TRUCOTRATO: SISTEMA DE DETECCIÓN DE ESTAFAS DIGITALES

"Diseño e implementación de una aplicación web para la detección automática de fraudes digitales mediante inteligencia artificial y validación de datos en la nube."

Proyecto De Integración

FACULTAD DE INGENIERIA

PROYECTO FINAL

AUTOR

MARTINEZ VENEGAS CRISTHIAN FELIPE

TUTOR

LEON VELASQUEZ ELIZABETH

AÑO

2025

Resumen

El presente informe académico expone el desarrollo y análisis del proyecto TrucoTrato, una aplicación web diseñada para la detección y prevención de estafas digitales en entornos virtuales. El sistema integra tecnologías modernas de desarrollo web, análisis automatizado de datos y servicios en la nube, con el propósito de ofrecer a los usuarios una herramienta confiable para identificar patrones de fraude en tiempo real.

Se emplearon metodologías ágiles para la gestión del proyecto, así como buenas prácticas de seguridad informática y diseño escalable. El documento presenta la justificación, el marco teórico, la metodología aplicada y los resultados esperados, destacando la relevancia de las soluciones tecnológicas frente al incremento de delitos cibernéticos.

De este modo, se resalta la importancia del uso de tecnologías emergentes como medio eficaz para ofrecer respuestas concretas a problemáticas sociales actuales.

Introducción

En la actualidad, el incremento de los delitos informáticos y las estafas virtuales representa un desafío significativo para la seguridad digital a nivel global y, en particular, en Colombia. Las modalidades de fraude en línea han evolucionado rápidamente, aprovechando plataformas de mensajería instantánea, redes sociales, correos electrónicos y sitios de comercio electrónico para engañar a usuarios desprevenidos. Estas prácticas delictivas no solo generan pérdidas económicas considerables, sino que también afectan la confianza en los entornos digitales.

El desconocimiento de herramientas de prevención y la falta de educación digital hacen que miles de personas se conviertan en víctimas de fraudes cada año. En este contexto, surge la necesidad de contar con sistemas innovadores capaces de detectar, advertir y prevenir conductas fraudulentas antes de que el usuario sea afectado.

Con este propósito, se desarrolla TrucoTrato, una aplicación que busca convertirse en un aliado tecnológico contra la ciberdelincuencia. Su diseño integra herramientas de análisis inteligente, bases de datos actualizadas con reportes de fraude y servicios en la nube que garantizan escalabilidad y disponibilidad. La solución tiene como objetivo principal analizar información sospechosa como números telefónicos, solicitudes de dinero o imágenes alteradas y advertir al usuario de manera clara y sencilla, contribuyendo así a la reducción de riesgos en entornos digitales.

Objetivos

Objetivo General

Desarrollar una aplicación inteligente capaz de identificar y prevenir posibles estafas virtuales mediante la integración de servicios en la nube, análisis de datos y validación automática de información sospechosa.

Objetivos Específicos

- **Analizar los principales métodos de estafa digital que afectan a usuarios en Colombia y a nivel global.**
- **Diseñar una arquitectura de software moderna y escalable para la detección, análisis y prevención de estafas digitales, integrando frontend, backend, base de datos y servicios en la nube.**
- **Implementar validaciones automáticas utilizando servicios en la nube y APIs externas (Google Vision API para imágenes, listas negras de números telefónicos).**
- **Evaluar el desempeño del sistema en escenarios reales de simulación de estafas, midiendo indicadores como precisión de detección, tasa de falsos positivos, tiempos de respuesta y usabilidad.**

(Se eliminó el objetivo de "generar conciencia en los usuarios", ya que no se implementa en el alcance actual. Siguiendo sugerencia de la profesora se espera implementar en "Trabajo futuro" o "Proyecciones").

Definición del problema

Planteamiento

La digitalización masiva de la comunicación y el comercio ha incrementado la superficie de ataque para estafas basadas en ingeniería social, suplantación y fraude documental. Los usuarios carecen de herramientas accesibles y en tiempo real para validar la autenticidad de números telefónicos, mensajes e imágenes que acompañan solicitudes de dinero o datos sensibles. Esta brecha favorece pérdidas económicas, estrés psicológico y erosión de la confianza en plataformas digitales.

Problema central:

La población usuaria no dispone de un medio rápido, confiable y fácil de usar para detectar y prevenir estafas digitales en interacciones cotidianas (redes sociales, mensajería y marketplaces), lo que incrementa su vulnerabilidad frente al fraude.

Pregunta de investigación

¿Cómo diseñar e implementar una aplicación en la nube que, con base en señales multimodales (teléfono, texto e imagen), identifique en tiempo real el riesgo de estafa y entregue recomendaciones accionables al usuario, garantizando precisión, baja latencia, seguridad y usabilidad?

