RECURSO TÉCNICO #10

**Autor:** Miguel Serrano

**Estándar:** OpenAPI 3.1.0 / JSON Schema 2020-12

# Plantilla OpenAPI 3.1: Conexión de Agentes y Custom GPTs

Especificación técnica normalizada para integrar asistentes LLM con endpoints backend de forma determinista mediante autenticación Bearer y restricciones de tipos.

## 1. REGLAS DE VALIDACIÓN PARA EVITAR ALUCINACIONES

| PARÁMETRO OPENAPI 3.1 | EFECTO EN EL MODELO LLM | IMPACTO EN PRODUCCIÓN |
|---|---|---|
| `operationId: camelCase` | Identificador único de invocación | Garantiza que el agente llame la función sin ambigüedad |
| `enum: ["val1", "val2"]` | Restricción categórica estricta | Elimina sinónimos inventados por el LLM en runtime |
| `pattern: "^regex$"` | Validación sintáctica en cliente | Fuerza identificadores con formato exacto (ej. UUID, slugs) |
| `additionalProperties: false` | Cierre estricto de esquema | Impide que el modelo inyecte claves no autorizadas |

## 2. ESPECIFICACIÓN YAML MAESTRA (LISTA PARA PRODUCCIÓN)

```yaml
openapi: 3.1.0
info:
  title: "API de Infraestructura y Automatizaciones"
  version: "1.0.0"
servers:
  - url: https://api.xcaleta.com/v1
paths:
  /nodos/{nodo_id}/metrica:
    get:
      operationId: consultarMetricaNodo
      summary: "Consulta estado de CPU y RAM de un servidor"
      parameters:
        - name: nodo_id
          in: path
          required: true
          schema: { type: "string", pattern: "^srv-[a-z0-9-]+$" }
      responses:
        '200':
          content:
            application/json:
              schema:
                type: object
                properties:
                  estado: { type: "string", enum: ["optimo", "degradado", "alerta"] }
                  uso_cpu: { type: "number", minimum: 0, maximum: 100 }
                required: ["estado", "uso_cpu"]
                additionalProperties: false
components:
  securitySchemes:
    BearerAuth:
      type: http
      scheme: bearer
      bearerFormat: "JWT"
security:
  - BearerAuth: []
```

## 3. CHECKLIST DE DESPLIEGUE EN CHATGPT ACTIONS / SDK

| PASO OPERATIVO | INSTRUCCIÓN TÉCNICA |
|---|---|
| **Configuración de Auth** | Seleccionar *API Key > Bearer* e introducir el token generado en el servidor backend. |
| **CORS y Headers** | Habilitar en el servidor: `Access-Control-Allow-Origin: *` para peticiones OPTIONS/GET/POST. |
| **Políticas de Privacidad** | Vincular obligatoriamente la URL pública: `https://xcaleta.com/privacidad/`. |