglas registradas en el sistema.
3. Botón "Recargar Motor de Reglas" sirve para refrescar y actualizar el motor de reglas en caso de que se haya hecho alguna modificación.

9.2.1.19 Crear reglas

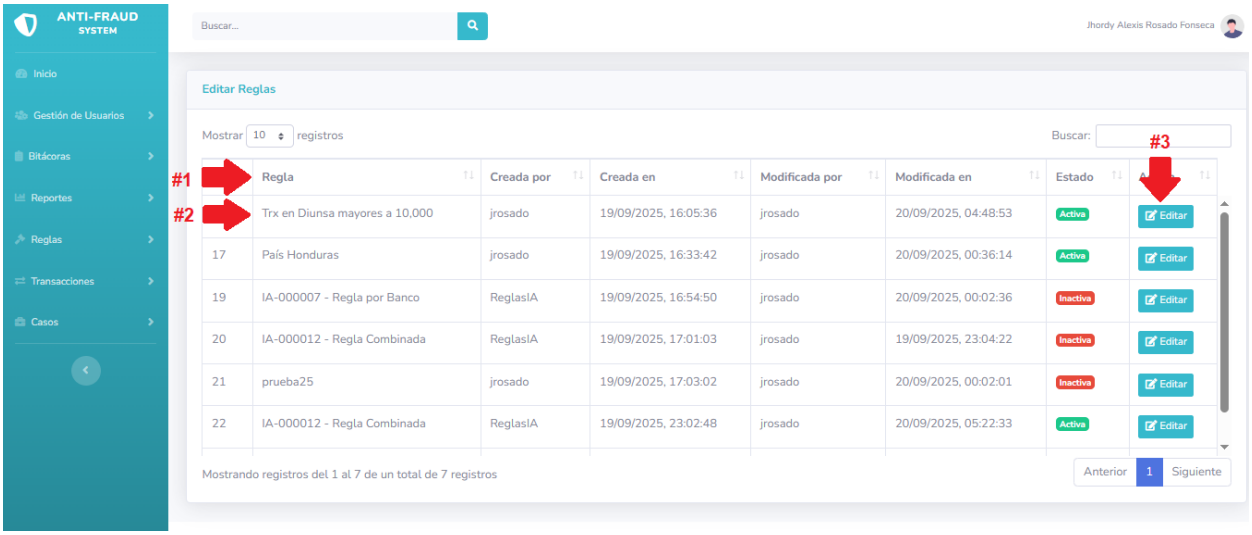


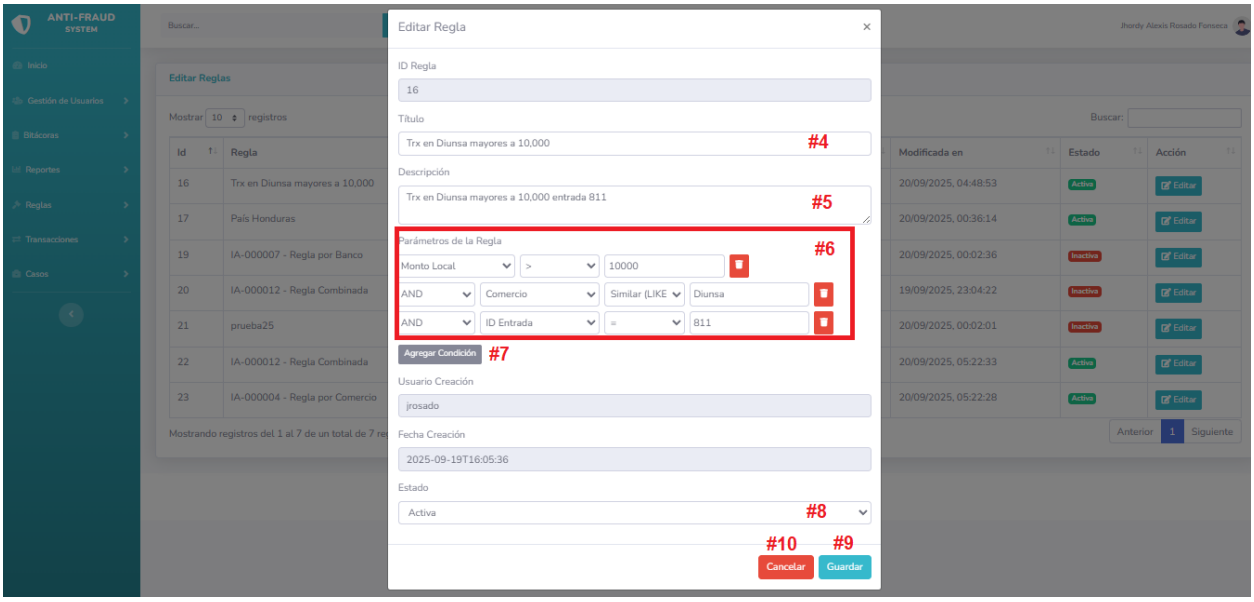
Este es el módulo principal para crear las reglas que generarán las transacciones sospechosas en el sistema, se compone de:

1. Un espacio para crear el título de la regla.
2. Un espacio para describir los parámetros de la regla, esta debe ser una descripción que busque en la medida de lo posible explicar el propósito de la regla.
3. parámetros de la regla: en otras palabras, aquí se seleccionan los criterios que la regla va a tomar en cuenta para generar las transacciones sospechosas, por ejemplo: nombre de comercio, identificador de dispositivo, modo de entrada, monto de la transacción, etc.
4. Botón para agregar más condiciones: se pueden agregar todas las condiciones que el usuario administrador estime conveniente.
5. Botón para guardar la regla.

9.2.1.20 Editar reglas

Modulo principal para editar las reglas que ya se encuentran registradas en el sistema.





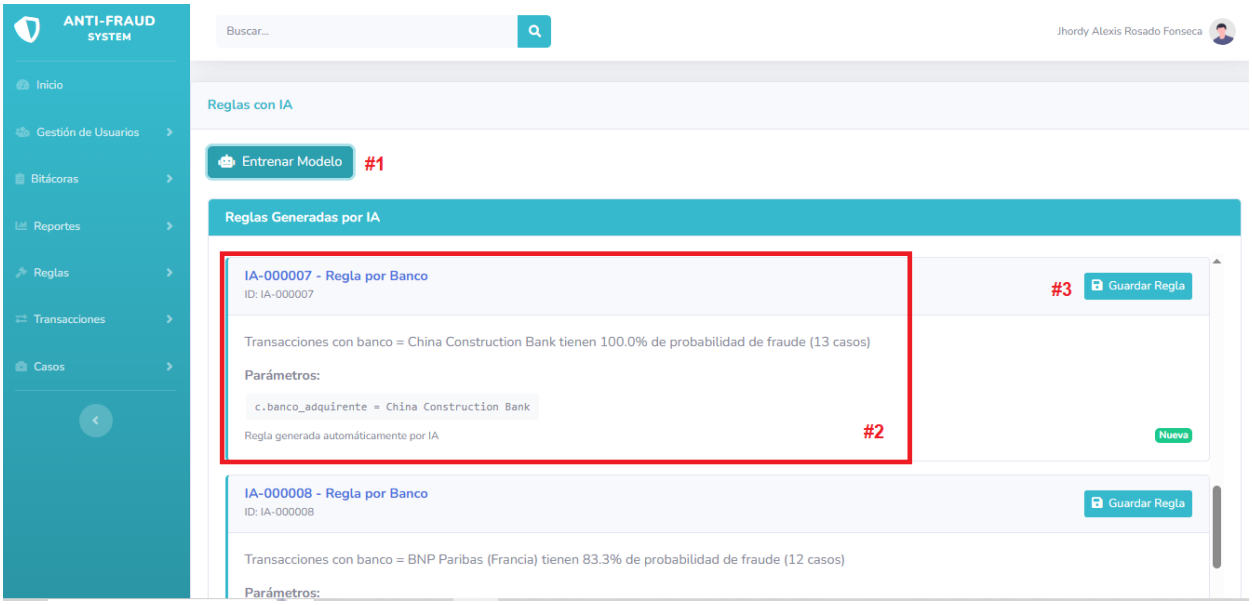
El módulo se compone de los siguientes elementos:

1. Columnas de la tabla de reglas: se encuentran elementos útiles como el identificador único de la regla, título, fecha de creación, usuario de creación, así como el usuario y fecha de modificación de la regla (en caso de que ya haya sido modificada anteriormente).
2. Filas correspondientes a cada una de las reglas disponibles para editar.

3. Botón “Editar” el cual despliega los campos principales de la regla dándonos la posibilidad de editarlos.
4. Espacio para modificar el título de la regla en caso de que se considere necesario.
5. Espacio para modificar la descripción de la regla en caso de que se considere necesario.
6. Espacio para modificar los parámetros de la regla que van a identificar las transacciones sospechosas.
7. Botón para agregar una nueva condición en caso de que se considere necesario.
8. Menú desplegable para editar el estado de la regla (activa o inactiva).
9. Botón para guardar todos los cambios realizados.
10. Cancelar todo el proceso de edición de regla.

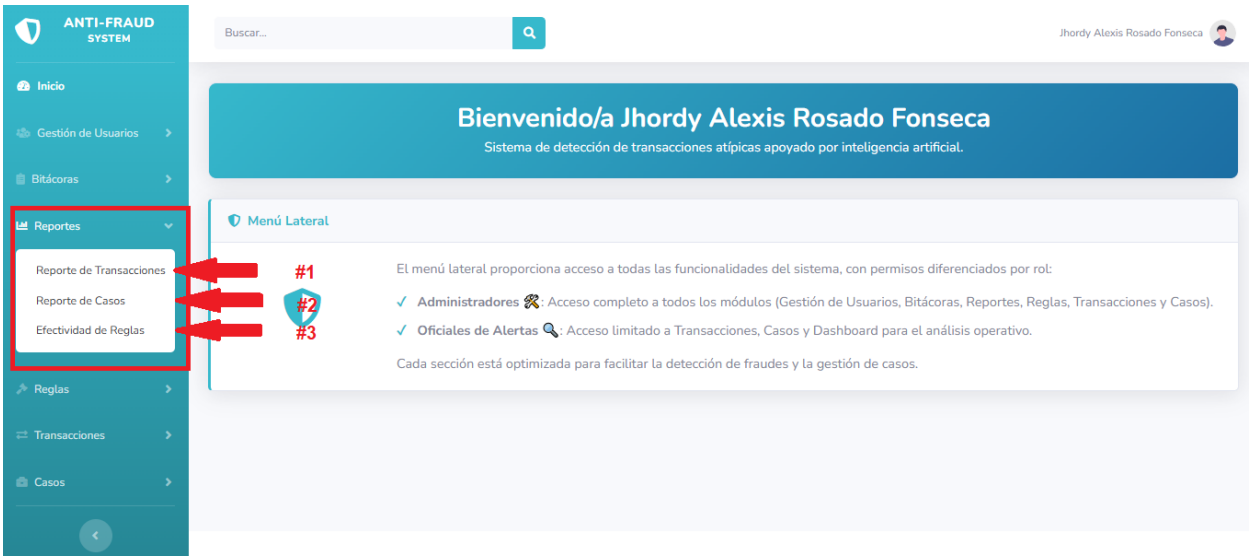
9.2.1.21 Reglas con IA

En el módulo de reglas con IA se tiene la posibilidad de utilizar el modelo de inteligencia artificial que tiene el sistema para detectar comportamientos fraudulentos, este modelo analiza todas las transacciones que contiene el sistema e identifica similitudes entre las transacciones que ya fueron marcadas como fraude con el fin de crear reglas con los parámetros específicos para detectar futuras transacciones con el mismo comportamiento.



1. Botón “Entrenar Modelo” al dar clic el modelo empieza a analizar todas las transacciones e identifica comportamientos fraudulentos con el fin de generar reglas automáticamente.
2. Una vez el modelo haya finalizado el entrenamiento en la sección “Reglas Generadas por IA” podremos ver el título de la regla, descripción, y el comportamiento de fraude identificado que podremos trasladar al motor de reglas, con el fin de detener futuras transacciones con el mismo comportamiento.
3. Botón para guardar la regla en el “motor de reglas”.

9.2.1.22 Reportes



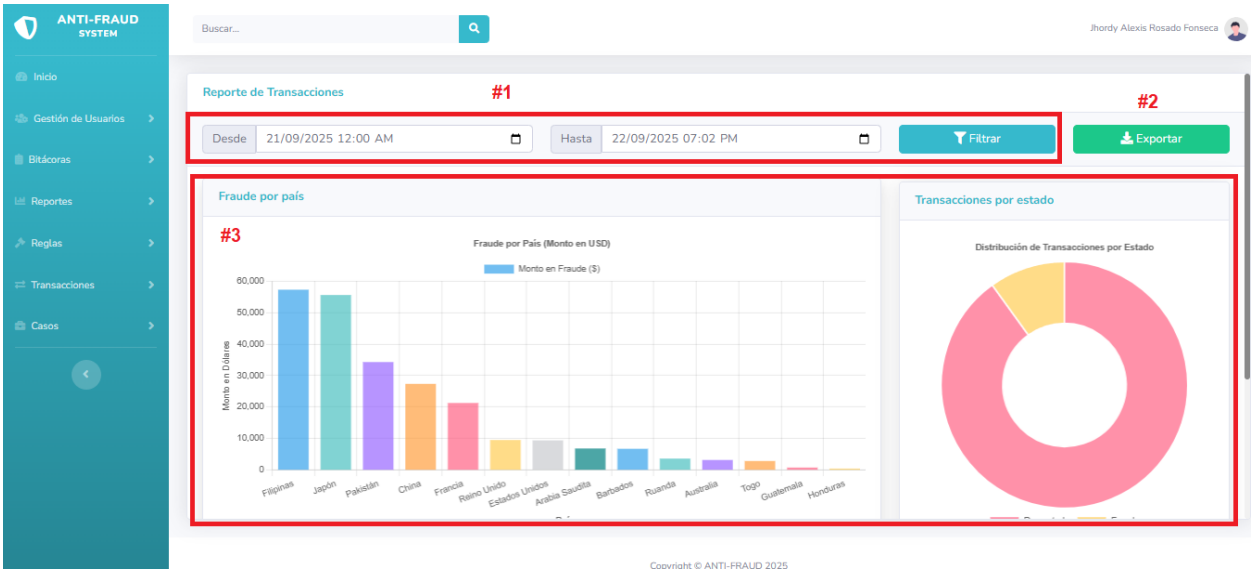
Dando clic en la opción del menú lateral “Reportes” tiene la posibilidad de ingresar a tres módulos:

1. Reporte de Transacciones
2. Reporte de casos
3. Efectividad de Reglas

A continuación, en la siguiente sección se explica el funcionamiento de cada uno de ellos.