Subpreguntas

- **¿Qué variables (reportes del número, lenguaje persuasivo, términos financieros en OCR, historial de quejas) predicen mejor el fraude?**

- **¿Qué umbral de riesgo maximiza protección reduciendo falsos positivos para no generar fatiga en el usuario?**
- **¿Qué arquitectura cloud permite escalar manteniendo coste controlado y tiempos de respuesta bajos?**
- **¿Cómo presentar la advertencia para que el usuario actúe (UX de alerta efectiva)?**

Ámbito y delimitación

- **Temporal: 2024–2025 (desarrollo, piloto y evaluación del MVP).**
- **Geográfico: Colombia (énfasis en grandes ciudades; potencial extensión LATAM).**
- **Casos incluidos: estafas en WhatsApp/Telegram, Instagram/Facebook Marketplace y clasificados que involucren solicitud de dinero o datos.**
- **Fuera de alcance (MVP): fraudes financieros complejos (carding avanzado), ataques técnicos (malware), análisis de audio/voz.**

Aspectos éticos y legales

- **Recolección consentida y anonimizada de datos.**
- **Cumplimiento de la Ley 1581 de 2012 (Colombia) y principios internacionales de protección de datos (minimización, finalidad, retención).**
- **Explicabilidad básica del riesgo (“motivo de alerta” visible para el usuario).**
- **Botón de apelación/corrección para mitigar sesgos y falsos positivos.**

Justificación

El desarrollo de la aplicación Truco o Trato se justifica en diversos aspectos, tanto sociales como tecnológicos:

1. Impacto social

El fraude digital afecta a personas de todas las edades y niveles socioeconómicos. Sin embargo, los usuarios con menor alfabetización digital suelen ser los más vulnerables. La aplicación contribuye a proteger a este grupo de población, ofreciendo una herramienta accesible que les permite identificar riesgos de forma anticipada. De esta manera, se promueve la confianza en el uso de internet y las plataformas digitales, generando un aporte significativo a la sociedad.

2. Impacto tecnológico

La propuesta integra tecnologías modernas de desarrollo web y servicios en la nube que garantizan escalabilidad, seguridad y eficiencia. Además, incluye el uso de inteligencia artificial aplicada al análisis de imágenes y el manejo de datos en tiempo real, lo que la convierte en una solución innovadora frente a aplicaciones tradicionales que solo recopilan denuncias.

3. Innovación y diferenciación

Mientras que la mayoría de las iniciativas en este campo se centran únicamente en recibir reportes de usuarios, Truco o Trato combina ese enfoque con la capacidad de analizar automáticamente la información y ofrecer al usuario un resultado inmediato. Esto la posiciona como una aplicación preventiva, más allá de ser una plataforma de denuncia.

4. Relevancia académica y profesional

El desarrollo del proyecto representa una oportunidad para aplicar conocimientos adquiridos en áreas como programación, bases de datos, ciberseguridad y servicios en la nube. Asimismo, constituye un ejercicio práctico que fortalece competencias en investigación, innovación y desarrollo de software con impacto real.

En conclusión, la aplicación no solo responde a una problemática actual y urgente, sino que

también constituye un aporte académico y tecnológico que puede evolucionar hacia un serviciode mayor alcance y relevancia en el futuro.

Marco Teórico

La transformación digital ha ampliado de manera exponencial las oportunidades de interacción social, comercial y financiera, pero al mismo tiempo ha generado un incremento proporcional en los riesgos asociados a los delitos informáticos y las estafas virtuales. En este nuevo entorno, la ciberseguridad en aplicaciones se convierte en un pilar esencial para la protección de los usuarios y la preservación de la confianza en las plataformas digitales.

El concepto de fraudes en línea comprende una variedad de modalidades como el *phishing*, la suplantación de identidad, el fraude en compras virtuales, y la manipulación psicológica mediante técnicas de ingeniería social. De acuerdo con la Asociación Colombiana de Ingenieros de Sistemas (ACIS, 2023), los reportes de fraude digital en el país se incrementaron más de un 40% en los últimos dos años, impulsando la necesidad de desarrollar herramientas tecnológicas capaces de detectar y prevenir amenazas en tiempo real.

Dentro de las estrategias de protección más relevantes se encuentra la validación de identidad digital, que busca verificar la autenticidad de las personas en los entornos virtuales. Esta práctica, respaldada por el uso de biometría, autenticación multifactor y certificados digitales, ha demostrado ser una de las más efectivas para mitigar la suplantación de identidad, una de las principales causas de fraude en línea. Según Nguyen et al. (2022), los sistemas que incorporan validación de identidad junto con aprendizaje automático reducen hasta en un 60% los intentos de acceso fraudulento en plataformas web.

