TRABAJO DE GRADO

Opción: Seminario en Metodologías Ágiles.

APLICACIÓN PARA EL REPORTE DE OPERACIONES SOSPECHOSAS (ROS)

Programa académico:

Ingeniería de Sistemas, Tecnología en Desarrollo de Software, Especialización Dirección de Operaciones

Autores del trabajo de grado:

Oscar Eduardo González Saavedra

Jessica Tatiana Cortés Rueda

Carlos Andrés Calderón

Tutor del trabajo de grado:

Alejandra Correa Giraldo

Facultad de Ingenierías

2025.

Tabla de Contenidos

Resumen

El presente proyecto desarrolla un prototipo de aplicación para gestionar Reportes de Operación Sospechosa (ROS) en entidades financieras, desde la captura de la información hasta su estructuración y envío oportuno a la UIAF, cumpliendo la normativa antilavado colombiana.

La solución propone una API REST que recibe los datos de alertas (transacciones y sujetos involucrados), los almacena y genera el formulario en formato estructurado (JSON/XML) para facilitar su validación y reporte. El objetivo central es mejorar la eficiencia y trazabilidad del proceso, reduciendo errores y tiempos de gestión.

Como marco de referencia, el trabajo se alinea con el SARLAFT y el rol de la UIAF como unidad de inteligencia financiera receptora y analítica de los reportes; se contextualiza además el conjunto de reportes exigidos (ROS, ausencia de sospechas y transacciones en efectivo).

Dado el corto tiempo para la proyección y desarrollo del proyecto, se adoptó la metodología Design Thinking con el fin de entender necesidades, definir problemas, idear alternativas y ajustar prototipos con retroalimentación continua, priorizando entregables funcionales.

La arquitectura del prototipo separa frontend y backend. El frontend, en HTML y JavaScript con Bootstrap, busca claridad y facilidad de uso, por su parte, el backend se implementa con FastAPI en Python, siguiendo un enfoque tipo microservicios y exponiendo un endpoint para el procesamiento del ROS. El almacenamiento se realiza en PostgreSQL para asegurar integridad, trazabilidad y compatibilidad con integraciones futuras.

Para llevar a cabo las pruebas, se priorizaron pruebas unitarias sobre la lógica y el endpoint principal, con trazabilidad mediante una matriz de casos (ID,

precondiciones, datos, pasos, resultado esperado). Se documentaron ejecuciones y evidencias, y se dejó como trabajo futuro ampliar a pruebas de integración y E2E.

En síntesis, el prototipo aporta un flujo técnico y normativo coherente para la gestión del ROS: captura estructurada, validación, persistencia y preparación para el reporte oficial, apoyándose en prácticas de diseño centradas en el usuario y en componentes tecnológicos modernos que favorecen la escalabilidad y el cumplimiento.

Palabras clave

Lavado de activos, prevención, análisis de riesgos, auditoría financiera, monitoreo transaccional.

Marco conceptual y contextual

A nivel global, los países han desarrollado marcos normativos y legales con el propósito de establecer directrices claras para que las entidades financieras puedan identificar, prevenir y reportar actividades relacionadas con el lavado de activos y la financiación del terrorismo (FATF, 2025). Estas regulaciones no solo buscan proteger la integridad del sistema financiero, sino también minimizar las consecuencias sociales y económicas que se derivan de estas actividades ilícitas, tales como el incremento en los índices de criminalidad, la expansión de redes de narcotráfico, la trata de personas, la corrupción y otros delitos conexos que desestabilizan el orden público y la economía formal (UNODC, 2025).

Dentro de estas normativas se describen de manera detallada los procedimientos que deben implementar los bancos, cooperativas, aseguradoras y demás instituciones sujetas a supervisión. También se especifica cuáles son las

entidades gubernamentales responsables de recibir los reportes generados por dichas instituciones, siendo común la creación de unidades de inteligencia financiera que analizan estos datos y los canalizan hacia las autoridades competentes.

Uno de los elementos fundamentales de estos esquemas de prevención es la elaboración de reportes o formularios específicos que documentan transacciones sospechosas. Estos documentos deben contener información precisa sobre la operación en cuestión, los montos involucrados, las partes que participan en la transacción y los motivos por los cuales se considera inusual o sospechosa. Su correcta elaboración y envío oportuno constituye una herramienta clave en la detección temprana de posibles delitos financieros.

A nivel continental, Estados Unidos y Canadá se destacan por el tamaño y la influencia de sus economías; el FMI clasifica a EE. UU. como la mayor economía mundial y ubica a Canadá dentro de las diez primeras (FMI, 2025). Debido a su peso geopolítico y financiero, estos países se encuentran constantemente expuestos a riesgos asociados con el crimen organizado transnacional y el terrorismo, lo que ha llevado a la creación de marcos regulatorios sólidos y el aprovechamiento de tecnologías avanzadas para reforzar sus sistemas de prevención.

En el caso de Canadá, la entidad encargada de recibir y analizar la información relacionada con transacciones sospechosas es el *Financial Transactions and Reports Analysis Centre of Canada* (FINTRAC). Esta institución exige a las entidades financieras el reporte de operaciones inusuales mediante los formularios denominados STR (*Suspicious Transaction Reports*). Para facilitar este proceso, FINTRAC ha desarrollado una interfaz de programación de aplicaciones (API) que permite la carga masiva de formularios en formato JSON. Esta API no solo define una estructura estandarizada para la entrega de los datos, sino que también incorpora un sistema de validación que asegura que la

información cumpla con los requisitos técnicos y normativos antes de ser aceptada.

Por su parte, Estados Unidos cuenta con la *Financial Crimes Enforcement Network* (FinCEN), organismo dependiente del Departamento del Tesoro que cumple funciones similares. Las instituciones financieras deben reportar las actividades sospechosas mediante el formulario FinCEN SAR Form 111. A diferencia del sistema canadiense, en este caso no se utiliza una API, sino que la transmisión de los reportes se realiza a través del método conocido como *Secure Direct Transfer Mode* (SDTM). Además, los formularios se presentan en formato XML, lo que exige un cumplimiento estricto de la estructura definida por FinCEN para asegurar la integridad y compatibilidad de los datos transmitidos.

