

Planificación preliminar (6 meses)

Sistema agéntico para apoyo a evacuación médica

(MEDEVAC)

2 de febrero de 2026

Resumen

Este documento describe un proyecto para desarrollar un sistema agéntico (no un flujo tipo DAG) que apoye la evacuación médica (MEDEVAC) en entornos complejos (combate, desastre natural y zonas remotas). El sistema está compuesto por una red de agentes de inteligencia artificial que colaboran, toman decisiones locales, se comunican dinámicamente mediante A2A (agent-to-agent) y acceden a herramientas a través de servidores MCP (Model Context Protocol). La decisión final siempre permanece en manos humanas (HILT), y el sistema se diseña para ser explicable, auditável y reutilizable tanto en operaciones como en simulación y entrenamiento.

1. Descripción del proyecto

1.1. Motivación y alcance

La evacuación médica en entornos complejos requiere coordinar información médica, táctica y logística bajo incertidumbre y restricciones operativas. El objetivo del proyecto es construir una **red de agentes** que colaboren para:

- Evaluar la severidad clínica de las bajas y priorizar atención/evacuación.
- Planificar rutas y medios de evacuación (tierra/aire/otros) equilibrando tiempo, riesgo y recursos.
- Gestionar recursos médicos y activos MEDEVAC.
- Detectar y anticipar amenazas y riesgos que afecten a las bajas y a la evacuación.
- Automatizar comunicaciones y reporting (p. ej. extracción de 9-Line MEDEVAC).
- Supervisar la estabilidad del sistema con un agente metacognitivo y activar escalado a humano.

1.2. Principios de diseño (requisitos de primer orden)

El sistema se diseña siguiendo estos principios:

1. **Sistema agéntico real (no DAG)**: los agentes planifican y deciden dinámicamente sus acciones en función del estado y objetivos, con replanificación por eventos y comunicación A2A.
2. **HILT (Human-in-the-loop)**: intervención humana explícita en puntos críticos (aprobación de COAs, congelar/escalar, ajuste de prioridades).
3. **Explicabilidad y auditabilidad**:

- Cada recomendación debe incluir *por qué* y *en base a qué* (inputs, trade-offs, reglas aplicadas, incertidumbres).

- Registro de decisiones y eventos para replay y AAR (After Action Review).
4. **Doctrina como constraint de primera clase:** la doctrina no se trata como “conocimiento blando”, sino como *norma evaluable* (reglas duras y recomendaciones).
 5. **Modularidad por servicios:** agentes y MCPs como servicios independientes, integrables y sustituibles.
 6. **Ejecución local (DGX):** todo el sistema (agentes, MCPs, UI) se ejecuta en una única máquina (Nvidia DGX). Modelos locales disponibles: `qwen2.5:14b-instruct`, `deepseek-r1:32b`, `qwen2.5:3b-instruct`, `qwen2.5-coder:7b`, `qwen3-v1:8b` y embeddings `bge-m3`.
 7. **Skills como objetos de primera clase:** capacidades versionadas con contratos de entrada/salida, precondiciones, costes y tests asociados.

1.3. Arquitectura conceptual (visión completa)

La visión completa del sistema incluye (entre otros) los siguientes componentes:

Agentes (visión completa).

