

# DICTAMEN DE CERTIFICACIÓN TÉCNICA: FRAMEWORK

IDENTIFICADOR DE AUDITORÍA: UNCASE-2026-001-OBJ

ENTIDAD AUDITADA: UNCASE Open-Source Framework (SCSF)

VERSIÓN DEL SOFTWARE: 1.0.0-alpha

FECHA DE EMISIÓN: 28 de Febrero de 2026

CLASIFICACIÓN: Informe Técnico de Grado de Ingeniería

## 1. DECLARACIÓN DE ALCANCE

La presente auditoría certifica el estado técnico del pipeline de orquestación de datos sintéticos, evaluando la integridad estructural desde la ingesta de semillas (Layer 0) hasta el entrenamiento de adaptadores LoRA (Layer 4). El análisis se fundamenta en principios de ingeniería de software asíncrona y seguridad de datos.

## 2. MATRIZ DE HALLAZGOS TÉCNICOS

### A. FORTALEZAS ESTRUCTURALES (VALORACIÓN: ALTA)

- Aislamiento de Capa de Transporte: Implementación de interceptores de privacidad que operan en el flujo de I/O, garantizando la detección de PII mediante modelos estadísticos antes de cualquier operación de persistencia.
- Validación de Esquemas de Datos: Uso de Pydantic v2 para la coerción de tipos y validación de estructuras en tiempo de ejecución, eliminando la propagación de errores por datos malformados de LLMs.
- Trazabilidad Relacional: Arquitectura de base de datos que vincula de forma determinista cada artefacto generado con su semilla de origen y su reporte de calidad, permitiendo una reconstrucción forense del dataset.

### B. VULNERABILIDADES Y DEBILIDADES (VALORACIÓN: CRÍTICA)

- Déficit de Validación Semántica: El sistema depende de métricas de superposición léxica (Jaccard/ROUGE-L). Técnicamente, esto representa una incapacidad para certificar la veracidad factual de los diálogos generados.
- Inestabilidad de Privacidad Diferencial: La integración de DP-SGD mediante parches en el optimizador se considera una deuda técnica de alto riesgo, dada su dependencia de la estructura interna volátil de librerías externas.
- Serialización de Cómputo: El orquestador presenta una ejecución lineal en etapas críticas de generación, lo que introduce una latencia ineficiente para despliegues de escala industrial.

## 3. ÍNDICE DE CUMPLIMIENTO TÉCNICO

- Seguridad de Datos y Privacidad: 92/100 (Sobresaliente)
- Integridad Arquitectónica: 85/100 (Sólida)
- Validez de Datos Generados: 45/100 (Deficiente - Requiere Validación Semántica)
- Escalabilidad de Proceso: 50/100 (Media)

## 4. DICTAMEN FINAL DEL AUDITOR

El Framework UNCAGE demuestra una arquitectura de software superior en términos de organización y seguridad de flujo. Sin embargo, para alcanzar un grado de Certificación de Producción Crítica, es obligatorio reemplazar las heurísticas de validación actuales por modelos de recompensa (Reward Models) o validadores semánticos basados en embeddings.

ESTADO DE CERTIFICACIÓN: APROBADO CON RESERVAS TÉCNICAS.

---

Firma Digital de Ingeniería  
\*Senior ML Engineer & Data Architect\*

---

Firma del Auditor Principal

Sello de Integridad Técnica