Ambos países demuestran con estas medidas un enfoque integral, moderno y tecnológicamente avanzado para enfrentar el delito financiero, apoyándose en plataformas digitales seguras y esquemas de reporte bien definidos que permiten una detección oportuna de operaciones ilícitas.

En Colombia, las entidades financieras y otros sujetos obligados deben implementar y cumplir con los lineamientos del SARLAFT, es decir, el Sistema de Administración del Riesgo de Lavado de Activos y de la Financiación del Terrorismo. Este marco regulatorio establece una serie de medidas preventivas que buscan detectar, mitigar y reportar actividades sospechosas relacionadas con el delito financiero. Dentro de las obligaciones establecidas por el SARLAFT se encuentran la generación y envío de diferentes tipos de reportes, tales como el ROS (Reporte de Operación Sospechosa), el Reporte de Ausencia de Operaciones Sospechosas y el Reporte de Transacciones en Efectivo.

La entidad responsable de recibir, validar y analizar esta información es la Unidad de Información y Análisis Financiero (UIAF), organismo adscrito al Ministerio de Hacienda y Crédito Público, que actúa como la unidad de inteligencia financiera del país. Su función principal es recolectar y procesar información para detectar

posibles actividades relacionadas con el lavado de activos o la financiación del terrorismo, y canalizar estos hallazgos hacia las autoridades competentes.

El marco legal colombiano en esta materia se basa en varios instrumentos normativos. Entre ellos se destaca el Código Penal (Ley 599 de 2000), especialmente su artículo 323, que tipifica el delito de lavado de activos. También es fundamental la Ley 190 de 1995, conocida como el Estatuto Anticorrupción, y la Ley 526 de 1999, que dio origen a la UIAF. Además, la Superintendencia Financiera de Colombia (SFC) ha emitido regulaciones clave como la Circular Básica Jurídica 007 de 1996 y sus actualizaciones posteriores, como la Circular Externa 029 de 2014 y la Circular 055 de 2016, en las que se detalla la obligatoriedad de implementar el sistema SARLAFT y se establecen parámetros específicos para su adecuada gestión.

En el presente informe técnico se propone el diseño y desarrollo de un prototipo de aplicación para la creación y gestión de formularios ROS (Reportes de Operación Sospechosa). Este prototipo incluirá una API REST que recibirá la información generada por las alertas, es decir, los datos relacionados con las transacciones y los sujetos involucrados que la entidad financiera ha identificado como potencialmente sospechosos. Una vez recibida, dicha información será almacenada en una base de datos y, de forma automatizada, se invocará un servicio encargado de generar el formulario correspondiente en formato estructurado (por ejemplo, utilizando JSON o XML según el estándar requerido).

El objetivo principal de esta aplicación es facilitar la gestión eficiente de los formularios ROS, garantizando su correcta validación y permitiendo que sean reportados de manera oportuna a la Unidad de Información y Análisis Financiero (UIAF), en cumplimiento con la normativa vigente sobre prevención del lavado de activos y financiación del terrorismo.

Dado que el proyecto dispone de un plazo de tiempo corto, se ha elegido la metodología Design Thinking, un enfoque centrado en las personas que permite

generar, prototipar y validar ideas en ciclos breves: al iniciar con la empatía y la definición, transformamos rápidamente los hallazgos en soluciones tangibles, ajustando los prototipos con la retroalimentación obtenida para no perder tiempo; la colaboración multidisciplinaria y la visualización constante de avances mediante bocetos o maquetas facilitan decisiones ágiles y alineadas con el valor que el usuario necesita, de modo que cada iteración entregue resultados funcionales y útiles sin comprometer el cronograma.

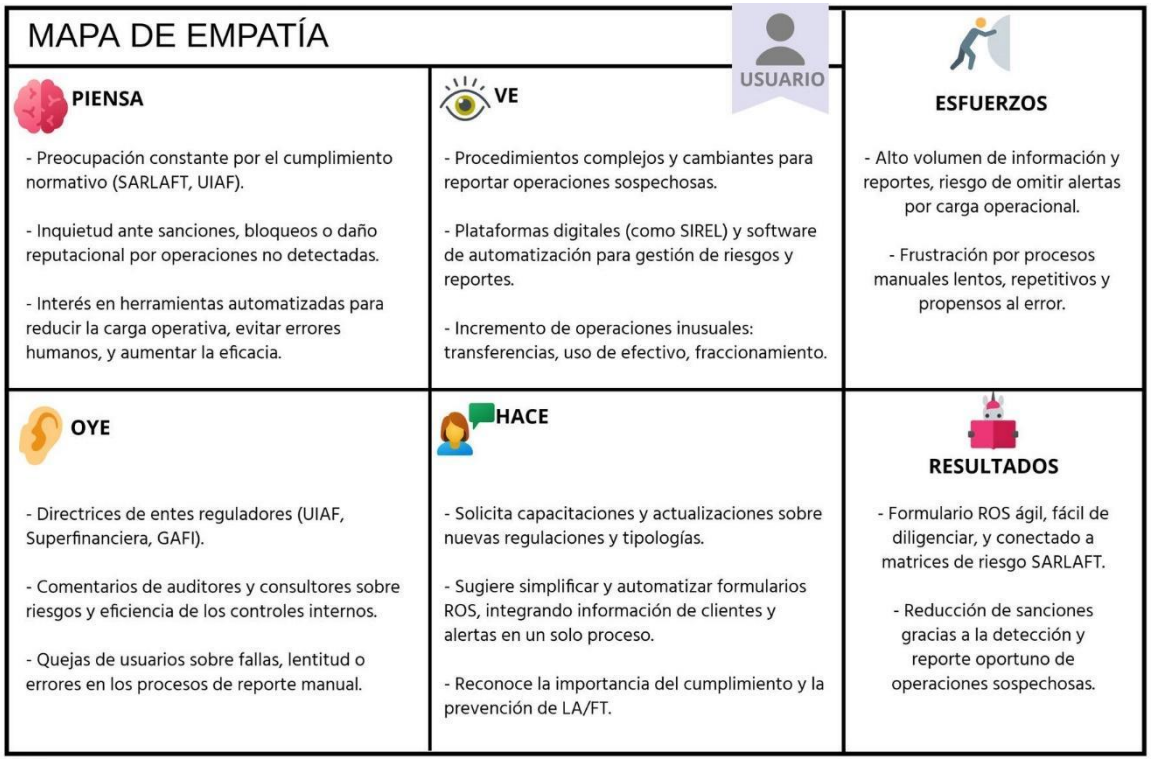
Desarrollo e implementación del aprendizaje

