FACULTAD MILITAR CONJUNTA

Universidad de la Defensa Nacional

La Escuela Superior de Guerra Conjunta como punto de inflexión estructurante del Sistema Educativo Militar: hacia un modelo de Estado Mayor Cognitivo para Escenarios 4.0

Informe final

Proyecto de Investigación DD 67/2023/FMC: Seguridad Estratégica del Estado 4.0 - El impacto de intangibles tecnológicos disruptivos en la Defensa

Director: Comodoro (R) Mág. Pablo Andrés Farias

Finalizado: 31/12/2024

Fecha de entrega y publicación del Informe final: 11/05/2026

Resumen

La transformación digital y la aceleración del ciclo decisional, impulsadas por la inteligencia artificial (IA), la automatización cognitiva y la ciencia de datos, redefinen la naturaleza del planeamiento y la conducción en el nivel operacional.

La Escuela Superior de Guerra Conjunta (ESGC), dependiente de la Universidad de la Defensa Nacional (UNDEF), se consolida como institución bisagra y estructurante del Sistema Educativo de la Defensa (SED) en el ámbito militar, articulando doctrina, ciencia y tecnología para formar Oficiales de Estado Mayor capaces de comprender, anticipar y decidir en entornos complejos 4.0.

Este Proyecto de Investigación, iniciado en 2024 y de desarrollo progresivo, estableció como exigencia inicial estructurante abordar las bases y fundamentos epistemológicos, doctrinarios y operativos de un modelo de Estado Mayor Cognitivo (EMC) como categoría doctrinaria y organizacional. Dicho modelo se expresa en una arquitectura estratégico-operacional flexible, orientada a producir superioridad decisional en el PPMC en escenarios 4.0 o superiores, caracterizados por la disputa de la dimensión cognitiva y por la necesidad de preservar la autonomía del juicio crítico.

En ese marco, el EMC se concibe como la integración de personas, métodos, datos y tecnologías digitales auditables, incorporando controles cognitivos orientados a sostener calidad decisional (gestión de supuestos e incertidumbre, validación adversarial y trazabilidad de evidencia). Todo ello se operacionaliza bajo el principio de control humano significativo, garantizando responsabilidad identificable, registro de racionalidad y gobernanza verificable del proceso.

La investigación adopta un diseño cualitativo a partir de un estudio de caso orientado a la "reingeniería curricular de la FMC/ESGC - Nivel 1" y al desarrollo de un modelo de Estado Mayor Cognitivo (EMC) con alcance exclusivo FMC/ESGC, sustentado en un repositorio trazable 2012-2026 vinculado a hitos CPDN/PEM, con procedimientos auditables y control humano significativo. La expansión a otras unidades académicas queda fuera del alcance del presente documento

Este documento, elaborado en el marco del Programa de Investigación ESGCFMC, presenta una reflexión institucional sobre el impacto de las tecnologías disruptivas -como se expresó en el proyecto Seguridad Estratégica del Estado 4.0- en la formación del Oficial de Estado Mayor e impacto en la Academia de la Defensa. Se propone una estrategia de desarrollo e integración en el marco del Sistema Educativo Nacional (SEN) y actores estratégicos de interés que consolide un modelo cognitivo, ético y soberano de educación militar.

El informe se sustenta en el diseño, desarrollo y evaluación del empleo de asistencia de IA en el PPMC. Comprende una arquitectura por fases —entorno seguro, perfiles por rol, herramientas doctrinarias y plataforma integradora— y la identificación de brechas doctrinarias (glosario), tecnológicas (latencia y hardware), culturales (resistencia) y metodológicas (validación).

Se concluye a partir de esta primera etapa, que la ESGC puede funcionar como "Centro de Gravedad Intelectual" del Sistema Educativo de la Defensa (SED), a la par de la Infraestructura Tecnológica asociada, si institucionaliza en el marco del desarrollo del Estado Mayor Cognitivo (EMC): (1) repositorio trazable 2012–2026 vinculado a hitos CPDN/PEM (Gestión del Conocimiento), (2) glosario doctrinario y trazabilidad (Epistemología y lenguaje), (3) validación adversarial y control de sesgos (Auditoría de IA) y (4) estrategia curricular 2026-2030 (Soberanía Cognitiva).

Palabras Clave: Educación Militar, Defensa 4.0, Estado Mayor Cognitivo, Inteligencia Artificial, Proceso Planeamiento, Gestión del Conocimiento.

1. Introducción

El escenario geopolítico y tecnológico del siglo XXI fuerza un ajuste de fondo: el diferencial estratégico se desplaza, crecientemente, hacia la capacidad de procesar información, construir sentido, sostener legitimidad y decidir con precisión en condiciones de incertidumbre.

La velocidad del cambio, impulsada por la inteligencia artificial (IA), la automatización cognitiva y la ciencia de datos, redefine la naturaleza y características del planeamiento y la conducción. En este contexto, la educación militar adquiere un valor estratégico: formar oficiales capaces de comprender, anticipar y decidir en entornos complejos.

La Escuela Superior de Guerra Conjunta (ESGC) dependiente de la Universidad de la Defensa Nacional (UNDEF) conceptualiza este desafío como transición hacia un modelo cognitivo, cooperativo e innovador, donde los "intangibles tecnológicos" (conocimiento, información, datos y algoritmos) adquieren centralidad en el poder nacional.

Este enfoque converge con marcos internacionales que señalan que la transformación digital exige rediseñar capacidades institucionales (no solo adquirir tecnología): fortalecer gobernanza del dato, formación de capital humano, evaluación, y sistemas de aseguramiento de calidad.

En educación, UNESCO propone reconfigurar el contrato social educativo; en desarrollo, el BID enfatiza transformación digital como política pública. En defensa, CESEDEN y NATO subrayan desafíos y oportunidades de IA para la seguridad y la conducción.

En el nivel operacional, esta transformación no es un debate abstracto: se traduce en tensión entre velocidad, volumen informacional, sesgos y exigencia de juicio profesional. En ese punto aparece el núcleo del trabajo: pasar de "Estado Mayor informatizado" a "Estado Mayor Cognitivo".

En este contexto, la ESGC representa el núcleo del pensamiento militar conjunto y el centro de convergencia cognitiva del sistema educativo de la defensa. Su función trasciende la docencia: actúa como nodo articulador de la doctrina con la investigación y la innovación tecnológica, en correspondencia con los lineamientos de la Directiva de Política de Defensa Nacional (2021) y el Plan de Capacidades Militares (2023).

2. Planteamiento del problema

2.1 Problema general

Existe una brecha institucional entre exigencias del Entorno 4.0 (zona gris, multidominio, desarrollo de operaciones bajo disputa informacional - Centros de Gravedad), y capacidad del Sistema Educativo Militar Conjunto para generar y transferir conocimiento y competencias que produzcan superioridad decisional en el PPMC.

Este proyecto plurianual FMC/ESGC lo define como vacancia estructural por impacto de tecnologías disruptivas e IA, y prescribe investigación aplicada para mejorar calidad educativa, integrando docencia, investigación y extensión, con retroalimentación desde la práctica y estándares nacionales.

2.2 Problema específico (operacional)

La evidencia aplicada IA-PPMC muestra que el desafío central no es "usar IA", sino gobernar su integración que asegure articulación doctrina, trazabilidad y juicio crítico, a la par de:

Articulación Doctrinaria: La IA no debe operar de forma aislada, sino integrarse en los manuales de procedimiento, tácticas y la doctrina militar vigente (adecuación del lenguaje), asegurando que las decisiones automatizadas o semiautomatizadas estén alineadas con la estrategia nacional.

Trazabilidad: Es necesario documentar el ciclo de vida completo de los algoritmos -desde los datos de origen hasta los resultados- para garantizar transparencia y responsabilidad (*accountability*) en las decisiones operativas.

Juicio Crítico: Se debe mantener el control humano sobre las decisiones críticas, evitando el sesgo de automatización y asegurando que los operadores puedan cuestionar y validar las recomendaciones de la IA.

Compatibilidad y Entorno Seguro: La infraestructura debe ser segura, confiable y capaz de integrarse con sistemas heredados y, fundamentalmente, ser compatible con futuras evoluciones tecnológicas, garantizando la soberanía de los datos.

Resistencia cultural a abandonar métodos tradicionales aun con herramientas consistentes

3. Hipótesis

Si la ESGC institucionaliza un EMC integrado por especialistas, métodos, datos y tecnologías auditables dentro del PPMC, incrementará la superioridad decisional y reducirá las brechas entre educación, doctrina e innovación en escenarios 4.0.

En ese sentido, “la eficacia del EMC -en esta primera etapa- dependerá más de arquitectura de procesos (glosario, trazabilidad, validación adversarial, control humano) que de la herramienta aislada. El IA-PPMC evidencia que la mayor dificultad fue conceptual/doctrinaria (parámetros) y de gobernanza, que no “tener IA”.

4. Objetivos

4.1 Objetivo General

Desarrollar un modelo de EMC para la FMC/ESGC que produzca superioridad decisional en el PPMC mediante la integración de especialistas, métodos, datos y tecnologías auditables, bajo control humano significativo.

4.2 Objetivos Específicos

Identificar brechas institucionales (doctrina, currícula, cultura y tecnología).

Anexo 3 - Estado del Arte y Vacancia Estructural (Inteligencia Artificial (IA) y Tecnologías Disruptivas (TD) en el Nivel Operacional) o Anexo 5 - IA como asistente cognitivo en PPMC, con trazabilidad y control humano significativo

Definir competencias del OEM 4.0[1] para EMC (multidominio, CDG -CoG-), zona gris, auditoría de IA).

[1] OEM 4.0: Oficial de Estado Mayor para Escenarios 4.0

3 Propósito: detectar brechas (vacancias) relevantes para un Estado Mayor Cognitivo, Cada registro del repositorio corresponde a un Producto de Conocimiento (PK), entendido como: documento,

Anexo 6 - Competencias del OEM conjunto y conformación del Estado Mayor Cognitivo (EMC)

Establecer hoja de ruta curricular y escalamiento institucional plurianual, incluyendo el SOP EMC-PPMC como instrumento transversal de implementación y control de calidad.

Anexo 7 - Fundamentación Empírica del Estado Mayor Cognitivo (EMC) en Escenarios 4.0 o Anexo 8 - Formulario Operativo EMC (Control de avance del proceso de investigación aplicada - FMC/ESGC)

Construir repositorio trazable FMC/ESGC 2012-2026 con vínculo a hitos CPDN/PEM[3].

Anexo 1 - Repositorio Trazable FMC/ESGC 2012-2026 (vinculación CPDN/PEM) o Anexo 2 - Repositorio Digital FMC/ESGC 2012-2026 (Tabla Operativa) o Anexo 4 - Mapa de Conocimiento 2012-2026 + sincronía CPDN/PEM + repositorio trazable

Nota General: El contenido de los distintos Anexos, si bien buscan avanzar en objetivos específicos, están vinculados -por su transversalidad- a los distintos objetivos del presente y "ejes" consignados en el Proyectos de Investigación Plurianual correspondiente[2].

Nota metodológica: El SOP EMC-PPMC (checklist, plantillas y criterios de aceptación) se incorpora como Anexo 8 -transversal- que operacionaliza y estandariza la producción, validación y trazabilidad de los productos vinculados a cada objetivo específico. En consecuencia, su aplicación es común a los Anexos 1-7 y constituye el instrumento de aseguramiento de cumplimiento de metas, criterios y calidad del proceso.

5. Metodología

Estudio de caso (ESGC - Nivel 1) de abordaje cualitativo alineado al proyecto plurianual (diagnóstico, revisión, hipótesis, recolección, análisis, resultados orientados a innovación); sobre un corpus de indagación, investigación y hallazgos (años 2024, 2025 y 2026 en el marco del desarrollo de actividades curriculares de la ESGC Nivel 1), empleando como técnica de análisis codificación temática por categorías, triangulación y matriz "hallazgo-evidencia–brecha-recomendación EMC" en las siguientes dimensiones:

Políticas y estrategias institucionales

Competencias del OEM para EMC

Adecuación curricular y Adopción tecnológica-gobernanza

Repositorio digital y sincronía CPDN/PEM

6. Marco Teórico

La integración de la inteligencia artificial (IA) en las operaciones militares representa una oportunidad significativa para obtener ventajas asimétricas en el ámbito de la seguridad nacional.

---

informe, TFI, artículo, clase-contenido, guía metodológica, protocolo, resultado de ejercicio, publicación o evento académico con evidencia documental disponible.

[2] Programa de Investigación ESGC-UNDEF (2024) - **Seguridad Estratégica del Estado 4.0 - El impacto de intangibles tecnológicos disruptivos en la Defensa (2024)**

Para aprovechar plenamente este potencial, los líderes y responsables políticos militares de las grandes potencias / emergentes adoptan un enfoque integral que contempla diversos imperativos estratégicos interrelacionados.

El mantenimiento de la superioridad tecnológica y la posición de vanguardia en contextos de seguridad nacional depende de la aceleración del desarrollo e investigación en IA y avance del aprendizaje automático (ML).

Este objetivo requiere no solo priorizar la inversión en investigación, sino también fomentar alianzas estrechas con el sector académico, la industria y socios internacionales, asegurando así la incorporación continua de tecnologías de IA de última generación en las aplicaciones militares[3].

Junto con los avances tecnológicos, resulta fundamental establecer directrices éticas, legales y sociales para el uso responsable de la IA. Definir y hacer cumplir límites alineados con los valores y principios nacionales permite garantizar que las tecnologías de IA se utilicen de manera ética y legal en todos los contextos, además de facilitar la cooperación internacional, un elemento esencial para el desarrollo exitoso de la IA[6].

Al respecto, el desarrollo de una estrategia integral de IA constituye una extensión natural de estas consideraciones éticas. La formulación de una estrategia nacional de ciberseguridad que incluya objetivos claros, hitos y métricas proporciona una hoja de ruta para el desarrollo y despliegue de tecnologías de IA, asegurando que las fuerzas armadas permanezcan a la vanguardia de la innovación y promoviendo la resiliencia e interoperabilidad de la IA en las distintas ramas militares[4].

En cuanto a la resiliencia e interoperabilidad, la implementación de métodos de entrenamiento adversarial fortalece la confiabilidad verificable de los sistemas de IA y ML, reduciendo su vulnerabilidad ante datos maliciosos y facilitando la integración fluida de estas tecnologías. Ello sienta las bases para la creación de un marco de IA multidominio, capaz de integrarse en todas las áreas de operaciones militares: tierra, mar, aire, espacio y ciberespacio, lo que permite una mayor interoperabilidad y colaboración[5].

La consolidación de este marco requiere la formación de una fuerza profesional capacitada en IA. La inversión en programas de educación, formación y reclutamiento enfocados en habilidades de IA y ML entre el personal militar constituye un paso crucial para garantizar el desarrollo efectivo de estas tecnologías en operaciones de defensa nacional.