9.2.1.23 Reporte de Transacciones

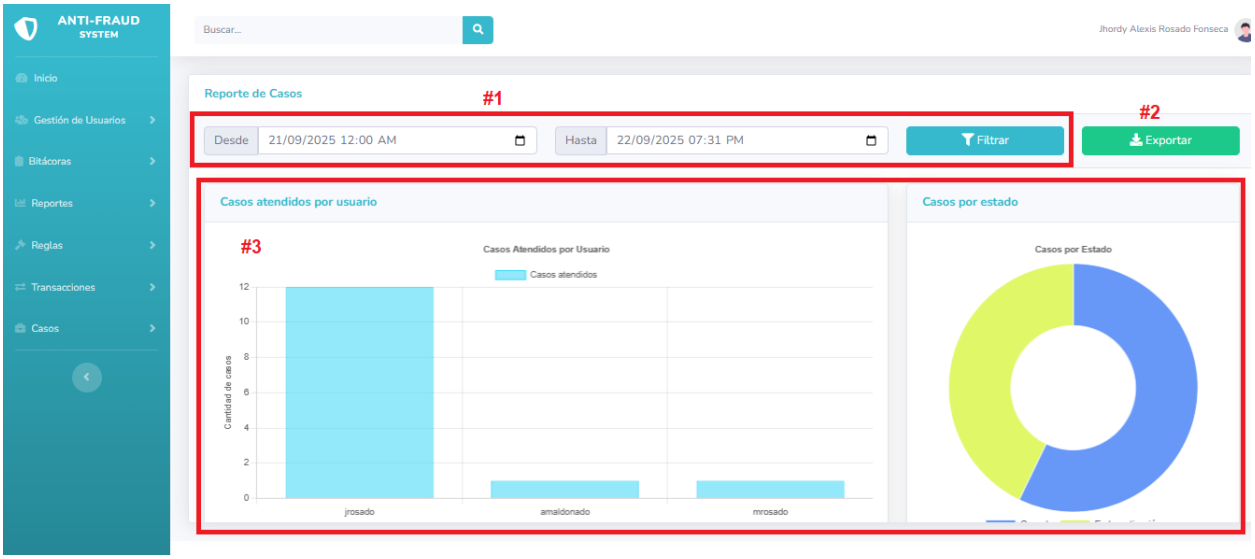
En el módulo de reporte de transacciones se pueden observar gráficos referentes a las tendencias de fraude identificadas en las transacciones, se pueden ver fraudes por país, grafico de transacciones por estado y algunas cifras referentes a fraudes en general.



1. Filtro de fechas personalizadas ya explicado en módulos anteriores.
2. Botón para exportar los datos de las transacciones analizadas en los gráficos, se obtiene toda la trama de datos en un archivo que puede ser leído en Excel.
3. Gráficos referentes a las transacciones en general.

9.2.1.24 Reporte de Casos

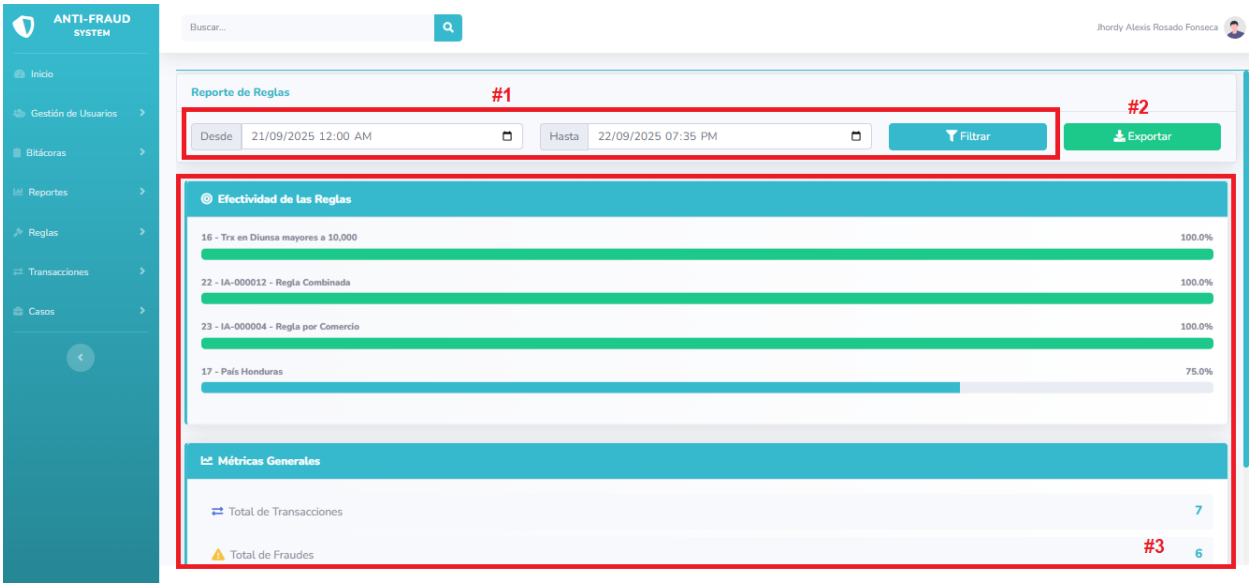
En el módulo de reporte de casos se pueden observar gráficos referentes a los casos registrados en el sistema, se pueden ver casos por usuario, grafico de casos por estado y algunas cifras referentes al historial de acciones como cantidad de llamadas realizadas por los oficiales, mensajes de WhatsApp, SMS, etc.



1. Filtro de fechas personalizadas ya explicado en módulos anteriores.
2. Botón para exportar los datos de los casos analizados en los gráficos, se obtiene toda la trama de datos en un archivo que puede ser leído en Excel.
3. Gráficos referentes a los casos en general.

9.2.1.25 Efectividad de Reglas

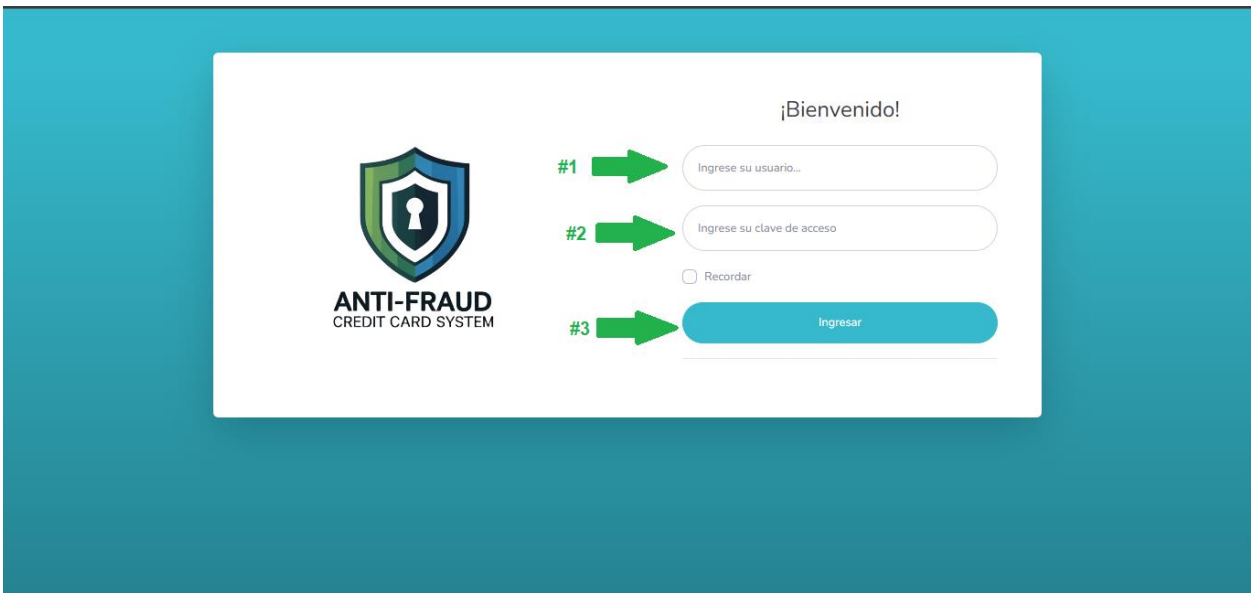
En el módulo de efectividad de reglas se pueden observar un gráfico referente a la efectividad de cada una de las reglas activas en el sistema.



1. Filtro de fechas personalizadas ya explicado en módulos anteriores.
2. Botón para exportar los datos de las reglas analizadas en el gráfico, se obtiene toda la trama de datos en un archivo que puede ser leído en Excel.
3. Gráficos referentes a las reglas en general.

9.2.2 MANUAL DE USUARIO PARA OFICIALES DE ALERTAS

9.2.2.1 Inicio de sesión



Para poder ingresar debe contar con un usuario y contraseña válidos y activos registrados previamente en la base de datos por el proveedor del sistema o por otro usuario administrador.

1. Campo donde debe ingresar su usuario.
2. Campo donde debe ingresar su contraseña.
3. Una vez ingresado su usuario y contraseña debe dar clic en el botón “Ingresar” para poder acceder al sistema (tiene la posibilidad de recordad sus credenciales dando clic en “Recordar” justo arriba del botón “Ingresar”).

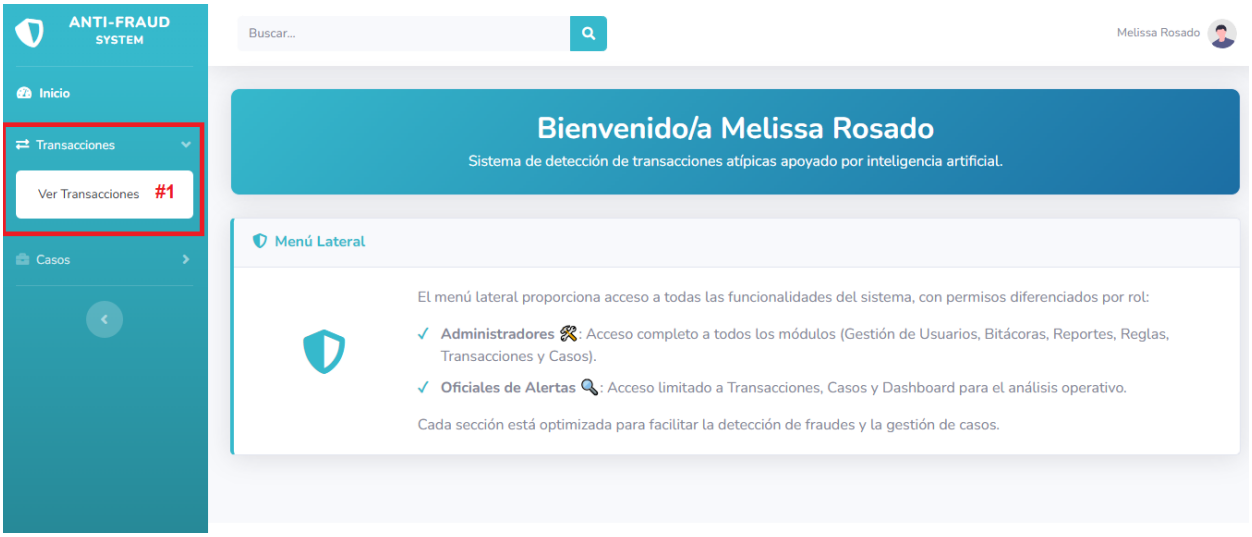
9.2.2.2 Pantalla Principal

Esta es la primera pantalla que observará al ingresar al sistema, cuenta con un mensaje de bienvenida al sistema, así como una pequeña explicación del menú lateral izquierdo.

1. Menú lateral: este es el menú principal que sirve para acceder a todas las funcionalidades del sistema, organizadas por similitudes entre funcionalidades para facilitar el uso.

2. Perfil: desde esta sección puede acceder a ver la información de su perfil desde la opción “Ver Perfil” o en su defecto salir del sistema dando clic en “Cerrar sesión”.