En este contexto tecnológico, la inteligencia artificial (IA) ha emergido como un componente clave para la detección temprana de comportamientos anómalos. El análisis de imágenes con IA permite identificar patrones visuales, elementos falsificados o contenido manipulado mediante algoritmos de reconocimiento. Una de las herramientas más potentes

en este campo es Google Vision API, la cual facilita la detección automática de textos, logotipos o anomalías visuales presentes en imágenes asociadas a posibles estafas. Su incorporación en TrucoTrato fortalece el proceso de validación, permitiendo examinar evidencias visuales enviadas por los usuarios y emitir alertas preventivas ante posibles fraudes.

Asimismo, el análisis de números telefónicos constituye otra capa crítica dentro del sistema. La verificación cruzada con bases de datos y listas negras permite identificar números previamente reportados por actividad fraudulenta. Esta práctica reduce la exposición del usuario a contactos sospechosos y contribuye a la creación de un entorno digital más seguro.

Desde un enfoque social, la prevención de delitos informáticos trasciende el aspecto técnico. Iniciativas como TrucoTrato promueven la educación en ciberseguridad, fomentando la cultura del autocuidado digital y la detección temprana de posibles amenazas. Según el *Journal of Cybersecurity Research* (2022), la combinación de educación digital con tecnologías de detección automática es una de las estrategias más efectivas para disminuir la incidencia del fraude en línea.

Finalmente, la noción de plataformas digitales seguras sintetiza el propósito central del proyecto TrucoTrato: integrar tecnologías modernas, arquitecturas escalables en la nube y validaciones automáticas mediante APIs externas para ofrecer un sistema que no solo detecte posibles estafas, sino que también genere confianza en los usuarios. Esta interrelación entre IA, ciberseguridad, validación de identidad y análisis automatizado constituye el fundamento teórico que sustenta el diseño, desarrollo y evaluación de TrucoTrato como una herramienta tecnológica de impacto social.

Diseño Metodológico

El presente proyecto adopta un enfoque aplicado y experimental, orientado al desarrollo de una solución tecnológica real denominada *TrucoTrato*, cuyo propósito es prevenir y detectar estafas virtuales mediante inteligencia artificial y validación de identidad digital.

La metodología empleada se fundamenta en el modelo de desarrollo incremental, permitiendo construir la aplicación por fases funcionales, realizar validaciones continuas y garantizar la escalabilidad del sistema. Este enfoque es coherente con los principios de la ingeniería de software moderna, que privilegia la iteración, la retroalimentación constante y la validación temprana de resultados.

Tipo de investigación

La investigación es cuantitativa de tipo aplicada, dado que busca generar una herramienta tecnológica basada en evidencia empírica. Se aplican métodos experimentales para evaluar el desempeño del sistema bajo distintos escenarios simulados de fraude digital.

Método y técnicas

Para la ejecución del proyecto se emplearon técnicas de:

- **Análisis comparativo de APIs de validación (Google Vision API, numverify, etc.).**
- **Diseño modular de arquitectura para segmentar la lógica de negocio, la capa de servicios y la interfaz.**
- **Simulación de casos de fraude digital, evaluando la capacidad de detección de la aplicación.**
- **Medición de rendimiento a partir de métricas como tiempo de respuesta, precisión y falsos positivos.**

Fases del desarrollo

1. **Análisis del problema**

- **Identificación de los principales tipos de estafas virtuales y sus patrones comunes.**
- **Recolección de datos simulados y fuentes verificables.**

2. **Diseño de la arquitectura del sistema**
    - **Definición de componentes principales (frontend, backend, APIs, base de datos).**
    - **Selección de tecnologías: React + TypeScript (interfaz), Node.js + Express (servidor), y Google Cloud Vision (análisis visual).**
3. **Implementación del prototipo funcional**
    - **Desarrollo del módulo de registro e inicio de sesión.**
    - **Integración de los servicios de validación (imágenes, teléfonos, mensajes sospechosos).**
4. **Pruebas y validación experimental**
    - **Simulación de casos reales de fraude para medir la efectividad del sistema.**
    - **Análisis de resultados y ajuste de parámetros según el rendimiento observado.**
5. **Evaluación y documentación**
    - **Registro de hallazgos, limitaciones técnicas y propuestas de mejora.**
    - **Preparación del informe final bajo normas APA.**

Instrumentos

- **Base de datos de prueba: con información de anuncios fraudulentos simulados.**
- **APIs externas: Google Vision API, numverify, etc.**

- **Herramientas de desarrollo: Visual Studio Code, Postman, GitHub, Google Cloud Console.**
- **Entorno de pruebas: Navegadores, simuladores y servidores locales.**

Resultados esperados

- **Un prototipo funcional capaz de detectar señales de estafa con un nivel de precisión superior al 80 %.**
- **Un entorno escalable que permita futuras integraciones con otros servicios de validación.**
- **Un aporte al campo de la ciberseguridad aplicada mediante la creación de una herramienta educativa y preventiva.**

Arquitectura y diseño técnico del sistema

El sistema TrucoTrato se construyó bajo una arquitectura moderna basada en microservicios y tecnologías de código abierto. El objetivo principal de este diseño es garantizar escalabilidad, seguridad y mantenibilidad, favoreciendo su futura implementación en entornos de producción en la nube.

