VOL.6 - N°06
SANTIAGO DE SURCO
LIMA, PERÚ
ENE - JUL 2023

Instituto Científico y Tecnológico del Ejército

Uso de la Inteligencia Artificial en el Ejército del Perú: Desafíos y Oportunidades

Use of Artificial Intelligence in the Peruvian Army: Challenges and Opportunities

AUTORES

Carlos Quinto Huamán[1],
Rosa Marcela Picón Huacarpuma[2]

[1]Universidad Complutense de Madrid
[2]Cibernos España

RECIBIDO: 17/06/2023, PUBLICADO: 12/09/2023

RESUMEN

El uso de la inteligencia artificial (IA) en el Ejército del Perú plantea desafíos y ofrece oportunidades significativas para el futuro estratégico de las operaciones militares y procesos clave. En este trabajo, se analiza rigurosamente los desafíos asociados con la implementación de la IA en el Ejército, incluyendo la capacidad de procesamiento y almacenamiento de los datos, la capacitación del personal militar, la seguridad y privacidad de los datos, la interoperabilidad de sistemas de información, las consideraciones éticas y de responsabilidad, la adquisición y gestión de datos, la ética y transparencia, las limitaciones en entornos adversos, entre otros. Por otro lado, se aprovecha el estudio de los desafíos para transformarlos en oportunidades que la IA brinda al Ejército y proponer algunas soluciones tecnológicas, centrándose en la mejora de la toma de decisiones estratégicas que es vital para la institución, el desarrollo de sistemas robóticos y vehículos autónomos donde interviene la investigación aplicada, la optimización de recursos y la mejora en el entrenamiento. Además, se menciona el análisis avanzado de inteligencia para adoptar medidas preventivas, el apoyo en operaciones de rescate y desastre, la ciberseguridad, la mejora de la logística, entre otros.

Palabras clave: Inteligencia Artificial, desafíos, oportunidades, toma de decisiones estratégicas, entrenamiento y simulación, análisis de inteligencia.

ABSTRACT

Using artificial intelligence (AI) in the Peruvian Army presents significant challenges and opportunities for the strategic future of military operations and administrative processes performed by the Peruvian Army.

This paper rigorously analyzes the challenges associated with the implementation of AI in the Army, including data processing and storage capacity, training of military personnel, data security, and privacy, interoperability of information systems, ethical and accountability considerations, data acquisition and management, ethics and transparency, limitations in adverse environments, among others. On the other hand, the study of the challenges is used to transform them into opportunities that AI offers the Army, focusing on the improvement of strategic decision-making, which is vital for the Institution, the development of robotic systems and utonomous vehicles where applied research, resource optimization, and improved training are involved. It also mentions advanced intelligence analysis for preventive measures, support in rescue and disaster operations, cybersecurity, and improved logistics, among others.

Keywords: Artificial Intelligence, challenges, opportunities, strategic decision-making, training and simulation, intelligence analysis.

I. INTRODUCCIÓN

El uso de la Inteligencia Artificial (IA) sigue expandiéndose de manera exponencial, abarcando numerosos aspectos de la sociedad (Schepman y Rodway, 2020). Entre ellos, los sistemas de IA con los cuales las personas interactúan en su vida cotidiana, dentro de sus hogares como el altavoz inteligente. En 2021, se estimó que se enviaron más de 186 millones de unidades de altavoces inteligentes en todo el mundo, y se proyecta que esta cifra pueda superar los 200 millones para finales del 2023 (Laricchia, 2021). El avance de la IA ha generado una amplia gama de posibles aplicaciones en el ámbito militar (McNeish et al., 2020). Estas aplicaciones incluyen, entre otros, el apoyo logístico, la simulación, el reconocimiento de objetivos y la vigilancia de amenazas (Taddeo et al., 2021).

Sin embargo, este potencial aún no se ha materializado por completo, y tanto la investigación como el uso de la IA en el ámbito militar se encuentran en sus primeras etapas, como se refleja en las estrategias y políticas actuales de países europeos (Defense Innovation Board, 2019; Ministerio de Defensa del Reino Unido, 2022).

La implementación de la IA en el Ejército del Perú representa un nuevo y emocionante horizonte en el ámbito de la defensa y seguridad nacional. La IA ofrece un amplio espectro de posibilidades y ventajas estratégicas que pueden transformar positivamente los procesos estratégicos, misionales y de soporte. Sin embargo, también plantea desafíos que deben abordarse de manera efectiva para garantizar un uso responsable y exitoso de esta tecnología emergente. En este contexto, el presente estudio se centra en plantear una visión integral de los desafíos y oportunidades que surgen en la implementación de la IA en el Ejército del Perú. Reconociendo el potencial transformador de esta tecnología, se resaltan las oportunidades estratégicas que pueden fortalecer las capacidades militares.

Al mismo tiempo, se abordan los desafíos técnicos, éticos y organizativos que deben superarse para garantizar un uso efectivo y responsable de la IA en el contexto militar. Este análisis busca sentar las bases para una implementación exitosa de la IA, aprovechando al máximo sus beneficios y mitigando sus posibles riesgos.

II. INTELIGENCIA ARTIFICIAL EN EL CONTEXTO MILITAR

Existen muchas definiciones sobre IA en el contexto militar, pero generalmente no se discuten con frecuencia en la literatura de investigación.