Sobre esta base, la incorporación de capacidades de IA en los procesos de toma de decisiones militares mejora significativamente la conciencia situacional y la toma de decisiones en entornos complejos y dinámicos.

El uso de IA para el análisis y procesamiento de datos en tiempo real permite a los líderes militares tomar decisiones mejor fundamentadas, manteniendo la ventaja estratégica en entornos complejos. Además, la integración de simulaciones y juegos de guerra impulsados por IA en el entrenamiento militar incrementa la preparación y la eficacia operativa[6].

---

[3] Madison, A., McDowell, K., Goecks, V. G., Hansberger, J., Olney, C. M., Ahern, C., et al. (2025). 'New' challenges for future C2: Commanding soldier-machine partnerships [6]
Idem.
[4] Idem.
[5] Idem
[6] Madison, A., McDowell, K., Goecks, V. G., Hansberger, J., Olney, C. M., Ahern, C., et al. (2025).

Finalmente, la adaptación de los procesos, conceptos y doctrinas militares para incorporar perspectivas y riesgos asociados a la IA es esencial para facilitar su adopción e implementación exitosa. La actualización de estos elementos permite que las fuerzas armadas se mantengan ágiles y adaptables en un entorno tecnológico en constante evolución, aprovechando plenamente el potencial estratégico de la IA en sus operaciones.

La incorporación de la inteligencia artificial (IA) en los dominios de comando y control militar exige comprender tanto sus ventajas operativas como sus riesgos inherentes. El informe de Brundage (2018) definió el marco de referencia sobre los potenciales usos maliciosos de la IA, subrayando la necesidad de estrategias nacionales que equilibren innovación y seguridad[7].

A partir de esta preocupación, los trabajos posteriores se han centrado en la resiliencia operativa de los sistemas de aprendizaje profundo desplegados en entornos hostiles. Kurakin[8] demostraron la viabilidad de ataques físicos contra modelos de visión por computadora, alertando sobre vulnerabilidades críticas para plataformas autónomas y sistemas de reconocimiento en el campo de batalla.

Más recientemente, Ilyas[9] profundizaron en la naturaleza de las perturbaciones adversarias, demostrando que éstas pueden explotar características aprendidas legítimas del modelo, lo que complica su mitigación mediante técnicas defensivas tradicionales.

En conjunto, esta línea de investigación ha impulsado la adopción de prácticas de desarrollo seguro, ciclos de prueba en condiciones operativas y la integración de contramedidas adaptativas; estructuras organizativas que combinan analistas humanos y agentes de IA para la toma de decisiones tácticas y estratégicas. Así, la literatura ha evolucionado desde la identificación de amenazas hasta la formulación de arquitecturas resilientes, piedra angular de cualquier estrategia contemporánea de implementación de IA militar.

6.1. Principios fundamentales de la inteligencia artificial en el ámbito militar

Uno de los principios fundamentales en la implementación de inteligencia artificial (IA) en el ámbito militar es la transparencia, que se manifiesta en la capacidad de los sistemas para comunicar de manera clara sus niveles de incertidumbre y los fundamentos de sus recomendaciones.

La trazabilidad se presenta como un elemento esencial para garantizar la transparencia, permitiendo que los procesos de toma de decisiones de los sistemas de IA sean comprensibles y auditables por los operadores humanos.

La utilización de métodos de inteligencia artificial explicable contribuye a que los usuarios comprendan cómo y por qué el sistema llega a determinadas conclusiones, lo que resulta crucial en contextos donde las decisiones pueden tener consecuencias significativas. Esta transparencia no solo

---

'New' challenges for future C2: Commanding soldier-machine partnerships

[7] Brundage, M., Avin, et al (2018). The malicious use of artificial intelligence: Forecasting, prevention, and mitigation.

[8] Kurakin, A., Goodfellow, I. J., & Bengio, S. (2016). *Adversarial examples in the physical world* (arXiv:1607.02533). arXiv. https://arxiv.org/abs/1607.02533

[9] Ilyas, A., Santurkar, S., Tsipras, D., Engstrom, L., Tran, B., & Madry, A. (2019). *Adversarial examples are not bugs, they are features* (arXiv:1905.02175). arXiv. https://arxiv.org/abs/1905.02

facilita la confianza en el sistema, sino que también permite una supervisión efectiva y la posibilidad de intervención humana cuando sea necesario[10].

La justicia y la proporcionalidad son principios éticos que guían la aplicación de la IA militar, asegurando que las acciones derivadas de los sistemas automatizados se alineen tanto con los objetivos humanitarios como con los militares.

La proporcionalidad implica que las respuestas generadas por la IA deben estar equilibradas en relación con la amenaza identificada y los posibles daños colaterales, respetando los principios del derecho internacional humanitario, estableciendo procedimientos operativos estándar (SOP) y las reglas de enfrentamiento (ROE).

Estos principios se ven reflejados en la capacidad de los sistemas para identificar situaciones en las que, por ejemplo, la presencia de niños o heridos impide la designación de un objetivo como legítimo[14].

La gobernabilidad se refiere a la necesidad de mantener el control humano sobre los sistemas de IA, asegurando que los operadores puedan supervisar y, en caso necesario, anular las decisiones automatizadas. Este principio es fundamental para preservar las Fuerzas y la responsabilidad humanas en la toma de decisiones críticas.

La responsabilidad implica que, aunque la IA pueda asistir en el proceso de toma de decisiones, la rendición de cuentas recae en última instancia sobre los operadores humanos, quienes deben garantizar que las acciones se ajusten a los marcos legales y éticos establecidos.

Finalmente, la confiabilidad se relaciona con la confiabilidad verificable y la consistencia de los sistemas de IA, asegurando que funcionen de manera predecible y segura en entornos operativos complejos y dinámicos. La integración de estos principios en el diseño y desarrollo de la IA militar es esencial para fomentar la confianza y la aceptación de estas tecnologías en procesos de decisión reales[11].

7. Estado del arte: la educación militar en la era de la inteligencia artificial

Las tendencias internacionales en defensa muestran una convergencia entre inteligencia artificial, simulación operacional y educación avanzada. Documentos como la Estrategia de IA para la Defensa y la Seguridad de la OTAN (2023) y los estudios del CESEDEN (2022) destacan que la IA transforma tanto la conducción como la formación, imponiendo un nuevo paradigma de "aprendizaje operativo continuo"; ambos sostienen que la IA influye sobre inteligencia, C2, apoyo a decisión y diseño de fuerzas; desplazando el punto crítico hacia integración responsable, interoperabilidad y control humano.

En América Latina, el Banco Interamericano de Desarrollo (BID, 2023) y la UNESCO (2022) señalan la necesidad de vincular educación, tecnología e innovación con seguridad y desarrollo sostenible; encuadran la transformación digital como política pública que requiere capacidades estatales: gobernanza, competencias, evaluación y ética. Esto es relevante porque el EMC no se

[10] Anneken, M. (2025). Ethical considerations for the military use of artificial intelligence in visual reconnaissance [14] Idem.
[11] Idem.

legitima solo por rendimiento técnico, sino por su alineamiento con valores institucionales, trazabilidad y responsabilidad.

Algunas líneas técnicas relevantes para institucionalizar un EMC destacan:

“Responsible development and fielding” de IA en contextos de seguridad nacional: prácticas y políticas recomendadas.

Supervisión y complementariedad humano-máquina en combate: equipos humanos con roles explícitos de control.

Riesgo de usos maliciosos de IA y necesidad de mitigación: amenaza transversal que afecta dominio informacional y seguridad institucional.

Comunicaciones tácticas y networking con IA: resiliencia, interoperabilidad multidominio y amenazas adversariales.

La adopción de inteligencia artificial en defensa se está materializando en proyectos de gran envergadura, listado no exhaustivo, como Project Maven, GIDE, ATLAS, DARPA OFFSET, Iron Dome, ASTRAEA y SOPRENE, que ejemplifican la sinergia entre tecnologías avanzadas y capacidades militares.

Estos proyectos impulsan una nueva era de automatización, eficiencia y superioridad estratégica, sentando las bases para el desarrollo de un Estado Mayor Cognitivo capaz de anticipar, adaptarse y responder de manera autónoma a los desafíos del entorno operativo moderno.

El enfoque futuro se centra en el fortalecimiento de la colaboración entre diferentes dominios tecnológicos, promoviendo la interoperabilidad, la seguridad y la resiliencia, y asegurando que la inteligencia artificial se despliegue de manera responsable y efectiva en el ámbito militar[12].

El proyecto Seguridad Estratégica del Estado 4.0 - El impacto de intangibles tecnológicos disruptivos en la Defensa (Farías, 2024) indaga en un marco teórico pionero que introduzca el concepto de “intangibles tecnológicos” -conocimiento, información, algoritmos y datos- como elementos constitutivos del PPMC.

Este busca avanzar en un proceso de reflexión: la educación militar debe incorporar la dimensión cognitiva y tecnológica de la defensa en su estructura curricular, sus estrategias pedagógicas y sus mecanismos de evaluación.

NOTA: Anexo 3 - Estado del Arte y Vacancia Estructural (Inteligencia Artificial (IA) y Tecnologías Disruptivas (TD) en el Nivel Operacional)

7.1. La ESGC como bisagra estructurante del Sistema Educativo de la Defensa

En este proceso, la ESGC constituye una bisagra epistemológica y organizacional entre las Escuelas Superiores de las Fuerzas y el Sistema Universitario Nacional; coordinando la homologación doctrinaria, integración científica y articulación institucional con el rol de convertir producción académica en un marco común de pensamiento conjunto medible, transferible y auditable.

[12] Monzón Baeza, V., Parada, R., Concha Salor, L., & Monzo, C. (2025). AI-driven tactical communications and networking for defense: A survey and emerging trends.

Su tarea estructurante se manifiesta en tres ejes:

Homologación doctrinaria: define estándares de competencia del nivel operacional conforme al RC-20-01 y a los lineamientos del EMCFFAA.

Integración científica: vincula la docencia militar con la investigación académica y tecnológica.

Articulación institucional: coordina con la UNDEF, el MINDEF y el Sistema Educativo Nacional la producción de conocimiento estratégico.

La ESGC traduce la experiencia operacional en saber científico, garantizando que la educación militar sea una práctica reflexiva y no sólo instructiva.

Nota: Anexo 8 - Formulario Operativo EMC (Control de avance del proceso de investigación aplicada - FMC/ESGC), en el marco de la hoja de ruta curricular y escalamiento institucional.

7.2. Impacto en la Academia de la Defensa

La Academia de la Defensa, conformada por la UNDEF y los Institutos dependientes del EMC/EEMMGG constituyen el ecosistema de formación y pensamiento estratégico militar. La introducción de la IA y las tecnologías disruptivas obliga a reformular las funciones de investigación, docencia y extensión.

En ese sentido, un impacto que se evidencia en las siguientes dimensiones:

Académica: necesidad de actualizar los programas de posgrado (especializaciones) y maestrías con contenidos de procesos de decisión, simulación, ética algorítmica y análisis de datos.

Institucional: redefinición de las estructuras de gobierno educativo para integrar ciencia y doctrina.

Epistemológica: surgimiento de una “racionalidad cognitiva de la defensa”, donde el conocimiento estratégico se convierte en recurso crítico del Estado.

La ESGC actúa como un primus inter pares que lidera este proceso, actuando como “laboratorio cognitivo” que prueba metodologías, herramientas IA y modelos de planeamiento con trazabilidad doctrinaria.

8. Desarrollo de actividades de Campo (ESGC - Nivel 1 - con participación de alumnos de las Cohorte 2024, 2025 y 2026 conforme políticas de investigación de la FMC).

Esta actividad estuvo centrada en generar actividades de gabinete de EM orientadas a identificar las condiciones -preliminares- para la conceptualización, desarrollo, implementación y validación de un EMC entendido como una capacidad organizacional y enfoque doctrinario del Estado Mayor para generar superioridad decisional en el nivel operacional, integrando especialistas, métodos, datos y tecnologías digitales (incluida IA) en el PPMC.

Desde este abordaje, el EMC constituye una cultura estratégica que convierte la tecnología en ventaja decisional solo cuando existen procedimientos auditables que aseguren -a partir de un lenguaje doctrinario- trazabilidad de supuestos y evidencia, validación adversarial sistemática y control humano significativo en el proceso de decisión y conducción militar; sin este andamiaje, la velocidad informacional acelera errores en lugar de decisiones responsables.

Dentro de los aspectos críticos abordados para evaluar las características de un EMC, se consideró, entre otros, la mutación del centro de gravedad - CDG (CoG) en escenarios 4.0, así como su impacto y trascendencia en los procesos de decisión operacionales y tácticos. En consecuencia, se analizó la contribución de las tecnologías disruptivas (TD) y la IA en la identificación y evaluación del CDG (CoG), las vulnerabilidades críticas, la construcción de escenarios probables y la reducción de la incertidumbre mediante el análisis sistemático de datos.

En este sentido, y particularmente en escenarios de zona gris, la mutación del CDG (CoG) puede desplazarse hacia factores intangibles como la legitimidad, la cohesión, la narrativa, la arquitectura de decisión y la resiliencia cognitiva. Esto exige que el EMC incorpore controles y productos orientados al dominio cognitivo (supuestos, percepción, aceptabilidad y análisis de sensibilidad).

En paralelo, se refuerza la exigencia de control humano significativo en funciones y/o eventos críticos: no solo en funciones letales, sino también en C2 y en los procesos de decisión. En términos operativos, ello se traduce en la determinación de puntos de decisión indelegables, trazabilidad de supuestos, evidencia mínima y firma responsable.

Esta aproximación holística preliminar, cuyo detalle se amplía en los anexos correspondientes, permitió profundizar en las precisiones de alcance y contenido de los distintos Objetivos Particulares, asociados a los ejes del Proyecto de Investigación. En consecuencia, dichos objetivos orientaron las actividades desarrolladas con alumnos (trabajo de gabinete e investigación aplicada) de las distintas cohortes del ESGC Nivel 1.

Políticas y estrategias institucionales

La ESGC define orientación a modelo cognitivo e integración ciencia y tecnología; establece base para laboratorios cognitivos (Actividades y capacidades) y articulación con SEN.

Brecha crítica: Desarrollo parcial de instancias formales que institucionalicen estrategias e instrumentos asociados de implementación y control: capacidades, repositorio, SOP, glosario (ambigüedad terminológica es un riesgo doctrinario), criterios de evaluación.

o Anexo 3 - Estado del Arte y Vacancia Estructural (Inteligencia Artificial (IA) y Tecnologías Disruptivas (TD) en el Nivel Operacional). o Anexo 5 - IA como asistente cognitivo en PPMC, con trazabilidad y control humano significativo.

Competencias del OEM para EMC

En zona gris, la dinámica de evolución/mutación impacta en el juicio profesional/critico; el OEM debe fortalecer y desarrollar competencias de filtrado crítico, comunicación estratégica, manejo de incertidumbre y coordinación multidominio.

