Desafío Técnico · Customer Success Engineer — Laburen.com

Fase Conceptual: Diseño de un agente de IA que vende productos vía API propia y base de datos PostgreSQL.

Endpoints Propuestos (REST)

Método	Endpoint	Propósito
GET	/health	Chequeo de salud del servicio.
GET	/products?search=&category=&limit=&offset=	Listado/búsqueda de productos.
GET	/products/{product_id}	Detalle de un producto.
POST	/carts	Crea un carrito (retorna cart_id).
GET	/carts/{cart_id}	Obtiene el estado del carrito.
POST	/carts/{cart_id}/items	Agrega ítem (product_id, quantity).
PATCH	/carts/{cart_id}/items/{item_id}	Edita cantidad o variantes.
DELETE	/carts/{cart_id}/items/{item_id}	Remueve ítem del carrito.
POST	/orders	Crea orden a partir del carrito (checkout).
POST	/webhooks/whatsapp	Recibe mensajes del canal WhatsApp.
POST	/webhooks/payments	Confirma pagos (asíncrono).
GET	/orders/{order_id}	Consulta estado de la orden.
POST	/agent/actions/http	Habilita al agente a ejecutar requests firmados.

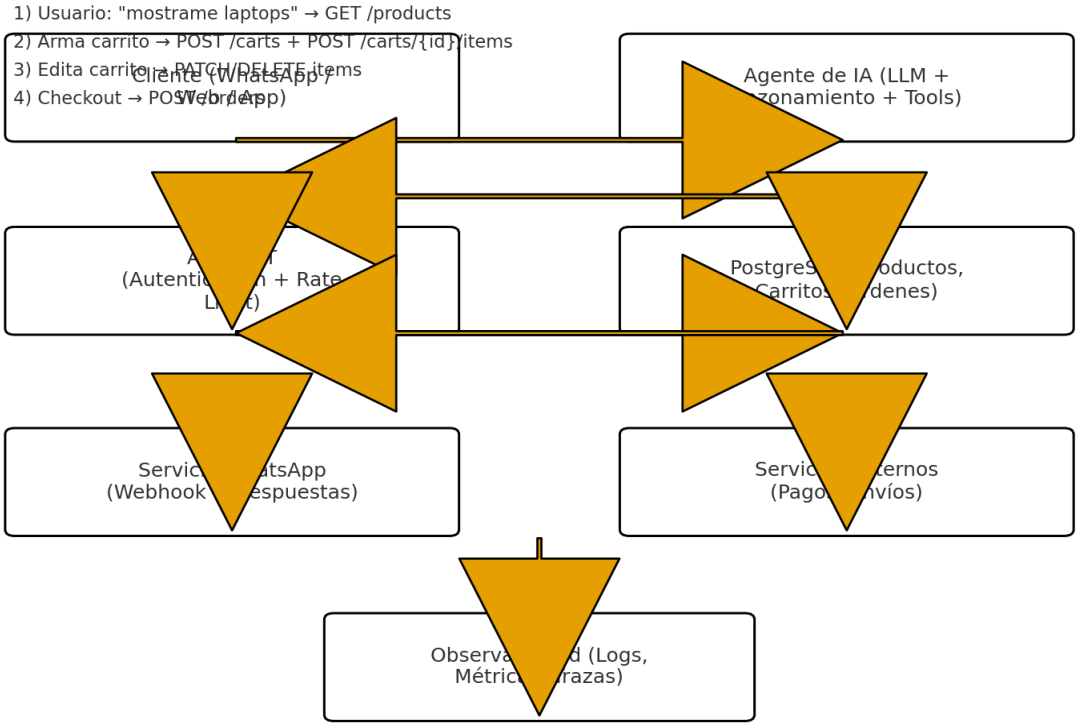
Flujo del Agente (resumen)

- Explora productos: el agente interpreta intención y hace GET /products con filtros.
- Arma carrito: crea carrito (POST /carts) y agrega items (POST /carts/{id}/items).
- Edición (extra): modifica o borra items (PATCH/DELETE).
- Checkout: crea la orden (POST /orders) y envía resumen por WhatsApp.

Arquitectura de Alto Nivel

• Agente de IA (LLM): interpreta intención, planifica y ejecuta herramientas HTTP (con guardrails).
• API REST: capa de negocio que valida entradas, aplica autenticación (API Key/JWT), rate limiting y logging.
• PostgreSQL: catálogo de productos, carritos, órdenes. Índices para búsqueda por texto/categoría.
• Canal WhatsApp: webhook para recibir mensajes y devolver respuestas del agente.
• Servicios externos: pagos y envíos, integrados en el checkout.
• Observabilidad: trazas por request, métricas (p95), tableros y alertas.

Diagrama de Flujo (vista simplificada)



Notas de Seguridad

• Autenticación: API Key para el agente + JWT para usuarios finales si corresponde.
• Autorización: el agente sólo puede llamar endpoints permitidos (lista blanca) y con schema validado.
• Validación: contratos OpenAPI/JSON Schema; límites de cantidad y monto en carrito/orden.
• Audit Logs: registrar todas las acciones del agente (IP, payload, resultado).