9.2.2.3 Transacciones

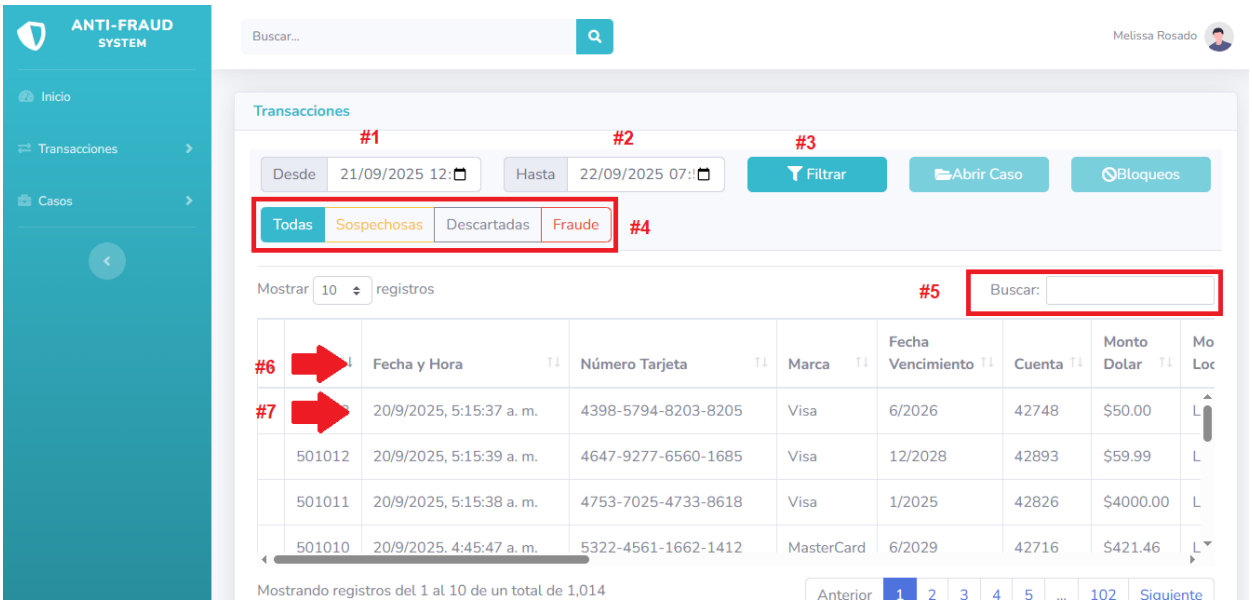


Dando clic en la opción del menú lateral “Transacciones” tiene la posibilidad de ingresar a un módulo:

1. Ver Transacciones

A continuación, en la siguiente sección se explica el funcionamiento del módulo.

9.2.2.4 Ver Transacciones



El módulo “Ver Transacciones” funciona como el apartado principal donde se registran todas las transacciones con tarjetas de crédito procesadas por la institución bancaria, aquí se registran las transacciones sospechosas, descartadas y fraude. Aquí se puede observar toda la información referente a la transacción, así como aplicar otras gestiones como abrir un caso de investigación o aplicar un bloqueo o desbloqueo a la tarjeta.

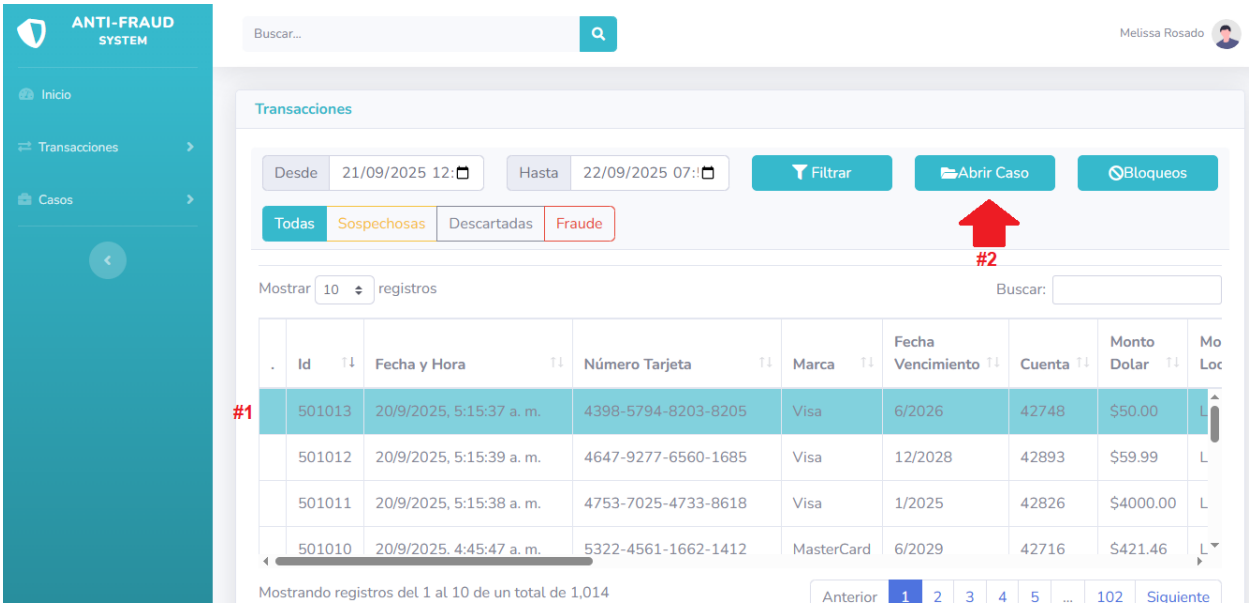
Este módulo se compone de los siguientes elementos:

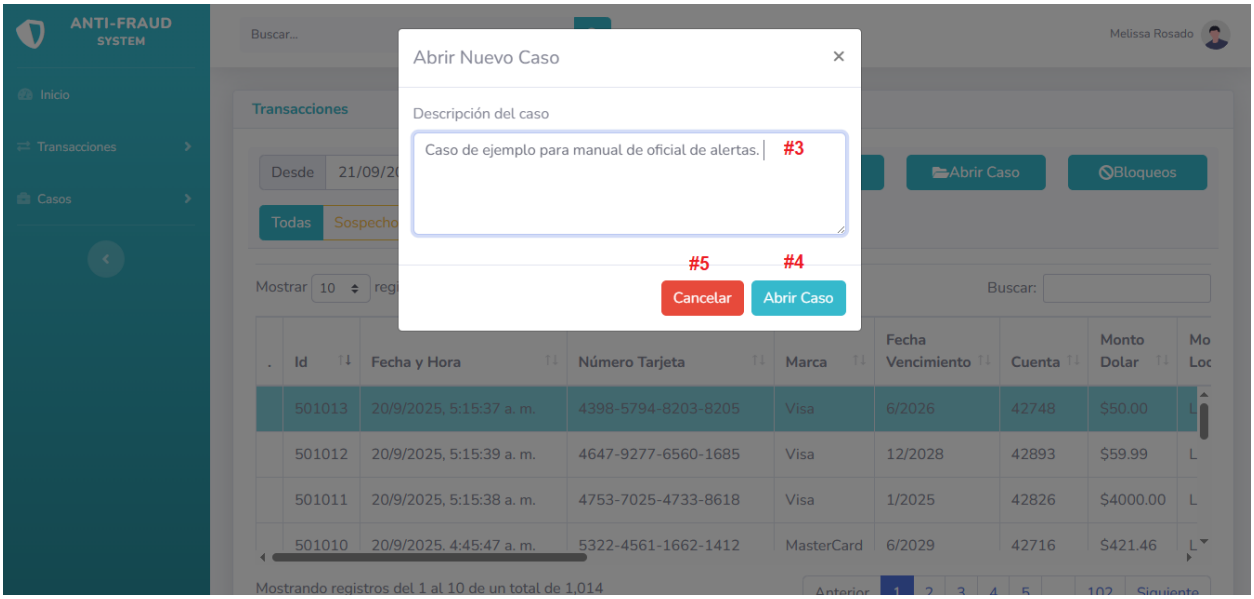
1. Misma funcionalidad que en el módulo de “Bitácoras de Sesión”
2. Misma funcionalidad que en el módulo de “Bitácoras de Sesión”
3. Misma funcionalidad que en el módulo de “Bitácoras de Sesión”
4. Filtro de transacciones por estado: los botones “Todas”, “Sospechosas”, “Descartadas” y “Fraude” permite mostrar en la tabla solo las transacciones que tengan el estado que el usuario seleccionó.
5. Misma funcionalidad que en el módulo de “Bitácoras de Sesión”

6. Columnas de la tabla transacciones: todos los campos relevantes de una transacción, se encuentran elementos como: número de tarjeta, fecha de vencimiento, comercio, país, monto dólar, monto local, cuenta, estado de la tarjeta de crédito, estado de la transacción, etc.
7. Filas de la tabla transacciones: donde se registra la información de cada transacción.

A continuación, se muestras más funcionalidades de este módulo de ver transacciones.

9.2.2.4.1 Abrir un caso de investigación

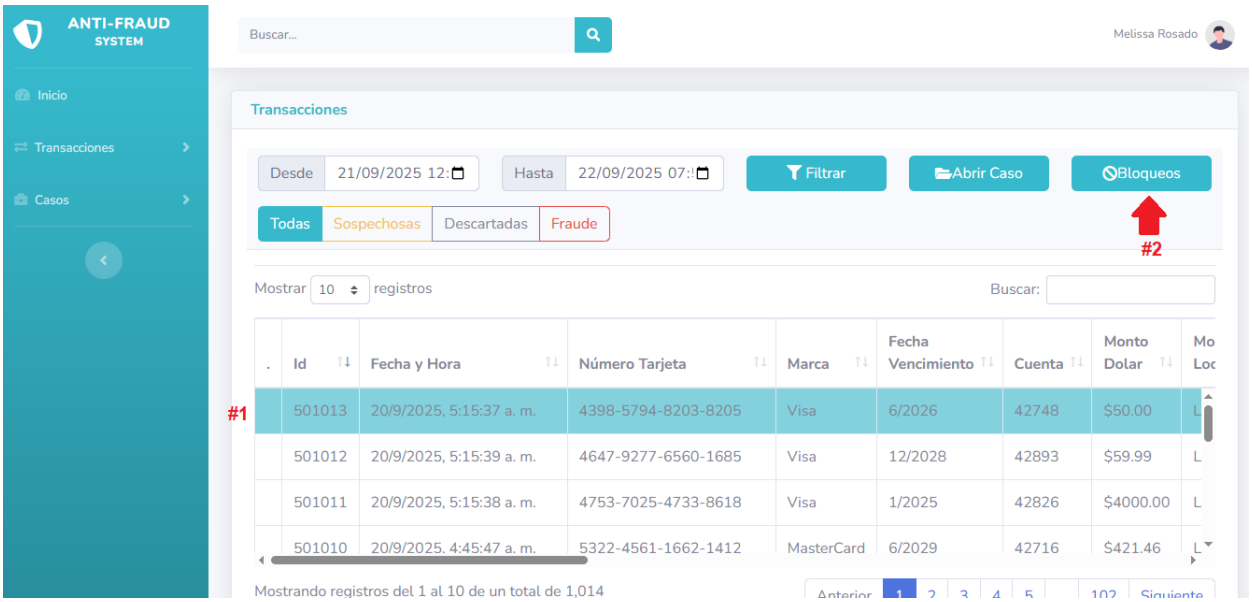


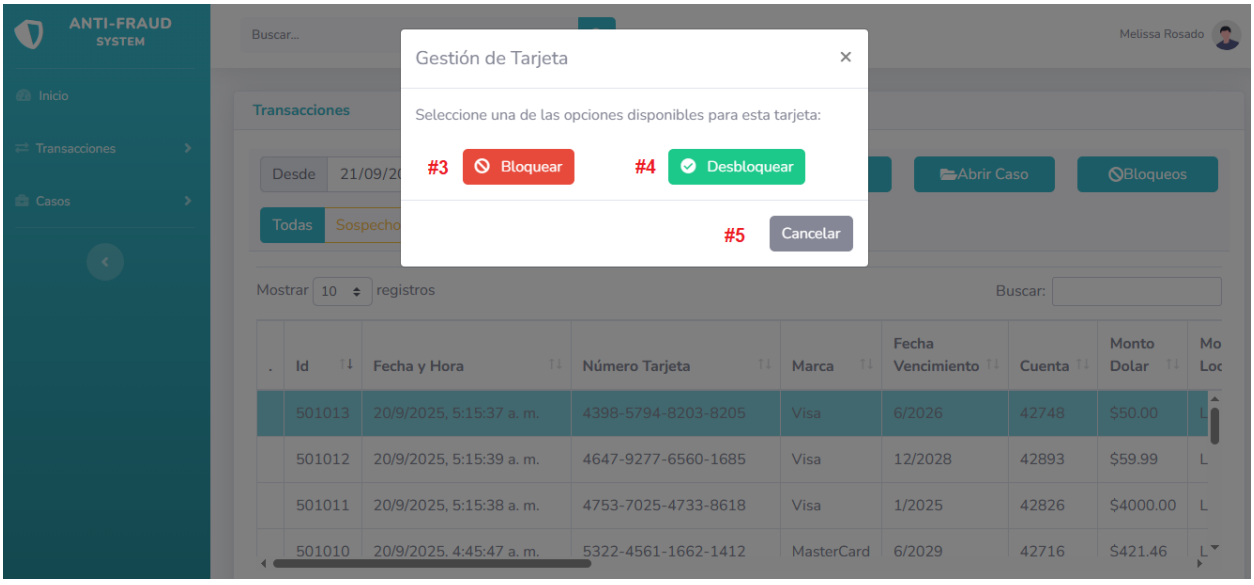


Para abrir un caso de investigación se necesita seguir los siguientes pasos:

1. Se debe seleccionar una o más transacciones que el usuario del sistema estime que necesiten ser investigadas, en general se abren casos de investigación por transacciones que tienen un estado “Sospechosa”.
2. Una vez seleccionada(s) la(s) transacción(es) se puede abrir un caso de investigación y poder gestionar de mejor manera esa investigación, para ello se da clic en el botón “Abrir Caso”.
3. En este punto se debe desplegar un apartado para colocarle un texto descriptivo al caso, ese texto debe describir características relevantes del caso, por ejemplo: “Caso de investigación por compras en Panamá en comercio Apple”.
4. Una vez tengamos la descripción del caso procedemos a guardarlo dando clic en “Abrir Caso”.
5. Botón para cancelar el proceso.