Brecha crítica: Ausencia de matriz competencia, evidencia PPMC y criterio de aprobación (evaluación real).

Anexo 6 - Competencias del OEM conjunto y conformación del Estado Mayor Cognitivo (EMC).

Adopción tecnológica y gobernanza

La IA-PPMC implica diseño proyecto, proceso por fases, desarrollo de infraestructura y exigencias de compatibilidad segura del entorno; la arquitectura por roles y funciones como condición de calidad (Doctrina y Cultura).

La gestión de eventuales procesos de inercia y/o resistencia cultural requiere la concreción de objetivos y productos tecnológicos intermedios, en el marco de un desarrollo progresivo de las

políticas y estrategias adoptadas. En términos prácticos, ello implica avanzar mediante hitos sucesivos de demostración, capacitación y aplicación, que permitan validar resultados, reducir fricción organizacional y consolidar la adopción.

Brecha crítica: gobernanza formal embrionaria (proyectos, objetivos, roles, control de versiones, registro de decisiones, auditoría).

Anexo 7 - Fundamentación Empírica del Estado Mayor Cognitivo (EMC) en Escenarios 4.0.

Anexo 8 - Formulario Operativo EMC (Control de avance del proceso de investigación aplicada - FMC/ESGC).

• Repositorio 2012-2026 y sincronía CPDN/PEM

El proyecto exige mapa de generación de conocimiento (evidencia) y sincronía con hitos CPDN/PEM, incluyendo relevamiento de repositorios digitales.

Brecha crítica: falta de SOP EMC-PPMC de repositorio trazable producto-hito, conforme a las exigencias de gestión de la calidad y a los estándares de producción, validación y auditoría del dato, la información y el conocimiento (checklist + plantillas + criterios de aceptación).

Anexo 1 - Repositorio Trazable FMC/ESGC 2012-2026 (vinculación CPDN/PEM).

Anexo 2 - Repositorio Digital FMC/ESGC 2012-2026 (Tabla Operativa).

Anexo 4 - Mapa de Conocimiento 2012-2026 + sincronía CPDN/PEM + repositorio trazable.

8.1 Evolución del concepto del Estado Mayor Tradicional

El desarrollo de actividades de EM en entornos híbridos e informacionales, en el marco de aceleración tecnológica de procesos, conllevó hacia la evolución de un "Estado Mayor Cognitivo" entendido como una estructura organizativa y operativa en la que la colaboración entre especialistas y sistemas de inteligencia artificial (IA) resulta fundamental para la toma de decisiones y la conducción de operaciones militares.

Esta articulación no se limitó a la simple coexistencia de especialistas y sistemas, sino a la integración profunda de las fortalezas de ambos. La resiliencia operativa y adaptabilidad del Estado Mayor Cognitivo radicó en la capacidad de los especialistas de EM para comprender y gestionar los procesos de toma de decisiones de la IA, así como en la habilidad de alternar entre diferentes modelos de IA según las exigencias del PPMC [17].

Las competencias digitales de operadores adquieren una importancia central, debiendo poseer habilidades y competencias para interpretar y supervisar el funcionamiento de la IA, asegurando así la selección de la herramienta más adecuada para cada situación producto del Proceso de Planeamiento.

La adaptabilidad y la flexibilidad se convierten en atributos esenciales del Estado Mayor Cognitivo, permitiendo que los equipos de especialistas-IA sean más ágiles y eficaces que los sistemas operados únicamente por especialistas.

17 Feldman, P., Dant, A., & Dreany, H. (2024). War elephants: Rethinking combat AI and human oversight

La evolución del Estado Mayor Cognitivo pone de manifiesto una transición de conceptos tradicionales de mando y control hacia una simbiosis avanzada entre especialistas y sistemas de IA.

Una simbiosis que se vuelve esencial para alcanzar la superioridad en entornos altamente dinámicos y competitivos.

El desarrollo comparado de actividades de gabinete que contemplaron por un lado la integración de la intuición y experiencia de especialistas con la capacidad de procesamiento y análisis de la IA que desestabilizaron el ciclo OODA (Observar, Orientar, Decidir, Actuar) de los equipos comprometidos (EMT[13] y Red Team), anticipando y superando -con aceptable grado de aproximación- los productos esperados.

Procesos que evidenciaron, las necesidades de alfabetización digital, la adaptación integral de las asignaturas curriculares al fin perseguido y la adecuación doctrinaria asociada. En ese sentido, la capacidad de especialistas para captar matices y contextos específicos resultó crítica en la toma de decisiones complejas; a la par de las perspectivas y habilidades que proporcionaron profundidad de comprensión no replicada por los modelos de IA empleados.

8.2 Integración de la inteligencia artificial en la toma de decisiones estratégicas-operacionales

La integración de la inteligencia artificial (IA) en la toma de decisiones estratégicas militares requiere un enfoque integral que priorice el desarrollo tecnológico y la colaboración intersectorial. Mantener la superioridad tecnológica en el ámbito de la defensa nacional depende de la aceleración de la investigación y el desarrollo en IA y aprendizaje automático (ML).

Para lograrlo, es fundamental establecer alianzas sólidas con el sector académico, la industria y socios estratégicos. Estas colaboraciones permiten que las tecnologías de IA se incorporen de manera sustentable en las aplicaciones militares, asegurando que las fuerzas armadas se mantengan a la vanguardia de la innovación tecnológica.

Por otro lado, esta integración exige la creación de directrices éticas y legales que regulen su uso; definir y hacer cumplir límites que reflejen los valores y principios nacionales es esencial para garantizar que las tecnologías de IA se utilicen de manera ética y legal en todos los contextos operativos.

Este enfoque fortalece tanto la legitimidad interna y externa de las operaciones militares, como la cooperación internacional, un aspecto clave en el desarrollo exitoso de tecnologías de IA en un entorno de seguridad global.

La resiliencia y la interoperabilidad de los sistemas de IA y ML son componentes críticos para su integración en la toma de decisiones estratégicas/operacionales. La adopción de métodos de entrenamiento adversarial fortalece la resiliencia operativa de estos sistemas frente a vulnerabilidades y facilitando una integración fluida en un marco multidominio que abarque tierra, mar, aire, espacio y ciberespacio.

NOTA: Anexo 5 - IA como asistente cognitivo en PPMC, con trazabilidad y control humano significativo

[13] EMT: Estado Mayor Tradicional; Blue Team / Red Team: Equipo asistido por IA: prueba de colapso, alternativa obligatoria, criterio de aceptación, registro de decisiones.

8.3 Arquitectura del Estado Mayor Cognitivo

La arquitectura del Estado Mayor Cognitivo se fundamenta en principios de diseño orientados a maximizar la articulación humano-IA y la unidad de esfuerzo en entornos militares.

Entre estos principios destaca la organización de la información clave en torno a los objetivos estratégicos-operacionales, permitiendo que tanto los especialistas como los sistemas contribuyan a un enfoque coherente, verificable y auditable, con trazabilidad de supuestos, evidencia mínima y control humano significativo.

Además, se enfatiza el soporte a procesos avanzados de conciencia situacional (SA), como la comprensión y la proyección, que son esenciales para anticipar y responder a dinámicas operacionales complejas, minimizando la carga informativa en entornos operativos saturados de datos.

Un componente esencial de esta arquitectura es la interfaz de usuario, que debe facilitar la actualización dinámica de modelos mentales compartidos mediante la transparencia.

Esto implica comunicar de manera clara cualquier cambio en las capacidades, comportamientos o posibles sesgos de la IA, permitiendo que los operadores humanos mantengan el control y puedan intervenir eficazmente cuando sea necesario; asegurando una toma de decisiones más eficiente y fundamentada.

La transparencia y la experiencia de usuario adecuada no solo mejoran la eficiencia en la toma de decisiones, sino que también fomentan la confianza y la formación de modelos mentales compartidos entre los miembros del Estado Mayor Cognitivo[14.]

La implementación de tecnologías de computación espacial constituye un pilar innovador en la arquitectura del Estado Mayor Cognitivo; permiten la interacción fluida entre los entornos físico y digital, utilizando interfaces de realidad aumentada, realidad virtual y realidad mixta para crear espacios de trabajo inmersivos y contextualmente conscientes (Ejemplo plataforma OpsVision, diseñada específicamente para personal de mando y control (C2) y equipos de Estado Mayor) brindando una visión comprensiva del entorno operacional, permitiendo a los comandantes explorar y simular diferentes escenarios estratégicos.

Este enfoque facilita la planificación detallada, la alineación de esfuerzos y la coordinación efectiva entre todos los elementos de la misión. Las herramientas de comunicación integradas y la plataforma visual compartida refuerzan la colaboración y la unidad de esfuerzo, elementos críticos para enfrentar la complejidad y el dinamismo de los escenarios de guerra modernos.

Así, la arquitectura del Estado Mayor Cognitivo, apoyada en la computación espacial y plataformas colaborativas, se orienta a crear entornos de batalla más adaptativos, receptivos y eficaces frente a los desafíos contemporáneos[20].

[14] Madison, A., McDowell, K., Goecks, V. G., Hansberger, J., Olney, C. M., Ahern, C., et al. (2025). 'New' challenges for future C2: Commanding soldier-machine partnerships [20]
Idem.

9. Estrategias de implementación de la inteligencia artificial en Fuerzas Armadas

9.1 Impulso de la superioridad tecnológica y colaboración multisectorial

La implementación efectiva de la inteligencia artificial (IA) en las fuerzas armadas requiere un enfoque estratégico que priorice la superioridad tecnológica. Para mantener una posición de autonomía en el ámbito de la defensa nacional, es fundamental acelerar el desarrollo e investigación en IA y aprendizaje automático (ML).

Este impulso no solo implica una inversión significativa en investigación, sino también el establecimiento de alianzas sólidas con el sector académico, la industria y socios en el ámbito nacional. Estas colaboraciones permiten que las fuerzas armadas incorporen de manera continua tecnologías de IA y procesos de capacitación de vanguardia, asegurando procesos sostenibles de desarrollo e incorporación de capacidades.

La integración de conocimientos y recursos provenientes de diferentes sectores facilita la transferencia de tecnología y la adaptación rápida a los avances emergentes, consolidando la posición estratégica de las fuerzas armadas en el entorno de la Defensa.

9.2 Gobernanza ética, legal y social de la IA militar

Junto con el desarrollo tecnológico, la implementación de la IA en el ámbito militar exige la creación de directrices éticas, legales y sociales claras. Definir y hacer cumplir límites que reflejen los valores y principios nacionales es esencial para garantizar el uso responsable de la IA en todos los contextos operativos.

Esta gobernanza no solo previene posibles abusos y riesgos asociados al uso de tecnologías autónomas, sino que también fomenta la cooperación internacional, un aspecto clave en el despliegue exitoso de la IA en escenarios de seguridad global.

La formulación de una estrategia nacional en IA que incluya objetivos, hitos y métricas claras proporciona una hoja de ruta para el desarrollo y despliegue de tecnologías de IA, promoviendo la resiliencia y la interoperabilidad entre las distintas Fuerzas de las fuerzas armadas.

9.3 Resiliencia e interoperabilidad de los sistemas de IA

La resiliencia y la interoperabilidad son pilares fundamentales en la integración de la IA en operaciones militares. La adopción de métodos de entrenamiento adversarial fortalece la confiabilidad verificable de los sistemas de IA y ML, reduciendo sus vulnerabilidades

Este enfoque contribuye a la creación de un marco de IA multidominio, capaz de integrarse de manera fluida en operaciones terrestres, marítimas, aéreas, espaciales y cibernéticas. La interoperabilidad entre dominios permite una colaboración más efectiva y una respuesta coordinada ante amenazas complejas, mientras que la resiliencia asegura la continuidad operativa incluso en entornos hostiles o bajo ataques cibernéticos.

9.4 Desarrollo de talento y capacitación en IA

El éxito de la implementación de la IA en las fuerzas armadas depende en gran medida de la existencia de especialistas capacitados. El desarrollo de programas de educación, formación e

incorporación de especialistas de IA -bajo condiciones flexibles- enfocados en habilidades de IA y ML es un paso crucial.

La creación de una base sólida de conocimientos técnicos entre el personal militar garantiza que las tecnologías de IA puedan ser desarrolladas y gestionadas de manera efectiva en operaciones de Defensa Nacional.

9.5 Integración de la IA en la toma de decisiones y adaptación doctrinal

La incorporación de capacidades de IA en los procesos de toma de decisiones militares mejoró significativamente la conciencia situacional y la capacidad de respuesta simulada en entornos complejos y dinámicos.

El uso de IA para el análisis y procesamiento de datos en tiempo real permitió en entornos de gabinete controlados (fines educativos) tomar decisiones mejor fundamentadas, manteniendo así una ventaja estratégica (Ciclo OODA).

Estos procesos evidenciaron las exigencias esenciales de adaptación de procesos, conceptos y doctrinas para incorporar perspectivas y riesgos asociados a la IA.

9.6 Desafíos éticos y de seguridad en la adopción de inteligencia artificial militar

Uno de los principales desafíos éticos en la adopción de inteligencia artificial (IA) en el ámbito militar radica en la necesidad de alinear los sistemas de IA con los valores democráticos y el Estado de derecho.

La rápida evolución de la tecnología y sus aplicaciones ha generado debates sobre la urgencia de establecer normas y mejores prácticas que garanticen el desarrollo y empleo responsable de la IA. En el contexto, resulta indispensable disponer (MINDEF/EMCFFAA) de principios específicos para guiar el desarrollo y uso de la IA en el ámbito de la Defensa Nacional; con el objeto de asegurar la traducción en acciones operacionales con la formulación de objetivos éticos de alto nivel.

Este desfase se presentará especialmente cuando se avance en el desarrollo de opciones operacionales asistidos por IA de alto riesgo, con implicaciones directas en la preservación de la vida y/o elementos protegidos en el marco del Derecho Internacional[15].

9.7 Prácticas de ingeniería y desempeño del sistema

El desarrollo responsable de sistemas de IA militar requiere la implementación de prácticas de ingeniería que aseguren la confiabilidad y comprensibilidad de los sistemas (seguridad y resiliencia).

Estas prácticas deben abarcar todas las fases del ciclo de vida de la IA, desde la concepción y el diseño temprano, pasando por el desarrollo y las pruebas, hasta el empleo, la monitorización y el mantenimiento (fiabilidad y transparencia).

Si bien las recomendaciones actuales establecen un umbral mínimo para el desarrollo y despliegue responsable de tecnologías de IA, mejores prácticas evolucionarán con el tiempo y resultará

[15] Monzón Baeza, V., Parada, R., Concha Salor, L., & Monzo, C. (2025). AI-driven tactical communications and networking for defense: A survey and emerging trends

necesario establecer instancias de investigación y desarrollo de estándares específicos para el sector militar[16].

