Respuesta a Observaciones del Proyecto "DeCam"

A continuación, se detallan las respuestas técnicas, operativas y jurídicas a las observaciones planteadas. Asimismo comparto el modelo de negocios para mayor ilustración.

1. Arquitectura y tecnología.

¿Qué blockchain se utilizará para registrar los hashes de los videos? ¿Se usará una blockchain pública o una privada?

Se utilizará la red Ethereum, pero operando sobre una solución de Capa 2 (Layer 2) basada en ZK-Rollups (Zero-Knowledge Rollups).

Criterio institucional y legal: Se elige una red pública (Ethereum) como capa base (Capa 1) para garantizar la inmutabilidad absoluta y la transparencia (evitando que el Estado o un privado puedan reescribir la historia, como podría ocurrir en una blockchain privada). Sin embargo, al operar en la Capa 2 con ZK-Proofs, garantizamos la privacidad de los datos procesales: la red pública solo ve "pruebas matemáticas" de que una validación ocurrió, pero nunca expone los datos de la causa, el video o la identidad del usuario. Es un modelo "público en su infraestructura, pero privado en su capa de datos".

¿Quién será el responsable legal y administrativo de la red? ¿Qué implicancias tiene que los datos estén fuera de servidores estatales?

El responsable legal de la plataforma será DeCam S.A., actuando como "Proveedor de Infraestructura Tecnológica" (orquestador).

Respecto a los datos fuera de servidores estatales, es vital comprender el paradigma actual: hoy en día, la evidencia privada ya está fuera de servidores estatales (reside en memorias externas, celulares de vecinos o servidores de WhatsApp). DeCam mejora drásticamente esto. Los videos en DeCam se almacenan en IPFS de forma encriptada y fragmentada. El Estado no pierde el control; por el contrario, gana la exclusividad del acceso, ya que solo el Ministerio Público Fiscal posee la llave criptográfica asimétrica para reconstruir y visualizar esa evidencia.

¿Cómo se garantiza la inmutabilidad de los datos en la blockchain?

La inmutabilidad se garantiza mediante el mecanismo de Hashing Criptográfico (SHA-256) anclado al consenso de la red Ethereum. Cada video genera una huella digital única. Para alterar un dato del pasado, un atacante necesitaría el 51% del poder computacional de toda la red global de Ethereum, lo cual es técnica y financieramente inviable. Adicionalmente, se realizarán auditorías externas (empresas como *CertiK*) sobre los Smart Contracts (ver TFI modelo de negocios, Cap. 6.3).

¿Cómo se acredita legalmente la validez del hash como evidencia judicial?

El *Hash* funciona como una Firma Digital Avanzada, amparada bajo la Ley Nacional de Firma Digital (Ley 25.506). En las Fases 1 y 2, la plataforma acompañará las extracciones con un informe pre-formateado de un Perito Informático que traduce la validación del *Smart Contract* a un lenguaje procesal tradicional. Esto sienta la jurisprudencia técnica ("Legalidad por Diseño") para que el sistema se adopte gradualmente por puro empirismo y eficiencia.

¿Cómo se gestionan los costos? ¿Qué modelo presupuestario se prevé?

Los costos transaccionales (*Gas fees* de la Blockchain) y de almacenamiento en IPFS están contemplados dentro del *Burn Rate* de la empresa (Capítulo 6.4 del TFI modelo de negocios). En la Capa 2 (ZK-Rollups), el costo por transacción es marginal (fracciones de centavo de dólar). Estos costos operativos se financian a través del cobro de suscripciones privadas (Planes BYOD y Leasing) y del modelo GovTech SaaS para el Estado: una licencia institucional de tarifa plana (mensual/anual) que otorga a las fiscalías acceso ilimitado a las validaciones, eliminando la fricción administrativa de pagar por cada evento.

2. Seguridad y privacidad.

¿Cómo se garantizará la seguridad y privacidad de los videos? ¿Quién actúa como responsable del tratamiento de datos?

La privacidad se garantiza mediante Pruebas de Conocimiento Cero (ZK-Proofs) (TFI modelo de negocios Cap 2.3). El ciudadano ("Nodo") es el titular soberano de sus datos. DeCam actúa únicamente como "Encargado de Tratamiento" (procesador de la encriptación), y la Justicia actúa como el destinatario final autorizado. Al no almacenar videos "en crudo" en bases de datos centralizadas, DeCam elimina el riesgo de hackeos masivos (*honeypots*).

¿Qué mecanismos se prevén para evitar videos manipulados o falsificados?

El protocolo Proof of Justice (PoJ) (TFI modelo de negocios Cap. 2.3) previene falsificaciones desde el origen operativo de la cámara (el *Edge*). El archivo se sella en el mismo instante de la grabación vinculando tres variables:

1. Timestamp Atómico (Sincronizado con blockchain).

2. Geolocalización encriptada desde el hardware para evitar *Spoofing*.
3. Huella de Hardware (Firma del sensor), que garantiza que el fotograma provino de un lente óptico homologado y no de una IA generativa (*Deepfake*).

3. Verificación y autenticidad.

¿Cómo se verifica que un video es auténtico y qué interfaz se usará?