- **Agente Coordinador (Coordination & MedC2 Interface):** núcleo operativo. Consolida propuestas, resuelve conflictos (tiempo vs riesgo vs recursos), decide prioridad final MEDEVAC, interactúa con BMS/MedC2. Usa LLM principalmente para *planificación de interacción* (a qué agentes/herramientas llamar) y para redactar explicaciones; no para aplicar doctrina o resolver optimización.
- **Motor de Doctrina (Doctrinal Validation Engine):** validador normativo. Aplica reglas duras (constraints) y recomendaciones (soft rules) derivadas de TCCC, PFC, doctrina MEDEVAC OTAN, ROE. Produce trazabilidad explícita (regla, evidencia, referencia).
- **Triaje y Severidad** (híbrido): clasificación clínica, detección de estados críticos, estimación de tolerancia a retrasos.
- **MEDEVAC Planning & Routing:** planificación táctica (medio, ruta, ETA, riesgo, viabilidad de LZ). Preferentemente no-LLM (heurísticas/optimización) con LLM para explicación o tool-calling.
- **PFC Decision Support:** soporte para cuidados prolongados bajo recursos limitados, con límites clínicos estrictos.
- **Logística Médica:** inventarios, predicción de consumo, reasignación.
- **Vigilancia y Alerta Temprana:** monitoriza amenazas y estima riesgo/posibles bajas; dispara triggers de preparación MEDEVAC.
- **Comunicaciones Médicas:** transcripción/interpretación y extracción automática de 9-Line y alertas formales.
- **Agente Metacognitivo:** supervisa estabilidad, detecta loops/deriva, ajusta confianza y decide freeze/escalate a humano.

Servicios MCP (visión completa).

- **CMOP / World State MCP:** estado autoritativo (Common Medical Operational Picture).
- **Medical Data MCP:** datos médicos normalizados (HL7/FHIR).
- **Battle Management MCP:** integración con BMS (para MVP será simulado).

- **Logistics & Assets MCP:** inventario, vehículos, consumibles.
- **Threat & CBRNE MCP:** amenazas, riesgos CBRNE.
- **Learning & Analytics MCP:** métricas, AAR, simulación.

Comunicación y coordinación.

- Todos los agentes **leen** del CMOP/World State.
- El Coordinador recibe outputs de agentes tácticos y decide el COA final.
- El Motor de Doctrina valida planes del Coordinador.
- El Metacognitivo observa al Coordinador y al Motor de Doctrina.
- Solo el Coordinador interactúa con el BMS (MVP: BMS simulado).

1.4. Figuras de referencia

El proyecto dispone de dos esquemas:

- **Figura 1:** visión extendida del sistema completo.
- **Figura 2:** recorte para una primera fase orientada a MVP.