9.8 Interacción humano-IA, responsabilidad y gobernanza

La interacción entre humanos y sistemas de IA en contextos militares plantea desafíos adicionales relacionados con la responsabilidad y la gobernanza.

Es fundamental que los sistemas sean comprensibles y que los operadores puedan interpretar y supervisar las decisiones tomadas por la IA, especialmente en situaciones críticas donde la preservación de vidas y elementos protegidos está en juego.

La rendición de cuentas y la gobernanza efectiva requieren mecanismos claros para atribuir responsabilidades en caso de fallos o consecuencias imprevistas derivadas del uso de la IA (8).

10. Impacto en la doctrina y operaciones militares

10.1 Transformación doctrinal y adaptación de procesos

La integración de la inteligencia artificial (IA) en el ámbito militar está impulsando una acelerada transformación en la doctrina, los procesos operativos y el desarrollo tecnológico, así como la adaptación doctrinal.

La actualización de los procesos, conceptos y doctrinas militares para incorporar perspectivas y riesgos asociados a la IA es esencial para facilitar su adopción exitosa.

Esta adaptación doctrinal permite la agilidad y capacidad de respuesta necesarias en un entorno tecnológico en constante evolución, asegurando que las innovaciones en IA se traduzcan en ventajas operativas tangibles.

De este modo, la doctrina militar evoluciona para incorporar la IA como un elemento central en la planificación y ejecución de operaciones, permitiendo una colaboración más estrecha entre dominios terrestres, marítimos, aéreos, espaciales y cibernéticos.

10.2 Impacto en la toma de decisiones y la preparación operativa

La incorporación de capacidades de IA en los procesos de toma de decisiones militares fortalece la conciencia situacional y la capacidad de respuesta en entornos complejos y dinámicos.

El uso de IA para el análisis y procesamiento de datos en tiempo real permite fortalecer el proceso de toma de decisiones; aspecto que se ve reforzado por la integración de simulaciones y juegos de guerra impulsados por IA en los programas de entrenamiento y ejercicios militares, lo que incrementa la preparación de los EM, ejecución de tareas y la eficacia operativa.

[16] Madison, A., McDowell, K., Goecks, V. G., Hansberger, J., Olney, C. M., Ahern, C., et al. (2025). ‘New’ challenges for future C2: Commanding soldier-machine partnerships

11. Perspectivas futuras y tendencias en el Estado Mayor Cognitivo

11.1 Tecnologías de aprendizaje profundo y refuerzo

El análisis de tendencias revela que el aprendizaje profundo (Deep Learning, DL) se está consolidando como la tecnología de inteligencia artificial predominante en aplicaciones militares, especialmente en tareas de análisis de imágenes, vigilancia y sistemas de inteligencia basados en sensores.

Esta prevalencia se debe a la eficacia demostrada de DL en la interpretación de grandes volúmenes de datos visuales y sensoriales, lo que resulta fundamental para la superioridad situacional y la toma de decisiones en tiempo real.

Paralelamente, el aprendizaje por refuerzo (Reinforcement Learning, RL) está emergiendo como una herramienta crucial para la toma de decisiones autónoma y la adaptación estratégica en entornos complejos y dinámicos, como los sistemas de combate automatizados y las operaciones de vehículos aéreos no tripulados (UAVs).

La tendencia apunta a una integración cada vez mayor de RL en sistemas autónomos, permitiendo una mayor capacidad de adaptación y respuesta ante escenarios imprevistos, lo que refuerza la autonomía y la resiliencia operativa del Estado Mayor Cognitivo[17].

11.2 Especialización en aplicaciones de inteligencia artificial militar

Si bien DL y RL dominan el panorama de la inteligencia artificial militar, técnicas como el aprendizaje supervisado (Supervised Learning, SL) y los algoritmos evolutivos mantienen roles especializados; fundamental en áreas como la guerra electrónica (EW), la ciberseguridad y la logística predictiva, donde la clasificación eficiente y la detección de fallos son esenciales para la continuidad operativa y la protección de infraestructuras críticas.

Los algoritmos evolutivos, aunque menos extendidos, son indispensables en sistemas de control de fuego y armas, optimizando la precisión de los objetivos y la predicción de trayectorias balísticas. Sin embargo, la integración de la inteligencia artificial en sistemas de guerra electrónica y control de fuego aún enfrenta desafíos significativos en términos de precisión y resiliencia frente a amenazas sofisticadas[18].

11.3 Interoperabilidad y evolución del Estado Mayor Cognitivo

El futuro del Estado Mayor Cognitivo estará marcado por la necesidad de mejorar la interoperabilidad entre tecnologías militares impulsadas por inteligencia artificial.

La integración eficiente de sistemas heterogéneos, capaces de compartir y procesar información en tiempo real, será clave para maximizar la eficacia operativa y la toma de decisiones colaborativa. Además, la seguridad de los datos y la resiliencia operativa frente a riesgos y amenazas se perfilan

[17] Monzón Baeza, V., Parada, R., Concha Salor, L., & Monzo, C. (2025). AI-driven tactical communications and networking for defense: A survey and emerging trends

[18] Monzón Baeza, V., Parada, R., Concha Salor, L., & Monzo, C. (2025). AI-driven tactical communications and networking for defense: A survey and emerging trends

como prioridades críticas, especialmente ante la creciente sofisticación de las amenazas cibernéticas y electrónicas.

La implementación ética de la inteligencia artificial en entornos militares será un eje central de investigación, buscando equilibrar la automatización y la eficiencia con el respeto a los principios legales y humanitarios[19].

11.4 Integración con el Sistema Educativo Nacional

La magnitud del desafío tecnológico planteado exige una estrategia cooperativa con el Sistema Educativo Nacional (SEN) a partir de un Sistema de Alianzas Estratégicas (SAE) que vincule la Defensa con universidades públicas, organismos científicos y empresas tecnológicas; ello con el objeto de:

Aprovechar la capacidad científica nacional en áreas de IA, ciberseguridad, robótica y análisis de datos.

Evitar duplicación de esfuerzos mediante proyectos interinstitucionales UNDEF-MINDEF-MCT.

Formar capital humano dual, con competencias aplicables tanto al ámbito civil como al militar.

Fortalecer la soberanía tecnológica mediante innovación colaborativa.

Un proceso en el que se identifican actores clave, con la escala y la especificidad necesaria, entre los cuales se encuentran:

Académicos: UBA, UNLP, UTN, UNSAM.

Tecnológicos: INVAP, ARSAT, CONAE, CITEDEF.

Internacionales: CESEDEN, NATO Defence College, BID, UNESCO.

Estas alianzas permiten que la educación militar se inserte en la economía del conocimiento, preservando su especificidad doctrinaria y su identidad nacional.

11.5. Perfil del Oficial de Estado Mayor en la era digital

El nuevo Oficial de Estado Mayor (OEM) se define por competencias cognitivas, tecnológicas y éticas; permitiéndole actuar como gestor del conocimiento estratégico, integrando pensamiento analítico, capacidad predictiva y prudencia ética.

Dimensión	Competencias
Cognitiva	Análisis sistémico, pensamiento crítico, gestión de información compleja.
Tecnológica	Alfabetización digital, modelado de procesos, control de IA.
Ética	Liderazgo responsable, trazabilidad de decisiones, control humano significativo.

Elaboración propia

El OEM ya no es solo planificador: es un líder cognitivo, un decisor asistido por IA que mantiene el sentido doctrinario y humano de la acción militar.

[19] Ídem.

NOTA: Anexo 6 - Competencias del OEM conjunto y conformación del Estado Mayor Cognitivo (EMC)

11.6 Implementación de la Función de Tutoría del OEM-EMC

La tutoría del OEM en un Estado Mayor Cognitivo (EMC) no es un apoyo académico accesorio, sino un dispositivo de aseguramiento de calidad cognitiva del Proceso de Planeamiento Militar Conjunto (PPMC) con el objeto de preservar y elevar el juicio profesional bajo condiciones de incertidumbre, velocidad y saturación informativa, evitando que la fluidez del lenguaje o la aparente precisión tecnológica afecten la calidad del proceso o sustituyan el juicio crítico.

En este marco, la tutoría opera como mecanismo institucional para sostener trazabilidad doctrinaria, disciplina crítica y control humano significativo sobre el producto final pudiéndose implementar bajo:

Modalidad presencial: la tutoría se organiza como ciclo de trabajo de gabinete y revisión por "gates" del PPMC, combinando producción guiada, clínica de validación y contraste adversarial. El tutor doctrinario asegura coherencia con la terminología y estándares del planeamiento; el tutor metodológico ordena evidencia, supuestos y registro; y el tutor cognitivo actúa como Red Team pedagógico para atacar hipótesis, revelar sesgos y forzar alternativas. El criterio de aprobación no es retórico: se basa en evidencia mínima, supuestos refutables, sensibilidad, coordinación intersecciones y firma responsable.

Modalidad híbrida: la tutoría integra presencia humana con plataforma y asistencia de IA, manteniendo una regla central: la IA no tutorea, solo asiste. La plataforma estructura el flujo de trabajo y la auditabilidad (versionado, fuentes por página/sección, supuestos, responsables), mientras que la IA actúa como prechequeo automático que detecta ambigüedades doctrinarias, afirmaciones sin evidencia, falta de alternativas o ausencia de sensibilidad. La intervención humana se concentra en lo indelegable: validación adversarial, fijación de criterios, aceptación de riesgo y decisión pedagógica sobre correcciones y estándares.

En ambos modelos, la tutoría se diseña como una arquitectura de filtros sucesivos: filtro doctrinario (glosario y formato), filtro de evidencia (fuente o supuesto explícito), filtro adversarial (Blue/Red Team) y filtro humano (control final con racionalidad documentada).

Su eficacia se medirá por indicadores verificables: aumento de outputs con trazabilidad, reducción de ambigüedad terminológica, cobertura total de Red Team en productos críticos y consolidación de lecciones aprendidas en el repositorio. Así, la tutoría EMC transformará el aprendizaje en capacidad institucional, y la asistencia tecnológica en superioridad decisional.

11.7. Propuestas de política educativa e innovación curricular

Actualización curricular ESGC-UNDEF 2027-2030: o Incorporar módulos de IA, simulación, ciberestrategia y ética algorítmica (en cooperación externa con centros especializados). o Fortalecer las competencias de investigación aplicada en defensa cognitiva.

Creación de la Red Nacional de Innovación Educativa en Defensa (RENIED): articulación con universidades y centros tecnológicos.

Desarrollo de laboratorios de simulación cognitiva: uso de IA generativa y *dashboards* doctrinarios.

Formación docente continua: programas de capacitación interdisciplinaria para profesores militares y civiles.

Publicación y transferencia del conocimiento: consolidar la Revista Accionar Militar Conjunto como plataforma de pensamiento estratégico y cooperación científica.

12. Conclusión

La ESGC se consolida como centro de gravedad intelectual del Sistema Educativo de la Defensa. Su rol bisagra entre las Fuerzas, la Academia y el Sistema Educativo Nacional le asigna la responsabilidad de liderar la transición hacia un modelo educativo cognitivo, cooperativo e innovador, capaz de traducir experiencia operacional en conocimiento auditado.

El análisis del Estado Mayor Cognitivo (EMC) y de la IA aplicada a la estrategia militar evidencia una transformación en la concepción, organización y operación de las Fuerzas Armadas. En términos prácticos, el EMC constituye una arquitectura socio-técnica viable, basada en roles funcionales, herramientas doctrinarias y una plataforma integradora.

La progresiva simbiosis humano-IA redefine la toma de decisiones al potenciar conciencia situacional, adaptación doctrinaria y eficiencia operativa. Sin embargo, en escenarios híbridos y de zona gris, el riesgo central es la degradación del juicio profesional. Por ello, el EMC debe blindar metacognición, validación y comunicación estratégica.

La integración de principios de gobernanza de IA (transparencia, trazabilidad, explicabilidad, equidad y gobernabilidad) resulta esencial para sostener legitimidad y confiabilidad en contextos militares. A la vez, la implementación enfrenta desafíos éticos, legales y de seguridad que exigen marcos normativos consistentes y verificables, alineados con valores democráticos y el Estado de derecho. La capacitación especializada y la gobernanza ética emergen como factores críticos para la sostenibilidad de estas capacidades.

Este abordaje plurianual del EMC, como arquitectura de gestión y desarrollo del PPMC, contempló cinco componentes: Especialistas (OEM 4.0), Método (PPMC con contrasesgos y validación), Conocimiento (repositorio trazable 2012-2026), Tecnología (perfiles IA por rol, herramientas doctrinarias y plataforma), y Gobernanza (“SOP” y control humano significativo).

En paralelo, se establecieron reglas mínimas: supuestos explícitos y refutables; glosario doctrinario obligatorio (RC 20-01)[26]; modo adversarial (Blue/Red Team) para CDG (CoG)[27], riesgos y comparación de MA; evidencia mínima y nivel de confianza por producto; control humano significativo[20] (firma responsable y racionalidad de decisión); y lecciones aprendidas incorporadas al repositorio.

RC 20-01. Se adopta como referencia doctrinaria para el planeamiento conjunto en el nivel operacional. En este trabajo, “RC 20-01” se utiliza como marco de terminología, criterios y productos del proceso de planeamiento, incluyendo definiciones y estándares aplicables a supuestos, comparación de cursos de acción, evaluación de riesgos y trazabilidad de decisiones.

CDG/CoG. A efectos de consistencia terminológica, se emplea CDG como Centro de Gravedad como denominación única en documentos previos o en bibliografía; Cuando se utilice CoG (Center of

[20] **Control humano significativo.** En el marco EMC-PPMC, se entiende como el conjunto de requisitos que aseguran que el juicio final permanezca en autoridad humana identificable: (a) puntos de decisión indelegables, (b) trazabilidad de supuestos y evidencia, (c) validación adversarial para productos críticos, y (d) firma responsable con racionalidad de decisión documentada.

Gravity) se considerará sinónimo operativo de CDG, salvo indicación doctrinaria específica que exija diferenciación.

Las perspectivas futuras apuntan a consolidar aprendizaje profundo y refuerzo, especializar aplicaciones militares y fortalecer interoperabilidad y seguridad. La adaptación doctrinaria y la integración multisectorial serán determinantes para maximizar el potencial del EMC en escenarios complejos y dinámicos.

En síntesis, la educación militar argentina debe sostener su autonomía doctrinaria dentro de una red nacional de conocimiento compartido. La ESGC, en su doble condición de escuela y laboratorio, es el instrumento idóneo para asegurar que la formación del Oficial de Estado Mayor responda a los desafíos de la era digital, manteniendo el equilibrio entre tradición, ciencia y futuro.

El proyecto Seguridad Estratégica del Estado 4.0 introdujo una nueva lógica: comprender la defensa también en su dimensión informacional y tecnológica. Hoy, esa lógica se traduce en una pedagogía de soberanía cognitiva: enseñar a pensar, decidir y liderar donde la información es poder.