En Defense Innovation Board (2019; p. 8) se presentó varias definiciones asociadas al uso de IA en ámbito militar: (i) "un sistema artificial que realiza tareas bajo circunstancias variables e impredecibles sin una supervisión humana significativa, o que puede aprender de su experiencia y mejorar su rendimiento cuando se expone a conjuntos de datos; (ii) un sistema artificial desarrollado en software informático, hardware físico u otro contexto que resuelve tareas que requieren percepción, cognición, planificación, aprendizaje, comunicación o acción física similares a las humanas; (iii) un conjunto de técnicas, incluido el aprendizaje automático, diseñado para aproximarse a una tarea cognitiva; Estas definiciones indican que, aparte del área específica de aplicación y los tipos de usos, hay poca diferencia en la aplicación de la IA dentro y fuera de del contexto civil y militar. Una definición más genérica es proporcionada, por Gillath et al. (2021) donde indica que la IA es la simulación de procesos de inteligencia humana por máquinas, especialmente sistemas informáticos. Estos procesos incluyen el aprendizaje (adquisición de datos y reglas para usar la información), el razonamiento (uso de reglas para llegar a conclusiones) y la autocorrección. Si bien es cierto, la viabilidad técnica de la IA es el foco de mucha investigación y desarrollo en varios ámbitos del contexto militar, las preocupaciones relacionadas con la confianza, la moralidad, la legalidad y la ética podrían plantear desafíos iguales o incluso mayores para la implementación efectiva de las capacidades lideradas por la IA (Wasilow y Thorpe, 2019. Una fuerte reserva relacionada con el uso de la IA en contextos militares se refiere a situaciones en las que las máquinas controladas por IA podrían tomar decisiones y/o quitar vidas humanas fuera del control directo de un operador humano (Morgan et al., 2020). Otras preocupaciones se centran en la posibilidad de que los sistemas de IA encargados del apoyo a la toma de decisiones puedan cometer juicios erróneos sobre los posibles objetivos que un operador humano podría identificar (Morgan et al., 2020). Varios países han comenzado a abordar las preocupaciones relacionadas con los sistemas de IA con un compromiso hacia el uso transparente y ético en contextos de defensa. Entre ellos, el Ministerio de Defensa del Reino Unido (2022) en su estrategia más reciente de Inteligencia Artificial en Defensa, donde reconoce preocupaciones relacionadas con la equidad, el sesgo y la confiabilidad. Las preocupaciones de equidad surgen de la dificultad de establecer toma de decisiones automatizada basada en valores y demuestran la necesidad de mantener un elemento humano integral en dichos procesos. Los sesgos en el aprendizaje automático se refieren a un impacto desproporcionado no deseado en grupos específicos, en este caso principalmente en el personal militar. La confiabilidad se refiere al rendimiento estable y libre de errores de los sistemas de IA. Se considera que la equidad, el sesgo y la confiabilidad están intrincadamente relacionados con cuestiones de responsabilidad y rendición de cuentas humanas, tanto en el lado de los desarrolladores como en el de los operadores. La responsabilidad y la rendición de cuentas deben mantenerse en el contexto de grandes cantidades de datos complejos para procesar en los plazos muy cortos implicados por los sistemas informáticos. La estrategia también destaca la necesidad de confianza pública en la IA y está completamente alineada con compromisos similares en la Estrategia Nacional de IA del Reino Unido (Gobierno del Reino Unido, 2022). Como parte integral de dicha estrategia, el compromiso con el público es una actividad crítica para asegurar que se comunique claramente un compromiso con el uso ético de dichas tecnologías por parte de quienes toman decisiones sobre su uso (Morgan et al., 2020).

III. DESAFÍOS EN LA IMPLEMENTACIÓN DE LA IA EN EL EJÉRCITO DEL PERÚ

a implementación de IA en el Ejército del Perú plantea una serie de desafíos que deben

abordarse de manera efectiva para garantizar su éxito en diversos procesos clave, sea estratégicos, misionales o de soporte. A continuación, se presentan los principales los desafíos que se alinean a la naturaleza del Ejército para su implementación:

1.Capacidad de procesamiento y almacenamiento (CPA): La implementación efectiva de la IA requiere una infraestructura robusta de procesamiento y almacenamiento para manejar grandes volúmenes de datos y ejecutar algoritmos complejos. Esto implica invertir en hardware y software adecuados para asegurar un rendimiento óptimo y eficiente (West, 2018).

2.Recursos humanos capacitados (RHC): Es esencial contar con personal militar y civil en el manejo de la IA, incluyendo la comprensión de los algoritmos, ciencia de datos, técnicas de aprendizaje automático y el manejo de la ética en la IA que actualmente es muy discutido por la comunidad académica. Esto implica ofrecer programas de capacitación en las Escuelas de Formación, Armas y Servicios e inclusive en instituciones educativas externas, a fin de lograr el desarrollo profesional, garantizando que los recursos humanos del Ejército adquieran las habilidades necesarias (Bughin et al., 2018).

3.Seguridad y privacidad de los datos (SPD): La IA depende en gran medida de la recopilación y análisis de datos sensibles, particularmente si se relaciones a operaciones militares o planes de inteligencia, lo que plantea desafíos en términos de protección de la seguridad y privacidad de estos datos. Por ello, se deben establecer políticas institucionales y prácticas robustas de gestión de datos para garantizar su integridad y confidencialidad (Arrieta et al., 2020).