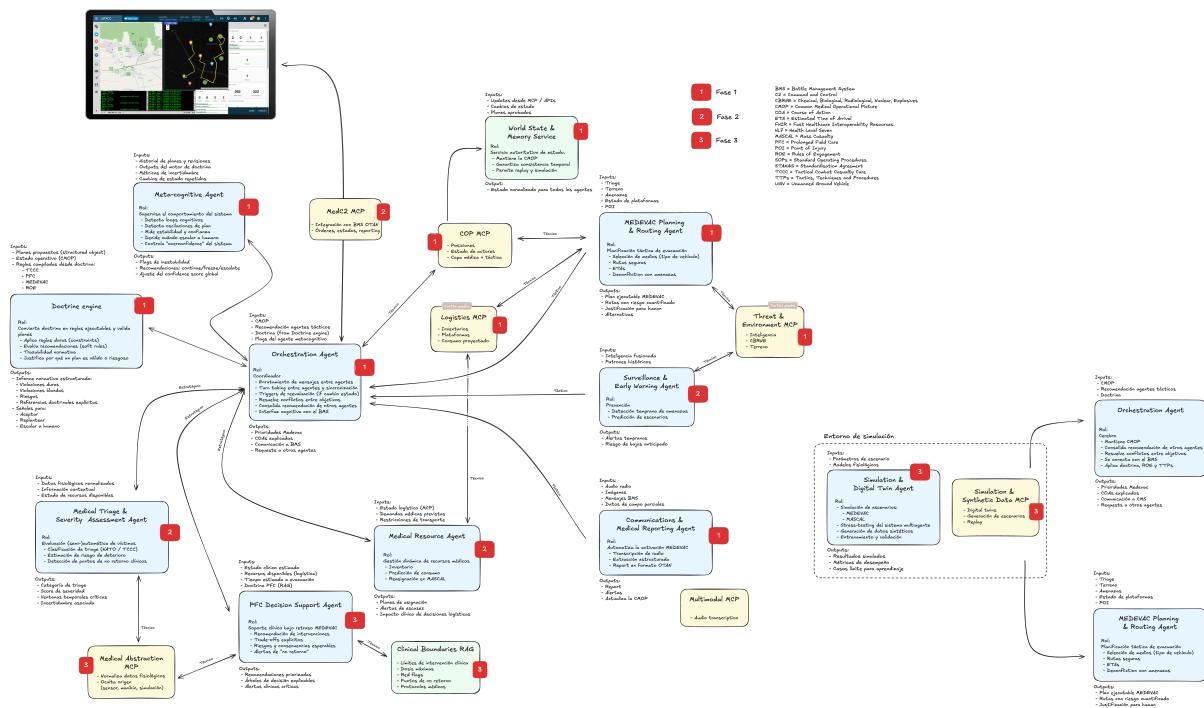


Figura 1: Figura 1: Arquitectura extendida (visión completa).

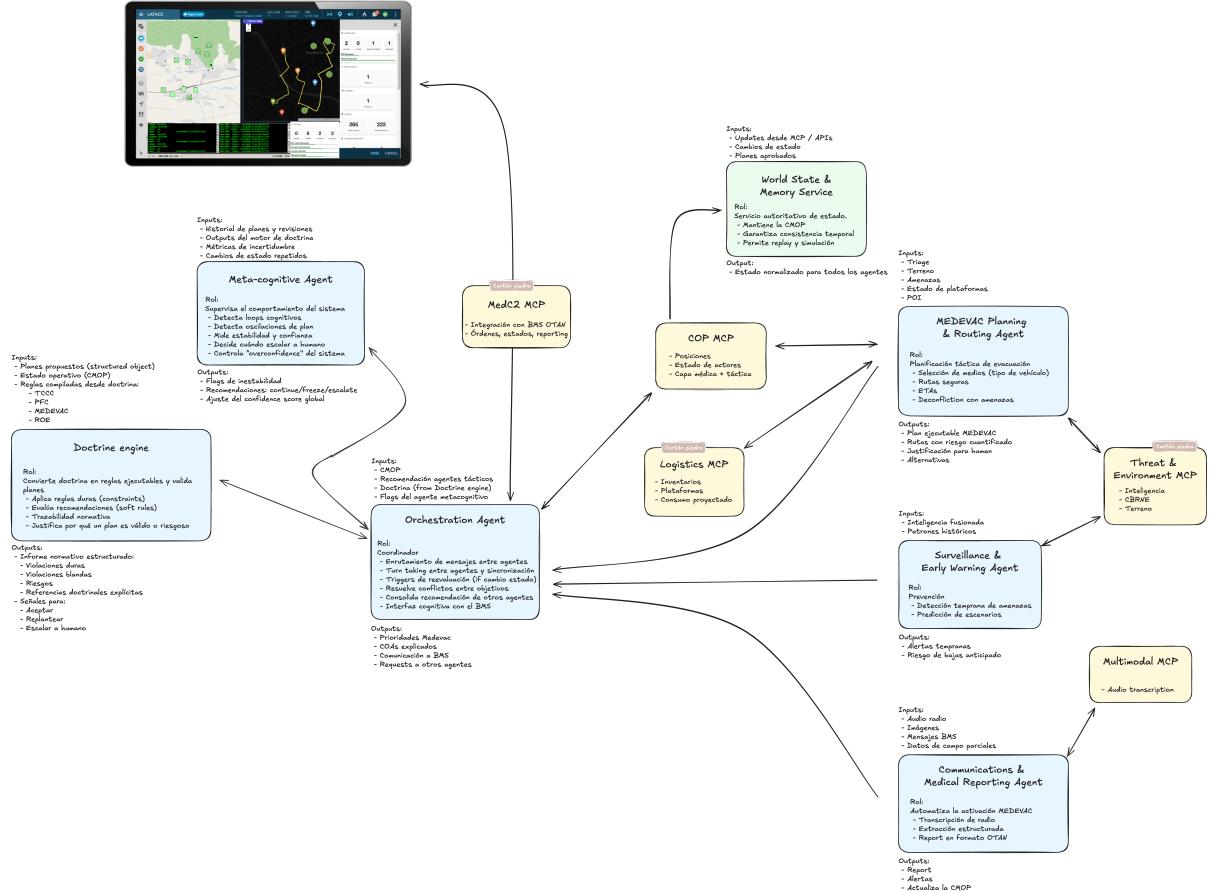


Figura 2: Figura 2: Arquitectura reducida (fase MVP).