Com. (R) Mág Pablo Andrés Farias

Director de Proyecto

ANEXOS:

ANEXO 1 - Repositorio Trazable FMC/ESGC 2012-2026 (vinculación CPDN/PEM)

ANEXO 2 - Repositorio Digital FMC/ESGC 2012-2026 (Tabla Operativa)

ANEXO 3 - Estado del Arte y Vacancia Estructural (Inteligencia Artificial (IA) y Tecnologías Disruptivas (TD) en el Nivel Operacional)

ANEXO 4 - Mapa de Conocimiento 2012-2026 + sincronía CPDN/PEM + repositorio trazable

ANEXO 5 - IA como asistente cognitivo en PPMC, con trazabilidad y control humano significativo

ANEXO 6 - Competencias del OEM conjunto y conformación del Estado Mayor Cognitivo (EMC)

ANEXO 7 - Fundamentación Empírica del Estado Mayor Cognitivo (EMC) en Escenarios 4.0

ANEXO 8 - Formulario Operativo EMC (Control de avance del proceso de investigación aplicada - FMC/ESGC)

Bibliografía

Ágreda, Á. G. (2019). *Usos militares de la inteligencia artificial, la automatización y la robótica (IAA&R)* (Documento de trabajo 04/2019). Centro Superior de Estudios de la Defensa Nacional (CESEDEN), Ministerio de Defensa (España).

Aguilar, O. A. (2023). *La inteligencia artificial como herramienta del proceso de comando y control del comandante del teatro de operaciones* (Trabajo Final Integrador, Escuela Superior de Guerra Conjunta).

Anneken, M., Burkart, N., Jeschke, F., Kuwertz-Wolf, A., & Mueller, A. (2025). *Ethical considerations for the military use of artificial intelligence in visual reconnaissance* (arXiv:2502.03376). arXiv. https://arxiv.org/abs/2502.03376

Banco Interamericano de Desarrollo. (2023). *Educación y transformación digital en América Latina*. BID.

Brundage, M., Avin, S., Clark, J., Toner, H., Eckersley, P., Garfinkel, B., Dafoe, A., Scharre, P., Zeitzoff, T., Filar, B., Anderson, H., Roff, H., Allen, G. C., Steinhardt, J., Flynn, C., Ó hÉigeartaigh, S., Beard, S. J., Belfield, H., Farquhar, S., & Amodei, D. (2018). *The malicious use of artificial intelligence: Forecasting, prevention, and mitigation* (arXiv:1802.07228). arXiv. https://arxiv.org/abs/1802.07228

Centro Superior de Estudios de la Defensa Nacional. (2018). *La inteligencia artificial aplicada a la defensa*. CESEDEN, Ministerio de Defensa (España).

Centro Superior de Estudios de la Defensa Nacional. (2019). *Usos militares de la inteligencia artificial, la automatización y la robótica (IAA&R)*. CESEDEN, Ministerio de Defensa (España).

CESEDEN. (2022). *Inteligencia artificial y defensa: Perspectivas y desafíos*. Ministerio de Defensa (España).

Delmau, P. (2020). *Empleo de inteligencia artificial para el desarrollo de las funciones operacionales* (Trabajo académico, Escuela de Guerra Naval).

Escuela Superior de Guerra Conjunta de las Fuerzas Armadas. (2024). *Tecnologías disruptivas en el ámbito operacional* (Proyecto de investigación). FMC-UNDEF.

Estado Mayor Conjunto de las Fuerzas Armadas. (2019). *Glosario de términos de empleo militar para la acción militar conjunta (PC 00-02)*. Ministerio de Defensa (Argentina).

Estado Mayor Conjunto de las Fuerzas Armadas. (2019). *Planeamiento para la acción militar conjunta (RC 20-01)*. Ministerio de Defensa (Argentina).

Estado Mayor Conjunto de las Fuerzas Armadas. (2023). *Plan de Capacidades Militares (PLANCAMIL 2023)* (Resolución 1365/23).

Farías, P. A. (2024). *Seguridad Estratégica del Estado 4.0: El impacto de intangibles tecnológicos disruptivos en la Defensa* (Proyecto de investigación FMC–ESGC).

Farías, P., Martínez, V., Micha, L., & Rodríguez, R. (2022). Generando conceptos que faciliten el debate y orientación de estrategias. En L. Micha (Ed.), *Inteligencia artificial y sistemas de armas autónomas* (pp. 61-112). Facultad de Ciencias Sociales, Universidad de Buenos Aires.

Feldman, P., Dant, A., & Dreany, H. (2024). *War elephants: Rethinking combat AI and human oversight* (arXiv:2404.19573). arXiv. https://arxiv.org/abs/2404.19573

Horvitz, E., Young, J., Elluru, R. G., & Howell, C. (2021). *Key considerations for the responsible development and fielding of artificial intelligence* (arXiv:2108.12289). arXiv. https://arxiv.org/abs/2108.12289

Kurakin, A., Goodfellow, I. J., & Bengio, S. (2016). *Adversarial examples in the physical world* (arXiv:1607.02533). arXiv. https://arxiv.org/abs/1607.02533

Lewis, L. (2017). *Perspectivas para la tercera compensación: Abordar los desafíos de la autonomía y la inteligencia artificial en las operaciones militares*. Center for Naval Analyses (CNA).

Lloret, J. C. (2022). *Retos de la inteligencia militar aplicada a la defensa*. Dirección General de Armamento y Material, Ministerio de Defensa (España).

Ilyas, A., Santurkar, S., Tsipras, D., Engstrom, L., Tran, B., & Madry, A. (2019). *Adversarial examples are not bugs, they are features* (arXiv:1905.02175). arXiv. https://arxiv.org/abs/1905.02

Madison, A., McDowell, K., Goecks, V. G., Hansberger, J., Olney, C. M., Ahern, C., et al. (2025). *"New" challenges for future C2: Commanding soldier-machine partnerships* (arXiv:2503.08844). arXiv. https://arxiv.org/abs/2503.08844

Madotto, A., & Attardi, G. (2017). *Question dependent recurrent entity network for question answering* (arXiv:1707.07922). arXiv. https://arxiv.org/abs/1707.07922

Mikhailov, D. I. (2023). *Optimizing national security strategies through LLM-driven artificial intelligence integration* (arXiv:2305.13927). arXiv. https://arxiv.org/abs/2305.13927

Ministerio de Defensa. (2021). *Directiva de Política de Defensa Nacional*. Presidencia de la Nación (Argentina).

Monzón Baeza, V., Parada, R., Concha Salor, L., & Monzo, C. (2025). *AI-driven tactical communications and networking for defense: A survey and emerging trends* (arXiv:2504.05071). arXiv. https://arxiv.org/abs/2504.05071

Moressi, A. (2023). El impacto de la inteligencia artificial en la defensa. *Revista Pucará Defensa*.

NATO. (2023). *Artificial intelligence strategy for defence and security*. Allied Command Transformation.

Olier, E., & Corchado, J. M. (2022). *Inteligencia artificial: Aplicaciones a la defensa*. Instituto Español de Estudios Estratégicos.

Palacio, A. F. (2021). *La inteligencia artificial en el contexto militar internacional y sus posibles aplicaciones en el Ejército Nacional de Colombia* (Ensayo). Escuela Superior de Guerra del Ejército (Colombia).

Ram, A., & Nagappan, M. (2018). *Supervised sentiment classification with CNNs for diverse SE datasets* (arXiv:1812.09653). arXiv. https://arxiv.org/abs/1812.09653

Serrano, M. F. (2019). El liderazgo militar en los tiempos de la inteligencia artificial. *Visión Conjunta* (ESGC).

Tudela, J. M. (2019). La inteligencia artificial y la fricción de la guerra. En Instituto Español de Estudios Estratégicos (Ed.), *Documentos de Seguridad y Defensa, 79: La inteligencia artificial aplicada a defensa* (pp. 99-124). Ministerio de Defensa (España).

UNDEF. (2023). *Manual de metodología de investigación en ciencias militares*. Editorial UNDEF.

UNESCO. (2022). *Reimaginar juntos nuestros futuros: Un nuevo contrato social para la educación*. UNESCO.

ANEXO 1 - Repositorio Trazable FMC/ESGC 2012-2026 (vinculación CPDN/PEM)

Propósito. Institucionalizar un repositorio digital trazable y auditable de productos de conocimiento producidos o adoptados por la FMC/ESGC (docencia, investigación, extensión, doctrina, procedimientos, ejercitación y herramientas), con el objeto de evidenciar contribuciones, identificar vacancias y sostener la transición hacia un Estado Mayor Cognitivo (EMC) en escenarios 4.0.

1.1 Unidad de análisis

Cada registro corresponde a un Producto de Conocimiento (PK) FMC/ESGC: documento, informe, TFI/ensayo, artículo, clase-contenido, guía metodológica, protocolo, resultado de ejercicio, publicación o evento académico con evidencia documental accesible.

1.2 Ficha mínima de catalogación (campos obligatorios)

ID-Repo: FMC-ESGC-AAAA-###

Año (2012–2026)

Tipo: Docencia | Investigación | Extensión | Doctrina/Procedimiento | Ejercitación | Herramienta

4. Producto (título formal)

Autoría y rol: autor/es, tutor, cátedra/área, dependencia FMC/ESGC

Oferta/espacio: Nivel 1 | curso | seminario | proyecto | ejercicio

7. Resumen analítico (150–250 palabras)

Palabras clave normalizadas: IA, PPMC, EMC, zona gris, multidominio, CDG, ética, trazabilidad, etc.

Vínculo CPDN/PEM: hito/demanda asociada (directo | indirecto | contextual) + justificación (≤120 palabras)

Producto PPMC asociado (si aplica): paso/artefacto (MA, CDG, riesgos, etc.)

11. Evidencia primaria: archivo/link + página/sección exacta

Nivel de evidencia (0–3):

0 no verificable.

1 verificable parcial.

2 verificable con soporte documental.

3 verificable + replicable (método/datos/protocolo).

Nivel de validación: borrador | evaluado | validado | adoptado.

Brecha institucional que revela: doctrinaria | curricular | cultural | tecnológica | metodológica.

Recomendación EMC (1 párrafo): acción concreta derivada del hallazgo

Metadatos de auditoría: fecha de carga, responsable, versión.

1.3 Reglas de calidad y auditabilidad

Regla 1. Evidencia obligatoria: ningún PC ingresa con evidencia 0.

Regla 2. Trazabilidad explícita: cada PC debe responder “qué demanda/hito CPDN/PEM toca y cómo”.

Regla 3. No extrapolación: si el vínculo es indirecto, se declara como tal.

Regla 4. Versionado: toda modificación registra fecha, autor, motivo y cambio.

1.4 Salida estándar para el capítulo “Resultados”

Cada semestre se produce una matriz: Categoría, Subcategoría, Evidencia, Hallazgo, Brecha y Recomendación EMC, con consolidación anual (2012– 2016 / 2017–2021 / 2022–2026).

Com. (R) Mág Pablo Andrés Farias

Director de Proyecto

ANEXO 2 - Repositorio Digital FMC/ESGC 2012-2026 (Tabla Operativa)

Propósito del repositorio: sostener un “catálogo trazable” de productos (docencia-investigación-extensión) que permita sincronía con hitos CPDN/PEM y cierre de brechas institucionales (calidad, pertinencia, actualización tecnológica, etc.).

Convención de estado

Núcleo: entra sí o sí al repositorio (base del EMC).

Soporte: complementa y aporta evidencia secundaria.

Pendiente: requerido por el diseño, pero aún no cargado.

ID Repo	Período	Producto (título)	Tipo	Unidad	Estado	Aporte al EMC (1 línea)	Evidencia / trazabilidad
R-00	2012 2022	Mapa de Conocimiento CPDN/PEM 2012-2026 (catálogo de productos + vínculo con hitos)	Dataset + informe	FMC ESGC	Pendiente (obligatorio)	Permite medir brechas y sincronía academia–planeamiento	El proyecto exige “establecer exigencias CPDN 2012/2026” y “Mapa de Generación de Conocimiento” y “sincronía” con hitos CPDN.
R-01	2024 2025	Seguridad Estratégica del Estado 4.0 (formulario/proyecto, FMC-ESGC)	Proyecto (marco)	FMC ESGC	Núcleo	Define objetivo plurianual, vacancia estructural y lógica de investigación aplicada	Declara enfoque de investigación aplicada, vacancia estructural “Tecnologías Disruptivas-IAEscenarios 4.0”, y finalidad de transformación académica.
R-02	2024	Tecnologías disruptivas en el ámbito operacional (insumo metodológico del proyecto)	Documento técnico/metodológico	FMC ESGC	Núcleo	Fija metodología (revisión documental, entrevistas, checklist, análisis cualitativo) y variables	Establece “Mapa del Conocimiento” + metodología cualitativa y variables para el programa plurianual.
R-03	2025	Informe IA - PPCM (RC 20-01) (lecciones aprendidas y correcciones)	Informe aplicado	ESGC	Núcleo	Prueba operativa de IA como asistente cognitivo con control humano	Estandarización, delimitación de roles C-1/C-9, coordinación entre perfiles, trazabilidad supuestos-evidencia.

ID Repo	Período	Producto (título)	Tipo	Unidad	Estado	Aporte al EMC (1 línea)	Evidencia / trazabilidad
R-04	2026	La ESGC como bisagra… hacia un Estado Mayor Cognitivo	Ensayo doctrinario	FMC ESGC	Núcleo	Traduce EMC a política educativa: currícula, laboratorios, red de innovación, revista	Define OEM como “líder cognitivo”, propone actualización curricular y “control humano significativo”.
R-05	2026	Zona Gris y Estados Mayores Cognitivos	Ensayo/	ESGC	Soporte	Enmarca EMC en zona gris, atrofia cognitiva, superioridad decisional y ethos	Plantea hipótesis de transición a EMC para sostener vigencia ante desafíos contemporáneos.
R-06	2026	Habilidades y Competencias del OEM	Ensayo/	ESGC	Soporte	Aporta matriz competencial: multidominio, IA, ciber, negociación, incertidumbre	Explicita competencias para operar en dominios múltiples y usar IA sin perder control crítico.
R-07	2026	Integración de IA en el PPMC (RC 20-01) (trabajo “de investigación”)	Documento aplicado	ESGC	Soporte	Identifica límites técnicos (latencia on-premise), glosarios, riesgos por área C-1/C-4	Define IA como asistente cognitivo, advierte ambigüedad terminológica y necesidad de glosarios doctrinarios.
R-08	2026	Comandos operativos - IA (compilación)	Compendio bibliográfico	no ESGC	Soporte	Base para formación de fuerza “AI- ready” y workforce por capas	Compila marcos de fuerza y educación (fuentes JFQ/DoD/etc.).
R-09	(histórico)	SAAL	Doc. Histórico doctrinario	no ESGC	Soporte (con- texto)	Útil como antecedente de ROE/estándares y trazabilidad, pero fuera de 2012–2026	Propone estándares éticos, ROE y trazabilidad para sistemas autónomos (útil como marco).

