Aislamiento DLP: Protegiendo scripts de infraestructura matriz

Estantería: DevSecOps e Infraestructura

Subtema: Gobernanza

mercedev.es — 2026-05-23 | Epic 5 - Fase 1

El Desafío (Síntoma)

El agente `merci-showcase.py` se utilizaba exclusivamente para desplegar el entorno de demostración del Boilerplate empleando credenciales de la autora. Mantenerlo en el directorio público `scripts/merci/` exponía esta herramienta de despliegue a los usuarios y, al no documentarlo en las instrucciones públicas para evitar confundirlos, el auditor de deriva documental (`merci-drift.py`) bloqueaba el pipeline por "fuga semántica".

La Maniobra (Lógica)

Se aplicó el principio de Defensa en Profundidad (DLP - Data Leak Prevention). El script destructivo fue reubicado a un recinto de cuarentena (`scripts/matriz/`), el cual fue excluido explícitamente en el archivo `.gitignore` . Para no perder la comodidad operativa, el enrutador inteligente (`merci()`) en Zsh fue refactorizado para buscar también en esta carpeta privada, invocando las herramientas con total transparencia.

El Aprendizaje / Deuda Técnica

Lo que es operativo para el proyecto matriz no siempre es útil para el derivado. Tratar de esconder scripts privados en carpetas públicas parcheando el linter (añadiendo excepciones en el código de auditoría) genera deuda técnica. El aislamiento físico de la propiedad intelectual es siempre superior a la ofuscación lógica.

En resumen

Existía un programa encargado de borrar datos privados y subir la demostración a internet que no debía ser público porque solo sirve para la dueña del proyecto. En lugar de complicar el código intentando ocultarlo del escrutinio del sistema, se movió a una carpeta secreta y se le indicó a la terminal cómo encontrarlo. Así, el público no lo ve, el sistema no lanza errores y se puede seguir utilizando con total comodidad.