A continuación, se muestra el desarrollo del proyecto usando la metodología Design Thinking.

1. Empatizar

Este proceso está enfocado en las actividades de un ámbito ilícito cometidas en una o varias transacciones de carácter financiero, en este sentido y evidenciando las circunstancias de la situación actual el proceso por el cual se ejecutan. El diligenciamiento de este formato en especial hace que se pierda toda credibilidad en su proceso, por tal es la necesidad de hacerlo en forma virtual, para que de esta forma el proceso sea ejecutado de una forma transparente y sin ser manipulado.

Desarrollamos el mapa de empatía enfocado al sector financiero y procesos de reporte de operaciones sospechosas (ROS) en la lucha contra el lavado de activos, la financiación del terrorismo, la UIAF, SARLAFT y la automatización de procesos.



2. Definir

La automatización del SARLAFT y el reporte eficiente ante la UIAF son esenciales para fortalecer la prevención ante LA/FT, es por esto que, el usuario (oficial de cumplimiento) busca soluciones ágiles, seguras y que le permitan concentrarse en la gestión de riesgos y prevención, y no en tareas meramente administrativas.

En nuestras reuniones definimos los objetivos del proyecto, las historias de usuario y los roles.

A. Objetivos del proyecto:

En la siguiente tabla se detallan los objetivos a desarrollar con la implementación de la mejora y optimización del proceso de reporte de operaciones sospechas.

ID	Objetivo	Responsable
US-1	Crear una plataforma para el procesamiento del formulario ROS.	Product owner Desarrollador senior DBA Arquitecto
US-2	Como administrador de la plataforma quiero poder modificar datos cuando sea necesario.	Tester Product Owner Desarrollador Senior DBA Desarrollador Lead
US-3	Poder obtener la información en tiempo real para transferirla a la entidad encargada.	Arquitecto Product Owner Desarrollador Senior DBA
US-3	Crear una API que transfiera la información obtenida y aprobada a la entidad encargada.	Desarrollador Senior Desarrollador Lead DBA Tester

B. Historias de Usuario:

Para comprender a fondo las necesidades, deseos y motivaciones de los usuarios del sector financiero en relación con los reportes de operaciones sospechosas (ROS), la lucha contra el lavado de activos, la financiación del terrorismo, la UIAF, el SARLAFT y la automatización de procesos, es fundamental atender tanto las dinámicas regulatorias como los procesos internos en las organizaciones, la percepción de riesgo y el uso de tecnologías.

Análisis estructurado desde el punto de vista de usuario:

1. Motivaciones de los usuarios y entidades

- Cumplimiento normativo y protección reputacional: Las entidades financieras y sus empleados buscan cumplir rigurosamente las políticas y regulaciones (UIAF, SARLAFT) para evitar sanciones, proteger la reputación de la entidad y prevenir el involucramiento en delitos financieros.

- Seguridad y confianza en el sistema: Los usuarios y oficiales de cumplimiento requieren procesos reservados y confiables para el envío de ROS, así como la protección de la información reportada.

- Agilidad y simplificación del proceso: Hay un deseo creciente de automatizar procedimientos —como la generación y seguimiento de alertas, los procesos de reporte y conservación documental— para reducir la carga operativa y los errores asociados al factor humano. La automatización también responde al volumen y la complejidad transaccional del sector.

2. Identificación de necesidades y señales de alerta

- Capacitación y sensibilización: El personal debe estar permanentemente entrenado para identificar señales de alerta que indiquen operaciones inusuales, como cambios drásticos en patrones transaccionales, justificaciones insuficientes para determinadas operaciones, documentos alterados o comportamientos financieros incoherentes con el perfil del cliente.

- Claridad en roles y responsabilidades: Usuarios como los oficiales de cumplimiento y líderes de procesos requieren protocolos definidos para identificar,

analizar y reportar operaciones sospechosas. Deben tener el apoyo continuo de áreas especializadas para fortalecer la cultura de prevención.

- Herramientas analíticas y minería de datos: La capacidad de perfilar y monitorear clientes mediante herramientas estadísticas, integración de bases de datos y tecnologías de data mining, facilita la detección de patrones atípicos que pudieran estar vinculados al lavado de activos o financiación del terrorismo. Los usuarios esperan sistemas transparentes, flexibles y robustos en monitoreo y reporting.

3. Proceso de reporte (ROS) y la UIAF

- El ROS no es una denuncia: Está basado en sospechas fundamentadas, es anónimo, reservado y orientador para la UIAF, la cual lo utiliza para alimentar investigaciones financieras y, si es el caso, judiciales. Esto reduce los miedos de represalias y responsabilidades jurídicas a quienes reportan.

- Proceso Eficiente: El proceso inicia con la identificación de la operación, continúa con el análisis y culmina con el reporte mediante herramientas establecidas como SIREL de la UIAF, asegurando trazabilidad, conservación documental y retroalimentación al denunciante sobre la gestión realizada.

4. SARLAFT y automatización

- Prevención y monitoreo: SARLAFT y SIPLAFT establecen procedimientos para el conocimiento del cliente (KYC), clasificación y monitoreo de riesgos, capacitación constante y generación de reportes obligatorios. Esto permite anticipar amenazas y responder rápidamente ante transacciones atípicas.