4.Interoperabilidad de sistemas (ISI): La integración de las plataformas de IA con los sistemas existentes en el Ejército deben tener procesos claros para el intercambio de información ya que este aspecto puede ser un desafío debido a la heterogeneidad de las plataformas y la necesidad de compartir y procesar datos de manera eficiente. Se requiere una planificación cuidadosa y una arquitectura flexible para lograr una interoperabilidad efectiva (Kocabas, 2021).

5.Consideraciones éticas, legales, responsabilidad y confiabilidad (CEL): El uso de la IA en el Ejército debe abordar aspectos éticos, responsabilidad y confiabilidad, los cuales garantizan el uso responsable de todas sus capacidades. Esto implica establecer claramente los marcos regulatorios y políticas institucionales para guiar el desarrollo y uso de la IA en cada nivel de la organización, así como garantizar la transparencia y veracidad de las decisiones tomadas por las plataformas que incorporan la IA como principal tecnología (Jobin, Ienca, Vayena, 2019; McKinsey Global Institute, 2019). Un claro ejemplo es el uso de modelos de lenguaje como ChatGPT, que plantea desafíos en términos de confiabilidad y ética. Este sistema inteligente puede ser de gran ayuda en el ámbito militar; no obstante, es importante tener en cuenta que podría generar respuestas sesgadas, incorrectas o inapropiadas en algunos casos; incluso podría ser usado en investigaciones realizadas en los diversos programas de estudios que gestiona el Ejército. Por ello, es importante aplicar un control adecuado, especialmente cuando se utiliza en entornos militares o de seguridad nacional.

6.Adaptación al entorno operativo (AEO): El entorno operativo del Ejército presenta desafíos singulares, como condiciones geográficas variadas, operaciones en zonas remotas, interferencias electrónicas y condiciones climáticas extremas. Entre otros lugares, estos desafíos se presentan en el Valle de los ríos Apurímac, Ene y Mantaro (VRAEM), donde la IA debe adaptarse a estas condiciones y ser capaz de operar de manera efectiva en diferentes entornos y situaciones (Russell & Norvig, 2016). Asimismo, se deben desarrollar algoritmos y sistemas robustos que puedan funcionar de manera confiable en situaciones adversas y hostiles (Susskind & Susskind, 2018). Por ejemplo, la IA debe capturar imágenes satelitales y posteriormente procesarlas para identificar en tiempo real la posición de grupos

terroristas, tipo de armamento, entre otros. Por ejemplo, la IA debe capturar imágenes satelitales y posteriormente procesarlas para identificar en tiempo real la posición de grupos terroristas, tipo de armamento, entre otros.

7.Integración con sistemas existentes (ISE): El Ejército ya utiliza una variedad de sistemas de información, bases de datos y tecnologías. Entre los sistemas se destacan el sistema de personal, evaluación, planillas, presupuesto y control de bienes, abastecimiento; en cuanto a tecnologías se usa el lenguaje de programación Java y PHP, en el ámbito de persistencia predomina Oracle en múltiples versiones; mientras que como sistema operativo para servidores se prioriza Windows. Este tipo de características hace que se requiera una integración efectiva entre los sistemas existentes y la IA. Además, implica superar obstáculos técnicos y logísticos para garantizar una integración sin problemas y un funcionamiento conjunto eficiente (Chui, Manyika, & Miremadi, 2016).

8.Adquisición y gestión de datos (AGA): La implementación eficiente de la IA requiere una amplia cantidad de datos de alta calidad, por ejemplo, el historial clínico de un Oficial proporcionado por el Hospital Militar Central (HMC) o los datos personales del personal de tropa del servicio militar voluntario generado por el Comando de Reserva y Movilización del Ejército (COREMOVE). Esto plantea desafíos en términos de adquisición, almacenamiento y gestión de datos, incluyendo la creación de mecanismos eficientes para recopilar y preprocesar los datos necesarios para el entrenamiento y funcionamiento de las plataformas de IA (Veloso & Carbonell, 2018).

9.Implementación gradual y planificada (IGP): La implementación de la IA en el Ejército debe realizarse de manera gradual y planificada. Esto implica identificar casos de uso prioritarios orientado a solucionar problemas que afectan a los procesos misionales de la institución. Asimismo, se debe establecer hitos y metas claras, y luego realizar pruebas y evaluaciones continuas para minimizar los riesgos y garantizar una transición suave, esto con la finalidad de promover la mejora continua (Brynjolfsson & McAfee, 2017). Para este desafío se debe considerar el uso de metodologías de gestión de proyectos como PMBOK, PRINCE2, entre otros.

10.Inversión financiera (IFI): Implementar IA requiere una inversión significativa en aspectos de infraestructura, tecnología y capacitación (World Economic Forum, 2020). Esto implica que el Ejército debe destinar recursos financieros adecuados para adquirir y mantener la infraestructura necesaria. Además, se de solventar la capacitación oportuna del personal militar en temas técnicos y asegurar una implementación integral y exitosa.

11.Aceptación y confianza (ACO): La adopción de la IA requerirá ganar la aceptación y confianza de los miembros del Ejército, particularmente de aquellos que evitan el uso de nuevas tecnologías o quienes se sienten amenazados por algo que automatizará un proceso que se realiza de manera manual. Esto implica educar y comunicar de manera efectiva sobre los objetivos, los beneficios y el propósito de la implementación de la IA de manera institucional, así como abordar cualquier preocupación o percepción negativa (Lepri et al., 2020).