9.2.2.4.2 Bloqueos de tarjetas





1. Para aplicar un bloqueo o desbloqueo de tarjeta de crédito primero se debe seleccionar una transacción dando clic en la fila correspondiente a la misma.
2. Posteriormente se da clic en el botón “Bloqueos”

3. En este punto se despliega un submenú que permite seleccionar una opción para la tarjeta seleccionada, si da clic en “Bloquear” a la tarjeta se le aplicaría un bloqueo preventivo lo que es útil cuando se tiene un caso de investigación por transacciones sospechosas.
4. Este botón sirve para desbloquear la tarjeta de crédito seleccionada, útil cuando el oficial de alertas ya contactó al tarjetahabiente y confirmó que las transacciones sospechosas fueron realizadas por él.
5. Cancela todo el proceso de bloqueo o desbloqueo.

9.2.2.5 Casos

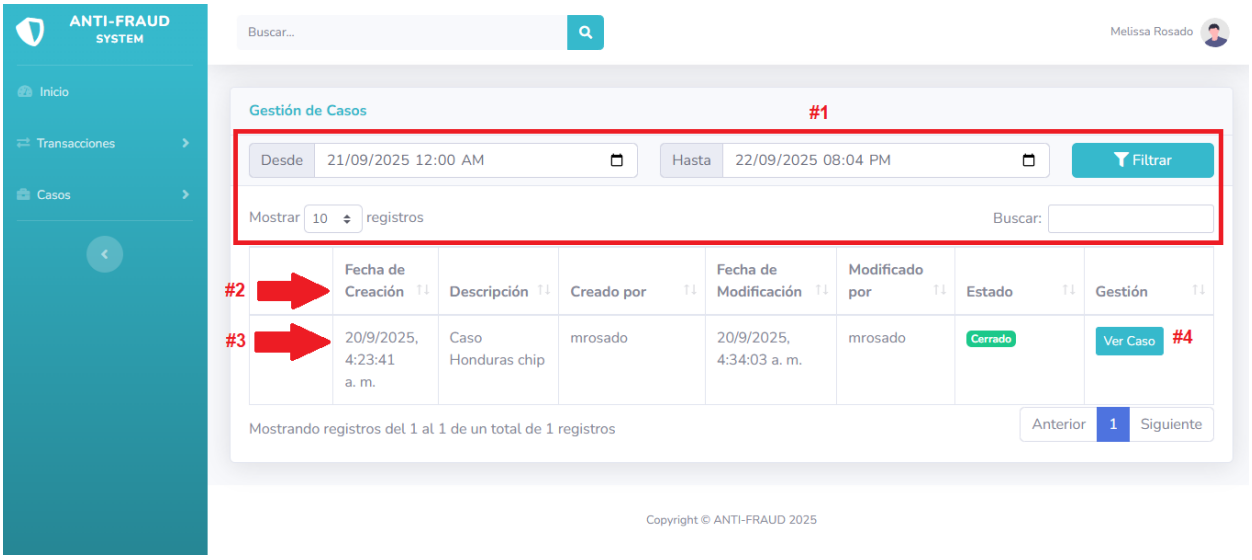
Dando clic en la opción del menú lateral “Casos” tiene la posibilidad de ingresar a dos módulos:

1. Mis casos Sospechosos
2. Casos Sospechosos

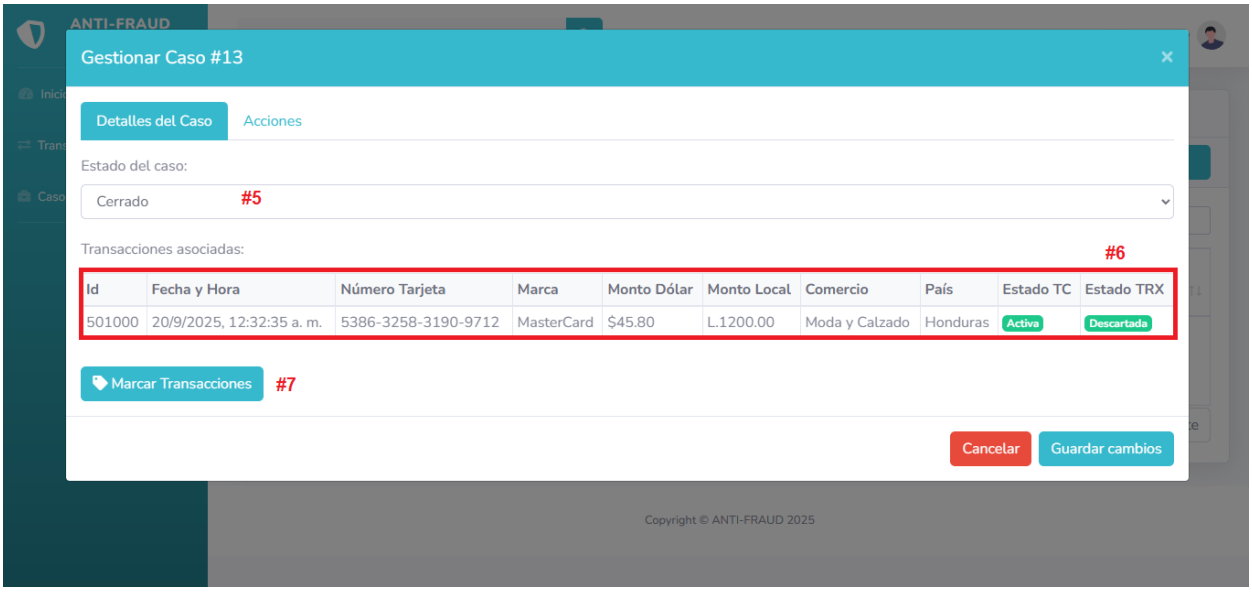
A continuación, en la siguiente sección se explica el funcionamiento de cada uno de ellos.

9.2.2.6 Mis Casos Sospechosos

Este es el módulo principal para gestionar todos los casos de investigación que se abrieron previamente desde el módulo de “Ver Transacciones”, se especifica que en este módulo solo se observan los casos que el usuario conectado al sistema ha creado, para ver todos los casos registrados incluyendo lo de los demás usuarios se puede utilizar el módulo de “Casos Sospechoso”.

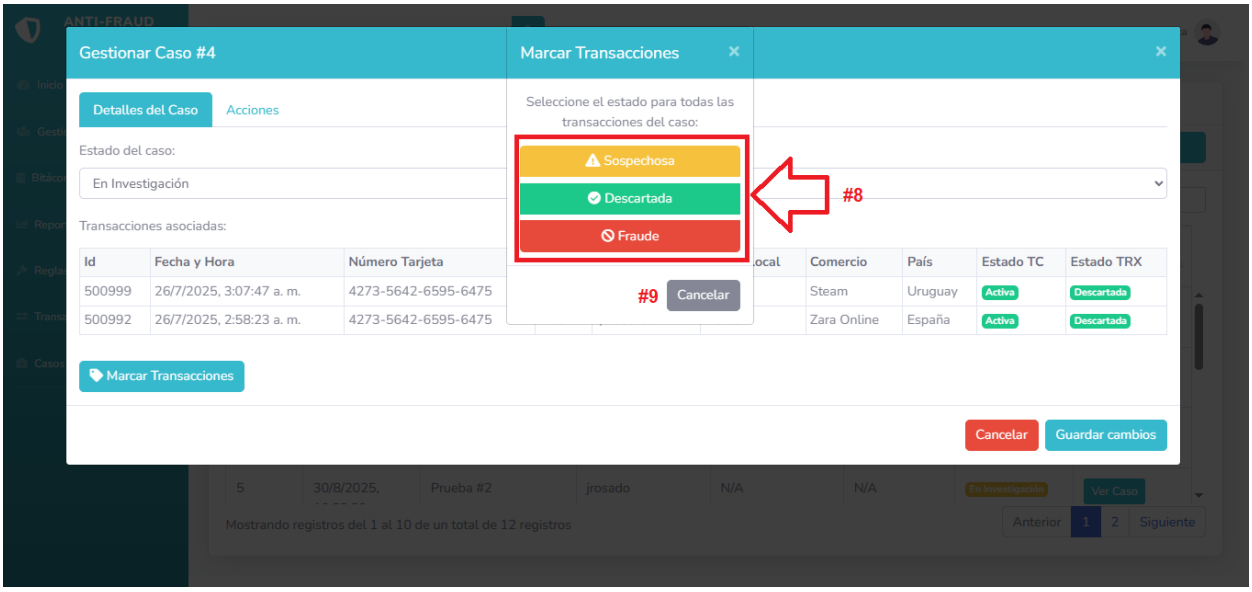


1. Opciones de filtrado que han sido explicado en módulos anteriores, puede dirigirse a la explicación del módulo “Bitácoras” para más detalles.
2. Columnas de la tabla Casos: aquí se observan columnas relevantes de los casos registrados en el sistema, por ejemplo: identificador del caso, fecha de creación, usuario de creación, fecha de modificación y usuario de modificación, así como también el estado del caso que puede ser “En investigación” o “Cerrado”.
3. Filas donde se puede ver la información de cada caso.
4. Botón de “Ver Caso” que sirve para ver todos los detalles del caso de investigación.

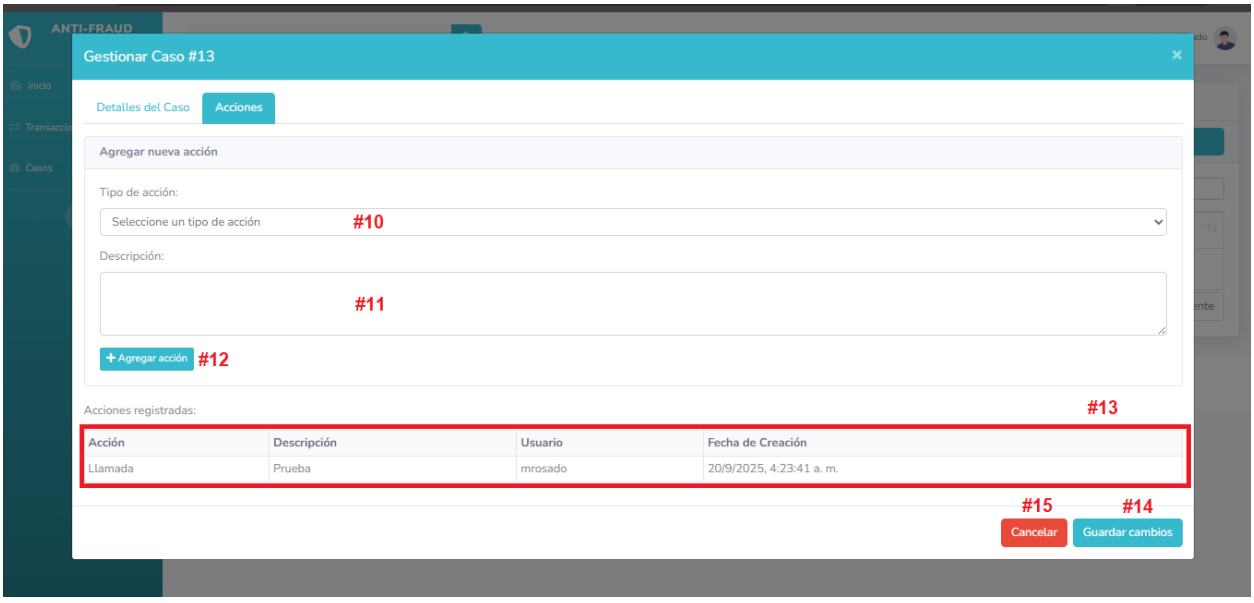


Una vez que haya dado clic en “Ver Caso” se despliega la siguiente pantalla con dos pestañas: “Detalles del caso” y “Acciones”

5. Menú desplegable de opciones que permite cambiar el estado del caso, puede ser “En investigación” o “Cerrado”.
6. Tabla donde se muestran todas las transacciones asociadas al caso en investigación.
7. Botón que sirve para cambiar el estado de las transacciones.



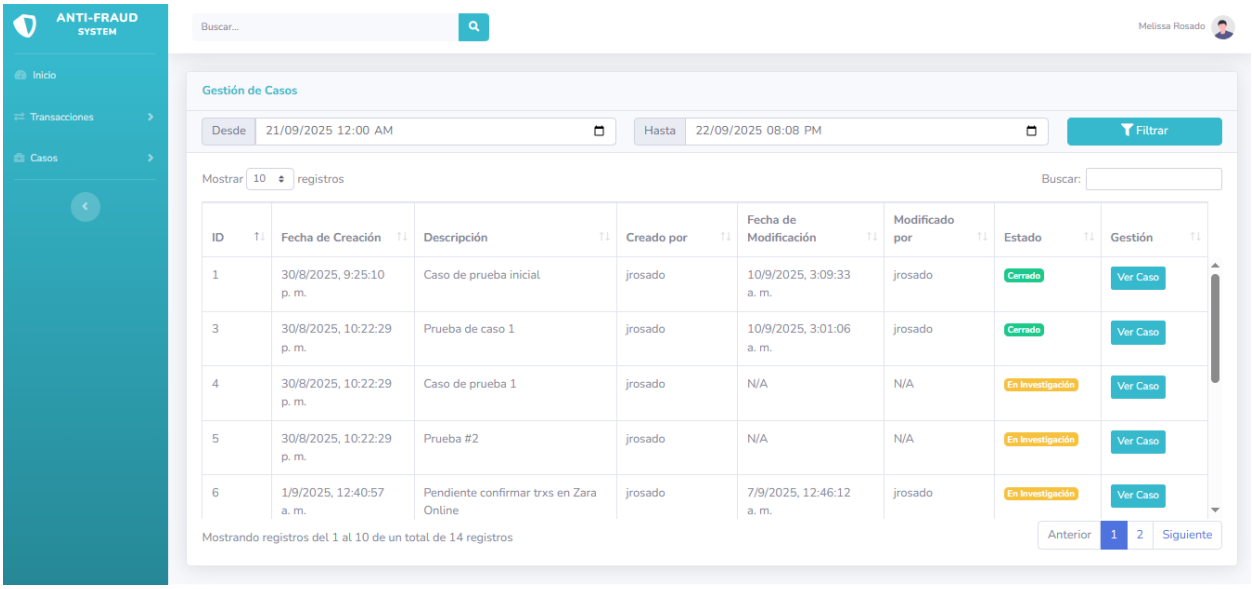
8. Una vez que haya dado clic en “Marcar Transacciones” se despliega una pequeña pantalla donde puede seleccionar el nuevo estado de la transacción, puede elegir entre: sospechosa, descartada y fraude, este estado dependerá de la resolución que el oficial de alertas le dio al caso.
9. Botón para cancelar todo el proceso.