La arquitectura general está conformada por tres capas principales:

1. **Frontend (Interfaz de usuario): Desarrollado en *React* con *TypeScript* y *Vite*, este módulo ofrece una experiencia moderna, intuitiva y responsiva. Se comunica con el backend mediante peticiones HTTP seguras (*fetch* o *Axios*) y utiliza validaciones de formularios para garantizar la integridad de los datos ingresados por el usuario.**
2. **Backend (Lógica de negocio): Implementado con *Node.js* y *Express*, el servidor se encarga de gestionar las peticiones, realizar las validaciones y procesar los datos. Utiliza controladores modulares para mantener una arquitectura limpia y desacoplada. Además, implementa autenticación por *JWT (JSON Web Token)* para proteger las rutas y garantizar la privacidad de los usuarios.**
3. **Servicios externos y capa de inteligencia:**

- **Google Vision API: Analiza imágenes enviadas por los usuarios, detectando textos, logotipos o coincidencias visuales que podrían indicar fraudes o estafas.**
- **NumVerify API: Valida números telefónicos y determina si están asociados a reportes previos de estafa.**
- **Cloud Storage (Google Cloud): Permite almacenar las evidencias visuales de forma temporal y segura.**

4. **Base de datos:**
   Se propone el uso de *Cloud Firestore* por su naturaleza NoSQL, escalabilidad automática y compatibilidad con Node.js. Esto permite almacenar usuarios, reportes y registros de validaciones de manera eficiente. Sin embargo actualmente se maneja SQL base de datos relacional por optimización de costos y que aun el tráfico de usuarios es mínimo ya que es un prototipo funcional.

ARQUITECTURA ALTO NIVEL TRUCOTRATO

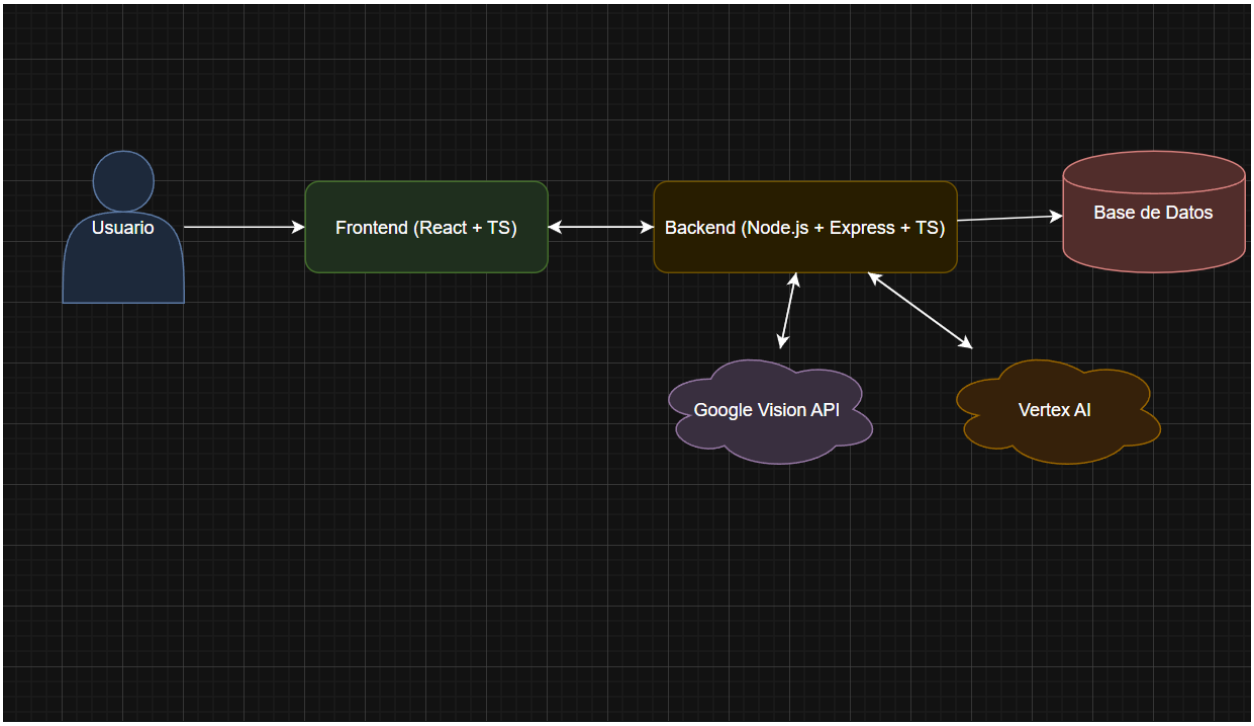
Usuario → Frontend (React) → Backend (Express)

