



Universidad Distrital Francisco José de Caldas  
Facultad de Ingeniería  
Programa de Ingeniería de Sistemas

**Prototipo para apoyar el registro y trazabilidad de estados en el proceso de fotocomparendos aplicando tecnologías de redes distribuidas**

**Presentado por:**

Laura Catalina Preciado Ballén  
Cristian Stiven Guzmán Tovar

**Director:** Julio Barón Velandia, PhD

**Jurado:** Roberto Pava Díaz, PhD

# Agenda

Contexto y formulación del problema

Objetivos

Metodología e implementación

Validación y pruebas

Demostración del prototipo

Conclusiones y aportes

Trabajo futuro

Espacio de preguntas

## **Contexto y formulación del problema**

---

# Contexto: el sistema de fotocomparendos en Bogotá

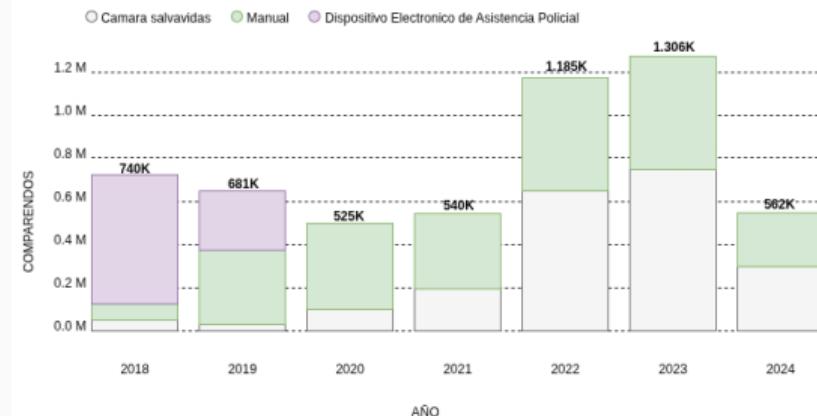
## Escala operativa (Sistema FÉNIX):

- **1.9 millones** de comparendos emitidos entre 2018–2024 (Secretaría Distrital de Movilidad, 2024)
- **457,000** comparendos semestrales en promedio
- Arquitectura centralizada (BD relacional)

Figura 1

*Comparendos emitidos por semestre*

### Comparendos por medio de detección y año



Fuente: Secretaría Distrital de Movilidad (2024).

# Indicadores de la problemática

## Gestión ciudadana

- Tasa de impugnación: **34.1 %**
- Carga operativa: **155,854 PQRSD semestrales**

## Impacto fiscal

- Presunto detrimento patrimonial: **\$8,000 millones** (Contraloría de Bogotá, 2024)

## Vulnerabilidades identificadas:

- Fraude a ciudadanos mediante intermediarios ilegales (Semana, 2023)
- Confianza en administradores centrales sin garantías criptográficas
- Inmutabilidad no verificable por la ciudadanía
- Auditoría opaca para el control institucional

# Formulación del problema

## Pregunta de investigación

*¿Cómo mitigar el riesgo de pérdida o alteración de la integridad de los datos asociados a todos los estados en el proceso de fotocomparendos en Bogotá mediante el uso de tecnologías de redes distribuidas que garanticen el registro, la trazabilidad, la autenticidad y la confidencialidad de la información?*

**Limitaciones del modelo actual (FÉNIX):** confianza en administradores centrales, inmutabilidad no garantizada criptográficamente, trazabilidad dependiente de controles internos, auditoría opaca para la ciudadanía.

## Hipótesis

Las tecnologías de redes distribuidas (blockchain + IPFS) pueden proporcionar garantías criptográficas de integridad y transparencia verificable sin intermediarios en el sistema de fotocomparendos en Bogotá.

## Objetivos

---

# Objetivo general

## Objetivo general

Desarrollar un prototipo software tecnológico que facilite el registro y la trazabilidad de los estados en el proceso de fotocomparendos en Bogotá, mediante la aplicación de tecnologías de redes distribuidas, para el fortalecimiento de la integridad y autenticidad de la información reduciendo los riesgos asociados a su confidencialidad.