Si vamos a la pestaña de “Acciones” tenemos la posibilidad de registrar una pequeña bitácora de acciones realizadas por el oficial de alertas, aquí se puede registrar el seguimiento que se le dio al caso, por ejemplo, llamadas realizadas, SMS, mensajes de WhatsApp, etc. Así como también puede servir como una sección de notas recordatorias para el oficial de alertas.

10. Menú desplegable que permite seleccionar una acción, por ejemplo: llamadas realizadas, SMS, mensajes de WhatsApp, etc.
11. Espacio donde el oficial puede escribir en esa acción, por ejemplo: registrar el número de teléfono del cliente u otra nota útil para el seguimiento del caso.
12. Botón “Agregar acción” para guardar los cambios realizados en esa acción en específico.
13. Pequeña tabla de todas las acciones registradas en el caso de investigación.
14. Botón de “Guardar” para registrar todos los cambios realizados en el caso.
15. Cancelar todo el proceso.

9.2.2.7 Casos Sospechosos



Este es el módulo principal para gestionar todos los casos de investigación que se abrieron previamente desde el módulo de “Ver Transacciones”, se conservan todas las funcionalidades de “Mis Casos Sospechosos”, en este módulo a diferencia del módulo de “Mis Casos Sospechoso” se pueden ver todos los casos registrados en el sistema, incluyendo los creados por los demás usuarios.

BIBLIOGRAFÍA

JSON Web Token Introduction. (30 de noviembre de 2024). Obtenido de JWT.IO: https://www.jwt.io/introduction#what-is-json-web-token

¿Qué es CSS? Explicamos el Cascading Style Sheets. (12 de julio de 2021). Obtenido de IONOS Digital Guide: https://www.ionos.com/es-us/digitalguide/paginas-web/diseno-web/que-es-css/

¿Qué es el aprendizaje supervisado? (28 de diciembre de 2024). Obtenido de IBM: https://www.ibm.com/es-es/think/topics/supervised-learning

¿Qué es el fraude de tarjeta no presente? | Stripe. (14 de Marzo de 2024). Obtenido de stripe: https://stripe.com/es/resources/more/what-is-card-not-present-fraud-what-businesses-need-to-know

¿Qué es el phishing? (s.f.). Obtenido de IBM: https://www.ibm.com/es-es/think/topics/phishing

¿Qué es JavaScript (JS)? (s.f.). Obtenido de AWS: https://aws.amazon.com/es/what-is/javascript/

¿Qué es la ingeniería social? (30 de Julio de 2025). Obtenido de Kaspersky: https://latam.kaspersky.com/resource-center/definitions/what-is-social-engineering?srsltid=AfmBOor8TcIJDArYDmqPhWO76a72ehQvcBlkSbOSzUxCp0lmfKqHWAfo

¿Qué es la protección de datos? (s.f.). Obtenido de Seguridad de Microsoft: https://www.microsoft.com/es-ar/security/business/security-101/what-is-data-protection

¿Qué es machine learning? (s.f.). Obtenido de IBM: https://www.ibm.com/mx-es/think/topics/machine-learning

¿Qué es Python? (s.f.). Obtenido de Oracle Nueva Zelanda: https://www.oracle.com/nz/developer/what-is-python-for-developers/

¿Qué es un indicador de fraude? (30 de Julio de 2025). Obtenido de Financial Crime Academy: https://financialcrimeacademy.org/es/que-es-un-indicador-de-fraude/#:~:text=Los%20indicadores%20de%20fraude%20sirven,evitar%20que%20se%20produzcan%20fraudes.

¿Qué es una API REST? (s.f.). Obtenido de IBM: https://www.ibm.com/es-es/think/topics/rest-apis

Akamai. (s.f.). *What is web skimming? | Akamai*. Obtenido de Akamai: https://www.akamai.com/glossary/what-is-web-skimming

Alberca, A. S. (12 de mayo de 2022). *La librería Numpy*. Obtenido de Aprende con Alf: https://aprendeconalf.es/docencia/python/manual/numpy/

Alberca, A. S. (14 de junio de 2022). *La librería Pandas*. Obtenido de Aprende con Alf: https://aprendeconalf.es/docencia/python/manual/pandas/

Asociación Hondureña de Instituciones Bancarias. (s.f.). *Taller de Modalidades de Fraude en el Sector Financiero*. Obtenido de AHIBA: https://ahiba.hn/taller-de-modalidades-de-fraude-en-el-sector-financiero/

Atkins, L., Banerjee, S., Craig, L., Hao, G., Greis, J., Boer, M., & Idler, M. (11 de Marzo de 2024). *El reloj cibernético no se detiene: Reducir el riesgo de las tecnologías emergentes en los servicios financieros*. Obtenido de McKinsey & Company: https://www.mckinsey.com/featured-insights/destacados/el-reloj-cibernetico-no-se-detiene-reducir-el-riesgo-de-las-tecnologias-emergentes-en-los-servicios-financieros/es

Banco Interamericano de Desarrollo, & Organización de los Estados Americanos. (2020). *Ciberseguridad: riesgos, progreso y el camino a seguir en América Latina y el Caribe*. Obtenido de https://doi.org/10.18235/0002513

Carga: ¿qué significa en computación? (s.f.). Obtenido de Lenovo Perú: https://www.lenovo.com/pe/es/glosario/carga-en-computacion/?orgRef=https%253A%252F%252Fwww.google.com%252F

Comision Nacional de Bancos y Seguros . (Abril de 2025). *Informes y cifras de las supervisadas.* . Obtenido de CNBS: https://publicaciones.cnbs.gob.hn/dashboard/https%3A%2F%2Fapp.powerbi.com%2Fview%3Fr%3DeyJrIjoiYmQ0YThiOTEtNzE1Yi00NGE3LWFkYWQtN2ZiNzY0NWY3ZTUxIiwidCI6ImZlNDA4MTE2LWZkMTMtNDhjMy04MzJiLTc5NDU3ZGNjNmUyMyJ9%26language%3Des%26formatLocale%3Des-HN

Comisión Nacional de Bancos y Seguros. (2024). *CIRCULAR CNBS No.018/2024* . Obtenido de CNBS: https://circulares.cnbs.gob.hn/Archivo/Viewer/3640/018-2024%20LINEAMIENTOS%20OPERACIONES%20NO%20RECONOCIDAS%20TARJETAS.pdf

Comisión Nacional de Bancos y Seguros. (2024). *Reporte de inclusión financiera 2024*. Obtenido de CNBS: https://www.cnbs.gob.hn/inclusion-financiera/wp-

content/uploads/2024/07/REPORTE-DE-INCLUSION-FINANCIERA-2024_FINAL_JULIO-12072024.pdf

Comisión Nacional de Bancos y Seguros. (Marzo de 2025). *Instituciones Supervisadas por la CNBS - Marzo 2025.xlsx - Informes y cifras de las supervisadas*. Obtenido de cnbs.gob.hn: https://publicaciones.cnbs.gob.hn/Home/Viewer/Instituciones%20Supervisadas%2FListado%20de%20Instituciones%2F2025/1.%20Instituciones%20Supervisadas%20por%20la%20CNBS%20-%20Marzo%202025.xlsx

Credit card fraud – Ways to detect and prevent it. (03 de Mayo de 2024). Obtenido de fraud.com: https://www.fraud.com/post/credit-card-fraud

Datadome. (11 de Junio de 2025). *How AI is used in fraud Detection in 2025*. Obtenido de Datadome: https://datadome.co/learning-center/ai-fraud-detection/

Datos cuantitativos. (s.f.). Obtenido de QuestionPro: https://www.questionpro.com/es/datos-cuantitativos.html

Decision Intelligence. (s.f.). Obtenido de MasterCard: https://www.mastercard.com.mx/es-mx/empresas/empresas-pequenas-medianas/digital-security/decision-intelligence.html

Deepfakes: Qué es, tipos, riesgos y amenazas. (s.f.). Obtenido de LISA Institute: https://www.lisainstitute.com/blogs/blog/deepfakes-tipos-consejos-riesgos-amenazas?srsltid=AfmBOor9gyA8op9p-cxDdslDrF2yV6aqULBpM_bphZQkx89EL1XNDuiZ

Deloitte Spanish Latin America. (2023). *Deloitte*. Obtenido de Reporte de Transparencia en Calidad de Auditoria: https://www2.deloitte.com/content/dam/Deloitte/gt/Documents/audit/reporte-transparencia-calidad-2023.pdf

Diccionario de la lengua española. (s.f.). Obtenido de algoritmo | Diccionario de la lengua española.: https://dle.rae.es/algoritmo

E, U., Soberón, M., & Acosta E , Z. (2008). FUENTES DE INFORMACIÓN PARA LA RECOLECCIÓN DE INFORMACIÓN CUANTITATIVA Y CUALITATIVA. *FUENTES DE INFORMACIÓN PARA LA RECOLECCIÓN DE INFORMACIÓN CUANTITATIVA Y CUALITATIVA*.

El Heraldo. (22 de Agosto de 2024). *¿Cuál es el mayor reclamo de los usuarios financiero en Honduras?* Obtenido de elheraldo.hn: https://www.elheraldo.hn/economia/cual-mayor-reclamo-usuarios-financiero-honduras-MC21012482

Esmartcity. (20 de Septiembre de 2018). *Ahorrar dinero y tiempo son las principales razones que llevarían a los consumidores a utilizar la inteligencia artificial*. Obtenido de Esmartcity: https://www.esmartcity.es/2018/09/20/ahorrar-dinero-tiempo-principales-razones-llevarian-consumidores-utilizar-inteligencia-artificial

Estrada, S. (4 de Junio de 2024). *El Economista*. Obtenido de El Economista: https://www.eleconomista.com.mx/sectorfinanciero/Se-aceleran-transacciones-digitales-pero-se-incrementan-los-riesgos-20240603-0134.html

False Positive Meaning & Definition. (2 de abril de 2024). Obtenido de Zevo Health: https://www.zevohealth.com/glossary/false-positive/

FastAPI. (s.f.). Obtenido de FastAPI: https://fastapi.tiangolo.com/es/

Fernando, J., & Rodriguez , P. (29 de Febrero de 2024). *Card-Present fraud: what it is, how it works, example*. Obtenido de Investopedia: https://www.investopedia.com/terms/c/cardpresent-fraud.asp

Financial Ecosystem. (4 de diciembre de 2023). Obtenido de PayAlly. : https://payally.co.uk/glossary/financial-ecosystem/

Fraud.com International. (31 de Marzo de 2023). Obtenido de Artificial Intelligence – How it's used to detect financial fraud: https://www.fraud.com/post/artificial-intelligence

GEIFG - Educación Financiera. (11 de Julio de 2023). Obtenido de CNBS: https://www.cnbs.gob.hn/educacionfinanciera/prestamos-y-creditos/la-tarjeta-de-credito/

Guía de prevención de fraude: reconoce y detén las estafas en los pagos | Stripe. (22 de Enero de 2022). Obtenido de Stripe: https://stripe.com/mx/resources/more/six-types-of-payment-fraud

Guía para la detección del fraude basada en reglas. (s.f.). Obtenido de SEON ES: https://seon.io/es/recursos/guias/deteccion-fraude-en-base-a-reglas/

Herrero, M. P., Bajuelos, A. L., & Lava, I. (14 de Octubre de 2024). *Inteligencia artificial, ventajas y desventajas*. Obtenido de VIU Universidad Online: https://www.universidadviu.com/es/actualidad/nuestros-expertos/inteligencia-artificial-ventajas-y-desventajas

Instituciones financieras | BBVA México . (s.f.). Obtenido de BBVA: https://www.bbva.mx/educacion-financiera/blog/que-es-una-institucion-financiera.html

Monitoreo en tiempo real. (s.f.). Obtenido de Minery Report S.L.: https://mineryreport.com/ciberseguridad/glosario/conceptos-generales/termino/monitoreo-en-tiempo-real/

Murphy, R. (2024). *Global Economic Crime Survey 2024*. Obtenido de PwC: https://www.pwc.com/gx/en/services/forensics/economic-crime-survey.html

Ortega, C. (01 de Abril de 2025). *Investigación mixta. Qué es y tipos que existen*. Obtenido de QuestionPro: https://www.questionpro.com/blog/es/investigacion-mixta/

Parametrizar . (s.f.). Obtenido de Diccionario de la lengua española: https://dle.rae.es/parametrizar

Plataforma digital . (s.f.). Obtenido de Cognizant : https://www.cognizant.com/es/es/glossary/digital-platform

Qué es HTML y cuáles son sus aplicaciones. (30 de septiembre de 2024). Obtenido de Universidad Europea: https://universidadeuropea.com/blog/que-es-html/

RAE. (s.f.). *atípico, atípica «Diccionario Del Estudiante»*. Obtenido de Real Academia Española : https://www.rae.es/diccionario-estudiante/at%C3%ADpico

Sachis, G. (20 de marzo de 2024). *Análisis Forense Ciberseguridad*. Obtenido de Emancipatic: https://www.emancipatic.org/analisis-forense-ciberseguridad/

Sampieri, D. R. (2014). Metodologia de la Investigacion. En *Metodologia de la Investigacion* (pág. 175). Distrito Federea, Mexico: Mc Graw Hill Education.

