Entregable 2 — Descripción del avance

Resumen corto Se implementó una tarea funcional mínima: auditoría básica de logs del sistema. Este entregable demuestra la ejecución técnica del proyecto, con entradas y salidas claras, logs en formato JSON lines y documentación de uso.

Qué hace la tarea - Extrae eventos del sistema usando PowerShell. - Guarda resultados en formato CSV y HTML. - Genera un log estructurado en JSON lines con metadatos de ejecución. - Crea un resumen breve en texto (Resumen_Forense.txt).

Cómo ejecutar 1. Abrir PowerShell o terminal. 2. Ejecutar el script: python src/run_tarea1.py --desde 2025-10-01 --salida examples/ 3. Los resultados se guardan automáticamente en la carpeta /examples.

Entradas esperadas - --desde → fecha desde la cual se filtran eventos. - --salida → carpeta donde se guardan los resultados. - (Opcional) --clave-abuse, --capturar-ram.

Salidas generadas - eventos_Security_YYYYMMDD.csv — logs del sistema. - procesos_red_YYYYMMDD.html — reporte de procesos. - Resumen_Forense.txt — resumen general. - logs_ejecucion.jsonl — registro de pasos ejecutados.

Formato de logs Cada línea es un objeto JSON: {"timestamp":"2025-11-05T19:00:00Z","step":"leer_logs","status":"ok","message":"100 eventos leídos"}

Evidencia de ejecución - Código funcional en /src - Ejemplos y logs en /examples - Script de ejecución run_tarea1.py - Documentación técnica en /docs/entregable_2.md - README actualizado con el estado del proyecto

Fecha de creación: 2025-11-05