12.Regulaciones y políticas (RPO): Al Implementar IA se debe tener respaldo por marcos regulatorios y políticas institucionales, teniendo en consideración las normas del sector defensa, a fin de garantizar su uso de manera segura y conservar en todo momento los factores éticos. Se deben establecer normas y directrices que aborden aspectos como la privacidad, la responsabilidad y la seguridad en el uso de la IA en el contexto militar (Brynjolfsson & McAfee, 2014).

13. Cambios culturales y organizativos (CCO): El acogimiento de la IA puede requerir cambios culturales y organizativos en el Ejército, incluyendo nuevos roles en actividades clave y procesos de trabajo mucho más ágiles. Se deben implementar estrategias de gestión del cambio utilizando metodologías emergentes y programas de capacitación para facilitar la transición y maximizar los beneficios de la IA en la organización militar (Brynjolfsson & McAfee, 2017).

En la Figura 1, se muestra una visión general de la organización del Ejército del Perú para abordar los desafíos en la implementación de la IA. En la Tabla 1, se detalla la asignación de los desafíos identificados a las dependencias del Ejército con mayor grado de relación. Estas dependencias deben ser los líderes de grupos de trabajo para realizar un análisis riguroso de los desafíos de la IA y presentar soluciones eficientes en beneficio de la institución.

Fig. 1. Visión general de la organización del Ejército para abordar los desafíos en la Implementación de la IA

Tabla 1. Asignación de los desafíos identificados a las dependencias del Ejército con mayor grado de relación.

Nº	DESAFÍO	DEPENDENCIAS
1	Capacidad de procesamiento y almacenamiento (CPA)	CITELE|DIE|OPRE| DIPLANE|DICITECE|CICTE
2	Recursos humanos capacitados (RHC)	DIPERE|DIEDOCE|COEDE
3	Seguridad y privacidad de los datos (SPD)	CITELE|DIE|OAJE
4	Interoperabilidad de sistemas (ISI)	CITELE|DICITECE
5	Consideraciones éticas, legales, responsabilidad y confiabilidad (CEL)	CITELE|DIE|DICITECE|DIN FE
6	Adaptación al entorno operativo (AEO)	CITELE|DICITECE|CICTE
7	Integración con sistemas existentes (ISE)	CITELE|DICITECE|CICTE
8	Adquisición y gestión de datos (AGA)	CITELE|DIE|OPRE| DIPLANE|DICITECE|CICTE
9	Implementación gradual y planificada (IGP)	CITELE|DIE|OPRE| DIPLANE|DICITECE|CICTE
10	Inversión financiera (IFI)	OPRE|OEE
11	Aceptación y confianza (ACO)	CITELE|DIE|OPRE| DIPLANE|DICITECE|CICTE|OAJE
12	Regulaciones y políticas (RPO)	CITELE|DIE|OPRE| DIPLANE|DICITECE| CICTE|OAJE
13	Cambios culturales y organizativos (CCO)	CITELE|DIE|OPRE| DIPLANE|DICITECE| CICTE|OAJE|DINFE

IV. OPORTUNIDADES PARA EL EJÉRCITO DEL PERÚ

A pesar de que existen desafíos sustanciales, la implementación de la IA en el Ejército del Perú también ofrece excelentes oportunidades para mejorar todos sus procesos. A continuación, se presentan algunas de las oportunidades clave

1.Mejora de la toma de decisiones estratégicas (MTDE): La IA puede proporcionar al comando del Ejército herramientas y análisis avanzados para mejorar la toma de decisiones estratégicas. Esto incluye la capacidad de procesar y analizar grandes volúmenes de datos de inteligencia para obtener información relevante y apoyar la planificación y ejecución de operaciones (Acemoglu & Restrepo, 2019). Entre las alternativas, están los tableros de mando predictivos desde el nivel Unidad, utilizando conjuntos de datos procesados en ecosistemas distribuidos y optimizados con el uso de algoritmos sencillos como agrupamiento jerárquico o más complejos como redes neuronales. Además, se puede utilizar un sistema que permita analizar datos sobre patrones de los movimientos de remanentes terroristas en la zona del VRAEM, condiciones climáticas, terreno y otros factores relevantes para que el Comando tome decisiones acertadas y oportunas. Por otro lado, el modelado de escenarios y uso de simuladores pueden ayudar a reducir los riesgos y minimizar las pérdidas humanas al permitir que los encargados de liderar operaciones militares evalúen la efectividad de ciertas estrategias antes de ser ejecutadas en operaciones.

2.Robótica y vehículos autónomos (RVAU): Permite el desarrollo y despliegue de sistemas robóticos y vehículos autónomos en operaciones militares. En primera instancia, estos proyectos se deben realizar en colaboración con universidades e institutos de investigación del Perú, y en segunda instancia, participar en propuestas de proyectos internacionales con socios que ya cuentan con prototipos próximos a ser desplegados. Estas soluciones pueden realizar tareas peligrosas y complejas, así como mejorar la vigilancia y el reconocimiento en el campo de batalla (Manyika, Chui, & Miremadi, 2017). Entre algunas soluciones inmediatas está el apoyo a la Unidad Binacional de Desminado Humanitario del Perú y del Ecuador para la desactivación de explosivos, y el apoyo a la Primera Brigada Multipropósito en el marco de los nuevos roles que vienen asumiendo las Fuerzas Armadas en el mundo, en situaciones de desastre, explorando y realizando acciones de rescate en zonas inaccesibles para el ser humano.