## Objetivos específicos

1. **Analizar** el proceso actual de registro de fotocomparendos a partir del marco jurídico, regulatorio e informes de auditoría, para identificar vulnerabilidades, requisitos funcionales y no funcionales.
2. **Desarrollar** un prototipo con arquitectura híbrida basado en blockchain permisionado (Hyperledger Fabric) y blockchain público (Ethereum), integrando almacenamiento distribuido mediante IPFS.
3. **Evaluar** la viabilidad técnica y funcional mediante un plan de pruebas que incluya inmutabilidad, trazabilidad, rendimiento y verificación de integridad de documentos.

## **Metodología e implementación**

---

# Enfoque metodológico: desarrollo por prototipos

## Justificación del modelo:

- **Naturaleza exploratoria:** tecnologías emergentes sin antecedentes locales
- **Requisitos evolutivos:** marco normativo en constante cambio
- **Verificación temprana:** validar hipótesis antes de escalar

## Decisión metodológica

El modelo de prototipos permite mitigar riesgos técnicos y facilitar ajustes iterativos ante cambios normativos o tecnológicos.

## Ciclo iterativo de prototipado



# Arquitectura híbrida: decisión de diseño

**Problema:** una sola plataforma blockchain no satisface simultáneamente todos los requisitos.

- Privacidad de datos personales (Ley 1581/2012)
- Transparencia pública ciudadana (Ley 1712/2014)
- Rendimiento (457,000 comparendos semestrales)
- Costos operativos predecibles

**Tabla 1**

*Componentes de la arquitectura híbrida*

Componente	Tecnología	Justificación	TPS
Capa privada	Hyperledger Fabric v2.5	Control de acceso PKI, sin gas fees	2K–20K
Capa pública	Ethereum (Sepolia)	Verificación ciudadana	15–30
Storage privado	IPFS privado	Evidencias sensibles	–
Storage público	IPFS público	Hashes de verificación	–

Nota: Componentes de la arquitectura.

# Actores y funcionalidades principales

Figura 2

Diagrama de casos de uso



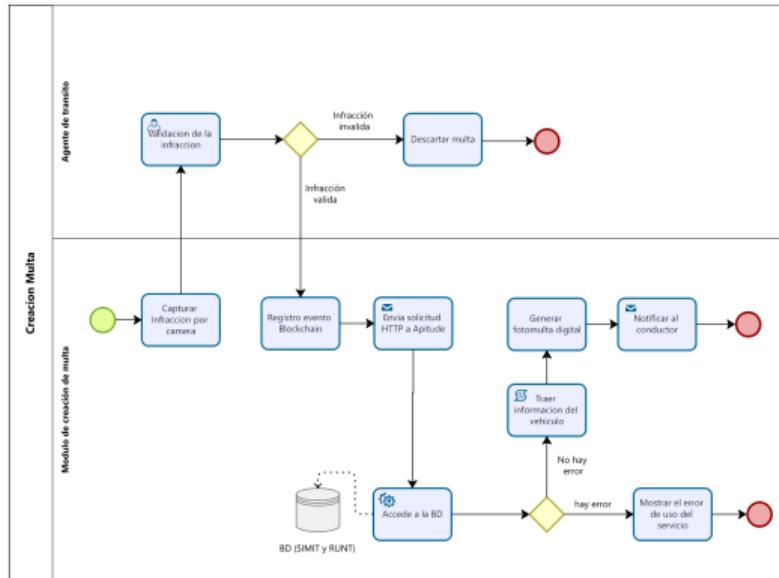
Nota: Modelado UML del sistema.

## Actores identificados:

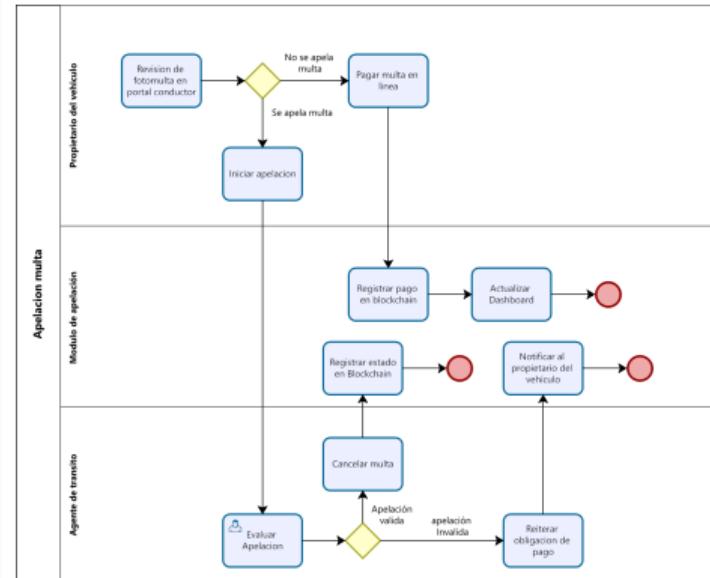
- 1. Agente de tránsito**
  - Registrar comparendo
  - Actualizar estado
- 2. Ciudadano**
  - Consultar multa
  - Verificar autenticidad
  - Apelar
- 3. Administrador**
  - Gestionar sistema
  - Auditlar operaciones