Sardanyés, E. (s.f.). *¿Qué es el formjacking?* Obtenido de ESED: https://www.esedsl.com/blog/que-es-el-formjacking

Sistema Antifraude: comprenda qué es y cómo funciona. (27 de Enero de 2025). Obtenido de SYDLE: https://www.sydle.com/es/blog/sistema-antifraude-66fc2a51ffdeaa3386d36bf0

Sistema antifraude: protección clave para el sector financiero en LATAM. (s.f.). Obtenido de Topaz: https://www.topazevolution.com/es/blog/sistema-antifraude-para-sector-financiero#:~:text=Un%20sistema%20antifraude%20es%20la,identificando%20riesgos%20antes%20de%20p%C3%A9rdidas.

SousaI, V. D., Driessnack, M., & Costa Mendes, I. A. (Junio de 2007). *An overview of research designs relevant to nursing: Part 1: quantitative research designs*. Obtenido de SciELO: https://doi.org/10.1590/s0104-11692007000300022

Stryker, C. (s.f.). *¿Qué es la inteligencia artificial o IA?* Obtenido de IBM: https://www.ibm.com/mx-es/think/topics/artificial-intelligence

Transacciones electrónicas: ¿Qué son y por qué son seguras? (4 de Agosto de 2022). Obtenido de Docusing: https://www.docusign.com/es-mx/blog/transacciones-electronicas

Transaction monitoring – Everything you need to know. (s.f.). Obtenido de Fraud.com: https://www.fraud.com/post/transaction-monitoring#Transaction_monitoring_rules

Universidad Europea. (21 de Septiembre de 2023). *¿Qué es una entrevista?* Obtenido de Universidad Europea: https://universidadeuropea.com/blog/que-es-una-entrevista/

Universidad Veracruzana. (s.f.). *Introducción a la Investigación: guía interactiva*. Obtenido de UV.MX: https://www.uv.mx/apps/bdh/investigacion/unidad3/encuesta.html

What is a Relational Database (RDBMS)? (18 de junio de 2021). Obtenido de Oracle : https://www.oracle.com/es/database/what-is-a-relational-database/

What is Behavioral Analytics? (s.f.). Obtenido de RudderStack.: https://www.rudderstack.com/learn/data-analytics/what-is-behavioral-analytics/

What is it? What's it for? DataScientest. (27 de noviembre de 2023). Obtenido de DataScientest: https://datascientest.com/en/sqlalchemy-what-is-it-whats-it-for

What is Predictive Modeling? Types & Techniques. (s.f.). Obtenido de Qlik: https://www.qlik.com/us/predictive-analytics/predictive-modeling

What is skimming in cybersecurity? . (s.f.). Obtenido de MasterCard: https://b2b.mastercard.com/news-and-insights/blog/what-is-skimming-in-cybersecurity/

ANEXOS

A.1. Instrumentos Utilizados en la Investigación

a. La Entrevista

A continuación, se muestra una captura de todas las preguntas utilizadas en el instrumento de investigación, en este caso la entrevista.

Unidad de Análisis	Entrevistado
¿Considera que el número de fraudes ha aumentado, disminuido o se ha mantenido en los últimos años? ¿A qué cree que se debe?	Especialista de Riesgo Transaccional
¿Cuáles son los principales desafíos que enfrenta su institución en relación con la detección o prevención de fraudes?	Especialista de Riesgo Transaccional
¿La institución ha considerado implementar soluciones avanzadas de detección de fraude como las ofrecidas por grandes proveedores (por ejemplo, Decision Intelligence de Mastercard)?	Especialista de Riesgo Transaccional
¿Qué factores limitan la posibilidad de adquirir este tipo de soluciones en su institución?	Especialista de Riesgo Transaccional
En su experiencia, ¿qué funcionalidades considera indispensables en un software de detección de fraude?	Oficial de alertas

¿Qué tipo de datos recopilan actualmente durante las transacciones con tarjeta de crédito?	Especialista de Riesgo Transaccional
¿Qué requisitos regulatorios en materia de seguridad de la información debe cumplir su institución al tratar con datos de tarjetas de crédito?	Especialista de Riesgo Transaccional
¿La institución cuenta con políticas específicas para la protección de datos personales de los clientes?	Especialista de Riesgo Transaccional

b. La Entrevista

A continuación, se muestra una captura de todas las preguntas utilizadas en el instrumento de investigación, en este caso la encuesta.

Sección 1 de 4

Desafíos y Prácticas en la Prevención de Fraude con Tarjetas de Crédito en Instituciones Financieras Medianas y Pequeñas

Esta encuesta forma parte de una investigación académica orientada a comprender la situación actual del fraude con tarjetas de crédito en instituciones financieras medianas y pequeñas de Honduras, así como las prácticas, limitaciones y herramientas utilizadas para su prevención.

La información recopilada será tratada de manera **confidencial y anónima**, y será utilizada únicamente con fines investigativos. Agradecemos su valioso tiempo y colaboración para enriquecer este estudio.

Datos Generales del Participante

Descripción (opcional)

Años de experiencia en el área de riesgo o prevención de fraude *

- ○ Menos de 1 año
- ○ 1 a 3 años
- ○ 4 a 6 años
- ○ Más de 6 años

Ubicación de la sede principal de su institución *

- ○ Tegucigalpa
- ○ San Pedro Sula
- ○ Otra...

Nombre del cargo que desempeña actualmente *

- ○ Especialista en Riesgo Transaccional o equivalente en su institución.
- ○ Oficial de revisión de Alertas o equivalente en su institución.

Sección 2 de 4

Sección para el Especialista de Riesgo Transaccional o equivalente en su institución.

Descripción (opcional)

¿Su institución cuenta actualmente con alguna herramienta tecnológica para la detección de fraudes con tarjetas de crédito? *

- ○ Sí
- ○ No

Sección 3 de 4

Si cuenta actualmente con alguna herramienta tecnológica para la detección de fraudes con tarjetas de crédito

Descripción (opcional)

¿Esa herramienta dispone de inteligencia artificial para parametrizar sus reglas de monitoreo y detección de fraude? *

- Sí
- No

¿Con qué frecuencia reciben reportes o reclamos relacionados con fraude en tarjetas de crédito? *

- Diariamente
- Semanalmente
- Mensualmente

¿Cuáles son los tipos de fraude más comunes que enfrentan en su institución? *

- Fraude con Tarjeta Presente
- Fraude con Tarjeta no Presente
- Skimming

¿Cuáles serían las características más valoradas en una herramienta de detección de fraude en tiempo real para su institución? *

- [ ] Parametrizacion apoyada por Intaligencia Artificial
- [ ] Reportes en base a gráficos
- [ ] Bloqueos automáticos de tarjetas con sospecha de fraude
- [ ] Facilidad de uso

¿Preferiría una herramienta lista para usarse o una que permita ajustes y personalización interna? *

- ( ) Lista para usarse
- ( ) Que permita ajustes y personalización interna

¿Ha considerado su institución alianzas con universidades o terceros para desarrollar soluciones internas de bajo costo? *

- ( ) Sí
- ( ) No

En su opinión, ¿sería viable desarrollar una herramienta propia si se cuenta con apoyo externo y bajo presupuesto? *

- ( ) Sí
- ( ) No

¿Se analizan patrones históricos de transacciones para detectar fraudes o alertas inusuales? *

- Si
- No

¿La institución tiene algún proceso para identificar y reducir falsos positivos en sus alertas de fraude? *

- Sí
- No

¿El personal actual de su área tiene conocimientos sobre inteligencia artificial, análisis de datos o programación? *

- Sí
- No

Sección 4 de 4

Oficial de revisión de Alertas o equivalente en su institución.

Descripción (opcional)

¿Cuáles serían las características más valoradas en una herramienta de detección de fraude en tiempo real para su institución? *

- [ ] Facilidad de uso
- [ ] Bitacora de acciones tomadas en cada caso de fraude
- [ ] Gestión de casos amigable
- [ ] Reporte de casos automático por correo electrónico

A.2. Factibilidad del Proyecto

A.2.1 Técnica

A.2.1.1 Hardware

No.	Dispositivo	Especificaciones técnicas
1	Servidor de Aplicaciones	Un servidor de alto rendimiento, basado en arquitectura de doble zócalo con amplia capacidad de expansión de RAM y soporte para unidades de procesamiento gráfico (GPU), diseñado específicamente para ejecutar cargas de trabajo de Inteligencia Artificial de forma concurrente y eficiente. Este servidor garantizará la capacidad de procesamiento necesaria para analizar el volumen de 25,000 transacciones diarias con modelos de inferencia complejos, ofreciendo la flexibilidad para operar en un entorno físico o virtualizado y la escalabilidad para absorber futuros incrementos en la demanda o complejidad de los algoritmos de detección de fraude.
5	Computadoras Escritorio	Equipos con procesador Core i5 de décima generación o superior, memoria RAM de 16 GB, almacenamiento SSD de 512 GB o superior para garantizar alta velocidad en la ejecución de aplicaciones de análisis y supervisión, y tarjeta gráfica discreta básica (opcional para soporte de múltiples monitores). Deberán incluir puertos USB 3.0, USB-C y conexión Ethernet Gigabit para garantizar transferencia rápida de datos y conectividad estable.
2	Computadoras Laptop	Mismas características del equipo de escritorio.

Fuente: elaboración propia.

A.2.1.2 Software

No.	Software	Licencias, versiones, etc.
1	Windows	Windows 11 Pro (para estaciones de trabajo). Windows Server 2022 Standard Edition (para el servidor). Licencias por volumen Open Value u Open License para la organización.
2	MS-Office 365	Microsoft 365 Business Premium. Incluye las aplicaciones de escritorio, 1 TB de almacenamiento en OneDrive por usuario, y Exchange Online para correo corporativo. Licencia por usuario/anual.

3	MySql	MySQL Community Server 8.0 (gratuito, para desarrollo y entornos pequeños). Para el entorno de producción, considerar MySQL Enterprise Edition (licencia de suscripción anual) que incluye soporte técnico, herramientas de monitorización y características avanzadas de seguridad y alta disponibilidad.

Fuente: elaboración propia.

A.2.1.3 Comunicaciones

No.	Dispositivo	Características
1	Switch Administrable Capa 3	48 puertos Gigabit Ethernet, con al menos 4 puertos SFP+ de 10 Gigabit para uplinks. Es crítico para gestionar el tráfico de la red de forma inteligente, segmentar el tráfico (VLANs) para seguridad (ej., aislar el servidor) y proveer el ancho de banda necesario para la transferencia de datos de las transacciones.
2	Firewall de Próxima Generación (NG Firewall)	Appliance dedicado con licencias activas para IPS (Sistema de Prevención de Intrusiones) y Filtrado Web. Es el dispositivo de seguridad más importante, ya que protegerá toda la red interna y el servidor con las transacciones financieras de amenazas externas y accesos no autorizados.
3	Sistema de Respaldo de Energía (UPS)	UPS en torre o rackeable con capacidad suficiente para mantener el servidor, el switch y el firewall en funcionamiento durante al menos 30-45 minutos en caso de fallo eléctrico. Permite apagados automáticos controlados del servidor para prevenir daños por cortes de energía y pérdida de datos.

Fuente: elaboración propia.

A.2.1.4 Recurso Humano

1	Especialista en Infraestructura TI (SysAdmin)	Responsable de instalar, configurar y mantener el hardware (servidor) y el sistema operativo (Windows Server). Garantizará la estabilidad, seguridad y conectividad de la plataforma donde se aloja la aplicación.

2	Administrador de Bases de Datos (DBA)	Se encargará de la instalación, configuración, optimización y seguridad del servidor de MySQL (o la base de datos utilizada). Su rol es crítico para asegurar la integridad, disponibilidad y rendimiento de los datos de las transacciones.
3	Especialista en Ciberseguridad	Asegurará que la aplicación, el servidor y la base de datos cumplan con los protocolos de seguridad necesarios para manejar información financiera sensible, previniendo brechas de datos y accesos no autorizados.
4	Especialista en Riesgo Transaccional	Actúa como enlace entre el negocio y la tecnología. Definirá y ajustará las reglas de negocio, interpretará las alertas generadas por el sistema y validará los resultados para refinar el proceso de detección.
5	Oficial de Alertas	Encargado de utilizar la herramienta en la sección de monitoreo de transacciones.

Fuente: elaboración propia.

A.2.2 Operativa

El personal de las pequeñas y medianas instituciones financieras objetivo posee un conocimiento sólido del contexto de detección de fraude con tarjetas de crédito y ya utiliza un sistema básico para esta función, por lo que cuenta con la experiencia fundamental necesaria para operar el nuevo sistema. No se anticipa resistencia al cambio, ya que el sistema representa una mejora directa y una evolución natural de sus herramientas actuales, diseñado para asistirlos y no para reemplazar su criterio experto.