2. Fase 1: MVP (6 meses)

2.1. Objetivo del MVP

Construir un MVP **coherente, demostrable y extensible** que cubra un fragmento del sistema completo, manteniendo los principios clave: HILT, explicabilidad, auditabilidad, doctrina como constraint, y modularidad A2A+MCP.

2.2. Decisiones y supuestos del MVP

- Integración con **BMS simulado** para demo (BMS Stub MCP).
- Planificación de rutas con **grafo simple + penalizaciones** (sin tiles en MVP).
- No hay datasets ni simuladores: se desarrollará un **generador de escenarios + replay** (event sourcing) para pruebas y evaluación.
- Doctrina: objetivo ideal es **bloquear** planes con violaciones duras; si el coste es alto, se permite modo **flag + justificación** con decisión HILT.
- Interfaz HILT **visual** (web): mapas (coordenadas reales), capas tácticas, rutas y COAs, estado logístico, estadísticas de bajas, y trazabilidad.
- Todo desplegado en **una única DGX**.
- Entidad geográfica: **coordenadas reales (WGS84)**.

2.3. Componentes incluidos en el MVP

Agentes MVP.

- **Coordinador:** orquesta llamadas, consolida COAs, resuelve conflictos multiobjetivo, produce explicación y requests al BMS simulado.
- **MEDEVAC Planning & Routing:** genera 2–3 planes candidatos (medio, ruta, ETA, riesgo, consumo).
- **Comms/Reporting:** extracción y validación de 9-Line estructurado.
- **Metacognitivo:** detecta inestabilidad/loops/fallos de tools, ajusta confianza y fuerza escalado HILT.
- **Motor de Doctrina:** reglas hard/soft con reporte trazable (regla, evidencia, referencia, sugerencia).
- **Early Warning (mínimo):** opcional en MVP; versión ligera centrada en alertas por estado de amenaza y triggers de preparación.

MCPs MVP.

- **World State / CMOP MCP:** integración con API existente (estado autoritativo + eventos).
- **Threat MCP:** zonas/polígonos, severidad, vigencia temporal.
- **Logistics & Assets MCP:** activos, capacidades, disponibilidad, consumo estimado simple.
- **Routing MCP:** grafo, K rutas, coste con penalizaciones por amenaza/restricciones.
- **BMS Stub MCP:** ciclo de request/ack/cambios para la demo.

2.4. Artefactos de explicabilidad y auditoría (MVP)

- **Event sourcing:** registro append-only con *trace-id* por episodio y *decision-id* por recomendación.
- **Replay determinista “suficiente”:** snapshots + re-ejecución para reproducir decisiones y facilitar debugging.
- **Informe por COA:** inputs usados, riesgos, ETA, consumo, incertidumbres, reglas doctrinales aplicadas y trade-offs.
- **AAR exportable:** export de episodio (estado inicial, eventos, decisiones, reportes, outputs).

3. Timeline preliminar por semanas (24 semanas)

La siguiente planificación está orientada a producir incrementos demostrables de manera temprana (mapa, rutas, planes, doctrina, coordinación, metacognición), evitando dependencias circulares.