• Automatización de procesos: La automatización mejora la recolección de datos, evaluación de operaciones, consolidación de alertas y generación automática de reportes, minimizando errores humanos y fortaleciendo la eficiencia. Las soluciones tecnológicas soportan el cumplimiento de normas, mejoran la experiencia de usuario y reducen costos operativos.

En resumen, el usuario interno del sector financiero (oficiales de cumplimiento, auditores, empleados operativos) necesita claridad normativa, capacitación, confianza, herramientas tecnológicas robustas y procesos flexibles pero seguros para gestionar, identificar y reportar operaciones sospechosas. A su vez, la automatización es una respuesta tanto a la presión regulatoria como a la necesidad de eficiencia y reducción del riesgo operativo en la lucha contra el lavado de activos y la financiación del terrorismo.

C. Roles:

Rol	**Responsable**
Product Owner	Jessica Tatiana Cortés Rueda
Desarrollador Senior	Carlos Andrés Calderón
DBA	Oscar Eduardo González Saavedra
Tester	Jessica Tatiana Cortés Rueda
Arquitecto	Carlos Andrés Calderón
Desarrollador lead	Oscar Eduardo González Saavedra

3. Idear

Durante la fase de ideación generamos una lluvia de ideas y las organizamos en un mural colaborativo en Canva.

4. Prototipar

El desarrollo del prototipo se estructuró en dos componentes principales: el frontend y el backend. Dado que se trata de una aplicación web, el frontend fue implementado utilizando HTML y JavaScript, incorporando Bootstrap como framework de estilos para lograr una interfaz clara, responsiva y fácil de usar.

En cuanto al backend, se optó por una arquitectura orientada a microservicios, lo cual permite una mayor escalabilidad y mantenimiento del sistema a futuro. Para ello, se desarrolló una API REST utilizando el framework FastAPI en lenguaje Python, que expone un endpoint encargado de recibir y procesar la información de las alertas generadas por las entidades financieras.

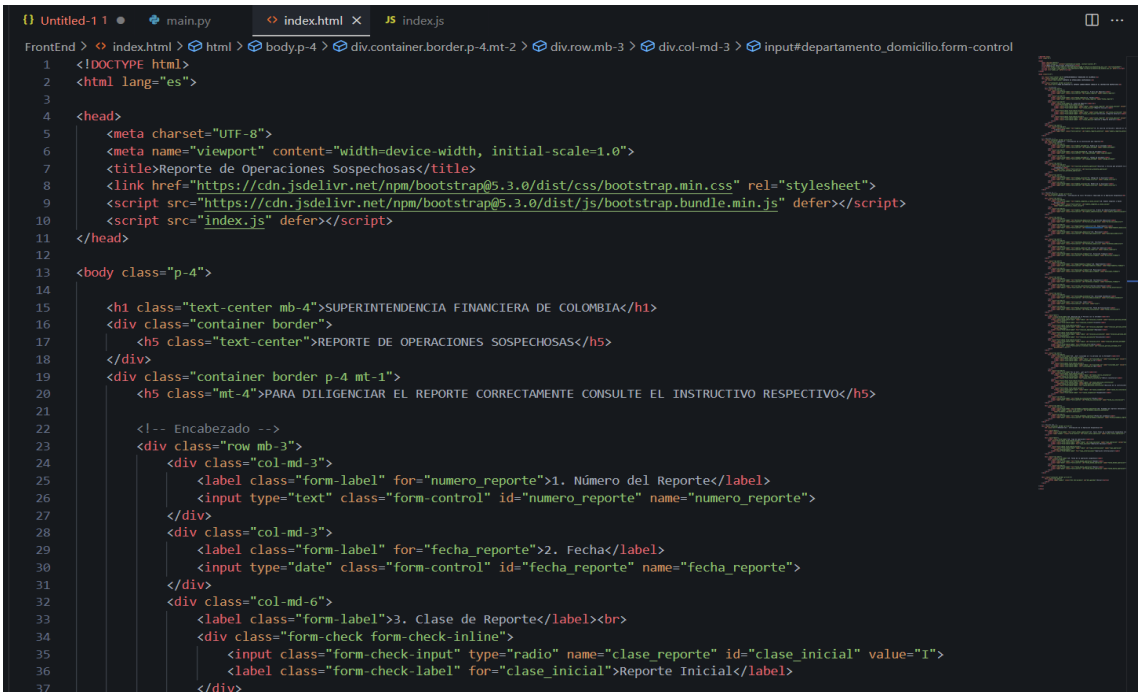
Para el almacenamiento de la información se utilizó una base de datos relacional, implementada con el sistema de gestión PostgreSQL, que permite organizar de manera estructurada los datos de las transacciones y los sujetos involucrados.

Esta arquitectura garantiza integridad, trazabilidad y compatibilidad con futuras integraciones o validaciones exigidas por la Unidad de Información y Análisis Financiero (UIAF).

A continuación, se incluirá el enlace al repositorio de GitHub que contiene el código fuente del proyecto, junto con capturas de pantalla representativas del código desarrollado para el prototipo.