La transición operativa será facilitada por el hecho de que el nuevo sistema se integrará en el flujo de trabajo existente, requiriendo principalmente una capacitación focalizada en la interpretación de las nuevas alertas generadas por la IA y en el manejo de la interfaz renovada. El pequeño tamaño del equipo de usuarios finales permite un programa de capacitación personalizado y ágil, asegurando una adopción rápida y efectiva. En cuanto a la infraestructura, las instituciones ya cuentan con el espacio físico necesario, como áreas de trabajo y un cuarto de servidores

adecuado para alojar la nueva solución, minimizando la necesidad de inversiones adicionales en adecuación de espacios.

A.2.3 Económica

A.2.3.1 Hardware

No.	Dispositivo	Cantidad	Precio	Valor	Adquisición
1	Servidor de Aplicaciones	1	L296,000.00	L296,000.00	L296,000.00
3	Computadoras Escritorio	5	L16,000.00	L80,000.00	-
3	Computadoras Laptop	2	L24,000.00	L48,000.00	-
Total					L296,000.00

Fuente: elaboración propia.

A.2.3.2 Software

No.	Software	Cantidad	Precio	Valor	Adquisición
1	Windows Server 2022 Standard	1	L60,000.00	L60,000.00	L60,000.00
2	Windows 11 Pro	7	L1,235.00	L8,645.00	-
3	MS-Office 365	7	L6,520.00	L45,640.00	-
4	MySQL Enterprise Edition	1	L123,500.00	L123,500.00	L123,500.00
Total					L.183,500.00

Fuente: elaboración propia.

A.2.3.3 Telecomunicaciones

No.	Dispositivo	Cantidad	Precio	Valor	Adquisición
1	Switch Administrable Capa 3	1	L61,000.00	L61,000.00	-
2	Firewall de Próxima Generación (NG Firewall)	1	L74,100.00	L74,100.00	L74,100.00
3	Sistema de Respaldo de Energía (UPS)	1	L37,000.00	L37,000.00	-
Total					L74,100.00

Fuente: elaboración propia.

A.2.3.4 Recurso Humano

No.	Cargo	Cantidad	Meses	Salario/Mes	Salario Año

1	Especialista en Infraestructura TI (SysAdmin)	1	3	25,000.00	-
2	Administrador de Bases de Datos (DBA)	1	3	30,000.00	-
3	Especialista en Ciberseguridad	1	3	35,000.00	-
4	Especialista en Riesgo Transaccional	1	6	25,000.00	-
5	Oficial de Alertas	4	6	19,000.00	-
Total					-

Fuente: elaboración propia.

A.2.3.5 Cuadro Resumen

	Lempiras
Hardware	296,000.00
Software	183,500.00
Telecomunicaciones	74,100.00
Total	1, 553,600

Fuente: elaboración propia.

A.3. Lista de Requerimientos del Sistema

Tabla 23 Tabla de lista de requerimientos del Sistema.

No.	Módulo	Requerimiento	Explicación
1	Autenticación	Usuario activo y respectiva contraseña	Este módulo es el encargado de gestionar e identificar los accesos al aplicativo.
2	Registrar usuario	Acceso a insertar registros dentro de la tabla "usuarios"	Módulo encargado de registrar un nuevo usuario dentro del sistema.
3	Mostrar usuarios	Acceso a leer los registros de la tabla "usuarios"	Módulo encargado de mostrar los usuarios que tienen acceso al sistema.
4	Editar usuarios	Acceso a actualizar los registros de la tabla "usuarios"	Módulo encargado de editar los usuarios que tienen acceso al sistema, así como también desactivarlos.
5	Bitácoras de sesión	Acceso al módulo de autenticación. Acceso al procedimiento almacenado "ObtenerBitacoraSesión"	Módulo encargado de mostrar todos los inicios de sesión en el sistema, tanto los fallidos como los exitosos.

6	Bitácoras de Usuarios	Acceso al procedimiento almacenado "ObtenerBitacoraUsuarios"	Módulo encargado de mostrar la bitácora de todos los cambios realizados en el módulo de usuarios, tanto inserciones como modificaciones.
7	Bitácoras de Casos	Acceso al procedimiento almacenado "ObtenerBitacoraCasos"	Módulo encargado de mostrar la bitácora de todos los cambios realizados en el módulo de casos, tanto inserciones como modificaciones.
8	Bitácoras de Reglas	Acceso al procedimiento almacenado "ObtenerBitacoraReglas"	Módulo encargado de mostrar la bitácora de todos los cambios realizados en el módulo de reglas, tanto inserciones como modificaciones.
9	Ver Reglas	Acceso al procedimiento almacenado "ObtenerReglasCompletas"	Módulo encargado de mostrar todas las reglas de monitoreo registradas en el sistema.

10	Crear Reglas	Acceso a insertar registros dentro de la tabla "TbReglas"	Módulo encargado de registrar una nueva regla de monitoreo en el sistema.
11	Editar Reglas	Acceso al procedimiento almacenado "ModificarReglasCompletas"	Módulo encargado de editar todas las reglas de monitoreo presentes en el sistema.
12	Reglas con IA	Acceso completo a la tabla "TbReglas" Acceso de lectura a la tabla "transacciones"	Módulo encargado de generar y guardar reglas en base al comportamiento de fraude identificado en las transacciones.

13	Ver Transacciones	Acceso de lectura a la tabla "transacciones" Acceso al procedimiento almacenado "ActualizarEstadoTarjetaPorTransaccion" Acceso de escritura a la tabla "clientes" Acceso de escritura a la tabla "comercios" Acceso de escritura a la tabla "cuentas" Acceso de escritura a la tabla "mcc" Acceso de escritura a la tabla "modos_entrada" Acceso de escritura a la tabla "paises" Acceso de escritura a la tabla "productos" Acceso de escritura a la tabla "tarjetas" Acceso de escritura a la tabla "casos" Acceso de escritura a la tabla "transaccionesxcaso"	Módulo encargado de mostrar y gestionar todas las transacciones que se obtienen desde el core bancario, esto incluye transacciones sospechosas, descartadas y fraude. Además, permite abrir un nuevo caso de investigación o bloquear o desbloquear una tarjeta.

14	Casos Sospechosos y Mis Casos Sospechosos	Acceso de lectura y escritura a la tabla "casos" Acceso de lectura a la tabla "transaccionesxcaso" Acceso de lectura y escritura a la tabla "accionesxcaso"	Módulo encargado de gestionar todos los casos de investigación registrados en el sistema, se puede: editar el estado del caso, modificar el estado de las transacciones, visualizar y agregar acciones en el caso.
15	Reporte de Transacciones	Acceso de lectura a la tabla "transacciones"	Módulo encargado de generar los gráficos que recopilan información referente a las transacciones registradas en el sistema.
16	Reporte de Casos	Acceso de lectura a la tabla "casos" Acceso de lectura a la tabla "accionesxcaso"	Módulo encargado de generar los gráficos que recopilan información referente a los casos de investigación registrados en el sistema.
17	Efectividad de Reglas	Acceso de lectura a la tabla "TbReglas"	Módulo encargado de generar los gráficos que recopilan información

		Acceso al procedimiento almacenado "ObtenerEfectividadReglasPorFecha"	referente a las reglas de monitoreo registradas en el sistema.

Fuente: Elaboración propia.

A.4. OWASP

A.4.1 Vulnerabilidades del sistema.

A continuación, se presentan los resultados obtenidos mediante la utilización de la herramienta OWASP ZAP V.2.16.1, para la detección de vulnerabilidades.

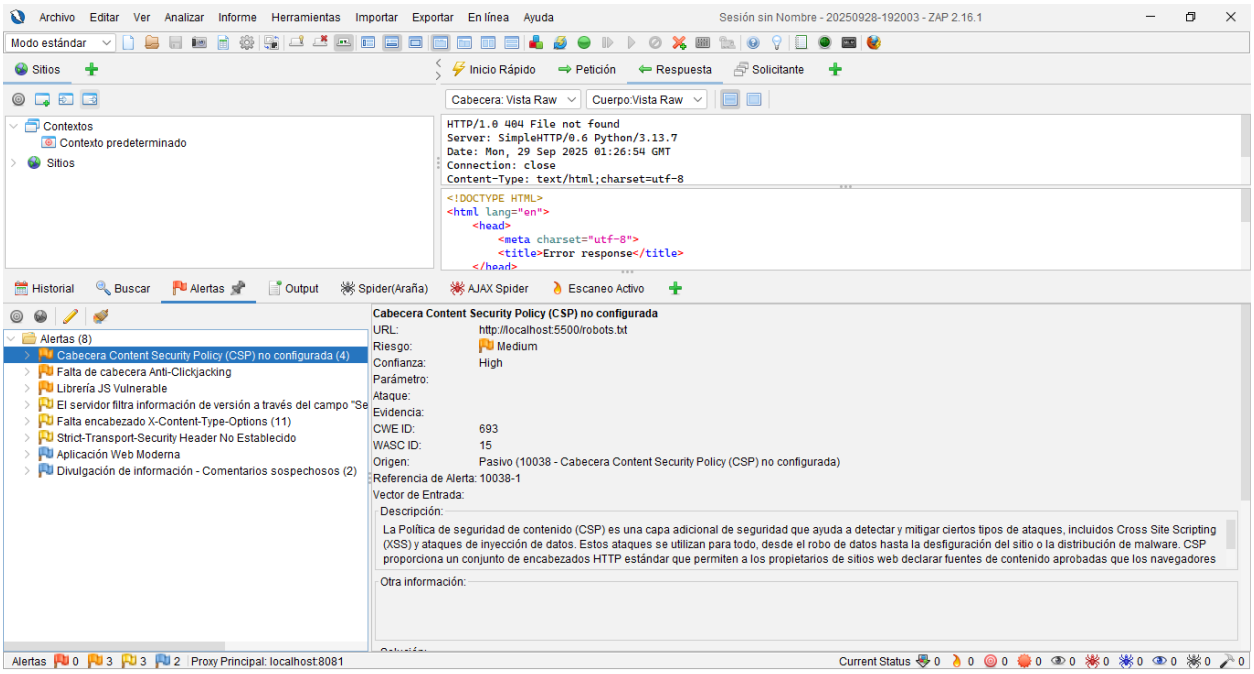


Ilustración 17 Vulnerabilidad Cabecera Content Security Policy (CSP) no configurada

Fuente: Herramienta OWASP ZAP.

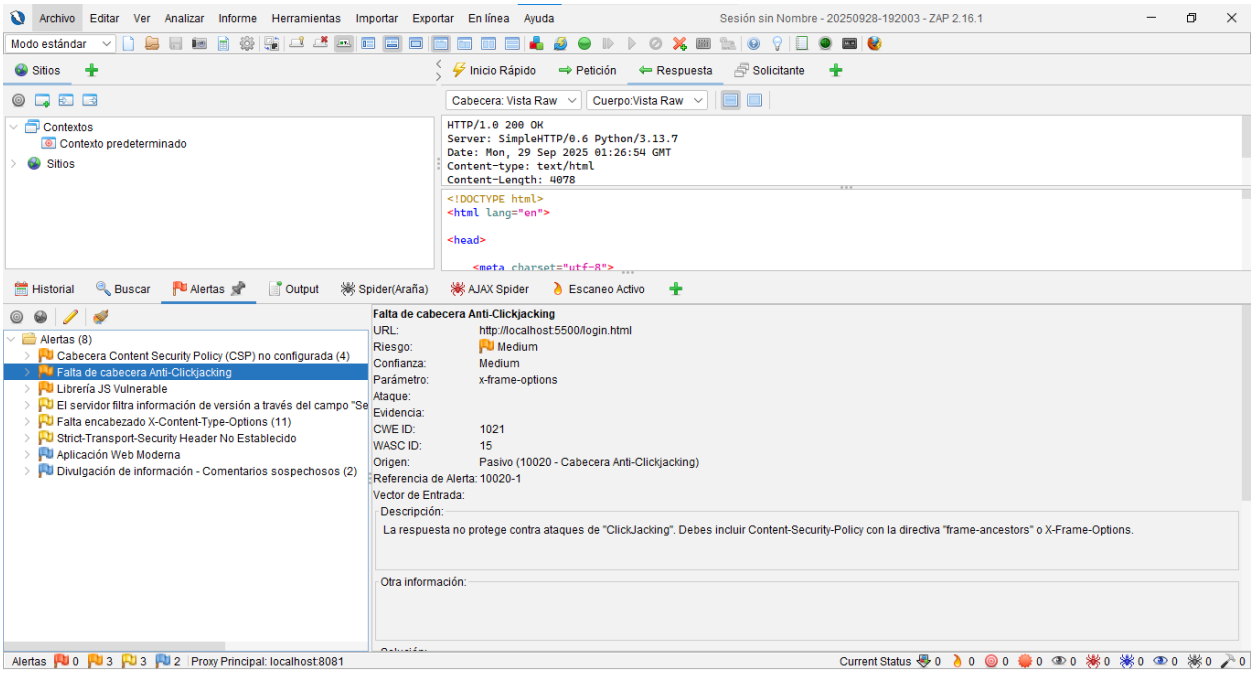


Ilustración 18 Vulnerabilidad Falta de cabecera Anti-Clickjacking

Fuente: Herramienta OWASP ZAP.

