GreenDelivery — Informe T2 (Equipo X)

1) Arquitectura y decisiones Cloud/IoT

Pipeline C4 (alto nivel): Edge (simulador MQTT) → Broker (Mosquitto) → Ingesta (Node-RED) → Storage (PostgreSQL) → Dashboard (Metabase) → Alertas (Slack). Rasgos NIST aplicados: elasticidad (escala lectores MQTT y workers), autoservicio (infra como código con docker-compose), pago por uso (servicios containerizados), alta disponibilidad (componentes desacoplados), amplio acceso a red (HTTP/MQTT). Las 5V: volumen y velocidad (stream cada 2s), veracidad (validación de tipos/rangos y raw_json), variedad (telemetría + etiquetas), valor (KPIs negocio).

2) Ingesta y almacenamiento

Node-RED valida JSON, normaliza a UTC y escribe en PostgreSQL con índice por (parcel_id, ts_utc). Resiliencia: se implementa cola de reintentos persistente (contextStorage) y MQTT QoS=1. Latencia esperada (local): 50–200 ms por evento con inserción batched opcional.

3) Modelo de Detección y KPIs

Regla N-consecutivos (N=3) con umbrales temp>8°C o g>2.5. Evaluación con analytics/labels.csv y script analytics/evaluate_model.py (mide Precision, Recall y F1). KPI1: % envíos en SLA. KPI2: Tiempo medio hasta detección. KPI3: % falsos positivos (comparando con tabla labels). Alertas con throttling por paquete.

4) Seguridad por Diseño (CIA) + Boss-Fight

Confidencialidad: secretos en .env, RBAC mínimo en BD. Integridad: validación de tipos y rangos; almacenamiento de raw_json para auditoría. Disponibilidad: cola persistente, QoS MQTT y contenedores reiniciables. Durante el Boss-Fight (DB caída 60s), la cola evita pérdida y se vacía al restaurar el servicio.