Enlace: https://github.com/Oscar-Ed-Gonzalez/SeminarioDeGradoAPIyForm.git

Imágenes Frontend:



FrontEnd > JS index.js > <function> > buildPayload > institucion_reportante

```
// index.js
(() => {
    "use strict";

    const API_URL = "http://127.0.0.1:8000/ros";

    const $ = id => document.getElementById(id);

    // ==== Construcción del JSON ====
    function buildPayload() {
        return {
            encabezado: {
                numero_reporte: $("numero_reporte").value.trim(),
                fecha_reporte: $("fecha_reporte").value || null,
                clase_reporte: document.querySelector('input[name="clase_reporte"]:checked')?.value || null,
                numero_reporte_anterior: $("numero_reporte_anterior").value.trim()
            },
            institucion_reportante: {
                nombre_entidad: $("nombre_entidad").value.trim(),
                tipo_entidad: $("tipo_entidad").value.trim(),
                codigo_entidad: $("codigo_entidad").value.trim(),
                sucursal_presenta_operacion: $("sucursal_presenta_operacion").value.trim(),
                codigo_sucursal: $("codigo_sucursal").value.trim(),
                nombre_sucursal: $("nombre_sucursal").value.trim()
            },
            persona_implicada: {
                nombre_completo_o_razon_social: $("nombre_completo_o_razon_social").value.trim(),
                numero_identificacion: $("numero_identificacion").value.trim(),
                direccion_domicilio: $("direccion_domicilio").value.trim(),
                departamento_domicilio: $("departamento_domicilio").value.trim(),
                municipio_domicilio: $("municipio_domicilio").value.trim(),
                telefonos_domicilio: $("telefonos_domicilio").value.trim(),
                camara_comercio: $("camara_comercio").value.trim(),
                direccion_trabajo: $("direccion_trabajo").value.trim(),
                departamento_trabajo: $("departamento_trabajo").value.trim(),
                municipio_trabajo: $("municipio_trabajo").value.trim(),
                telefonos_trabajo: $("telefonos_trabajo").value.trim(),
```

SUPERINTENDENCIA FINANCIERA DE COLOMBIA

REPORTE DE OPERACIONES SOSPECHOSAS

PARA DILIGENCIAR EL REPORTE CORRECTAMENTE CONSULTE EL INSTRUCTIVO RESPECTIVO

1. Número del Reporte: RPT-002
2. Fecha: 13/08/2025
3. Clase de Reporte: (●) Reporte Inicial ( ) Corrección a Reporte Anterior ( ) Adición a Reporte Anterior
4. En caso de corrección o adición al reporte número:

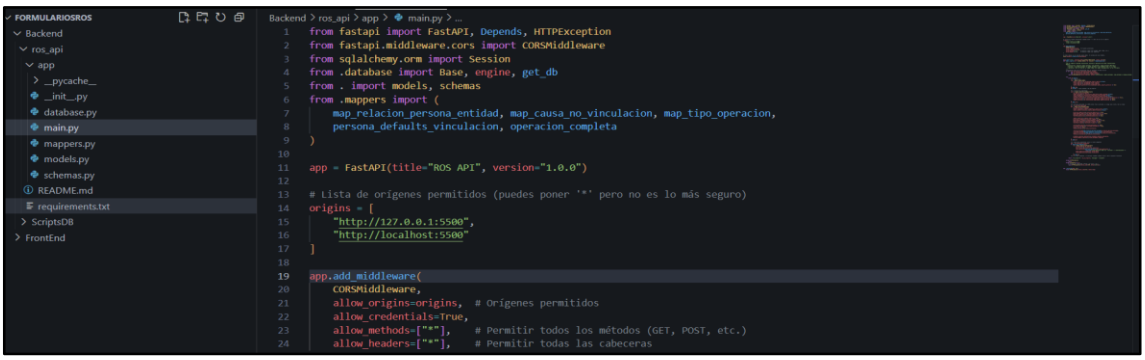
SECCIÓN I - Información de la Institución que reporta

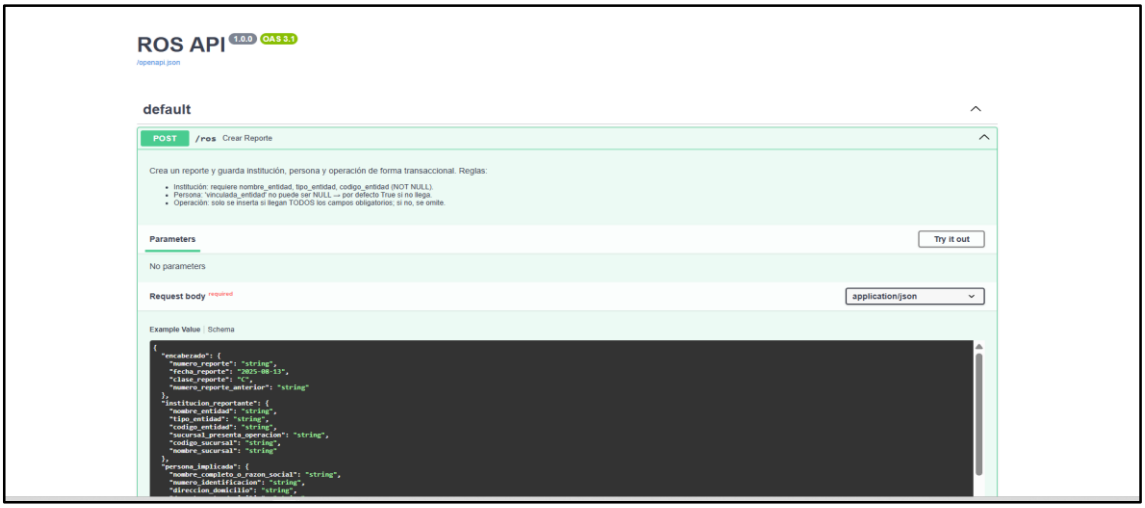
5. Nombre de la entidad: Bank Of New York
6. Tipo de entidad: Banco
7. Código de entidad: 111931
Sucursal u oficina que presentó la operación sospechosa:
8. Código de la Sucursal:
9. Nombre de la Sucursal:

SECCIÓN II - Información de la(s) Persona(s) Implicada en la Operación Sospechosa

10. Nombre Completo o Razón Social: Jessica Tatiana
11. Número de Identificación: 147852369
12. Dirección Domicilio:
13. Departamento:
14. Municipio:

Imágenes Backend:





5. Probar

Dado el tiempo del proyecto, se decidió no elaborar un plan de pruebas completo; en su lugar, se implementaron pruebas unitarias sobre la lógica de negocio y el endpoint principal, con trazabilidad mediante una matriz de casos (ID, precondiciones, datos de entrada, pasos, resultado esperado). Las ejecuciones se documentan en este informe y se incluyen las capturas de pantalla como evidencia. Como trabajo futuro, se considera ampliar la cobertura hacia pruebas de integración y E2E.

