

La importancia de los LLM personalizados: fiabilidad, costes, seguridad y soberanía

La necesidad de adaptar la inteligencia artificial a las exigencias de la formación militar

La incorporación de modelos de lenguaje de gran tamaño (Large Language Models, LLM) en los procesos formativos representa una oportunidad significativa para mejorar la preparación del personal militar, optimizar los ciclos de aprendizaje y facilitar el acceso al conocimiento. Sin embargo, el uso directo de modelos frontera desarrollados por terceros, como ChatGPT, Claude o Gemini, plantea una serie de limitaciones cuando se aplican en contextos militares, donde los requisitos de precisión, control, seguridad y disponibilidad son especialmente exigentes.

Estos modelos frontera han sido entrenados para resolver una amplia variedad de tareas y responder a usuarios de múltiples ámbitos. Esta versatilidad constituye una ventaja en escenarios abiertos, pero puede convertirse en una limitación cuando se requiere un comportamiento altamente especializado. En el ámbito formativo del Ejército, el conocimiento no solo debe ser amplio, sino también estar alineado con doctrinas, procedimientos, normativa interna, terminología específica, estándares de instrucción y objetivos pedagógicos concretos.

La formación militar exige herramientas capaces de proporcionar respuestas consistentes, verificables y adaptadas al entorno operativo. Un modelo generalista puede generar respuestas plausibles pero incorrectas, interpretar de forma inadecuada conceptos doctrinales o no distinguir entre información pública, información sensible y contenidos restringidos. Además, la dependencia de servicios tecnológicos externos introduce incertidumbres relacionadas con la continuidad del servicio, la evolución de los costes y las condiciones de uso o la gestión de los datos empleados durante la interacción.

Ante este escenario, resulta necesario avanzar hacia soluciones alternativas que cubran los aspectos anteriormente mencionados. La propuesta del IIC se centra en el desarrollo de modelos de inteligencia artificial especializados, diseñados o adaptados para funciones concretas dentro del ámbito formativo militar, combinada con una plataforma de RAG (Retrieval Augmented Generation) propia y completamente portable, desplegable en cualquier entorno.

Especialización de modelos

Esta alternativa consiste en utilizar LLM personalizados para tareas específicas, ajustados mediante técnicas de especialización, integración de conocimiento propio y adaptación a los objetivos formativos del Ejército. Estos modelos no necesariamente requieren alcanzar la escala de los grandes modelos frontera para ofrecer un rendimiento superior en dominios concretos. Un modelo más pequeño, correctamente entrenado y alimentado con fuentes autorizadas, puede superar a un modelo generalista en tareas específicas al estar optimizado para el contexto donde será empleado. Además, estos modelos se pueden incorporar a arquitecturas de tipo RAG que permiten referenciar las fuentes documentales empleadas en la síntesis de la respuesta.

La especialización aporta ventajas fundamentales en cuatro dimensiones: fiabilidad, costes, seguridad y soberanía.

Fiabilidad

La primera ventaja de los modelos personalizados es que mantienen la fiabilidad de los modelos generalista, pudiendo llegar a superarla dependiendo de la tarea. Un modelo especializado configurado dentro de una arquitectura RAG puede emplear únicamente fuentes de conocimiento previamente seleccionadas, incorporar criterios pedagógicos definidos por expertos y ofrecer respuestas coherentes con los objetivos de instrucción establecidos. Esto permite transformar la inteligencia artificial en un asistente formativo alineado con la doctrina y no simplemente en un generador de texto de propósito general. Además, la posibilidad de evaluar, auditar y mejorar progresivamente el modelo facilita un ciclo continuo de perfeccionamiento, en el que los errores detectados pueden corregirse mediante nuevos datos y ajustes específicos.

Costes

La utilización de modelos frontera externos implica habitualmente costes recurrentes asociados al consumo de tokens que depende del volumen de consultas. En entornos con un uso intensivo, como los procesos formativos permanentes, estos costes pueden crecer de forma significativa. No solamente hay que considerar el uso por parte de los alumnos, sino también los posibles costes de crear, traducir, o transcribir contenidos en los que se ven involucrado el uso de LLM.