Elaboración propia

NOTA: Salida operativa recomendada: este repositorio dispondrá de un catálogo mínimo por producto con: *año, tipo, eje (docencia/investigación/extensión), vínculo CPDN/PEM, evidencia (URL o PDF), hallazgos, brecha, recomendación EMC*.

Com. (R) Mág Pablo Andrés Farias

Director de Proyecto

ANEXO 3 - Estado del Arte y Vacancia Estructural (Inteligencia Artificial (IA) y Tecnologías Disruptivas (TD) en el Nivel Operacional)

Categoría	Subcategorías	Evidencia directa	Hallazgo	Brecha institucional	Acción EMC (propuesta)
Vacancia estructural	IA/TD y Escenarios 4.0	El proyecto define vacancia estructural “Impacto de TD-IA- Escenarios 4.0” en FMC/ESGC.	El problema está bien definido en términos de vacancia y necesidad de mejora de calidad educativa	Falta consolidación sistemática en productos curriculares y métricas de salida	Línea EMC como eje curricular transversal (IA + ética + doctrinario + validación)
Doctrina y planeamiento	IA en toma de decisiones / C2	Primer informe: IA y TD impactan toma de decisiones, inteligencia, maniobra, logística.	El enfoque cubre los 4 núcleos operacionales críticos	Riesgo de quedar en “enunciados” si no se traduce a productos y estándares	Convertir núcleos en competencias observables y rúbricas EMC (evaluación por desempeño)
Riesgo y ética	Control humano y ROE	Se explicita riesgo ético-legal y necesidad de ROE ante delegación algorítmica.	Se reconoce explícitamente “control humano” como condición	No hay SOP institucionalizado dentro del PPMC	SOP EMC para PPMC: checklist + prompts + trazabilidad

Elaboración propia

Com. (R) Mág Pablo Andrés Farias

Director de Proyecto

ANEXO 4 - Mapa de Conocimiento 2012-2026 + sincronía CPDN/PEM + repositorio trazable

Categoría	Subcategorías	Evidencia directa	Hallazgo	Brecha institucional	Acción EMC (propuesta)
Mapa de conocimiento	Repositorios + catálogo de productos	Se exige “Mapa de generación de conocimiento” y relevamiento de repositorios EMCFFAA/EEMMGG.	El diseño metodológico está explícito (qué se debe mapear)	No está ejecutado en el material cargado (no hay dataset 2012- 2026)	Construir “Repositorio 2012-2026” como dataset auditado (campos fijos + evidencias)
Sincronía con CPDN	Hitos CPDN/PEM vs productos académicos	Se exige “sincronía de hitos/procesos relevantes CPDN con academia”.	La tesis “bisagra” tiene base estructural verificable	Falta matriz de correspondencia (hito, producto, brecha y acción)	Matriz CPDN/PEM: hito, exigencia de conocimiento, producto ESGC, cobertura, gap, recomendación
Calidad y acreditación	Congruencia con estándares nacionales	Se advierte que toda mejora debe guardar congruencia con estándares de acreditación nacional.	Correcto enfoque de gobernanza	Falta instrumento de aseguramiento de calidad (QA) del repositorio	Comité EMC: control de calidad documental, versionado, control de citas, auditoría anual

Elaboración propia

Com. (R) Mág. Pablo Andrés Farias

ANEXO 5 - IA como asistente cognitivo en PPMC, con trazabilidad y control humano significativo

Categoría	Subcategorías	Evidencia directa	Hallazgo	Brecha institucional	Acción EMC (propuesta)
Gobernanza IA-PPMC	roles	Informe IA-PPMC: se corrigen alucinaciones con roles/parámetros inamovibles; se exige coordinación necesaria.	Hay prueba aplicada con correcciones concretas	Falta institucionalización como SOP EMC (no solo “lección aprendida”)	SOP EMC PPMC: plantilla CONFIG + glosario doctrinario + matriz de validación
Interoperabilidad del EM	Coordinación entre perfiles C- 1…C-9	Se detecta falta de coordinación y se corrige exigiendo “coordinaciones necesarias”.	IA mejora cuando la organización obliga coordinación explícita	Brecha cultural: tendencia a trabajar “en silos”	“Célula EMC”: integrador de trazabilidad (quién coordina con quién, qué producto, qué hito)
Límites técnicos	Latencia “on-premise”, hardware	Se reporta descarte inicial de LLM locales por latencia y hardware insuficiente.	Realismo técnico (evita soluciones fantasiosas)	Falta arquitectura tecnológica mínima para sostener ritmo PPMC	Requisitos mínimos de infraestructura EMC + política de uso (datos, seguridad, auditoría)

Elaboración propia

Com. (R) Mág. Pablo Andrés Farias

ANEXO 6 - Competencias del OEM conjunto y conformación del Estado Mayor Cognitivo (EMC)

Categoría	Subcategorías	Evidencia directa	Hallazgo	Brecha institucional	Acción EMC (propuesta)
Competencias OEM	Multidominio, IA, dominio informacional	Se explicita exigencia multidominio y articulación conjunta; IA como apoyo sin perder control crítico.	El perfil competencial está alineado con operaciones actuales	Falta evaluación por desempeño (no solo contenido)	Rúbricas EMC por competencia: integración, juicio, coordinación, validación, ética
Ethos y superioridad decisional	Zona gris, atrofia cognitiva, EMC	Ensayo Zona Gris: superioridad decisional, EMC, hipótesis de transformación formativa.	Se aporta marco conceptual fuerte (zona gris - EMC)	Falta traducir ethos a reglas de trabajo (hábitos + disciplina cognitiva)	“Disciplina EMC”: modo adversarial, red teaming, control de sesgos, bitácora de decisiones
Política educativa	Currícula, laboratorios, red de innovación, publicación	Bisagra propone actualización curricular y laboratorios; OEM como “líder cognitivo”.	Ya hay un paquete de política educativa listo	Falta plan de implementación por fases	Hoja de Ruta 2026-2030: módulos IA, simulación, ética algorítmica, publicación y repositorio

Elaboración propia

Com. (R) Mág Pablo Andrés Farias

Director de Proyecto

ANEXO 7 - Fundamentación Empírica del Estado Mayor Cognitivo (EMC) en Escenarios 4.0

Función del Anexo: aportar marco conceptual y argumental para la propuesta EMC-PPMC y para la reingeniería curricular FMC/ESGC.

Vinculación con el cuerpo principal: insumo de contextualización y justificación para los Resultados y Discusión (Objetivos Particulares 1, 2, 3 y 4). - Ejes 9.1, 9.4, 9.6 y 9.8 del Proyecto de Investigación.

Unidad y alcance de Campo: solo FMC/ESGC Nivel 1 (Cohorte 2024, 2025 y 2026)

Nota de trazabilidad: toda cifra o comparación cuantitativa se marca como estimación salvo que exista referencia documental específica en el cuerpo principal o en el repositorio trazable (PK-ID).

LA ESGC COMO EJE DE AUTONOMIA COGNITIVA OPERACIONAL EN ESCENARIOS DE DEFENSA 4.0

Un Cambio de Paradigma en la Seguridad Estratégica

La Defensa 4.0[21] debe entenderse como una transformación estructural del poder militar: el dominio físico converge con el digital y el diferencial estratégico se desplaza hacia intangibles tecnológicos. El núcleo operativo es la decisión: la ventaja competitiva no reside solo en medios, sino en la capacidad de procesar información, construir sentido, sostener legitimidad y decidir bajo incertidumbre.

La transición hacia la "Defensa 4.0", en el marco de la "Seguridad Estratégica del Estado 4.0", no es solo una actualización técnica, sino una transformación estructural de la base material del poder nacional.

En este marco, la ESGC se consolida como punto de inflexión estructurante porque puede traducir esa transformación en capacidades educativas, doctrinarias y organizacionales: formar Estado Mayor para operar con tecnologías disruptivas sin perder soberanía del juicio.

Para la Argentina, esta evolución encuentra un punto de inflexión en la reflexión "Malvinas 40 años después", actuando como puente entre el capital histórico-operacional y la necesidad de una conciencia colectiva ante los desafíos del siglo XXI.

En este contexto, el Oficial de Estado Mayor (OEM 4.0) debe evolucionar desde el planificador clásico hacia un líder cognitivo capaz de sostener superioridad decisional y coherencia doctrinaria bajo presión de tiempo, saturación informativa y riesgo de sesgos.

"Más allá de las ventajas de los avances tecnológicos, la guerra no ha cambiado en su naturaleza; el factor humano (su formación y moral) resulta vital y determinante de la conducción militar de la guerra." - Fuente: Proyecto de Investigación FMC-ESGC.

En ese sentido, se ponen en evidencia las funciones cognitivas indelegables a proteger:

Definir el problema (encuadre correcto).

Fijar criterios (qué significa “éxito”, aceptabilidad, riesgo).

---

[21] **Escenario 4.0**: convergencia multidominio + aceleración tecnológica + disputa informacional sostenida; sin perder de vista la velocidad de los cambios.

Aceptar riesgo y responsabilidad (decisión y firma).

Juicio político-operacional (adecuación fines-medios-modos).

Conducción y coherencia narrativa (unidad de concepción).

La IA puede apoyar, pero no debe fijar criterios ni sustituir la aceptación de riesgo.

Los tres motores que impulsan este cambio de paradigma son:

Tecnologías Disruptivas: La maduración exponencial de la IA, el aprendizaje automático y la computación en la nube, con una reducción drástica en los costos de inferencia y una convergencia de capacidades entre modelos abiertos y cerrados.

Escenarios Híbridos: Conflictos en la "zona gris" que exigen respuestas asimétricas y una vigilancia estratégica integral bajo la lógica de "Seguridad Estratégica del Estado".

Explosión de los "Intangibles Tecnológicos": La puesta en valor de los datos, la información y el conocimiento como recursos soberanos fundamentales para la disuasión y la defensa.

Este cambio estructural en el carácter/características del conflicto demanda una evolución imperativa hacia un OEM 4.0 como actor de este proceso.

Liderazgo Transformacional y Adaptativo

El liderazgo en la era de la Industria 4.0 requiere que el OEM sea un gestor de la transformación digital, capaz de navegar el ejercicio del mando potenciado por procesos algorítmicos. Según los estudios de la Escuela Superior de Guerra Conjunta (ESGC), el mando tradicional debe ser reemplazado por un enfoque transformacional que promueva el pensamiento inventivo y la agilidad resiliente.

Este nuevo perfil no es puramente técnico; la implementación de la IA demanda equipos interdisciplinarios que incluyan lingüistas, filósofos y antropólogos para asegurar una integración tecnológica con sentido humano.

Evolución de Modelos de Liderazgo (3.0 vs. 4.0)

Dimensión	**Liderazgo Tradicional (3.0)**	**Liderazgo Transformacional (4.0)**
Comunicación	Vertical y centrada en la orden directa.	Empatía, gestión de relaciones y generación de redes de conocimiento.
Visión	Ejecución de planes estáticos y reactivos.	Prospectiva, pensamiento inventivo y anticipación estratégica.
Gestión del Cambio	Resistencia o adaptación lenta ante la innovación	Disruptiva, centrada en la Resiliencia y la Preparación Cognitiva.
Interdisciplinariedad	Especialización técnica militar estanca.	Convergencia con humanidades y ciencias de datos para mitigar sesgos.

Elaboración propia

Este liderazgo Transformacional se vuelve ineficaz sin el dominio de las herramientas tecnológicas que definen la superioridad y la soberanía en el campo de batalla moderno.

El Imperativo Estratégico de la Defensa 4.0

La Escuela Superior de Guerra Conjunta (ESGC) se posiciona como el epicentro de un proceso integral de transformación cognitiva operacional, y la definitiva ruptura con la inercia de concepciones residuales “analógicas”, un proceso en el que las estrategias de supervivencia encierran el embrión vicioso que propicia en forma irremediable una desarticulación sistémica difícil de revertir -síndrome de la rana-.

En un entorno de amenazas híbridas, la capacidad de procesar lo intangible determina y/o contribuye a la eficacia de lo cinético; en ese escenario la ESGC constituye una articuladora de la maniobra de anticipación cognitiva, orientada a garantizar que el pensamiento militar (creatividad / juicio crítico) no sea cooptado por la velocidad algorítmica o aquellos actores que la utilicen (ciclo de reacción).

La evolución de las tecnologías disruptivas -especialmente la Inteligencia Artificial (IA) y el aprendizaje automático- ha desencadenado un desbalance exponencial en las relaciones de poder global. Los análisis de la Seguridad Estratégica 4.0 constituye un catalizador para apreciar las nuevas carreras armamentísticas y de proliferación que alteran de manera significativa la seguridad internacional.

Ante este escenario, el realismo estratégico impone una maniobra de anticipación político-estratégica: el desarrollo de capacidades nacionales que permitan mitigar los riesgos de la brecha operativa y explotar las ventajas de la digitalización.

En ese sentido, los intangibles tecnológicos constituyen elementos activos críticos del poder nacional moderno: el conocimiento, la información, los algoritmos y los datos. La “Soberanía Cognitiva” se convierte en un objetivo vital: la capacidad autónoma de generar, proteger y utilizar estos activos para decidir y actuar sin dependencias externas degradantes.

En el marco de este impacto estratégico, la educación militar superior se configura como una "genuina estrategia de anticipación" frente a los riesgos de obsolescencia cognitiva y desafíos de un proceso estructural de adaptación.

Ello no constituye un fin pedagógico tradicional, sino de un reaseguro de soberanía; un Instrumento Militar que domina la dimensión informacional, su capacidad de disuasión y reacción, esta visión exige una arquitectura institucional donde la ESGC funcione como el nodo central del ecosistema de educación militar -operacional y estratégica- de la defensa.

Integración de la IA en el Proceso de Planeamiento Militar Conjunto (PPMC)

La automatización de los procedimientos del PPMC (Nivel Operacional, RC 20-01) define a la IA como un asistente cognitivo. Su función es mitigar la saturación de información, actuando como un multiplicador que potencia, pero jamás sustituye, el juicio humano y la responsabilidad del Comandante.

Desde un abordaje de “realismo Tecnológico” y “Lecciones Aprendidas” el tratamiento en el ámbito de la ESGC 2024-2025-2026 en el marco de actividades previstas en el proceso de investigación / proceso de capacitación docente, evidenció que las pruebas iniciales con modelos de lenguaje de gran escala (LLM) en entornos locales (*On-Premise*) presentaron importantes restricciones (y en algunos casos descartadas) debido a la alta latencia y la insuficiencia de hardware no dedicado.