Semana(s)	Objetivos principales	Entregables / Gate
1–2	Congelar contratos (schemas) y esqueleto distribuido A2A+MCP. Definir auditoría, IDs y trazas.	Contratos: <code>WorldState</code> , <code>Incident</code> , <code>PlanCandidate</code> , <code>DoctrineReport</code> , <code>COA</code> . Demo mínima: 2 agentes + 1 MCP con logging unificado. Gate: replay básico consistente.
3–4	World State robusto: event sourcing, snapshots y replay. UI web v0 (mapa) leyendo CMOP.	Servicio World State/CMOP con eventos + snapshot; UI muestra capas (activos/amenazas/casualties) en coordenadas reales. Gate: “estadio vivo + replay”.
5–6	Routing MCP: grafo + penalizaciones + K rutas. Visualización de rutas en UI.	Routing MCP con API estable; UI dibuja rutas y muestra coste/ETA. Gate: demo de routing independiente (sin agentes).
7–8	Logistics MCP mínimo + Planner v1 (2–3 COAs) usando Routing+Threat+Logistics.	Planner produce candidatos con ETA/riesgo/consumo; UI lista COAs y los dibuja en mapa. Gate: COAs visibles y comparables.
9–10	Doctrina MVP v1: reglas hard/soft + reporte trazable. Integración con Planner/Coordinador.	Motor de doctrina con 10–15 reglas hard + 20–30 soft (inicial). UI panel de doctrina por COA. Gate: hard violations bloquean recomendación (o modo flag controlado).
11–12	Coordinador v1: consolidación multiobjetivo, resolución de conflictos, explicación estructurada.	Coordinador selecciona COA recomendado, justifica trade-offs y emite request al BMS stub (si existe). Gate: salida coherente y auditible por episodio.
13–14	Comms/Reporting: extracción 9-Line desde texto (audio opcional), validación de completitud/consistencia.	Pipeline 9-Line → objeto estructurado + errores; UI muestra 9-Line y permite iniciar incidente. Gate: incident end-to-end con entrada realista.
15–16	Metacognitivo v1: métricas (loops, oscilación, fallos MCP), políticas freeze/escalate/ask-human.	Scorecards de estabilidad/confianza, acciones de control, y trazabilidad. Gate: test de estrés simulado con fallos y escalado HILT.
17–18	BMS Stub MCP: ciclo request/ack/cambios; UI panel “C2 requests”.	Integración Coordinador → BMS stub (MCP); UI muestra requests/acks. Gate: demo de ciclo operativo completo simulado.

Continúa en la siguiente página

Semana(s)	Objetivos principales	Entregables / Gate
19–20	Generador de escenarios + suite de regresión con replay. Métricas mínimas de calidad/estabilidad.	20–50 episodios sintéticos; ejecución batch; métricas: violaciones hard, latencia, estabilidad, diversidad COAs. Gate: regresión automatizada.
21–22	Pulido UI: capas, filtros, comparación de COAs, timeline/auditoría, export AAR.	Interfaz HILT usable: mapa + COAs + doctrina + logística + timeline. Export AAR por episodio.
23–24	Demo pack y documentación: escenarios “de teatro”, checklist, límites y roadmap Fase 2.	5–10 escenarios de demo; documentación de arquitectura, contratos, reglas, extensibilidad. Gate final: demo consistente y reproducible.

4. Resultados esperados al final de la fase MVP

Al final de las 24 semanas se espera disponer de:

- Un sistema agéntico operativo (A2A) con herramientas accesibles vía MCP, ejecutándose íntegramente en DGX.
- UI HILT visual con mapa, capas tácticas, rutas, COAs comparables, y paneles de doctrina/logística/auditoría.
- Motor de doctrina MVP con trazabilidad y capacidad de bloquear (al menos reglas críticas).
- Metacognición básica que detecta inestabilidad y fuerza intervención humana.
- Replay/AAR para reproducibilidad y mejora iterativa, además de un generador de escenarios sintéticos.

5. Extensión a Fase 2 (líneas naturales)

Una vez completado el MVP, las extensiones típicas incluyen:

- Routing más avanzado (coste-tiles, terreno, dinámica temporal, restricciones más ricas).
- Doctrina ampliada (mayor cobertura, versionado, pruebas formales y reporting más completo).
- Simulación/digital twin y datasets (entrenamiento, evaluación estadística, AAR avanzado).
- Agentes clínicos ampliados (triaje avanzado, PFC con límites clínicos y verificación reforzada).
- Integración real con BMS/MedC2 (manteniendo el aislamiento y controles HILT).