

Profundización del Proyecto tras el Debate

1. Objetivo del documento

Este documento refuerza y profundiza en los aspectos más cuestionados durante el debate del Sprint 3, con el fin de preparar un pitch más sólido, reducir fragilidades, mejorar la coherencia interna del proyecto y evitar vulnerabilidades argumentales en futuras evaluaciones.

Además, integra los contenidos entregados previamente (Propiedad Intelectual, licencias, modelo de negocio, análisis de riesgos) para que todas las respuestas futuras del equipo estén alineadas y sean consistentes.

2. Principales Debilidades Detectadas en el Debate

Durante el debate con el Grupo 2 emergieron preocupaciones recurrentes sobre la viabilidad, la trazabilidad del modelo, la relación con la ONCE, los mecanismos de actualización y los riesgos legales asociados al tratamiento de datos visuales. Una parte de las preguntas se centró en las colaboraciones institucionales, especialmente la ONCE, cuestionando si existía ya un protocolo formal de negociación. Se respondió que la colaboración está prevista para fases avanzadas del desarrollo, una vez exista un prototipo. Otra línea de debate importante fue la viabilidad tecnológica en 2029, particularmente sobre el chip neuromórfico previsto para ejecutar el modelo localmente. Aunque en el debate se expuso que existía un plan B basado en modelos más ligeros, en este documento se desarrolla más profundamente la estrategia para garantizar la continuidad técnica del sistema incluso si la evolución del hardware no cumple las expectativas.

También se cuestionó la manera en la que el sistema podría recibir actualizaciones o corregir fallos graves sin comprometer la privacidad. En el debate se mencionó el reentrenamiento con datos sintéticos o el uso de reportes de los usuarios, pero es necesario explicar mejor este proceso, su trazabilidad y sus limitaciones. Asimismo, surgieron dudas sobre la tasa de fallo en la anonimización y las posibles responsabilidades legales. La respuesta fue que el sistema no almacena datos y que el procesamiento siempre es local, pero es necesario precisar cómo se garantiza el cumplimiento legal incluso ante errores puntuales. Finalmente, el debate planteó riesgos económicos, como la pérdida de financiación de entidades colaboradoras. Esto abrió la puerta a reforzar el modelo de negocio híbrido que ya se definió en el documento de Propiedad Intelectual.

Las áreas de vulnerabilidad identificadas fueron:

2.1. Relaciones externas y viabilidad institucional

Pregunta: ¿Existe realmente un protocolo de negociación con la ONCE?

Problema: la colaboración se presentó como segura sin evidencias reales.

2.2. Dependencia tecnológica (chips, edge AI, 2029)

Pregunta: ¿Qué pasa si no existe el chip neuromórfico?

Problema: exceso de confianza tecnológica sin justificar.

2.3. Actualizaciones del sistema

Preguntas:

¿Cómo se actualiza si es urgente?

¿Cómo se mejoran los modelos si no se recopilan datos?

Problema: falta de un protocolo de actualización realista, coherente con “no datos”.

2.4. Gestión de errores e indemnizaciones

Preguntas:

¿Tasa de fallo? ¿Qué pasa si falla la anonimización? ¿Cómo indemnizáis?

Problema: ausencia de cifras, procesos o políticas formales.

2.5. Sostenibilidad económica

Pregunta: ¿Qué pasa si ONCE u otras entidades dejan de financiar?

Problema: modelo económico poco descrito.

2.6. Inconsistencia entre modelo open-core y licencias CC BY-NC

Pregunta: ¿Cómo compatibilizáis un modelo open-core con CC BY-NC?

Problema: falta de claridad sobre cómo conviven licencias abiertas con componentes propietarios.

3. Profundización Técnica y de Viabilidad

Uno de los puntos más frágiles señalados es la dependencia del procesamiento local intensivo mediante Edge AI. El proyecto asume que en 2029 existirán chips móviles capaces de ejecutar modelos multimodales con eficiencia energética, lo cual hoy todavía no es tecnológicamente viable. Para reforzar esta hipótesis, establecemos un plan técnico escalonado que contempla la optimización del modelo mediante técnicas de quantization, distillation y modularización progresiva, así como la posibilidad de

operar un modelo alternativo más ligero que mantenga las funciones esenciales (detección de obstáculos y reconocimiento general de objetos) aunque limite la complejidad de las descripciones. Este plan B permite asegurar la viabilidad del dispositivo incluso si la tecnología no avanza al ritmo esperado.

Otro aspecto crítico es la detección automática de zonas sensibles, como baños o vestuarios, para evitar la activación del sistema en ubicaciones donde grabar imágenes sería ilegal. Aunque en el documento inicial se planteó esta capacidad como una función del sistema, debemos reconocer que la detección perfecta de escenas es un reto aún abierto en inteligencia artificial. Para reforzar esta parte del proyecto, introducimos un enfoque mixto que combina reconocimiento de entorno con geofencing opcional cuando existan infraestructuras que lo permitan (por ejemplo, balizas Bluetooth de edificios públicos accesibles). Este enfoque híbrido reduce la dependencia exclusiva de la visión artificial, aumentando la fiabilidad del apagado automático.