# Flujos de proceso: diagramas de actividades

**Figura 3**  
*Registro de multa*



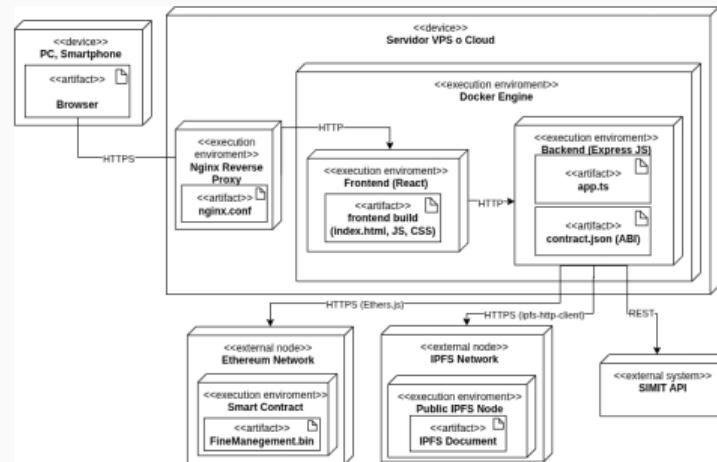
**Figura 4**  
*Proceso de apelación*



# Arquitectura del sistema

Figura 5

Diagrama de despliegue del sistema



Nota: Arquitectura del sistema desplegado.

**Capas:** 1. Frontend React — 2. API REST Node.js/Express — 3. Hyperledger Fabric (privado) — 4. Ethereum (público) — 5. IPFS (almacenamiento distribuido)

## Delimitaciones metodológicas del prototipo:

- **Datos sintéticos:** la verificación se realizó con datos generados mediante scripts de prueba, dado que no se dispuso de acceso a datos reales del FÉNIX, RUNT ni SIMIT.
- **Cobertura parcial de estados:** se implementaron 5 de los 8 estados del ciclo de vida (PENDING, PAID, APPEALED, RESOLVED\_APPEAL, CANCELLED).
- **Volumen controlado:** se emplearon entre 50 y 100 comparendos de prueba, frente a los 457,000 semestrales registrados en producción.
- **Verificación técnica:** los resultados corresponden a una *verificación* en entorno controlado, no a una *validación* operativa institucional.

### Nota metodológica

Se distingue entre *verificación* (el sistema cumple las especificaciones de diseño) y *validación* (el sistema opera adecuadamente en condiciones reales). Este trabajo se enmarca en la primera categoría.

## Validación y pruebas

---

# Plan de pruebas: cobertura del prototipo

Estrategia: 80 casos de prueba automatizados — Tasa de éxito: 100% — Tiempo total: 28.98s

Tabla 1

*Resultados del plan de pruebas por módulo*

Módulo	Pruebas	Éxito	Cobertura
Utilidades (Error Handler)	7	7/7	Manejo global de errores
Servicios IPFS	8	8/8	Subida, recuperación, CIDs
Integración IPFS	13	13/13	Inmutabilidad, content-addressed
Seguridad: Validación	16	16/16	XSS, SQL injection, path traversal
Seguridad: Archivos	10	10/10	Límites 10MB, tipos válidos
API REST	26	26/26	CRUD, blockchain/IPFS
<b>Total</b>	<b>80</b>	<b>80/80</b>	<b>100 % cobertura funcional</b>

Nota: Resultados de pruebas del prototipo.