La eficiencia del sistema depende de una infraestructura computacional suficiente y verificable que sostenga el ritmo del PPMC. Asimismo, se debe combatir la Ambigüedad Terminológica (lenguaje profesional operacional): la IA tiende a usar definiciones de la RAE (ej. para el término "Supuesto"), mientras que el planeamiento exige la definición técnica de la RC 20-01 ("hipótesis sobre situación

actual o futura que se da por verdadera ante la ausencia de hechos"). El desarrollo de Glosarios de Dominio (tokenización asociada) es una condición necesaria para evitar alucinaciones doctrinarias.

Nota: La ambigüedad terminológica es un riesgo operativo cuando se emplean modelos de lenguaje: términos como “supuesto”, “CDG”, “aceptabilidad”, “adecuación” o “factibilidad”, entre otros, tienen significados doctrinarios específicos en el PPMC y no deben quedar en acepción común; en este aspecto se aplicó la siguiente Regla EMC: glosario doctrinario obligatorio, definiciones técnicas como “verdad operativa”, versionado del glosario (quién cambió qué y cuándo) y reorientación explícita de prompts al glosario).

El valor militar de la IA y el ML se expresa cuando reducen fricción en tareas repetitivas y permiten anticipación analítica (no reemplazando el juicio profesional). En un EM operativo, la IA aporta principalmente en:

Inteligencia: detección/clasificación de patrones en volúmenes masivos de datos.

C2 y planeamiento: estructuración de alternativas, análisis comparativo, sensibilidad de supuestos.

Logística: optimización, predicción de consumos y vulnerabilidades.

Dominio informacional/cognitivo: detección de narrativas, anomalías, tendencias y señales tempranas.

Advertencia: La fluidez del lenguaje no equivale a validez. Por eso se impone una disciplina particular en el EMC: glosario + evidencia + validación adversarial.

Ello contribuye al Modelado de “Funciones” de Estado Mayor que conllevan a la automatización y/o asistencia a proceso de decisión, conforme a los siguientes ejemplos:

Área Funcional	**Contribuciones de la IA**	**Limitaciones y Riesgos (Materia de Supervisión)**
Personal (C-1)	Estimación de bajas (MMATT) y rotaciones.	Dificultad para modelar intangibles como moral y liderazgo.
Inteligencia (C-2)	Mapeo PMESII-FT; análisis de patrones.	Confusión entre objetivos tácticos y Centros de Gravedad (CDG).
Operaciones (C-3)	Generación exploratoria de Modos de Acción (MA).	Riesgo de homogeneización y falta de creatividad operativa.
Logística (C-4)	Cálculo de puntos culminantes y flujos.	Tendencia a subestimar restricciones de tiempo y espacio.

Elaboración propia

En el desarrollo de actividades de gabinete, y con el objeto de evitar la cooptación por outputs generalistas, el EMC desarrolló su actividad por roles funcionales del EM (C-1…C-9 y conducción). Esto constituyó una condición de calidad: cada rol tiene entradas/salidas, límites de competencia, definición de productos esperados y coordinación obligatoria.

En relación a productos críticos (CDG, riesgos, comparación MA, recomendación), se aplicó la siguiente Regla de coordinación: no se elevan productos sin coordinación mínima interceldas (ej. C-2/C-3/C-4), registro de supuestos/evidencia y validación adversarial.

En relación a los Pasos del PPMC, la contribución se evidenció -en este proceso preliminar. conforme al siguiente detalle:

Paso 1 y 2 (Inicio y Misión): La IA facilita el mapeo de factores políticos, militares, económicos, sociales, informativos y de infraestructura (PMESIIFT). No obstante, la jerarquización de los CDG (CC, RC, VC) requiere intervención humana experta para evitar la dispersión analítica.

Paso 3 y 5 (MA y Comparación): Permite la creación asistida de matrices de Aptitud, Factibilidad y Aceptabilidad (AFA).

NOTA: Se presenta una vacancia en la Bases de Datos en relación a bibliografía conjunta consolidada para el cálculo de degradación de capacidades y estimación de bajas a nivel operacional, situación que amerita un proceso de investigación y adaptación de doctrina internacional para nutrir las metodologías disponibles el marco del PPMC.

Por otro lado; en oportunidades se establecieron “Criterios de Aceptación” EMCPPMC, para elevar al decisor; por ejemplo, un producto se considera aceptable si cumple:

Alternativas explícitas: mínimo 2 hipótesis/COA comparables.

Supuestos críticos declarados: con refutadores observables.

Evidencia mínima: fuente/página o “sin evidencia disponible” explícito.

Sensibilidad: 3 supuestos que puedan invertir calificación o decisión.

Validación adversarial: registro de contrastación y correcciones.

Control humano significativo: decisión y firma humana con fundamento.

Nota: Si falla cualquiera de estos puntos, el producto vuelve a la fase de revisión.

En este proceso de experimentación, el desarrollo de actividades de celda paralela Transversal (núcleo básico de un "Estado Mayor Cognitivo"), permitió constatar -en el desarrollo selectivo de tareas- una reducción general del 40% al 60% -estimado conforme seguimiento de desarrollo actividades [22] - en el tiempo de preparación de comparaciones y análisis (acelerar análisis estructurado, estandarizar salidas, liberar tiempo para deliberación y elevar calidad por trazabilidad/validación).

Esta aceleración del ciclo OODA otorga una ventaja decisional crítica: decidir más rápido y con mejor información que el oponente, centrándose el empleo del tiempo en la etapa de los “diálogos de EM” de concepción-definición de la tarea y supervisión-validación de los resultados.

NOTA: La lectura doctrinaria correcta es: la ganancia no es “decidir más rápido”, sino ganar tiempo para validar, coordinar y sostener control humano significativo.

Finalmente, el riesgo principal no es técnico: es cognitivo. La IA puede imponer un “estilo de solución” por coherencia narrativa y velocidad, empujando al EM a aceptar una respuesta elegante sin validar supuestos (cooptación cognitiva sin no hay disciplina), la contramedida institucional constituye la dinámica (modo) adversarial y la trazabilidad.

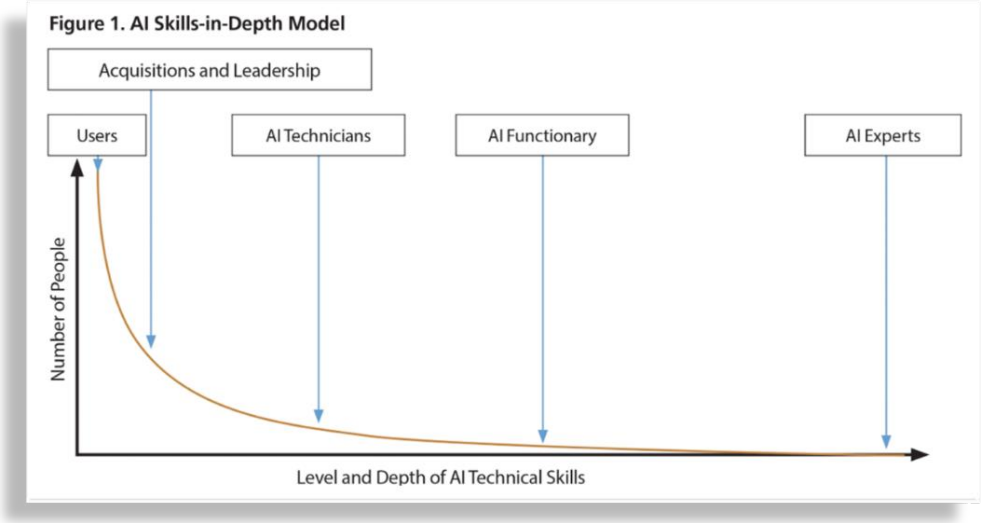
[22] **Nota metodológica (medición preliminar).** La mejora temporal reportada (**40–60%**) corresponde a una estimación de reducción de tiempo-hombre en tareas selectivas de análisis y comparación del **PPMC**

El Oficial de Estado Mayor (OEM) y Competencias Digitales 4.0 (ESTADO MAYOR COGNITIVO - EMC)

El OEM debe evolucionar de un planificador de cuadros a un líder cognitivo capaz de anticiparse y operar en Escenarios 5.0[23] La alfabetización digital no es un curso opcional, sino una competencia de comando crítica para la trazabilidad y ética de la decisión.

El Modelo de Competencias (*Skills-in-Depth*), siguiendo el modelo de

Cruickshank, los "Estados Mayores Operativos" deben estructurarse jerárquicamente[24]:



Usuarios: La vasta mayoría; emplean la tecnología y detectan fallos operativos.

Técnicos de IA: Mantienen modelos, gestionan datos y pipelines. Este es el perfil prioritario para la fuerza en actividad, dado que los expertos son costosos de producir y sus habilidades se atrofian sin un uso constante.

Funcionarios de IA: Diseñan soluciones *ad-hoc* para problemas específicos de la unidad.

Expertos en IA: Diseñan la teoría y arquitectura de sistemas complejos.

Este modelo clasifica la fuerza laboral en usuarios, técnicos, funcionarios y expertos en IA. En ese sentido, muestra cómo disminuye el número de personas a medida que aumenta la profundidad técnica, a la par de permitir estructurar planes de capacitación diferenciados, evitando exigir conocimientos avanzados a roles que no lo requieren.

Este modelo propone una estrategia escalonada de formación en IA, contemplando perfiles profesionales y currículos alineados a necesidades reales justificando inversiones en talento especializado.

El artículo explica que las organizaciones militares deben transformarse para operar con IA de forma responsable y efectiva. Los ejes centrales son:

Adopción institucional, no solo tecnológica.

[23] Escenarios 5.0 (operativo) evidencian un incremento de la autonomía técnica y de asociaciones humano-máquina, con disputa cognitiva más intensa y mayor necesidad de gobernanza de datos, auditoría y control humano significativo

[24] An AI-Ready Military Workforce, publicado por National Defense University (NDU, EE. UU.)

Capacitación masiva de usuarios y formación focalizada de expertos.

Gobernanza, liderazgo y políticas claras para integrar IA en operaciones.

La NDU argumenta que la IA no es solo una tecnología, sino un multiplicador estratégico en defensa y seguridad nacional; Enmarcando el desarrollo del ecosistema militar como un dominio estratégico donde la IA es un habilitador clave que Justificar políticas públicas para inversión en infraestructura digital (HPC, datos, simulación).

Por otro lado, El documento identifica brechas de talento críticas y recomendaciones para reducirlas: Falta de personal capacitado, Competencia con el sector privado por talento de alto nivel e Insuficiencia de programas de formación especializados en IA.

En ese sentido propone; centros de formación y certificación definidas según nivel técnico, políticas de Incentivos y retención de expertos y Creación de centros de excelencia en IA; enfatizándose en la importancia del liderazgo institucional; las doctrinas de uso, ética y regulación e integración de IA en todas las áreas operativas.

Por ello, la estrategia de desarrollo de capital humano para optimizar recursos debe priorizar la formación de técnicos uniformados sobre la de expertos de alto nivel. El concepto de “Reserva”, por las exigencias de experiencia y retención (Funcionarios de IA), se identifica como el lugar ideal para reclutar a expertos en IA, permitiendo que el Estado aproveche el talento de ciudadanos con carreras consolidadas en el sector tecnológico civil, eliminando la carga de mantenimiento de habilidades que la rutina militar podría degradar.

Se identifican los siguientes conocimientos, competencias y/o habilidades para el OEM en un EMC:

- Alfabetización Digital y Gestión de "Intangibles Tecnológicos"

De acuerdo con el PLANCAMIL 2023 y la DPDN 2021, el OEM debe poseer una alfabetización digital que le permita actuar como auditor de tecnologías cuya barrera de entrada se ha reducido drásticamente. El reporte AI Index 2025 (Página Oficial Stanford HAI)[25] destaca una

reducción de 280 veces en los costos de inferencia -estimado- desde 2022, lo que democratiza el acceso a la IA tanto para fuerzas propias como para adversarios. (*No nos vencerá la IA sino el que* la utilice mejor - Jensen Huang - CEO NVIDIA)[26].

El OEM / EMC debe dominar los siguientes componentes para sustentar la "Estrategia Militar-Operacional Disuasiva - Activa":

Inteligencia Artificial y Machine Learning: al beneficiar la "Multicapa de Restricción de Área", permitiendo ciclos de decisión predictivos que operan en las capas de "Anticipar" y "Prevenir".

Big Data y Ciencia de Datos: al impactar directamente en la "Logística de Sostenimiento de Precisión", optimizando la cadena de suministros y prediciendo demandas críticas mediante el análisis de patrones ocultos.

Ciberdefensa y Ciberseguridad: al garantizar la integridad del Sistema de Comando y Control (C2) frente a agresiones en el dominio no físico y la zona gris.

---

[25] Stanford Institute for Human-Centered Artificial Intelligence. (2025). *Artificial Intelligence Index Report 2025*. Stanford University. https://hai.stanford.edu/assets/files/hai_ai_index_report_2025.pdf

[26] Huang, 2025, como se cita en Milken Institute, 2025.

Internet de las Cosas (IoT) y Robótica: al permitir la sensorización total de la Zona de Operaciones, transformando datos brutos en conciencia situacional en tiempo real.

El manejo experto de estos datos es la piedra angular de la soberanía y autonomía tecnológica, pero su eficacia depende de un pensamiento crítico capaz de neutralizar la dependencia algorítmica.

- Pensamiento Crítico y Gestión de la Incertidumbre

La IA transforma las funciones cognitivas del mando, pero no reemplaza el juicio profesional del OEM. El análisis diferencia cuatro aspectos fundamentales afectados por la tecnología:

Inteligencia: Mejora de la detección y clasificación de amenazas mediante el procesamiento de volúmenes masivos de datos inabordables por el humano.

Conocimiento: Transformación de la información en saber estratégico para la "*Cognitive Readiness*" (Preparación Cognitiva). • Análisis de Riesgo: Identificación de vulnerabilidades críticas y centros de gravedad con mayor rigor científico.

Toma de Decisiones: Reducción de la ambigüedad en situaciones críticas, permitiendo al OEM decidir bajo riesgo calculado.

La Reducción del Ciclo OODA mediante IA actúa como una herramienta de inteligencia que acelera drásticamente el ciclo Observar-Orientar-Decidir-Actuar (OODA) al procesar datos en tiempo real, lo que permite al OEM orientarse más rápido que el oponente, despejando parcialmente la "*niebla de la guerra*".

Sin embargo, la aceleración tecnológica no debe diluir la responsabilidad del mando; el OEM debe compatibilizar las exigencias del proceso de la decisión frente a recomendaciones algorítmicas, manteniendo siempre el control del juicio final.

Esta eficiencia operativa debe estar siempre subordinada a un marco de responsabilidad institucional y control humano significativo.