Se verifica a través del emparejamiento entre el archivo descargado de IPFS y el Hash registrado en el *Smart Contract*. Si un solo píxel del video fue alterado, el Hash resultante será totalmente distinto al original, y el sistema lo rechazará automáticamente. Para la Justicia, se proveerá una plataforma Web Dashboard Institucional (TFI modelo de negocios Cap 4.2). El fiscal no necesita saber de criptografía; la interfaz mostrará un "Tick verde" de validación, detallando los metadatos inmutables (Hora, Coordenadas y Hash original).

¿Se prevé una integración con el sistema judicial?

Absolutamente. La estrategia "Demand-First" (TFI modelo de negocios Cap. 5.3) basa el lanzamiento en la integración temprana con el MPF. La plataforma contará con APIs que permitan, en el futuro, inyectar el video validado directamente en los sistemas de gestión de expedientes existentes de la justicia (ej. sistemas tipo Coirón o similares), asegurando la cadena de custodia desde DeCam hasta la carpeta judicial.

4. Escalabilidad y rendimiento.

¿Qué capacidad transaccional se proyecta y qué implicancias tiene la expansión?

Al utilizar una arquitectura de Capa 2 (ZK-Rollups) sobre Ethereum, la plataforma puede procesar miles de transacciones por segundo (TPS), superando con creces la demanda incluso si el 100% de las cámaras del AMBA emitieran alertas simultáneas. A nivel presupuestario, como la arquitectura es descentralizada (Nodos IPFS) y el modelo es *Asset-Light* / SaaS (TFI modelo de negocios Cap. 6.4), el costo marginal de añadir un nuevo usuario o cámara tiende a cero. Escalar de 100 a 10.000 cámaras no requiere construir un nuevo centro de datos estatal, sino

simplemente habilitar más contratos inteligentes, haciendo que la expansión metropolitana sea fiscalmente viable y financieramente escalable.

5. Smart Contract.

¿Qué procedimientos están previstos ante un error o manipulación?

La naturaleza de la blockchain asegura que si un video es manipulado (alteración de un solo bit), la función de hash criptográfico cambiará por completo. El Smart Contract comparará el hash original sellado al momento de la grabación con el hash del video presentado; si no coinciden de forma exacta, el contrato rechaza automáticamente la validación, impidiendo que material adulterado ingrese al proceso judicial.

¿Cómo se gestionará la responsabilidad y rectificación?

DeCam opera como un orquestador tecnológico, pero la "última milla" de validación siempre recae en el "Oráculo Humano" (el Fiscal). Si ocurre una falla en la lectura del contrato, el sistema prevé un mecanismo de *fallback* (respaldo) donde la prueba puede ser peritada de manera tradicional por el cuerpo forense del Estado, extrayendo los metadatos directamente del dispositivo físico emisor, garantizando que el proceso judicial nunca se detenga.

¿Se prevé auditoría?

Sí. Antes del despliegue en la red principal (Mainnet), los Smart Contracts de DeCam serán sometidos a auditorías de seguridad exhaustivas por firmas externas de ciberseguridad especializadas en Web3 (ej. CertiK o Hacken), cuyos reportes serán de acceso público para el GCBA.

6. Integración y uso práctico

¿Qué requerimientos de interoperabilidad se plantean?

DeCam está diseñada bajo una arquitectura "API-First". No buscamos reemplazar los sistemas de gestión documental del Estado (como el sistema Coirón del MPF), sino complementarlos. La plataforma proveerá APIs RESTful seguras que permitirán a los sistemas del Poder Judicial y Fuerzas de Seguridad consultar, verificar e importar la evidencia validada directamente a sus expedientes

electrónicos, asegurando una interoperabilidad fluida sin disrupciones operativas.

7. Costos y modelo de negocio

¿Qué modelo de precios se prevé para el uso del sistema?

Para el Estado, se propone un modelo B2G (GovTech SaaS) consistente en una licencia de suscripción institucional. En lugar de cobrar por extracción de video o por gigabyte almacenado (lo que generaría imprevisibilidad presupuestaria), el Ministerio Público Fiscal abonará una tarifa plana (mensual o anual) por jurisdicción.

¿Existen costos asociados a la verificación?

No existen costos variables ocultos para la Justicia. El pago de la licencia SaaS cubre el 100% de los costos transaccionales (Gas fees) de verificación en la red y la exportación de la evidencia.

8. Soporte y mantenimiento.

¿Cómo se prevé la gestión de actualizaciones y seguridad?

La actualización de los Smart Contracts se gestionará a través de un esquema de gobernanza multifirma (Multi-Sig Wallet), requiriendo el consenso de múltiples actores técnicos clave de DeCam para aprobar cualquier modificación en el código, evitando cambios unilaterales maliciosos. El mantenimiento de la red de almacenamiento IPFS es continuo y redundante por su propia naturaleza descentralizada.

¿Qué mecanismos de auditoría pública se prevén?

Al estar anclado en una red blockchain (Capa 2 sobre Ethereum), el sistema posee trazabilidad y transparencia inherente. Se proveerá un *Block Explorer* (Explorador de Bloques) customizado para la Ciudad de Buenos Aires, donde organismos de control, veedurías ciudadanas y la propia Auditoría General de la Ciudad podrán auditar en tiempo real la cantidad de validaciones realizadas y la integridad de la cadena de custodia, sin acceder jamás al contenido privado de los videos.