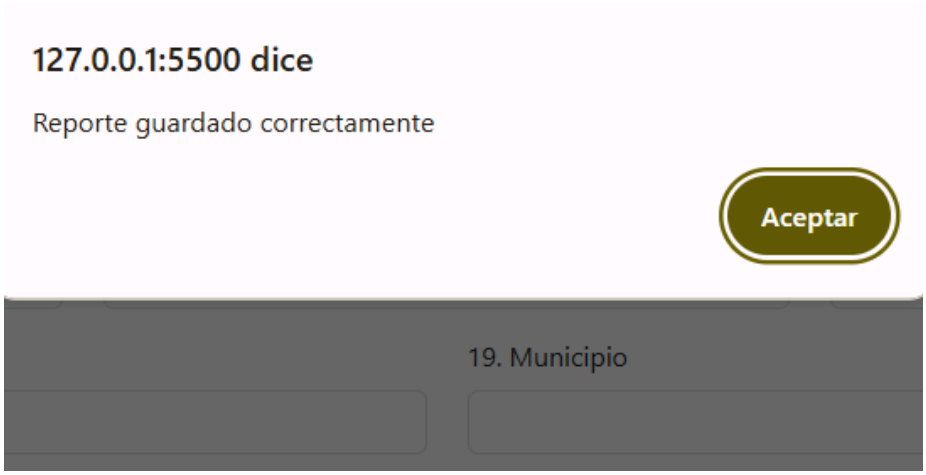
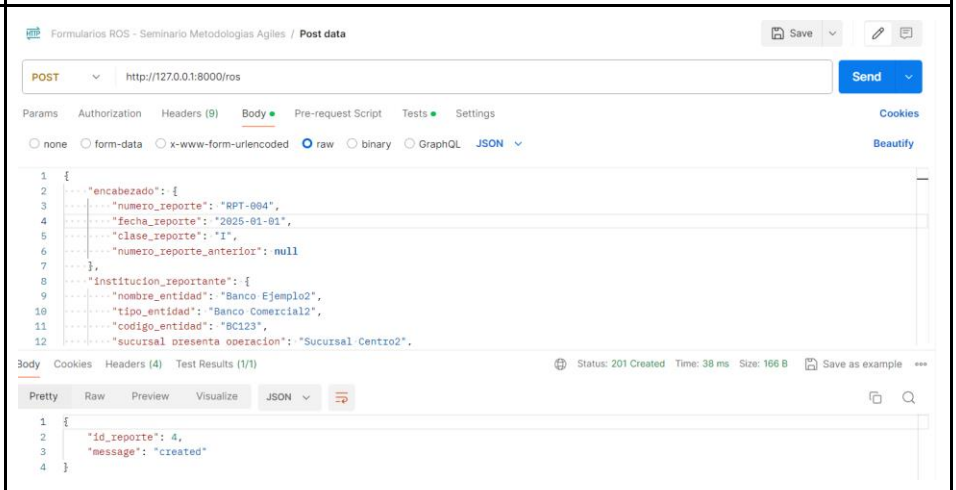
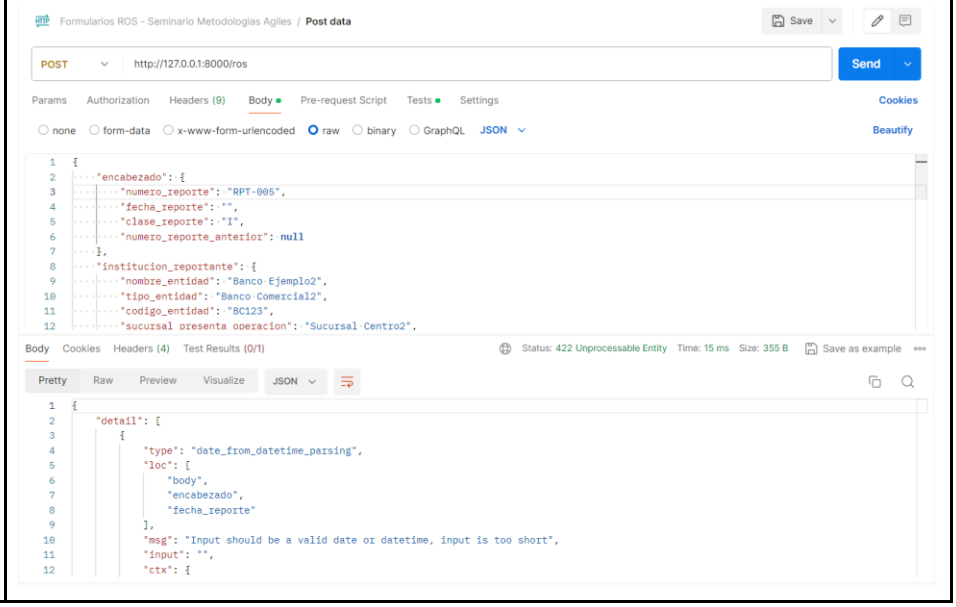
Matriz de casos:

ID	Dado/Cuando/Entonces	Datos	EndPoint/Flujo	Esperado
FD-001	Dado el formulario con campos obligatorios vacíos; Cuando el usuario hace clic en “Guardar”; Entonces no se llama al servicio y se muestran mensajes de requeridos.	El número de reporte y otros campos obligatorios están vacíos	Flujo UI “Nuevo ROS” → botón Guardar	Mensaje indicando los campos faltantes
FD-002	Dado datos válidos; Cuando el API devuelve 201; Entonces se muestra confirmación y se limpia el formulario (o redirige a detalle).	JSON válido	“Nuevo ROS” → Guardar	Alerta de éxito; formulario reseteado
BCKED-001	Dado un payload válido; Cuando hago POST; Entonces responde 201 con id_reporte numérico y un mensaje de éxito	JSON valido	POST /ros	201 + body con id_reporte
BCKED-002	Dado que falta un campo obligatorio; Cuando hago POST; Entonces responde 422 con detalle del campo.	JSON invalido	POST /ros	422 + mensaje con detalles del error del campo
BCKED-003	Dado un preflight CORS desde http://127.0.0.1:5500; Cuando	Origin http://127.0.0.1:5500	Network from browser	Access-Control-Allow-Origin, -Methods: POST

