AutoProduct AI — Brain + Agent Rebuild Plan (PRO)

UI: admin-agent/* (app-style) + Brain LLM-first + deterministic Agent tools

1. Objectives & Non-Goals

Objectives

- Conversational assistant with maximum LLM intelligence: perception, context, memory, follow-ups.
- No keyword/template routing as core. No “if says X then Y”.
- Safe execution: all WRITE operations require UI button confirmation.
- Debuggability: trace_id, debug panel, tool call logs.

Non-Goals

- Not rebuilding the old deterministic flow router (too bug-prone).
- Not allowing confirmation by text.

2. High-Level Architecture

Brain: conversation + LLM planner + memory + pending actions. Brain never directly mutates WooCommerce data.

Agent: deterministic tools (READ/WRITE), validation, execution. Enforces allowlists and permission checks.

UI: app-style modular admin-agent/* frontend. Displays messages, cards, trace/debug panel, pending actions.

2.1 Conversation State Machine (minimal)

Global states (only 3):

- IDLE: no missing info, no pending action.
- FILLING: missing details; Brain asks max 1–2 questions per turn.
- PENDING_CONFIRMATION: pending_action exists; user must click Confirm button.

3. What to Reuse / What to Avoid

Reuse as-is

- UI: assets/js/admin-agent/* and assets/css/admin-agent/*
- Trace/Telemetry: trace_id per request, debug panel payloads
- MemoryStore + ResponseBuilder pattern (simplified state)
- Context Lite/Full concept + Persona service
- Product search + selector UI
- QA harness / regression harness culture

Avoid bringing

- Explosion of deterministic flows for routing intentions (loops + fragility)
- Regex/pattern routing as core intent engine
- LLM restricted to ‘cannot create pending actions’ (kills assistant)
- Brain directly reading/mutating WooCommerce objects (tight coupling)

4. Data Contracts

4.1 Core Entities

- Focus entity: {type: 'product'|'order'|'category', id, label}
- Search result item: {id, label, meta}
- Pending action: see schema below.

4.2 Pending Action Schema (server-side)

```
{
  "id": "pa_abc123",
  "tab_id": "tab_01",
  "created_at": "2026-01-28T12:00:00Z",
  "expires_at": "2026-01-28T12:10:00Z",
  "risk": "low|medium|high",
  "type": "product.update|product.create|product.delete|category.create|order.update|bulk.update",
  "target": {
    "entity": "product|order|category|bulk",
    "id": 123,
    "ids": [1,2,3]
  },
  "changes": { "regular_price": "19.99", "stock_quantity": 20 },
  "human_summary": "Update price and stock for Product #123",
  "preview": {
    "count_affected": 1,
    "examples": [
      {"id":123, "before":{"regular_price":"18.00"}, "after":{"regular_price":"19.99"}}
    ]
  }
}
```

5. Endpoint Contract — Brain REST API

All endpoints return a trace_id and are scoped by tab_id. Confirm is only via button.

5.1 Chat

POST /wp-json/apai-brain/v1/chat

Primary chat endpoint. Accepts user message and returns conversational reply and optional draft/pending cards.

Request JSON	{
	  "tab_id": "tab_01",
	  "message": "Subí 10% el precio de las remeras",
	  "ui_context": {
	    "selected_ids": [],
	    "language": "es"
	  },
	  "debug": false
	}

Response JSON	{
	  "trace_id": "tr_001",
	  "state": "IDLE|FILLING|PENDING_CONFIRMATION",
	  "messages": [
	    {"role":"assistant","text":"¿A qué productos te referís con remeras? Puedo buscar por nombre
	  ],
	  "cards": [
	    {"type":"search_suggestion","query":"remera","entity":"product"}
	  ],
	  "pending_action": null
	}

Errors	400 invalid_request; 401 unauthorized; 500 brain_error

5.2 Confirm Pending Action

POST /wp-json/apai-brain/v1/confirm

Executes the current pending_action. Only callable from UI Confirm button.

Request JSON	{
	  "tab_id": "tab_01",
	  "pending_action_id": "pa_abc123"
	}

Response JSON	{
	  "trace_id": "tr_002",
	  "state": "IDLE",
	  "messages": [
	    {"role":"assistant","text":"Listo. Actualicé el precio de 12 productos (+10%)."}
	  ],
	  "cards": [
	    {"type":"result","status":"success","count":12}
	  ],
	  "cleared_pending": true
	}

Errors	409 no_pending_action / expired_pending_action; 422 validation_failed; 500 execution_error

5.3 Cancel Pending Action

POST /wp-json/apai-brain/v1/cancel

Cancels any existing pending action for the tab.

Request JSON	{
	  "tab_id": "tab_01"
	}

Response JSON	{
	  "trace_id": "tr_003",
	  "state": "IDLE",
	  "messages": [
	    {"role":"assistant","text":"Cancelado. No se aplicaron cambios."}
	  ],
	  "cleared_pending": true
	}

Errors	409 no_pending_action; 500 brain_error

5.4 State Snapshot

GET /wp-json/apai-brain/v1/state?tab_id=tab_01

Returns current memory/pending snapshot for UI rehydration.