# Pruebas de inmutabilidad

Tabla 2

*Resultados de pruebas de inmutabilidad*

ID	Caso de prueba	Resultado
IM-001	Modificación directa en ledger	Transacción rechazada por consenso
IM-002	Alteración de imagen en IPFS	CID diferente → Detección automática
IM-003	Verificación de trazabilidad	Historial inmutable preservado
IM-004	Validación de consenso	Consenso validado correctamente

Nota: Pruebas de inmutabilidad ejecutadas.

Evidencia: TX registro: 0xbc03e11f...42c3c069 — TX actualización: 0x611b696e...d315f3e48 — CID:  
QmadhsypxKm7...sp8eKMF

## Resultado

En el entorno experimental, el prototipo rechazó el 100 % de los intentos de modificación no autorizada.

# Métricas de desempeño

## Tiempos de respuesta medidos:

- Registro completo: < **3 segundos**
- Consulta de multa: < **1 segundo**
- Verificación de integridad: < **2 segundos**

## Criterios de éxito

- ✓ Tiempo de publicación  $\leq 3s$
- ✓ Coincidencia 100 % hash
- ✓ Trazabilidad completa en entorno de prueba

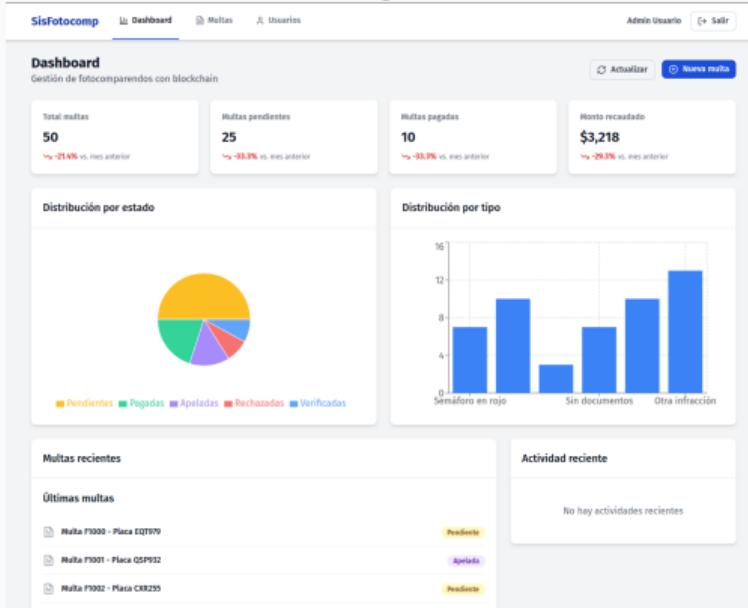
## Resultado general

Todos los criterios de aceptación fueron satisfechos en el entorno experimental. Los tiempos de respuesta se mantuvieron dentro de los umbrales definidos en el plan de pruebas.

# Interfaces del prototipo

## Figura 6

Dashboard del agente de tránsito



Nota: Interfaz del prototipo desarrollado.

## Figura 7

Consulta y verificación ciudadana

**Consulta de Multas**

Ingrese sus datos para consultar multas pendientes

**Placa del vehículo:** KOX256

**Verificación de seguridad:**

This reCAPTCHA is for testing purposes only. Please report to the site admin if you are seeing this.

I'm not a robot

reCAPTCHA  
Privacy - Terms

**Consultar**

Nota: Interfaz del prototipo desarrollado.

## Demostración del prototipo

---

# Demostración del prototipo

### Entorno de despliegue:

- **Servidor:** Grupo GNU Linux
- **Institución:** Universidad Distrital
- **URL:** [fotomultas.gldud.org](http://fotomultas.gldud.org)
- **Recursos:** 8 vCPU, 16GB RAM
- **SO:** Ubuntu Server 22.04 LTS

### Componentes desplegados:

- Backend API (Node.js - Puerto 3000)
- Frontend Web (React - Puerto 80)
- Red Hyperledger Fabric
- Nodo IPFS local
- Conexión Ethereum Sepolia

### Acceso al sistema

El prototipo está disponible públicamente para validación. Se demostrará el registro en Hyperledger Fabric, la publicación de hashes en Ethereum y el almacenamiento de evidencias en IPFS.

## **Conclusiones y aportes**

---

# Conclusiones principales

## 1. Viabilidad técnica demostrada:

- La arquitectura híbrida (Hyperledger Fabric + Ethereum + IPFS dual) demostró ser viable para la gestión de fotocomparendos en el entorno experimental.