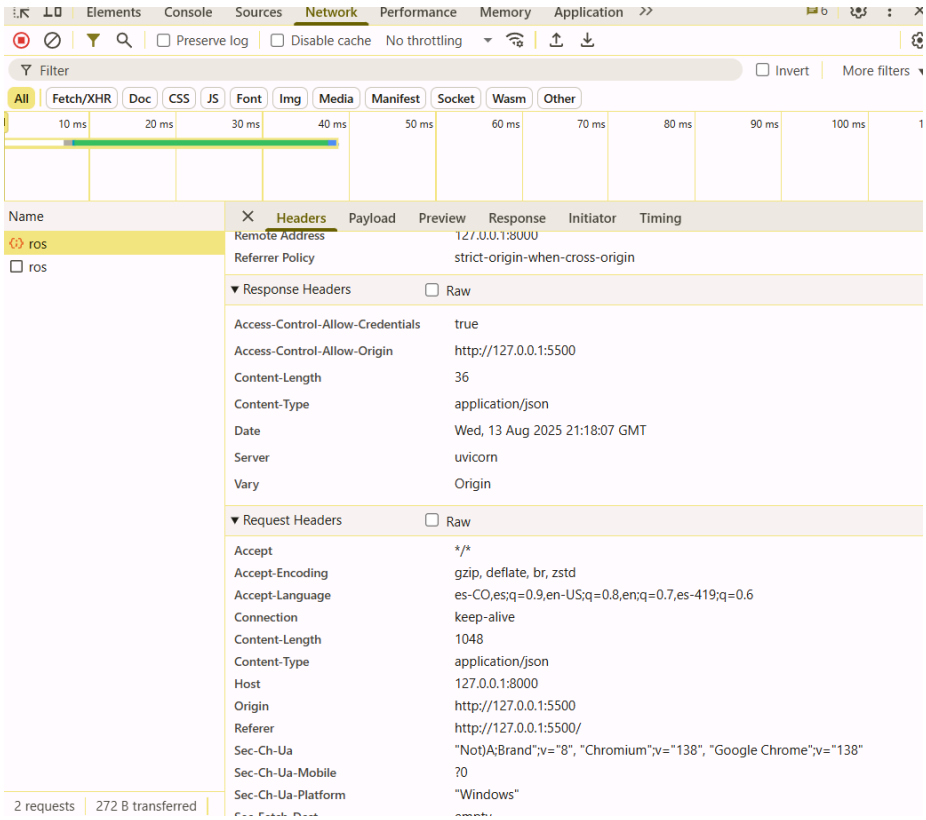
	hago OPTIONS; Entonces devuelve cabeceras CORS permitiendo POST.			
DB-001	Dado dos inserts válidos; Cuando se crean; Entonces id_reporte es único e incremental (PK).	Registros válidos	Inserción de reporte válida	IDs distintos; PK vigente
DB-002	Dado la tabla institucion_reportante con FK a reporte_ros; Cuando inserto con id_reporte inexistente; Entonces falla por FOREIGN KEY.	Id de reporte no registrado	INSERT INTO public.institucion_reportante	Error de FK (referencia inválida)

Resultado:

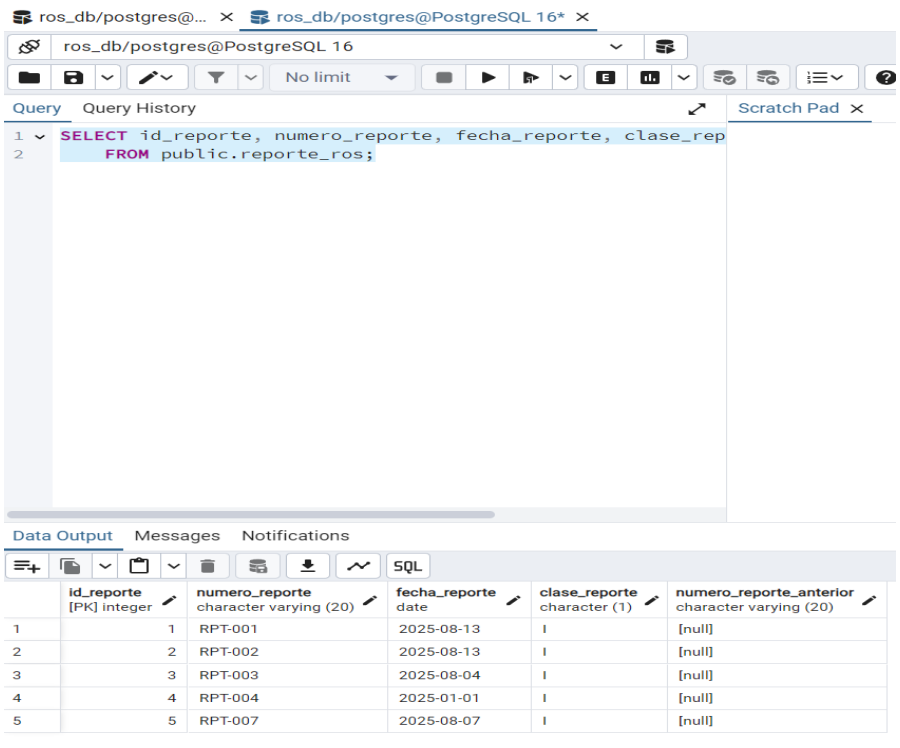
ID	Imagen
FD-001	

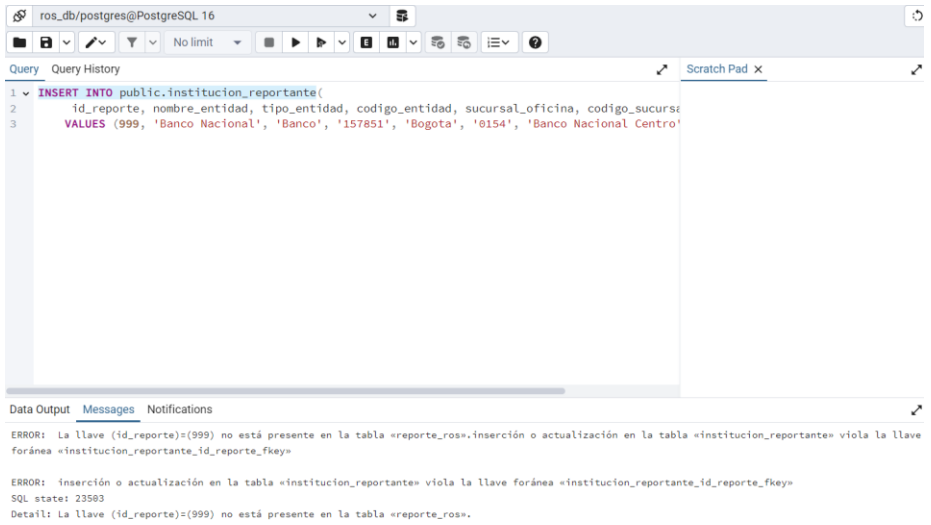
FD-002	
BCKED-001	
BCKED-002	

BCKED-003



DB-001



DB-002	

Conclusiones

- El enfoque de Design Thinking nos permitió integrar conocimientos de distintas carreras y sacar adelante un prototipo del formulario ROS. Aunque aún quedan pendientes en seguridad y escalabilidad, el resultado es consistente con los objetivos: validar la viabilidad y orientar un proyecto con potencial. Aplicamos todas las etapas de la metodología y las apoyamos con diagramas y estructuras; cada integrante aportó desde su experiencia técnica y conceptual.

- La elección de Python con FastAPI agilizó el desarrollo y nos permitió entregar un funcional a tiempo. Su ecosistema simplifica la construcción de endpoints y la puesta en marcha; además, Uvicorn facilitó el despliegue del prototipo. En nuestro contexto y cronograma, usar Java u otros stacks con mayor configuración (p. ej., servidores como Tomcat o un proxy como Nginx) habría añadido fricción y riesgo de retrasos.

- Profundizamos en los conceptos del lavado de activos y los sistemas que se implementan para evitarlo y combatirlo, identificando las instituciones colombianas a cargo de esta tarea, así como los marcos normativos y las metodologías que exige nuestro país, al final esto nos abre nuevas puertas para las áreas fintech, que a nuestra forma de ver nos ayudan a mejorar competitivamente y crecer profesionalmente.

Referencias

Financial Crime Academy. (s.f.). Las consecuencias del lavado de dinero son: comprender los impactos sociales, económicos y penales. *Financial Crime Academy*. https://financialcrimeacademy.org/es/consecuencias-del-blanqueo-de-capitales-conozca-las-amplias-consecuencias-del-blanqueo-de-capitales/

Financial Action Task Force (FATF). (2025). *The FATF Recommendations: International standards on combating money laundering, terrorist financing and proliferation financing*. https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Fatf-recommendations.html

United Nations Office on Drugs and Crime (UNODC). (2025). Money-laundering – Overview, de https://www.unodc.org/unodc/en/money-laundering/overview.html

FinCEN. (s. f.). *Frequently Asked Questions Regarding the FinCEN Suspicious Activity Report (SAR)*. https://www.fincen.gov/frequently-asked-questions-regarding-fincen-suspicious-activity-report-sar

Government of Canada, Financial Transactions and Reports Analysis Centre of Canada. (2025, 22 mayo). *Reporting suspicious transactions to FINTRAC | FINTRAC – Canada.ca*.

https://fintrac-canafe.canada.ca/guidance-directives/transaction-operation/str-dod/str-dod-eng

Unidad de Información y Análisis Financiero (UIAF). (s. f.). ¿Quiénes somos?.https://www.uiaf.gov.co/quienes-somos

Congreso de la República de Colombia. (1995). Ley 190 de 1995: Por la cual se dictan normas tendientes a preservar la moralidad en la administración pública y se fijan disposiciones con el fin de erradicar la corrupción administrativa (Estatuto Anticorrupción).
https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=321

Congreso de la República de Colombia. (1999). Ley 526 de 1999: Por la cual se crea la Unidad de Información y Análisis Financiero (UIAF) y se dictan otras disposiciones.
https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=6288

Congreso de la República de Colombia. (2000). Ley 599 de 2000: Código Penal.
https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=6388
Vlex. (s.f.). Circular Básica Jurídica 007 de 1996. https://vlex.com.co/vid/circular-externa-basica-juridica-398669581

Superintendencia Financiera de Colombia. (2014). Circular Externa 029 de 2014: Instrucciones relativas al Sistema de Administración del Riesgo de LA/FT (SARLAFT).
https://www.superfinanciera.gov.co/publicaciones/10083444/normativanormativa-generalcircular-basica-juridica-ce-parte-i-instrucciones-generales-aplicables-a-las-entidades-vigiladas-10083444/

Superintendencia Financiera de Colombia. (2016). Circular Externa 055 de 2016: Por la cual se modifican y adicionan instrucciones sobre el SARLAFT. https://www.superfinanciera.gov.co/loader.php?lServicio=Tools2&lTipo=descargas&lFuncion=descargar&idFile=1021869

Design Thinking en Español. (s.f.). *La primera plataforma online en difundir contenido libre en español sobre el método Design Thinking e innovación.* https://designthinking.es/?srsltid=AfmBOooiAqonhWaqWfjTQFh07RlHNg3B8oC6OThLdkOP4EVGymBuft5t