Request JSON	(querystring only)

Response JSON	{
	  "trace_id": "tr_004",
	  "state": "IDLE|FILLING|PENDING_CONFIRMATION",
	  "focus_entity": {"type":"product","id":123,"label":"Remera Negra"},
	  "last_results": [{"id":123,"label":"Remera Negra"},{"id":456,"label":"Remera Blanca"}],
	  "pending_action": null,
	  "summary": "User wants to update apparel prices."
	}

Errors	401 unauthorized; 500 brain_error

6. Endpoint Contract — Agent REST API (Tools)

Agent endpoints are deterministic. Brain uses them as tools. All writes are validated and allowlisted.

6.1 Product Search (READ tool)

GET /wp-json/apai-agent/v1/products/search?q=&page;=&per;_page=

Search products by query string (name/SKU). Used for disambiguation and selection.

Request JSON	`(querystring only)`

Response JSON	`{`
	`  "trace_id": "tr_a01",`
	`  "items": [`
	`    {"id":123,"label":"Remera Negra","sku":"REM-NEG","price":"19.99","stock":10},`
	`    {"id":456,"label":"Remera Blanca","sku":"REM-BLA","price":"18.00","stock":5}`
	`  ],`
	`  "page": 1,`
	`  "per_page": 20,`
	`  "total": 2`
	`}`

Errors	401 unauthorized; 500 agent_error

6.2 Product Get (READ tool)

GET /wp-json/apai-agent/v1/products/{id}

Get product details by id.

Request JSON	`(path param)`

Response JSON	`{`
	`  "trace_id":"tr_a02",`
	`  "product":{`
	`    "id":123,`
	`    "name":"Remera Negra",`
	`    "type":"simple",`
	`    "regular_price":"19.99",`
	`    "sale_price":null,`
	`    "stock_quantity":10,`
	`    "categories":[{"id":7,"name":"Remeras"}]`
	`  }`
	`}`

Errors	404 not_found; 401 unauthorized; 500 agent_error

6.3 Product Create (WRITE tool)

POST /wp-json/apai-agent/v1/products

Create a new product. Used only after confirmation via Brain pending_action.

Request JSON	{
	  "name":"Remera Azul",
	  "type":"simple",
	  "regular_price":"22.00",
	  "stock_quantity":15,
	  "categories":[7]
	}

Response JSON	{
	  "trace_id":"tr_a03",
	  "status":"success",
	  "product_id":789
	}

Errors	422 validation_failed; 401 unauthorized; 500 agent_error

6.4 Product Update (WRITE tool)

PATCH /wp-json/apai-agent/v1/products/{id}

Update product fields (allowlist enforced).

Request JSON	{
	  "regular_price":"24.00",
	  "stock_quantity":20
	}

Response JSON	{
	  "trace_id":"tr_a04",
	  "status":"success",
	  "updated_fields":["regular_price","stock_quantity"]
	}

Errors	404 not_found; 422 validation_failed; 401 unauthorized; 500 agent_error

6.5 Orders Search (READ tool)

GET /wp-json/apai-agent/v1/orders/search?status=&email;=&after;=&before;=

Search orders by status/email/date.

Request JSON	(querystring only)

Response JSON	{
	  "trace_id":"tr_a10",
	  "items":[
	    {"id":1001,"status":"processing","total":"45.00","customer":"Juan P.","created":"2026-01-27"}
	  ],
	  "total": 1
	}

Errors	401 unauthorized; 500 agent_error

7. UI Behavior Contract (admin-agent/*)

7.1 Confirm button rules

- UI shows pending_action card with summary + risk + preview.
- Confirm triggers /confirm endpoint only.
- Text confirmation is blocked: if user types “sí/ok/dale”, Brain replies to click Confirm.
- Cancel may be text (handled by Brain cancel detection) or UI button calling /cancel.

7.2 Cards Types (suggested)

Card type	Purpose
pending_action	Shows action summary, risk, preview, Confirm button
search_results	Selectable list of products/orders/categories
result	Success/failure summary after execution
error	User-facing errors with remediation suggestions
debug_trace	Raw LLM JSON/tool calls/memory snapshot (debug mode)

8. Error Handling & Status Codes

Brain errors

Code	Meaning	UI behavior
400 invalid_request	Missing tab_id/message	Show error card
409 no_pending_action	Confirm/cancel without pending	Refresh state
409 expired_pending_action	Pending TTL expired	Clear pending + inform user
422 validation_failed	Agent rejected changes	Show reasons + ask follow-up
500 brain_error	Unexpected failure	Show trace_id + retry option

Agent errors

Code	Meaning
404 not_found	Entity does not exist
422 validation_failed	Field not allowed / invalid value
401 unauthorized	Missing capability manage_woocommerce
500 agent_error	Unhandled error