Muchas necesidades pueden resolverse mediante modelos especializados más eficientes, ejecutados en infraestructuras propias o con un control más preciso del consumo. Esta estrategia permite reducir costes operativos a medio y largo plazo, además de favorecer una planificación presupuestaria más estable y predecible. Esta reducción puede ser realmente drástica (hasta tres órdenes de magnitud: de cientos de miles de euros al año, a cientos de euros) en escenarios con un consumo muy elevado.

Seguridad

La seguridad constituye una dimensión crítica en el ámbito militar. El empleo de modelos de terceros implica transferir determinadas interacciones y datos a infraestructuras externas, lo que puede generar riesgos relacionados con la confidencialidad, el almacenamiento de información o la exposición accidental de contenidos sensibles.

Los LLM personalizados se puede desplegar modelos en entornos controlados lo cual facilita la aplicación de medidas de protección, auditoría y cumplimiento normativo. De esta manera, se obtiene un mayor control sobre dónde se procesan los datos, cómo se gestionan los accesos y qué información puede utilizar el sistema.

Asimismo, la especialización, combinada con una arquitectura RAG, permite limitar el comportamiento del modelo, reduciendo respuestas no deseadas y evitando que el sistema acceda a fuentes o conocimientos incompatibles con el propósito formativo establecido.

Soberanía

La dependencia tecnológica de proveedores externos constituye un factor estratégico relevante. El desarrollo y empleo de modelos personalizados contribuye a reforzar la soberanía digital, al permitir disponer de capacidades propias de inteligencia artificial adaptadas a las necesidades nacionales y militares.

Contar con modelos especializados bajo control institucional garantiza mayor independencia frente a cambios comerciales, modificaciones de condiciones de servicio, cambios regulatorios o restricciones de acceso impuestas por terceros.

La soberanía no implica únicamente disponer de una infraestructura propia, sino también controlar el conocimiento incorporado al sistema, los procesos de actualización y la evolución futura de la herramienta.

Una ventaja operativa directa en la formación militar

La implantación de LLM personalizados y plataformas RAG aporta un beneficio operativo directo al mejorar la fiabilidad, seguridad y eficiencia de los procesos formativos. Estos sistemas pueden actuar como asistentes inteligentes de instrucción, capaces de adaptar contenidos al nivel del alumno, proporcionar apoyo continuo al aprendizaje, generar escenarios de entrenamiento y facilitar la consulta rápida de documentación validada.

El resultado es una formación más ágil, homogénea y personalizada, con capacidad para acelerar la adquisición de conocimientos y mejorar la preparación del personal. Al mismo tiempo, se mantiene el control institucional sobre la información utilizada y sobre el comportamiento del sistema.

En definitiva, proponemos una estrategia inteligente de especialización que permita identificar los ámbitos en los que resulta conveniente sustituir modelos frontera por modelos propios. Allí donde la precisión, la seguridad, los costes y la autonomía sean factores críticos, los LLM personalizados ofrecen una alternativa más fiable, eficiente y alineada con las necesidades del Ejército. Apostar por esta aproximación supone avanzar hacia una capacidad de inteligencia artificial más controlada, sostenible y preparada para responder a los retos presentes y futuros de la formación militar.

Esta visión se sustenta en una trayectoria consolidada de investigación y aplicación práctica en el ámbito de la inteligencia artificial. Los más de 35 años de experiencia del IIC en inteligencia artificial, analítica avanzada y procesamiento del lenguaje natural respaldan su capacidad para abordar iniciativas de alta complejidad tecnológica. La combinación de conocimiento científico, experiencia en el desarrollo de soluciones para entornos de elevada exigencia y una comprensión profunda de los retos asociados a la adopción de estas tecnologías nos permiten diseñar e implantar modelos de IA especializados, adaptados a las necesidades específicas de cada organización. Esta experiencia constituye una base sólida para impulsar capacidades de inteligencia artificial fiables, seguras, eficientes y sostenibles, alineadas con los requisitos estratégicos de la formación militar.