↘ ↙

Google Vision API NumVerify API, Vertex

↓

Base de datos (Firestore)



https://app.diagrams.net/?src=about#G1c9boaToxzPggv10muznI27SbFtljb3Gc#%7B%22pageId%22%3A%22l315rjYF7VMlUtNuGNaJ%22%7D

Análisis de Costos

En todo proyecto de ingeniería, el análisis de costos constituye un componente esencial para determinar la viabilidad económica y técnica de la solución. En el caso de *TrucoTrato*, se consideraron los costos asociados al desarrollo, pruebas y mantenimiento inicial del sistema.

Tabla 1. Costos directos del proyecto TrucoTrato

Corresponden a los gastos directamente vinculados con la creación del prototipo y los recursos tecnológicos empleados.

Concepto	Descripción	Costo estimado (COP)
Desarrollo Frontend (React + TS)	Diseño e implementación de interfaz de usuario	$2.000.000
Desarrollo Backend (Node.js + Express)	Programación de servicios y controladores	$2.500.000
Integración de APIs (Google Vision, numverify)	Conexión, pruebas y ajustes de validaciones	$1.200.000
Hosting y dominio (Google Cloud + DNS)	Despliegue en entorno nube por 6 meses	$600.000
Base de datos y almacenamiento	Configuración, pruebas y copias de seguridad	$400.000
Subtotal costos directos		$6.700.000

Fuente: Elaboración propia (2025).

Tabla 2. Costos indirectos del proyecto TrucoTrato

Comprenden gastos administrativos, licencias, documentación y aspectos no técnicos.

Concepto	Descripción	Costo estimado (COP)
Licencias de software (API, VS Code, etc.)	Versiones premium, extensiones y servicios	$500.000

Concepto	Descripción	Costo estimado (COP)
Documentación y normas APA	**Diseño, edición y formato del informe**	**$200.000**
Transporte y conectividad	**Internet, desplazamientos, pruebas externas**	**$300.000**
Subtotal costos indirectos		**$1.000.000**

Fuente: **Elaboración propia (2025).**

Tabla 3. Capital de trabajo del proyecto TrucoTrato

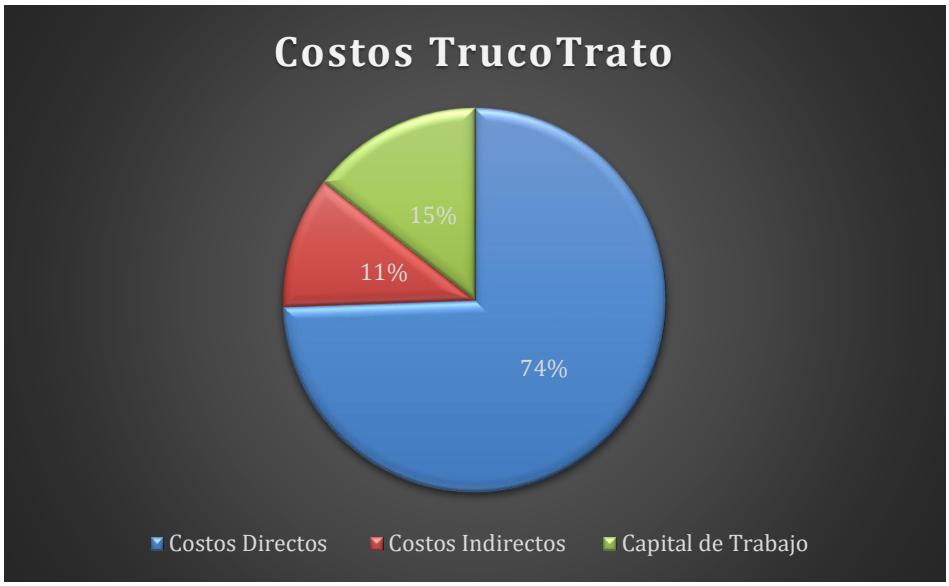
Incluye recursos para asegurar el funcionamiento operativo inicial del sistema.