## 2. Garantías criptográficas verificadas:

- 100 % de intentos de modificación no autorizada rechazados satisfactoriamente.
- Detección automática de alteraciones mediante *content-addressing* (CIDs).
- Tiempos de respuesta dentro de los criterios de aceptación ( $\leq 3s$ ).

## 3. Modelo de confianza alternativo:

- Transición hacia confianza criptográfica verificable, conciliando privacidad (Ley 1581/2012) y transparencia (Ley 1712/2014).

## Trabajo futuro

---

# Líneas de evolución

## 1. Validación operativa:

- Piloto controlado con 5,000–10,000 multas reales
- Integración con SIMIT/RUNT mediante APIs reales
- Estudios de aceptación tecnológica (TAM/UTAUT) con agentes de tránsito y ciudadanos

## 2. Escalamiento a producción:

- Red Fabric multi-organizacional (SDM, Policía, Contraloría)
- Migración a soluciones Layer 2 (Polygon, Arbitrum)
- Auditoría formal de seguridad (Slither, MythX)

## 3. Evaluación e integración con FÉNIX:

- Integración con el sistema FÉNIX de Bogotá
- Implementación de los estados faltantes del ciclo completo
- Módulo de pagos (PSE, billeteras digitales)

## 4. Replicabilidad:

- Adaptación para otras ciudades colombianas
- Estandarización de contratos inteligentes a nivel nacional
- Federación de redes Fabric intercity

## Perspectiva

Los resultados obtenidos constituyen una base técnica para futuras investigaciones orientadas a la validación operativa e institucional del sistema propuesto.

## Referencias principales (1/2)

- Contraloría General de la República de Colombia. (2024). Informe de Auditoría 170100-0054-24: Auditoría de Cumplimiento a la Secretaría Distrital de Movilidad [Auditoría realizada a la Secretaría Distrital de Movilidad de Bogotá D.C.].
- Yousfi, N., Kmimech, M., Abbassi, I., Hamdi, H., & Graiet, M. (2022). ITS Traffic Violation Regulation Based on Blockchain Smart Contracts. *International Conference on Computational Collective Intelligence*, 459-471. [https://doi.org/10.1007/978-3-031-16210-7\\_38](https://doi.org/10.1007/978-3-031-16210-7_38)
- Chen, C.-L., Tu, C.-Y., Deng, Y.-Y., Huang, D.-C., Liu, L.-C., & Chen, H.-C. (2024). Blockchain-enabled transparent traffic enforcement for sustainable road safety in cities. *Sustainable Cities: Smart Technologies and Cities*, 6, 1426036. <https://doi.org/10.3389/frsc.2024.1426036>
- Zheng, Z., Xie, S., Dai, H.-N., Chen, X., & Wang, H. (2018). Blockchain challenges and opportunities: A survey. *International journal of web and grid services*, 14(4), 352-375
- Adel, K., Elhakeem, A., & Marzouk, M. (2023). Decentralized System for Construction Projects Data Management Using Blockchain and IPFS. *Journal of Civil Engineering and Management*, 29(4), 342-359

## Referencias principales (2/2)

- Antonopoulos, A. M., & Harding, D. A. (2023). *Mastering Bitcoin: Programming the Open Blockchain*. O'Reilly Media
- Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System.
- van Steen, M., & Tanenbaum, A. S. (2017). *Sistemas Distribuidos* (3.<sup>a</sup> ed.) [Traducción de Distributed Systems, 3rd edition]. distributed-systems.net. <https://www.distributed-systems.net/index.php/books/ds3/>
- Cachin, C. (2018). Architecture of the Hyperledger Blockchain Fabric [Accessed: 2025-05-07]. *arXiv preprint arXiv:1801.10228*. <https://arxiv.org/abs/1801.10228>
- Benet, J. (2014). IPFS—Content Addressed, Versioned, P2P File System. <https://doi.org/10.48550/arXiv.1407.3561>



# Agradecimientos

**Universidad Distrital Francisco José de Caldas**  
Facultad de Ingeniería — Programa de Ingeniería de Sistemas

**Director**

Julio Barón Velandia, PhD

**Jurado**

Roberto Pava Díaz, PhD

**Grupo académico**

GLUD — GNU/Linux Universidad Distrital

## Espacio de preguntas

---