3.Colaboración y coordinación en tiempo real (CCTR): Mejora la capacidad del Ejército para colaborar y coordinar entre los Comandos de todos los niveles en tiempo real, facilitando una respuesta más rápida y efectiva. Esto incluye la capacidad de compartir información y comunicarse de manera eficiente (Ransbotham et al., 2018). Esta oportunidad se puede materializar creando una plataforma que integre múltiples fuentes de datos como sensores, sistemas de vigilancia, drones, radares, entre otros, para gestionar recursos como las municiones, combustible, equipo médico, optimizando su distribución y uso eficiente según las necesidades, y de esta forma proporcionar a todos los niveles de Comando una visión más amplia y actualizada de la situación de la zona de operaciones.

4.Mantenimiento predictivo (MPRE): Propicia la implementación de estrategias de mantenimiento predictivo, que permiten detectar y prevenir fallas en equipos militares y sistemas de armas antes de que ocurran.

4.Mantenimiento predictivo (MPRE): Propicia la implementación de estrategias de mantenimiento predictivo, que permiten detectar y prevenir fallas en equipos militares y sistemas de armas antes de que ocurran. Esto mejora la disponibilidad operativa y reduce los costos asociados con el mantenimiento y reparación de equipos militares (Brynjolfsson & McAfee, 2017). Una propuesta viable para el Ejército es implementar una aplicación de seguimiento en tiempo real del estado y rendimiento de los equipos militares, como vehículos, aviones, helicópteros, equipos de radios, sistemas de armamento, entre otros que se dispone. Esta herramienta, tendría la capacidad de analizar datos de sensores y registros de mantenimiento para identificar patrones y anomalías que puedan indicar posibles fallas o desgaste excesivo. Al predecir problemas potenciales antes de que ocurran, se pueden programar acciones de mantenimiento preventivo para evitar interrupciones en las operaciones y prolongar la vida útil de los equipos.

5.Entrenamiento y simulación avanzados (ESIA): Optimiza los programas de entrenamiento físico y simulación de operaciones militares, proporcionando escenarios realistas y adaptativos para el entrenamiento del personal militar. Además, tiene la capacidad de simular situaciones de combate y desarrollar estrategias eficaces en un entorno virtual (World Economic Forum, 2018). En concreto, la Escuela de Educación Física del Ejército (ESC EFIS) puede adaptar el entrenamiento militar para cada soldado de manera individualizada, teniendo en cuenta sus habilidades, fortalezas y debilidades. Cuando se analiza datos de rendimiento y retroalimentación, la IA puede ayudar a diseñar planes de entrenamiento personalizados que se ajusten a las necesidades específicas de cada soldado. Por otro lado, la ESC EFIS con un sistema de simulación y análisis de datos de entrenamientos anteriores puede identificar situaciones de alto riesgo y proporcionar recomendaciones para mejorar la seguridad y reducir lesiones durante el entrenamiento.

6.Inteligencia militar mejorada (IMME): Permite recopilar, analizar y procesar información de inteligencia de diversas fuentes, como por ejemplo implementando una herramienta robusta de Inteligencia de Fuentes Abiertas (OSINT) de uso exclusivo para la Dirección de Inteligencia del Ejército, pero con interfaces de distribución y consumo de datos distribuido, para implementar técnicas como Federarte Learning o aprendizaje federado. Una vez procesado los datos, y haciendo uso de la ciencia de datos y algoritmos de aprendizaje automático se puede identificar patrones y neutralizar o eliminar potenciales amenazas (Brynjolfsson & McAfee, 2014).

7.Operaciones logísticas eficientes (OLEF): Potencia y optimiza las operaciones logísticas. Interviene en la gestión de inventario o patrimonio y distribución de recursos en el campo de Intendencia y concretamente optimizaría los procesos clave del Comando Logístico del Ejército. Esto ayuda a reducir los costos y mejorar la eficiencia en el suministro y apoyo logístico a las fuerzas militares (Brynjolfsson & McAfee, 2017). Una alternativa es la implementación de una aplicación de transporte inteligente que analice datos de tráfico, condiciones del terreno, clima y otras variables o aspectos relevantes que permitan optimizar las rutas de transporte del personal militar para operaciones o eventos de despliegue en apoyo a las elecciones, y que ayuden a mejorar la entrega de los suministros en operaciones.

8. Ciberseguridad y defensa cibernética (CDEC): Fortalece las capacidades de ciberseguridad y defensa cibernética del Ejército. Además, permite la detección temprana de amenazas, la identificación de patrones de ataques y la respuesta automática a incidentes de seguridad, mejorando la resiliencia de los sistemas de información y comunicación (Acemoglu & Restrepo, 2020) El desarrollo de un Sistemas de Detección de Intrusiones (IDS) liderado por el Comando de Ciberdefensa y Telemática del Ejército permitirá analizar patrones de tráfico y identificando actividades sospechosas y alertando a los equipos de seguridad sobre posibles amenazas cibernéticas. Además, es pertinente promover la implementación de una herramienta de respuesta automatizada de incidentes cibernéticos, por ejemplo, ante un ataque de denegación de servicio distribuido (DDoS), la IA puede identificar y mitigar automáticamente el tráfico malicioso, permitiendo mantener la disponibilidad del servicio. Por otro lado, es necesario contar con una plataforma integral de autenticación mediante tecnologías biométricas avanzadas, utilizando características como reconocimiento facial, de voz o de huellas dactilares. Estos sistemas son más seguros y difíciles de falsificar.