En relación con las actualizaciones, el debate reveló la necesidad de explicar mejor cómo se puede mejorar un modelo sin almacenar imágenes. El proyecto adopta un sistema de actualizaciones centralizadas basadas únicamente en reportes anónimos de los usuarios y datos sintéticos generados internamente. Aunque esto limita la precisión del proceso de mejora, es un compromiso fundamental para mantener la privacidad. Por tanto, se priorizará un ciclo de mejoras anuales, no dependiente del envío de datos personales, basado en la evaluación de los fallos reportados y en la generación de datasets sintéticos adaptados a nuevos objetos o situaciones.

4. Profundización Legal y de Privacidad

La preocupación por la legalidad del procesamiento de datos visuales fue un punto recurrente. El sistema garantiza que no se almacenan imágenes ni se envían a la nube bajo ninguna circunstancia. El procesamiento es siempre efímero y local, lo cual elimina el riesgo de fugas o uso indebido de datos. Sin embargo, incluso el análisis local puede considerarse tratamiento de datos si incluye rostros o matrículas, por lo que el cumplimiento legal debe estar explícitamente fundamentado. Para ello, adoptamos un enfoque de minimización extrema, donde las caras se difuminan automáticamente y nunca se ejecutan técnicas de identificación, reduciendo el nivel de riesgo conforme al AI Act. Además, el sistema no toma decisiones automatizadas que afecten a la vida del usuario, sino que actúa como herramienta de apoyo, lo cual facilita su clasificación como sistema de asistencia y no como sistema autónomo.

En caso de un fallo en la anonimización —aunque sea improbable por el procesamiento efímero— la estructura legal del proyecto contempla un seguro de responsabilidad civil que cubra daños materiales o personales. La empresa mantiene la rendición de cuentas mediante revisión humana de todos los reportes, siempre sin almacenar imágenes, y con transparencia hacia el usuario. Este marco aumentará la confianza del sistema y responderá a una de las preguntas más insistentes del debate: cómo indemnizar ante un fallo si no hay datos almacenados.

5. Profundización Económica y de Modelo de Negocio

El debate dejó claro que la sostenibilidad económica del proyecto es un aspecto clave. La dependencia de una entidad como la ONCE para la distribución inicial fue criticada por su fragilidad. En respuesta, desarrollamos un modelo de negocio híbrido que combina un núcleo propietario con módulos abiertos bajo licencia MIT y datasets con licencias Creative Commons. Este enfoque permite atraer a desarrolladores externos, facilitar auditorías y al mismo tiempo mantener el control sobre los componentes sensibles. La principal fuente de ingresos provendrá de servicios como personalización para instituciones, mantenimiento, formación y actualizaciones periódicas.

Además, se establece un plan para diversificar las posibles colaboraciones, incluyendo museos, instituciones públicas y entidades tecnológicas que buscan mejorar la accesibilidad digital. En caso de pérdida de financiación de una organización grande, el proyecto puede seguir operando mediante acuerdos más pequeños o mediante financiación pública ligada a iniciativas de accesibilidad y no discriminación. Este modelo de negocio está alineado con las licencias elegidas y con los requisitos del AI Act, que exigen trazabilidad absoluta en sistemas de alto riesgo.

6. Coherencia y Profundización en Propiedad Intelectual

La estructura de licencias definida en el documento de Propiedad Intelectual se mantiene, pero es necesario reforzar su coherencia tras las preguntas del debate sobre cómo compatibilizar un modelo open core con una licencia CC BY-NC para el modelo entrenado. El componente propietario protege el núcleo del sistema y evita su explotación indebida, mientras que la licencia MIT del módulo de análisis visual fomenta la transparencia y la reutilización por parte de la comunidad. El modelo entrenado bajo CC BY-NC prohíbe usos comerciales no autorizados, lo que se alinea con la ética del proyecto. Los datos bajo CC BY-NC-SA aseguran que cualquier mejora de terceros permanecerá abierta. Finalmente, la documentación bajo CC BY facilita la citación académica y transparencia del proyecto.

Esta combinación de licencias no solo es legalmente compatible, sino que es éticamente beneficiosa: permite apertura controlada, evita la apropiación comercial

indebida y garantiza cumplimiento del AI Act. La elección de no adoptar una licencia copyleft estricta ni un modelo SaaS responde al principio fundamental del proyecto: el procesamiento local y la protección de la privacidad del usuario.

7. Mejoras en GitHub y Estándares de Comunidad

Tras la observación de que el README del repositorio era pobre y que la estructura debía organizarse por Sprints, se han incorporado mejoras sustanciales. El README ahora explica claramente el propósito del proyecto, su arquitectura, sus componentes y su estado de desarrollo. Se ha reorganizado el repositorio para que cada Sprint tenga su propio directorio, facilitando la trazabilidad y el cumplimiento de los entregables. Además, se han añadido los archivos de Community Standards: el Código de Conducta, la guía de contribución y la licencia. Estos documentos refuerzan la profesionalización del repositorio y aseguran que cualquier contribución externa sea coherente con los principios éticos y legales del proyecto.