- Ética Algorítmica y Control Humano Significativo

La implementación de IA en la defensa nacional debe alinearse con los principios del Derecho Internacional Humanitario (DIH) y los debates en la Convención sobre Ciertas Armas Convencionales (CCW) sobre los Sistemas de Armas Autónomas Letales (LAWS). Basado en el marco IA Ética, el OEM debe actuar como un "Embajador de la IA" responsable.

Principios Irrenunciables para el Oficial de Estado Mayor (Pilares IA Ética):

Integración de Valores: Asegurar que el uso de la IA refleje la identidad ética y los estándares de la institución militar.

Confianza y Transparencia: Garantizar la trazabilidad de los procesos de decisión y la auditoría de la calidad de los datos para evitar "cajas negras".

Potenciación del Crecimiento Humano: Diseñar sistemas centrados en el humano que minimicen tareas monótonas y potencien la creatividad estratégica.

Alineación de Impulsores Estratégicos: Vincular la innovación tecnológica con los objetivos de crecimiento y eficiencia de la Defensa Nacional.

Mitigación de Sesgos: Vigilancia activa sobre sesgos de género, étnicos y geográficos que puedan infiltrar los algoritmos de entrenamiento.

Responsabilidad ante el DIH/Plexo Legal-Normativo: Asumir la responsabilidad jurídica nacional e internacional por el empleo de sistemas asistidos o autónomos.

El empleo de IA en defensa exige gobernanza ética-operacional y reglas explícitas que delimiten automatización, responsabilidad y trazabilidad. Este Anexo sostiene la necesidad de ROED (Reglas de Empeñamiento Digitales) como condición doctrinaria del EMC.

Este documento no es apéndice legal: define límites de automatización, puntos indelegables y accountability; pudiendo identificar ROED mínimos para outputs IA en PPMC (bloque operativo):

Prohibición de decisión autónoma: la IA no autoriza decisiones finales; solo asiste.

Separación obligatoria: evidencia vs inferencia vs supuesto (etiquetado).

Trazabilidad: toda afirmación crítica debe citar fuente o marcarse como supuesto.

Control de versiones: prompts, glosario y outputs versionados y firmados.

Modo adversarial obligatorio: Red Team para CDG/MA/riesgos /recomendación.

Registro indelegable: firma humana, racionalidad breve y aceptación de riesgo.

Este marco ético garantiza que el Oficial de Estado Mayor sea el garante final de la legalidad-legitimidad de las operaciones en la era digital; la integración de la IA no exime de responsabilidad. El principio de Control Humano Significativo debe ser el eje inamovible de toda operación, especialmente en el uso de armamento no cinético o algoritmos de análisis de objetivos.

Toda delegación de funciones a algoritmos debe estar estrictamente encuadrada en los preceptos del Derecho Internacional de los Conflictos Armados (DICA) y Políticas-Limitaciones Políticas-Estratégicas-Operacionales. La automatización exige el diseño de específicas Reglas de Empeñamiento Digitales (ROED), donde la trazabilidad de la decisión, responsabilidad y actuación del EM y las estructuras de soporte sean siempre identificables y auditables.

- El Perfil del Oficial de Estado Mayor 4.0

El Oficial de Estado Mayor 4.0 se define como un gestor del conocimiento estratégico-operacional, capaz de articular doctrina, ciencia y tecnología bajo un modelo de soberanía y autonomía Cognitiva.

Dimensión	**Competencia Clave**	**Resultado Esperado en el Terreno**
Cognitiva	Análisis sistémico y "Cognitive Readiness".	Reducción de la Incertidumbre (Niebla de la Guerra) y decisiones fundamentadas.
Tecnológica	Auditoría de IA y alfabetización digital.	Explotación de la superioridad tecnológica y resiliencia en multidominio.
Ética	Control Humano Significativo	Trazabilidad Doctrinaria y cumplimiento estricto del DIH/DDHH.

Elaboración propia

Sistema de Alianzas Estratégicas (SAE) y Gobernanza

La soberanía tecnológica es colectiva. La ESGC se inserta en la economía del conocimiento nacional a través de un esquema cooperativo con el Sistema Educativo Nacional (SEN) y los organismos de ciencia y técnica que presentaría -inicialmente- los siguientes desafíos:

La creación de la Red Nacional de Innovación Educativa en Defensa (RENIED): ello con el objeto de evitar la duplicación de esfuerzos entre el Ministerio de Defensa y el Sistema Científico Nacional.

El Desarrollo Dual: Formación de capital humano con competencias transferibles entre los ámbitos civil y militar.

Este objetivo presenta el siguiente “Mapa de Actores Clave”:

Académicos Nacionales: UBA, UTN, UNLP, UNSAM, entre otros.

Tecnológicos: CITEDEF (como actor central), INVAP, CONAE, ARSAT.

Internacionales: NATO Defence College, CESEDEN (España), BID y UNESCO.

La concreción de un sistema de alianzas contribuye a que el Instrumento Militar no quede aislado (capacidades altamente especificas cuyo desarrollo requiere -por costos y/o barreras- la escala y masa crítica adecuada).

El abrir las instituciones a la academia y la industria, la Defensa se convierte en un “motor de innovación nacional”, asegurando que la tecnología desarrollada sea soberana y adaptada a las realidades estratégicas de la nación.

Estas estrategias de desarrollo -autónomas y “cooperativas”-, permitan abordar líneas de acción paralelas que propician tanto el avance progresivo de capacidades, como el acceso a la “frontera del conocimiento” y “transferencia”; evitando centrarse en el desarrollo de procesos “endógenos” -en oportunidades ineficaces en naturaleza y oportunidad- conforme a los efectos perseguidos a corto y mediano plazo.

Consideraciones Finales: La ESGC como bisagra estructurante del Sistema Educativo Militar de la Defensa.

En el marco de lo expuesto, la ESGC desarrolla un rol epistemológico vital, cerrando la brecha entre las doctrinas particulares de las fuerzas y el sistema científico-universitario nacional (UNDEF); una función que valida la experiencia operacional como dato científico con trazabilidad doctrinaria, evitando que el saber militar quede aislado en compartimentos estancos -un Accionar Militar Conjunto entendido como interagencialidad multinivel e interoperabilidad multidimensional-; proceso que contempla los siguientes ejes estructurantes:

Homologación doctrinaria: estandarización de las competencias del nivel operacional conforme a la normativa RC 20-01, articulada con la estructura doctrinaria asociada y con indexación trazable de fuentes.

Integración científica: conversión sistemática de lecciones aprendidas del ámbito militar en conocimiento científico, integrando docencia e investigación avanzada mediante una base de datos de conocimiento validado (aprendizaje organizacional y de sistemas).

Articulación institucional: consolidación de la ESGC como nodo de coordinación entre el Ministerio de Defensa, la UNDEF y el Sistema Educativo Nacional (SEN), habilitando interagencialidad epistemológica y transferencia institucional del conocimiento.

Esta estrategia de Anticipación de ese camino de transición hacia una Academia Militar de la Defensa del Escenario 4.0 (Big Data/TIC), conlleva implícito el diseño de una estrategia asociada de desarrollo al Escenario 5.0 (Colaboración Humano-IA) que redefinen la Academia Militar de la Defensa en tres dimensiones:

Dimensión Académica: Actualización de posgrados en ética algorítmica, ciber estrategia y defensa cognitiva.

Dimensión Institucional: Una gobernanza educativa que integre de forma sistémica la ciencia y la doctrina.

Dimensión Epistemológica: La consolidación de una "racionalidad cognitiva" donde el conocimiento estratégico es el recurso más crítico y escaso del Estado.

Un ámbito que opera como un "laboratorio cognitivo", la ESGC es el nodo que garantiza que el Instrumento Militar evolucione de una práctica instructiva a una reflexiva. Esto previene la obsolescencia del mando, permitiendo que el oficial de Estado Mayor no solo ejecute procesos, sino que gestione la complejidad de la guerra moderna con herramientas digitales de vanguardia y aptitudes de liderazgo requeridas (autonomía, creatividad y juicio crítico en las etapas críticas de concepción-supervisión-validación).

Por ello, la ESGC se posiciona como el Centro de Gravedad Intelectual del sistema educativo militar (capacitación y validación). La tecnología es el facilitador que disipa la "niebla de la guerra", pero el pensamiento militar profesional es garante de la confiabilidad de proceso de decisión críticos en la era digital (EMC).

Un proceso estratégico de “Soberanía Cognitiva”, no es solo una hoja de ruta técnica, es un proceso institucional-educativo estratégico que propicia una Maniobra de Anticipación; enseñar a pensar y decidir donde la información es poder. El futuro del Instrumento Militar de la Defensa Nacional depende de la capacidad para fusionar el talento humano con la potencia analítica de la IA.

Es por ello que la Escuela Superior de Guerra Conjunta (ESGC) se posiciona como la bisagra estructurante del Sistema Educativo de la Defensa. Su misión fundamental es garantizar que esta formación integral convierta al Oficial de Estado Mayor en el líder adaptativo, ético y tecnológicamente soberano que la República Argentina demanda para proteger sus intereses vitales en la complejidad de la Defensa 4.0.

Com. (R) Mág Pablo Andrés Farias

Director de Proyecto

ANEXO 8 - Formulario Operativo EMC (Control de avance del proceso de investigación aplicada - FMC/ESGC)

_____

A) Identificación del registro

- ID de Registro EMC: EMC-INV-AAAA-###

Fecha / Hora: ____ / ____ / _____ – _____

Unidad: FMC/ESGC

Equipo / Célula: _____

Responsable del registro: _____

Revisor (control de calidad): _____

- Versión del registro: v._____

B) Enfoque del ciclo (qué estás haciendo hoy)

Marcar una sola:

☐ B1. Recolección documental

☐ B2. Codificación / categorización cualitativa

☐ B3. Construcción del repositorio (PK)

☐ B4. Validación adversarial (Red Team)

☐ B5. Síntesis de resultados / matriz 9.x

☐ B6. Diseño de propuesta (SOP/currícula/gobernanza)

☐ B7. Evaluación y cierre (calidad, límites, recomendaciones)

Objetivo operativo de esta sesión (1–2 líneas):

_____

_____

_____

C) Vinculación con ejes del proyecto (1, 2, 3 y 4)

Marcar lo que aplica:

☐ 1 Políticas/estrategias institucionales (TD/IA)

☐ 2 Mapa/repositorio + sincronía CPDN/PEM (2012-2026)

☐ 3 Procesos/competencias/habilidades (retroalimentación)

☐ 4 Capacidades, liderazgo, adopción, gobernanza y control humano

Pregunta específica que responde esta sesión:

_____

_____

D) Evidencia incorporada (trazabilidad mínima)

D1. Fuente primaria (obligatorio)

Tipo: ☐ Documento FMC/ESGC ☐ Informe ☐ Trabajo/TFI ☐ Programa/plan ☐ Acta/consigna ☐ Ejercicio ☐ Otro

Título/Nombre del documento:

_____

Ubicación: archivo/link: _____
Página/sección exacta: _____
Fecha del documento: ____ / ____ / _____
Autor/área: _____

D2. Evidencia secundaria (si aplica)

Tipo: ☐ Norma ☐ Doctrina ☐ Informe externo ☐ Paper ☐ Otro
Referencia: _____
Uso: ☐ Contexto ☐ Contraste ☐ Validación ☐ Marco teórico
Regla: si no hay página/sección, no es evidencia utilizable.
☐ Cumple

_____

E) Supuestos, inferencias y límites (control de sesgos)

E1. Supuestos críticos usados hoy (máx. 7)

_____ Refutador observable: _____
_____ Refutador observable: _____
_____ Refutador observable: _____

E2. Qué parte es inferencia (no evidencia)

☐ Inferencia declarada explícitamente
Texto breve:

_____

E3. Riesgo de sesgo (marcar lo que se detecta)

☐ Confirmación (busqué validar una hipótesis previa)
☐ Anclaje (la primera definición condicionó todo)
☐ Disponibilidad (sobrepeso de lo mediático/reciente)
☐ Encuadre (framing)
☐ Retrospectiva (todo parecía obvio)
☐ Halo (forma persuasiva ≠ validez)
☐ Ingroup (visión dominante)
Contramedida aplicada: _____

_____

F) Registro de output (producto de la sesión)

Marcar lo producido:
☐ F1. Ficha PK para repositorio
☐ F2. Extractos codificados por categoría/subcategoría
☐ F3. Hallazgo + brecha institucional
☐ F4. Recomendación EMC (acción)
☐ F5. Ajuste de SOP / glosario / criterios de aceptación
☐ F6. Otro: _____

Output principal (resumen 5-7 líneas):

_____

_____

Nivel de confianza del output: ☐ Alto ☐ Medio ☐ Bajo

Por qué: _____

_____

G) Codificación cualitativa (para matriz de resultados)

G1. Categoría principal

☐ C1 ESGC bisagra (doctrina-ciencia-institución)

☐ C2 Arquitectura EMC/PPMC (roles, datos, herramientas)

☐ C3 Competencias OEM 4.0 (cognitivas, tecnológicas, éticas)

☐ C4 Cultura/adopción (resistencia, capacitación)

☐ C5 Ética/ROED/control humano significativo

☐ C6 Repositorio + sincronía CPDN/PEM

☐ C7 Alianzas/SAE/RENIED y escalamiento

G2. Subcategoría (texto corto)

_____

G3. Hallazgo (una frase, verificable)

_____

G4. Brecha institucional (una frase)

_____

G5. Recomendación EMC (acción concreta)

_____

_____

H) Validación adversarial (obligatorio para outputs críticos)

H1. ¿Se aplicó Red Team cognitivo?

• ☐ Sí ☐ No (si no, justificar):

_____

H2. Ataque Red Team (qué se intenta refutar)

Hipótesis/afirmación atacada: _____

Supuesto frágil detectado: _____-

Evidencia contraria hallada: _____

Modo de falla identificado: _____

H3. Resolución

☐ Se corrigió output

☐ Se mantiene con reservas

☐ Se descarta

Registro del cambio (qué cambió y por qué):

I) Alta al repositorio (si se generó PC)

Completar solo si se creó/actualizó una ficha:

ID-Repo PK: FMC-ESGC-AAAA-###

Tipo PC: ☐ Docencia ☐ Investigación ☐ Extensión ☐ Procedimiento ☐ Ejercicio ☐ Herramienta

- Nivel de evidencia (0–3): 0 ☐ 1 ☐ 2 ☐ 3 ☐

Nivel de validación: ☐ Borrador ☐ Evaluado ☐ Validado ☐ Adoptado

Responsable de carga: _____

Fecha de carga: ____ / ____ / _____

J) Próxima acción (plan de avance)

Próximo paso concreto (1): _____

Próximo paso concreto (2): _____

Dependencias (documento/persona/dato): _____

Fecha objetivo: ____ / ____ / _____

Criterio de cierre de sesión (firma)

Responsable: _____ Firma: _____

Revisor QA: _____ Firma: _____

Com. (R) Mág Pablo Andrés Farias

Director de Proyecto