9.Apoyo médico y sanitario (AMSA): Desempeña un papel importante en el apoyo médico y sanitario en el Ejército, a través del diagnóstico temprano de enfermedades optimizando los exámenes anuales, el monitoreo de la salud del personal militar desde los centros de salud de cada guarnición y el desarrollo de tratamientos personalizados en el Hospital Militar Central (HMC), mejorando así la satisfacción de personal militar (McKinsey Global Institute, 2017). En ese sentido, el Comando de Salud del Ejército (COSALE) y el HMC pueden promover el desarrollo de aplicaciones de asistencia virtual a los pacientes, basado en IA, que responda preguntas sobre síntomas, tratamientos y cuidados primarios en el hogar o en las Unidades a nivel nacional. Esto puede aliviar la carga del personal médico y brindar información oportuna y precisa a los pacientes. Además, es necesario crear una plataforma integral para analizar grandes conjuntos de datos, como imágenes de resonancias magnéticas, tomografías computarizadas y radiografías, para identificar patrones y características que puedan indicar enfermedades o afecciones médicas como el cáncer. Esto puede agilizar el proceso de diagnóstico y proporcionar una evaluación más precisa y oportuna para el personal médico del HMC.

10.Comunicaciones seguras y cifradas (CSCI): Mejora las capacidades de comunicación segura y cifrada en el Ejército. Proporciona la oportunidad de desarrollar algoritmos y plataformas de cifrado avanzados, así como la detección y prevención de ataques cibernéticos dirigidos a las comunicaciones militares (World Economic Forum, 2020). Por ejemplo, las Unidades especializadas de comunicaciones tienen la posibilidad crear estos algoritmos robustos que permitan identificar y clasificar automáticamente los datos sensibles en las comunicaciones durante las operaciones, como información clasificada o confidencial. En complemento, estos algoritmos, pueden aplicar mecanismos de protección adicionales para garantizar que estos datos estén adecuadamente protegidos durante la transmisión y su almacenamiento.

11.Respuesta humanitaria y desastres naturales (RHDN): La IA puede ser utilizada para mejorar la capacidad de respuesta del Ejército en situaciones de desastres naturales o emergencias humanitarias. Posibilita la coordinación de recursos con otras entidades, la identificación de áreas afectadas en tiempo real y la asignación eficiente de ayuda y asistencia a las poblaciones afectadas en coordinación con otros sectores (World Economic Forum, 2019). De manera particular, la Primera Brigada Multipropósito en coordinación con el Instituto Nacional de Defensa Civil (INDECI) serían los encargados de proponer soluciones integrales para mejorar la capacidad de respuesta a frente a desastres naturales.

12.Vigilancia fronteriza (VIFR): Mejora la capacidad del Ejército para realizar operaciones de vigilancia fronteriza que actualmente es un problema en el norte y sur del país. Esto incluye el uso de sistemas autónomos y algoritmos de procesamiento de imágenes para la detección temprana de actividades sospechosas o ilegales en áreas estratégicas (D. H., 2015). Una alternativa es desarrollar un sistema de drones de vigilancia que permitan rastrear e identificar automáticamente actividades sospechosas en las zonas fronterizas en apoyo a la Policía Nacional del Perú, como movimientos ilegales de personas o contrabando, y detectar personas y vehículos no autorizados en tiempo real haciendo uso del análisis de imágenes y videos capturados por cámaras de vigilancia.

13.Soporte en operaciones de contrainsurgencia (SOCO): Proporciona al Ejército herramientas y análisis avanzados para apoyar las operaciones de contrainsurgencia. Esto incluye la capacidad de identificar y rastrear a grupos insurgentes, así como de predecir y prevenir actividades terroristas (Manyika et al., 2019), particularmente en el VRAEM. Un enfoque viable es la implementación de una plataforma inteligente que permita prevenir ataques terroristas utilizando algoritmos sencillos como regresión logística o máquina de soporte vectorial, sumado a la explotación de conjuntos de datos abiertos como la base de datos mundial sobre terrorismo (GTD) que lo gestiona la Universidad de Maryland.

14.Optimización de recursos y planificación estratégica (ORPE): Ayuda al Ejército a optimizar el uso de sus recursos institucionales y realizar una planificación estratégica más efectiva. Facilita la asignación eficiente de personal, equipos y recursos en función de las necesidades operativas y la optimización de la distribución de fuerzas en el campo de batalla (World Economic Forum, 2021).

15.Desarrollo de capacidades tecnológicas nacionales (DCEN): La implementación de la IA en el Ejército brinda la oportunidad de desarrollar capacidades tecnológicas nacionales en el campo de la IA y la robótica. Esto incluye la promoción de la investigación y el desarrollo de tecnologías innovadoras, así como el fomento de la colaboración con la industria y las instituciones académicas (Frey & Osborne, 2017).