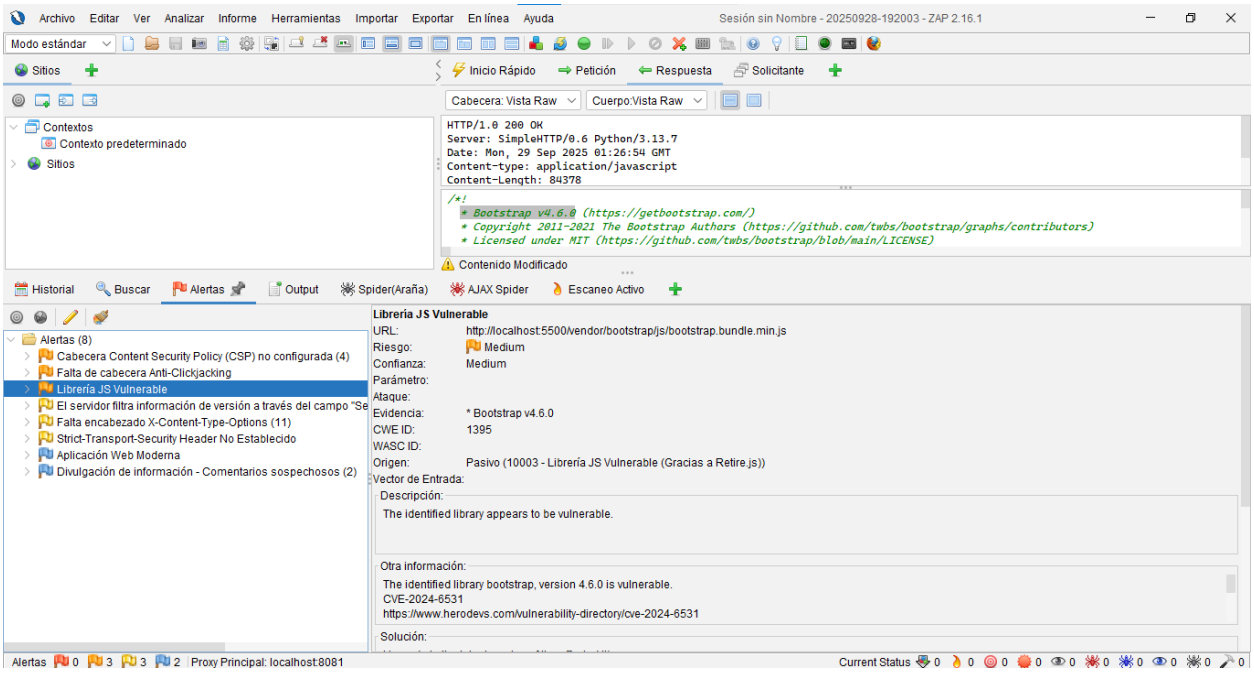


Ilustración 19 Vulnerabilidad Librería JS Vulnerable

Fuente: Herramienta OWASP ZAP.

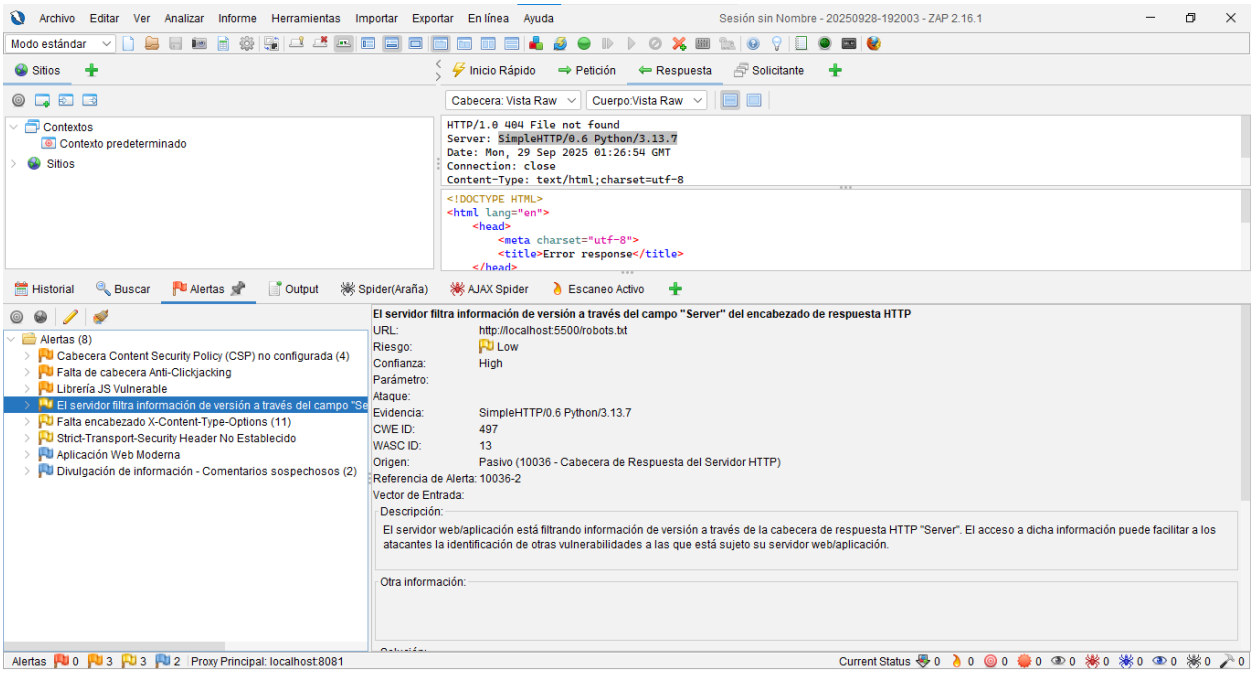


Ilustración 20 Vulnerabilidad El servidor filtra información de versión a través del campo "Server" del encabezado de respuesta HTTP

Fuente: Herramienta OWASP ZAP.

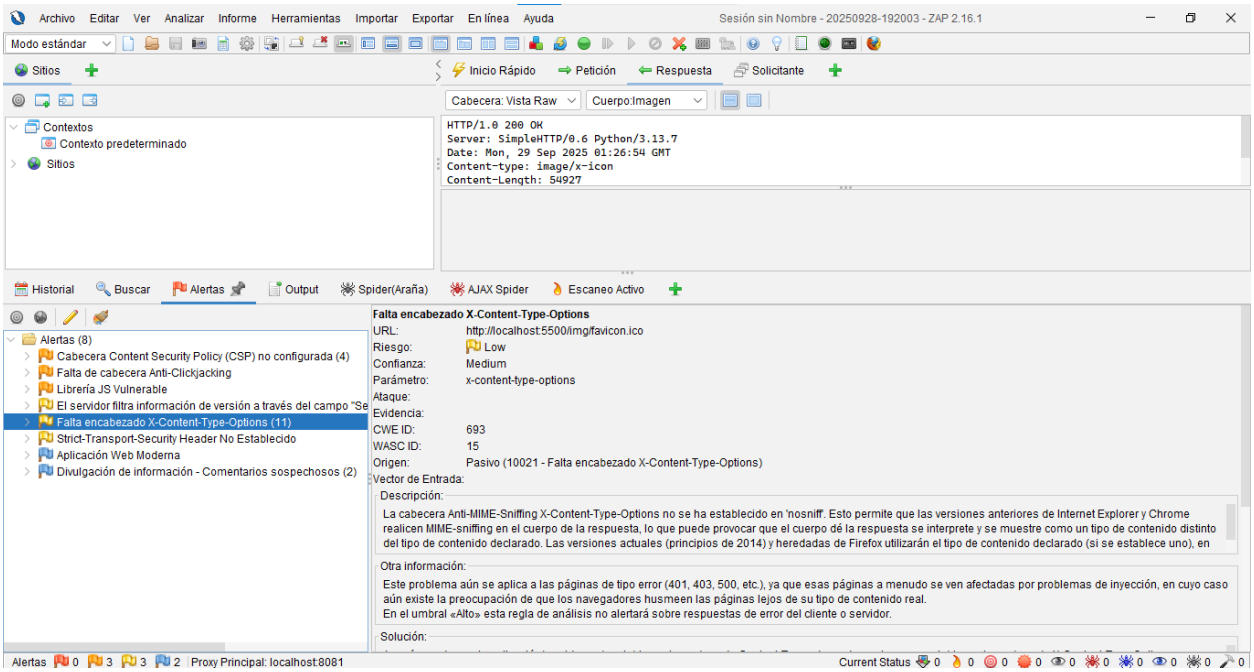


Ilustración 21 Falta encabezado X-Content-Type-Options

Fuente: Herramienta OWASP ZAP.

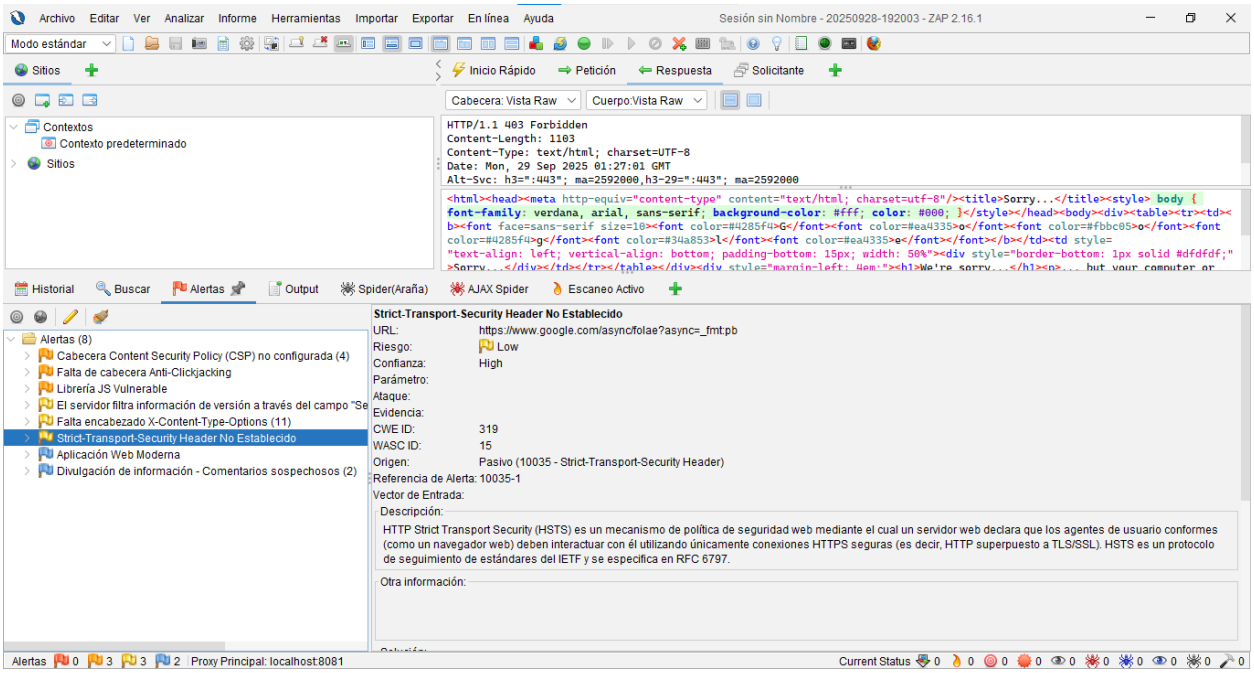


Ilustración 22 Vulnerabilidad Strict-Transport-Security Header No Establecido

Fuente: Herramienta OWASP ZAP.

A.4.2 Corrección de las vulnerabilidades del sistema.

A continuación, se presentan las correcciones aplicadas por las vulnerabilidades arrojadas por la herramienta OWASP ZAP V.2.16.1.

A.4.2.1 Vulnerabilidad Cabecera Content Security Policy (CSP) no configurada

Se realiza la configuración de las cabeceras CSP usando la librería FastAPI, usando el siguiente script:

```
from fastapi import FastAPI
from fastapi.middleware.httpsredirect import HTTPSRedirectMiddleware
from fastapi.middleware.trustedhost import TrustedHostMiddleware
```

```
app = FastAPI()


# Configurar CSP y otras cabeceras de seguridad
@app.middleware("http")
async def add_security_headers(request, call_next):
    response = await call_next(request)

    # Política de Seguridad de Contenido (CSP)
    response.headers["Content-Security-Policy"] = (
        "default-src 'self'; "
        "script-src 'self' 'unsafe-inline' https://cdnjs.cloudflare.com; "
        "style-src 'self' 'unsafe-inline' https://cdnjs.cloudflare.com; "
        "img-src 'self' data: https:; "
        "font-src 'self' https://cdnjs.cloudflare.com; "
        "connect-src 'self'; "
        "frame-ancestors 'none';"
    )

    # Otras cabeceras de seguridad importantes
    response.headers["X-Content-Type-Options"] = "nosniff"
    response.headers["X-Frame-Options"] = "DENY"
    response.headers["X-XSS-Protection"] = "1; mode=block"
    response.headers["Strict-Transport-Security"] = "max-age=31536000;
includeSubDomains"
    response.headers["Referrer-Policy"] = "strict-origin-when-cross-origin"
```

```
    return response


# Middleware para hosts confiables
app.add_middleware(TrustedHostMiddleware, allowed_hosts=["localhost",
"127.0.0.1", " localhost:5500"])


@app.get("/")
async def root():
    return {"message": "Correcto"}
```

A.4.2.2 Vulnerabilidad Falta de cabecera Anti-Clickjacking

Ya se configuró en la vulnerabilidad anterior usando:

```
# Cabecera Anti-Clickjacking
    response.headers["X-Frame-Options"] = "DENY"
```

A.4.2.3 Vulnerabilidad Librería JS Vulnerable

Se actualiza a la última versión de Bootstrap la cual es v5.3.8 mediante el link: Download · Bootstrap v5.3

A.4.2.4 Vulnerabilidad El servidor filtra información de versión a través del campo "Server" del encabezado de respuesta HTTP

Se agrega al encabezado la siguiente línea:

```
# Eliminar o modificar el encabezado Server
```

```
if "server" in response.headers:
    del response.headers["server"]
```

A.4.2.5 Vulnerabilidad Falta encabezado X-Content-Type-Options

Ya se soluciona con el script del punto 2.1 con esta línea:

```
response.headers["X-Content-Type-Options"] = "nosniff"
```