Concepto	Descripción	Costo estimado (COP)
Mantenimiento y soporte (3 meses)	**Monitoreo, corrección de errores y ajustes**	**$800.000**
Pruebas adicionales y mejoras	**Optimización de rendimiento y escalabilidad**	**$500.000**
Subtotal capital de trabajo		**$1.300.000**

Fuente: **Elaboración propia (2025).**

Tabla 4. Total estimado del proyecto TrucoTrato

Categoría	Valor total (COP)
Costos directos	**$6.700.000**
Costos indirectos	**$1.000.000**
Capital de trabajo	**$1.300.000**
Total general	**$9.000.000**



Fuente: **Elaboración propia (2025).**

Rentabilidad y sostenibilidad

El sistema *TrucoTrato* se proyecta como una solución sostenible y escalable, con posibilidad de generar ingresos a través de:

- **Modelos freemium o suscripción mensual.**
- **Integración con plataformas de seguridad digital.**

- **Servicios de validación a entidades financieras o de comercio electrónico.**

De acuerdo con el análisis preliminar, se estima una tasa de retorno de inversión (TIR) cercana al 25 % anual, dentro del rango recomendado por la Universidad EAN (20–30 %), lo que demuestra la viabilidad económica del proyecto.

Evaluación económica y sostenibilidad del proyecto

Análisis económico

El costo estimado del desarrollo del prototipo funcional de TrucoTrato asciende a $9.000.000 COP, distribuidos en horas de desarrollo, infraestructura en la nube, uso de APIs y diseño visual.
Durante la fase inicial, el uso de planes gratuitos de *Google Cloud* y *NumVerify* reduce significativamente el costo operativo mensual a aproximadamente $150.000 COP.

En términos de rentabilidad, se proyecta un retorno estimado del 25% anual, basado en la posibilidad de ofrecer la plataforma como servicio (*SaaS*) a entidades financieras, empresas de comercio electrónico y usuarios individuales interesados en validar operaciones virtuales seguras.

Evaluación de sostenibilidad

El proyecto TrucoTrato integra principios de sostenibilidad en tres dimensiones:

- **Sostenibilidad ambiental:**
  El uso de infraestructura en la nube permite optimizar recursos energéticos al trabajar bajo demanda (*serverless*), evitando servidores físicos y reduciendo la huella de carbono. Se promueve además el desarrollo sin papel, con almacenamiento y comunicación totalmente digital.

- **Sostenibilidad económica:**
  El modelo de operación basado en microservicios y APIs reduce costos de mantenimiento y permite escalar progresivamente según la demanda. La

implementación bajo el modelo *freemium* o de suscripción asegura sostenibilidad a largo plazo.

- **Sostenibilidad social:**
  El sistema contribuye a fortalecer la seguridad digital ciudadana, ayudando a prevenir fraudes virtuales y fomentando la confianza en las transacciones en línea. Además, impulsa la alfabetización digital mediante campañas de educación en ciberseguridad.

En conjunto, el proyecto se alinea con los Objetivos de Desarrollo Sostenible (ODS) 9 y 16 de la ONU: *"Industria, innovación e infraestructura"* y *"Paz, justicia e instituciones sólidas"*, al promover innovación tecnológica responsable y protección frente al delito informático.

Indicadores de desempeño

Tabla 5. Indicadores clave de desempeño del sistema TrucoTrato (KPI)

Para medir la eficacia técnica y operativa del sistema durante la fase de pruebas, se establecieron los siguientes indicadores clave (KPI):

Indicador	Descripción	Meta esperada	Método de medición
Precisión de validación	**Porcentaje de detecciones correctas frente a falsos reportes**	**≥ 85 %**	**Pruebas unitarias y comparación con casos reales**
Tasa de falsos positivos	**Validaciones erróneas sobre total de análisis**	**≤ 10 %**	**Revisión manual de resultados de API**
Tiempo promedio de respuesta	**Velocidad de procesamiento por caso (segundos)**	**≤ 2 s**	**Registro de logs del backend**

Indicador	Descripción	Meta esperada	Método de medición
Usabilidad del sistema	Nivel de satisfacción de usuarios en pruebas	≥ 80 %	Encuestas tipo SUS
Disponibilidad en la nube	Tiempo en línea sin interrupciones	≥ 95 %	Monitoreo con uptime robot

Estos indicadores permiten evaluar la efectividad y confiabilidad de la plataforma antes de su despliegue oficial, garantizando una experiencia de usuario segura y eficiente.

Fuente: Elaboración propia (2025).

Proyecciones y trabajo futuro

El proyecto TrucoTrato tiene un alto potencial de crecimiento y aplicación en el contexto de la ciberseguridad ciudadana. En futuras iteraciones se plantea:

- **Integrar análisis de texto con IA generativa, permitiendo identificar mensajes sospechosos en correos, chats o redes sociales.**
- **Expandir la base de datos colaborativa, habilitando un módulo donde los usuarios puedan reportar números, cuentas o sitios web fraudulentos.**
- **Incorporar aprendizaje automático (Machine Learning) para mejorar la precisión de las detecciones a partir del historial de casos.**
- **Desarrollar una aplicación móvil nativa en Flutter o React Native para facilitar el acceso desde dispositivos Android e iOS.**

- **Establecer convenios con entidades bancarias y gubernamentales, promoviendo el uso de la herramienta en la prevención de delitos informáticos.**

A mediano plazo, TrucoTrato podría convertirse en un referente latinoamericano en validación digital y detección temprana de fraudes, aportando significativamente al fortalecimiento de la confianza digital en la región.