En la Tabla 2, se muestra las oportunidades clave para la implementación de la IA en el Ejército del Perú.

Son quince (15) oportunidades que deben ser aprovechadas e implementadas, técnicamente bajo el liderazgo del Comando de Ciberdefensa y Telemática del Ejército (CITELE), Centro de Investigación Científico y Tecnológico del Ejército (CICTE) y el Instituto Científico y Tecnológico del Ejército. El soporte de todo el proceso debe ser dirigido por la Dirección de Ciencia y Tecnología (DICTECE), con apoyo de la Dirección de Planeamiento del Ejército (DIPLANE), Oficina de Asuntos Jurídicos (OAJE), Dirección de Inteligencia (DIE) y la Oficina de Presupuesto del Ejército (OPRE).

Tabla 2 Oportunidades clave para la implementación de la IA en el Ejército del Perú

Nº	OPORTUNIDADES	DEPENDENCIAS
1	Mejora de la toma de decisiones estratégicas (MTDE)	
2	Robótica y vehículos autónomos (RVAU)	
3	Colaboración y coordinación en tiempo real (CCTR)	
4	Mantenimiento predictivo (MPRE)	CITELE|CICTE| COEDE-ICTE| |DICITECE|DIPLANE|OAJE| DIE| OPRE|
5	Entrenamiento y simulación avanzados (ESIA)	
6	Inteligencia militar mejorada (IMME)	
7	Operaciones logísticas eficientes (OLEF)	
8	Ciberseguridad y defensa cibernética (CDEC):	
9	Apoyo médico y sanitario (AMSA)	
10	Comunicaciones seguras y cifradas (CSCI)	
11	Respuesta humanitaria y desastres naturales (RHDN)	
12	Vigilancia fronteriza (VIFR)	
13	Soporte en operaciones de contrainsurgencia (SOCO)	
14	Optimización de recursos y planificación estratégica (ORPE)	
15	Desarrollo de capacidades tecnológicas nacionales (DCEN)	

V. DISCUSIÓN Y RESULTADOS

Implementar la Inteligencia Artificial en el Ejército del Perú representa un nuevo horizonte en el ámbito de la defensa y seguridad nacional, con el potencial de transformar positivamente los procesos estratégicos, misionales y de soporte. Sin embargo, también plantea diversos desafíos que deben ser abordados de manera efectiva para garantizar su éxito y un uso responsable de esta tecnología emergente. En la sección desafíos identificados, se destacan trece aspectos críticos que el Ejército del Perú debe enfrentar en la implementación de la IA. Entre ellos se encuentran la necesidad de contar con una infraestructura de procesamiento almacenamiento adecuada, personal capacitado en el manejo de la IA, protección de la seguridad y privacidad de los datos, garantizar la interoperabilidad de sistemas, abordar aspectos éticos y de responsabilidad, adaptarse al entorno operativo, integrar los sistemas existentes, asegurar la adquisición y gestión de datos, realizar una implementación gradual y planificada, destinar inversión financiera adecuada, lograr la aceptación y confianza del personal militar, establecer regulaciones y políticas claras, y gestionar los cambios culturales y organizativos que la IA pueda implicar. El Ejército del Perú debe enfrentar estos desafíos de manera integral y estratégica. Para ello, es esencial que diferentes dependencias dentro de la institución asuman roles de liderazgo en la identificación y resolución de cada desafío. A todo esto, se debe sumar el uso de un enfoque multidisciplinario y colaborativo que es fundamental para garantizar el éxito en la implementación de la IA. Sobre las oportunidades que ofrece la IA al Ejército del Perú, se presentan quince áreas clave en las que esta tecnología puede mejorar y fortalecer las capacidades militares. Estas oportunidades incluyen mejorar la toma de decisiones estratégicas, emplear robótica y vehículos autónomos para tareas peligrosas y complejas, facilitar la colaboración y coordinación en tiempo real, implementar estrategias de mantenimiento predictivo, optimizar los programas de entrenamiento y simulación, mejorar la inteligencia militar, agilizar las operaciones logísticas, fortalecer la ciberseguridad y defensa cibernética, mejorar el apoyo médico y sanitario, asegurar comunicaciones seguras y cifradas, mejorar la respuesta humanitaria y en situaciones de desastres naturales, fortalecer la vigilancia fronteriza y en operaciones de contrainsurgencia, optimizar los recursos y la planificación estratégica, y desarrollar capacidades tecnológicas nacionales. Estas oportunidades permiten al Ejército mejorar la eficiencia y efectividad de sus procesos estratégicos, misionales y de soporte, así como ampliar su capacidad para enfrentar nuevos desafíos en el ámbito de la defensa y seguridad nacional. La IA puede ser una herramienta valiosa para fortalecer

la preparación y la capacidad de respuesta ante situaciones críticas, y mejorar la protección y seguridad del personal militar. Para aprovechar al máximo estas oportunidades, es fundamental establecer un enfoque estratégico y de planificación en la implementación de la IA. Esto incluye la identificación de casos de uso prioritarios, la asignación adecuada de recursos financieros y humanos, la promoción de la colaboración con instituciones y expertos externos, la definición de marcos regulatorios y políticas claras, y la adopción de medidas para fomentar la aceptación y confianza del personal militar hacia la IA.

VI. CONCLUSIONES

La implementación de la inteligencia artificial (IA) en el Ejército del Perú presenta una serie de desafíos y oportunidades que deben ser abordados de manera estratégica. Si bien la IA ofrece numerosas ventajas en términos de mejora de la toma de decisiones, optimización de recursos y desarrollo de capacidades avanzadas, también plantea desafíos en áreas como la interoperabilidad de sistemas, la seguridad de datos y la ética. Para superar estos desafíos, es crucial establecer un marco regulatorio y ético sólido que garantice el uso responsable y seguro de la IA en el ámbito militar. Además, se requiere una inversión significativa en infraestructura, tecnología y capacitación para asegurar una implementación exitosa. Es fundamental contar con personal capacitado en IA y establecer programas de formación continua para mantenerse al tanto de los avances y desafíos en esta área. El Ejército del Perú tiene la oportunidad de aprovechar al máximo los beneficios de la IA para fortalecer sus capacidades operativas y estratégicas. Sin embargo, se deben considerar cuidadosamente los aspectos éticos y legales para garantizar un uso responsable y transparente de esta tecnología. La colaboración con instituciones académicas, empresas y otros actores clave puede impulsar la investigación y el desarrollo de soluciones innovadoras basadas en IA.

En última instancia, el uso efectivo de la IA en el Ejército Peruano requerirá un enfoque integral que combine una sólida infraestructura tecnológica, políticas claras, recursos humanos capacitados y una mentalidad abierta a la innovación. Al enfrentar los desafíos y aprovechar las oportunidades de la IA, el Ejército del Perú puede avanzar hacia un futuro estratégico sólido y prepararse para los desafíos y exigencias cambiantes del entorno de defensa y seguridad nacional.

AGRADECIMIENTOS

El autor agradece al Grupo de Análisis, Seguridad y Sistemas de la Universidad Complutense de Madrid y al por permitir desarrollar la investigación y dotar de todas las facilidades.

SOBRE LOS AUTORES

Carlos Quinto Huamán, es investigador asociado del Grupo de Investigación Análisis, Seguridad y Sistemas de Facultad de Informática de la Universidad Complutense de Madrid, donde participa en proyectos europeos dentro del marco Horizonte Europa.

Rosa Marcela Picón Huacarpuma, es Ingeniero de Sistemas por la Universidad Nacional Jorge Basadre Grohmann de Tacna y Magíster en Project Management por la Universidad ESAN. Actualmente se desempeña como especialista en soluciones de información del Grupo Cibernos.

REFERENCIAS

Schepman, A., and Rodway, P. (2020). Initial validation of the general attitudes towards Artificial Intelligence Scale. Comput. Hum. Behav. Rep. 1:100014. doi: 10.1016/j.chbr.2020.100014

Laricchia, F. (2021). Global smart speaker market share 2016-2021:by vendor. Hamburg: Statista.

McNeish, D., Kamanda Dede-Benefor, A., and Taylor, I. (2020). Research roadmap: Trust, ethics and public perceptions of artificial intelligence and autonomous systems in defence and security. DSTL/TR122612. Porton Down: Defence Science Technology Laboratories.

Taddeo, M., McNeish, D., Blanchard, A., and Edgar, E. (2021). Ethical principles for artificial intelligence in national defence. Philos. Technol. 34, 1707–1729. doi: 10.1007/s13347-021-00482-3

Defense Innovation Board (2019). AI principles: Recommendations on the ethical use of artificial intelligence by the department of defense. Available online at: https://media.defense.gov/2019/Oct/31/2002204458/-1/-1/0/DIB_AI_PRINCIPLES_PRIMARY_DOCUMENT.PDF (accessed April 24, 2023).

UK Ministry of Defence (2022). Defence artificial intelligence strategy. Available online at: https://www.gov.uk/government/publications/defence-artificial-intelligence-strategy/defence-artificial-intelligence-strategy (accessed April 24, 2023).

Gillath, O., Ai, T., Branicky, M. S., Keshmiri, S., Davison, R. B., and Spaulding, R. (2021). Attachment and trust in artificial intelligence. Comput. Hum. Behav. 115:106607. doi: 10.1016/j.chb.2020.106607

Wasilow, S., and Thorpe, J. B. (2019). Artificial intelligence, robotics, ethics, and the military: A Canadian perspective. AI Mag. 40, 37–48. doi: 10.1609/aimag.v40i1.2848

Morgan, F., Boudreaux, B., Lohn, A., Ashby, M., Curriden, C., Klima, K., et al. (2020). Military applications of artificial intelligence: Ethical Concerns in an Uncertain World. Santa Monica, CA: RAND Corporation. doi: 10.7249/RR3139-1

West, D. M. (2018). How artificial intelligence is transforming the world. Brookings Institution.

Bughin, J., Hazan, E., Ramaswamy, S., Chui, M., Allas, T., Dahlström, P., & Henke, N. (2018). Artificial intelligence: The next digital frontier? McKinsey Global Institute.

Arrieta, A. B., Díaz-Rodríguez, N., Del Ser, J., Bennetot, A., Tabik, S., Barbado, A., ... & Herrera, F. (2020). Explainable artificial intelligence (XAI): Concepts, taxonomies, opportunities and challenges toward responsible AI. Information Fusion, 58, 82-115. https://doi.org/10.1016/j.inffus.2019.12.012