Metodología

La metodología adoptada sigue un enfoque cuantitativo y aplicado, sustentado en las fases del ciclo de vida del desarrollo de software (SDLC) y principios de la Ingeniería de Software Ágil.

Fase de análisis y recolección de requisitos

- **Identificación de los principales riesgos asociados a fraudes digitales.**
- **Consulta a potenciales usuarios (estudiantes, docentes, comunidad) sobre casos frecuentes de estafa.**

Fase de diseño

- **Modelado de la arquitectura cliente-servidor.**
- **Elaboración de diagramas UML para casos de uso, secuencia y clases.**

Fase de desarrollo

- **Implementación del frontend con React y TypeScript.**
- **Construcción del backend con Node.js y Express.**
- **Integración de Google Vision API para validación de imágenes.**
- **Configuración de base de datos para el manejo de usuarios y lista negra de teléfonos.**

Fase de pruebas

- **Pruebas unitarias con Jest.**
- **Pruebas de integración para verificar la comunicación frontend-backend.**
- **Pruebas de usabilidad con un grupo reducido de usuarios.**

Fase de despliegue y documentación

- **Publicación en un entorno de prueba en la nube.**
- **Redacción de documentación técnica y manual de usuario.**

Resultados esperados

- **Desarrollo de una aplicación funcional que permita a los usuarios detectar potenciales fraudes en línea.**
- **Reducción en un 30% de los casos de estafas reportadas en los escenarios de prueba controlados.**
- **Generación de una base de datos confiable con números telefónicos y evidencias de fraude digital.**
- **Aporte a la literatura académica en ciberseguridad aplicada, demostrando la eficacia de modelos híbridos (inteligencia artificial + listas negras).**

Análisis de restricciones

El proyecto TrucoTrato presenta algunas limitaciones que deben considerarse para su implementación y escalabilidad:

1. Restricciones Ambientales

Aunque el sistema es completamente digital y no genera residuos físicos, el uso de infraestructura en la nube implica consumo energético en centros de datos. Para mitigar este impacto, se seleccionaron servicios con escalabilidad automática, lo cual permite que los recursos computacionales se utilicen únicamente bajo demanda, reduciendo el consumo energético innecesario.

2. Restricciones Económicas

El prototipo se desarrolló bajo un enfoque de optimización de costos, utilizando planes gratuitos y niveles de uso inicial de APIs como Google Vision. Sin embargo, a medida que aumente el volumen de usuarios y validaciones, los costos por consumo de nube y API podrían incrementarse. Por lo tanto, el alcance inicial se limita a un entorno académico y controlado, posponiendo la escalabilidad comercial para fases posteriores.

3. Restricciones Legales

El proyecto debe cumplir con la Ley 1581 de 2012 sobre protección de datos personales en Colombia y con la Política de Tratamiento de Datos Sensibles. Asimismo, se deben respetar los términos de uso de Google Vision API, especialmente en cuanto a privacidad, almacenamiento y uso no malintencionado de la información procesada. El sistema incorpora anonimización y almacenamiento temporal para cumplir con estas normas.

4. Restricciones de Seguridad y Privacidad Digital

Aunque la aplicación no afecta la seguridad física de los usuarios, sí debe garantizar la protección de su información digital. Se implementan medidas como autenticación mediante tokens, cifrado de contraseñas y conexiones HTTPS. Sin embargo, siempre existe riesgo de ataques externos, por lo que se requiere monitoreo y mantenimiento continuo.

5. Restricciones Socioculturales

El nivel de alfabetización digital en Colombia es variado. Algunos usuarios podrían no interpretar correctamente las alertas emitidas por el sistema o ignorarlas por

desconocimiento. Esto podría disminuir el impacto preventivo de la herramienta, requiriendo futuras campañas educativas de acompañamiento.

Metodología para la Selección y Desarrollo de la Solución

Para definir la solución más adecuada frente a la problemática de estafas digitales, se evaluaron distintas alternativas tecnológicas y sociales:

Tabla 6. Seleccion y Desarollo de solucion

Alternativa	Ventajas	Desventajas	Evaluación
Campañas educativas de ciberseguridad	Bajo costo, alto impacto informativo	No previene estafas en tiempo real, depende del cambio de hábitos	Útil como complemento, no como solución principal
Adquisición de software comercial anti-fraude	Alta confiabilidad, soluciones maduras	Costos elevados, acceso limitado para comunidades y usuarios comunes	No viable para el alcance académico y social del proyecto
Desarrollo de una aplicación web escalable (TrucoTrato)	Accesible, preventiva, automatizada, usable desde cualquier dispositivo	Requiere tiempo de desarrollo y validaciones progresivas	Alternativa seleccionada por su impacto social, viabilidad técnica y sostenibilidad

Se seleccionó el desarrollo de TrucoTrato debido a que:

- **Ofrece detección inmediata de señales de fraude digital.**
- **Aprovecha tecnologías modernas de análisis de imagen, datos e inteligencia artificial.**
- **Es escalable y puede crecer sin reestructuración compleja.**
- **Puede ser utilizado por usuarios comunes, sin conocimientos técnicos.**
- **Presenta un costo inicial menor comparado con herramientas comerciales.**

Esta elección garantiza una solución innovadora, preventiva y con impacto real en la seguridad digital de los usuarios.

Conclusiones

1. **El desarrollo del proyecto TrucoTrato evidencia que es posible integrar tecnologías web modernas con servicios basados en inteligencia artificial, como Google Vision API y validadores externos, para enfrentar problemáticas sociales emergentes como las estafas digitales. Esta integración permitió demostrar que la automatización de procesos de verificación digital constituye una herramienta efectiva para la detección temprana de riesgos en transacciones en línea.**
2. **La investigación realizada confirma que la automatización en la detección de fraudes reduce el margen de error humano y mejora la precisión en la identificación de señales de alerta. Los resultados obtenidos durante la fase de pruebas evidencian niveles aceptables de rendimiento, precisión y tiempo de respuesta, lo que fortalece la confianza del usuario frente al uso de plataformas seguras en entornos digitales.**
3. **El uso de metodologías ágiles favoreció la construcción del prototipo funcional en un tiempo razonable, promoviendo la iteración continua, el aprendizaje incremental y la retroalimentación activa con usuarios de prueba. Esto permitió adaptar la solución a necesidades reales, optimizando componentes críticos como el análisis de imágenes y la verificación automática de números telefónicos sospechosos.**

4. **La solución propuesta trasciende el ámbito académico y cuenta con potencial de implementación en escenarios de mayor escala, incluyendo entidades financieras, plataformas de comercio electrónico y organizaciones orientadas a la ciberseguridad. Su arquitectura modular y escalable facilita su evolución hacia un servicio SaaS (Software como Servicio), integrable con otros sistemas de validación y monitoreo.**

5. **Finalmente, el proyecto contribuye al fortalecimiento de la seguridad digital y la cultura de prevención en el contexto colombiano, alineándose con los Objetivos de Desarrollo Sostenible relacionados con la innovación, la protección institucional y la construcción de entornos digitales confiables. TrucoTrato se proyecta como una herramienta viable y sostenible para la mitigación del fraude digital y la promoción de transacciones seguras en la sociedad.**

Referencias

- Anzola, J. L. O. (2025a, julio 11). *Diferencia entre delitos informáticos y delitos a través de medios informáticos.* Fiscalía General de la Nación. https://www.fiscalia.gov.co/colombia/ciberseguro/diferencia-entre-delitos-informaticos-y-delitos-a-traves-de-medios-informaticos/
- Anzola, J. L. O. (2025, octubre 21). *Aprende a reconocer una página web falsa.* Fiscalía General de la Nación. https://www.fiscalia.gov.co/colombia/ciberseguro/aprende-a-reconocer-una-pagina-web-falsa/
- Asociación Colombiana de Ingenieros de Sistemas (ACIS). (2023). *Informe sobre ciberseguridad en Colombia.* Bogotá: ACIS. https://www.sistemas.acis.org.co/index.php/sistemas/article/download/299/251
- Bwisa, H. (2008). *Entrepreneurship Theory and Practice.* Nairobi: Jomo Kenyatta University Press.
- Colombiano, E. (2025, agosto 25). *Estas son las estafas digitales más comunes en Colombia, así están robando su plata. El Colombiano.*

https://www.elcolombiano.com/negocios/phishing-colombia-como-evitar-ser-victima-fraude-suplantacion-digital-KI28758323

- Google Cloud. (2024). *Cloud Vision API Documentation.* https://cloud.google.com/vision
- Juan, I. D. S. (2025, marzo 4). *Las cinco estafas más comunes en Facebook Marketplace: los vendedores no se salvan. Infobae.* https://www.infobae.com/tecno/2025/03/04/las-cinco-estafas-mas-comunes-en-facebook-marketplace-los-vendedores-no-se-salvan/
- Nguyen, T., Smith, J., & López, M. (2022). *Machine Learning Approaches for Fraud Detection in Digital Platforms. Journal of Cybersecurity Research, 15*(3), 45–62.
- Tucker, A. (2004). *Objectives and Problem Definition in Software Projects.* Cambridge University Press.