Analysis of Optimal Digital Security Systems for the Armed Forces

Tipo de contribución: Work in Progress-WP

Formato: Full Paper (FP): reviews

George Kevin Ramírez Vargas[1], Luis Alex Alzamora de los Godos Urcia[2], Fiorella Sthefany Valladolid Marcos[2], Jully Pahola Calderón Saldaña[3], Marlene Pilar Aguilar Suares[1], María Fanny Aparicio Fernández[1], Javier Alejandro Pineda Medina[4]

Organización: 1: Escuela de Oficiales de la Fuerza Aérea del Perú - EOFAP - (PE); 2: Universidad Norbert Wiener - Programa Académico de Enfermería (PE); 3: Universidad San Martín de Porras - Escuela Profesional de Obstetricia (PE), 4: Pontificia Universidad Católica del Perú - Maestría en Gerencia Social - (PE);

Autor corresponsal : Dr. Luis Alex Alzamora de los Godos Urcia (Universidad Norbert Wiener - (PE), ID: 2566

Abstract* — *This article examines the modernization of security systems within the Peruvian Armed Forces through the integration of cutting-edge technologies, including facial and ocular recognition, multimodal biometrics, artificial intelligence (AI), and cloud-based data management. These innovations provide robust solutions for strengthening access control and safeguarding military installations. AI plays a pivotal role in automating surveillance processes and enhancing threat prediction capabilities, while cloud technologies facilitate secure and efficient data handling. The implementation of these advanced systems is projected to significantly reduce security vulnerabilities and improve overall operational efficiency in response to evolving threats. A phased adoption strategy is recommended, balancing readily available technologies with innovative approaches to fortify the defense infrastructure of military bases across Peru.

Keywords: Facial Recognition, Ocular Recognition, Multimodal Biometrics, Artificial Intelligence, Cloud Security, Peruvian Armed Forces

I. Introducción

La seguridad de las instalaciones militares es un componente fundamental para garantizar la defensa y la soberanía de cualquier nación. En el caso de Perú, las Fuerzas Armadas enfrentan desafíos considerables debido a la obsolescencia de sus sistemas de seguridad, especialmente en lo que respecta al control de acceso en sus bases militares. En la actualidad, los métodos manuales de verificación de identidades empleados por el personal militar no solo resultan lentos y propensos a errores humanos, sino que también presentan vulnerabilidades susceptibles de ser explotadas por actores malintencionados. Esta situación pone de manifiesto la necesidad urgente de modernizar los sistemas de seguridad, adoptando tecnologías más avanzadas que respondan eficazmente a las demandas de un entorno de seguridad cada vez más complejo y dinámico (Alejandra, 2016; Razikin & Soewito, 2022).

Dentro de las tecnologías emergentes, los sistemas de reconocimiento facial y ocular se presentan como soluciones robustas. Estos sistemas emplean algoritmos de inteligencia artificial (IA) que permiten la identificación precisa de individuos en tiempo real, lo que los convierte en herramientas poderosas para el control de acceso en entornos sensibles, como las bases militares. El reconocimiento facial ha ganado popularidad debido a su capacidad para procesar grandes volúmenes de datos y realizar comparaciones en fracciones de segundo, lo cual es crucial en instalaciones con un alto flujo de personal. Además, su eficacia se extiende a la identificación de individuos en diversas condiciones ambientales, lo que refuerza su aplicabilidad en bases militares de alta seguridad (Cascone, Pero, & Proença, 2023; Devi et al., 2022).

Otra tecnología relevante es el uso de sistemas de autenticación biométrica multimodal, que combinan varios métodos de identificación, como el reconocimiento de huellas dactilares, iris y rostro. Estos sistemas no solo mejoran la precisión de la identificación, sino que también proporcionan una capa adicional de seguridad al requerir múltiples formas de verificación antes de conceder acceso. Esta redundancia reduce considerablemente las posibilidades de fallos o suplantaciones, lo que los convierte en una opción atractiva para fortalecer la seguridad en entornos militares. No obstante, la implementación de sistemas biométricos multimodales puede resultar costosa y técnicamente compleja, lo que plantea un reto en cuanto a su viabilidad en función de las restricciones presupuestarias y logísticas de las Fuerzas Armadas peruanas (Mansour et al., 2024).

La adopción de tecnologías basadas en la nube para la gestión de datos de seguridad es otra alternativa que merece consideración. Los sistemas en la nube permiten la

centralización y actualización continua de la información, lo que facilita una gestión más eficiente y segura de los datos. Sin embargo, esta tecnología depende de la infraestructura de Internet, lo que plantea riesgos potenciales de vulnerabilidades cibernéticas si no se implementan mecanismos de seguridad adecuados. Por lo tanto, la integración de la nube debe considerar estos aspectos críticos para evitar posibles fallos en la protección de la información sensible (Douzis et al., 2018; Mohammed et al., 2023).

A pesar de las opciones más avanzadas, existen soluciones accesibles y menos complejas que también pueden ser implementadas como medidas iniciales para mejorar la seguridad en las bases militares. Entre estas opciones se incluyen los sistemas de control de acceso basados en tarjetas RFID y los sistemas de videovigilancia mejorados con análisis en tiempo real. Aunque estos sistemas son menos sofisticados que las soluciones biométricas o basadas en IA, ofrecen una mejora sustancial respecto a las prácticas actuales y pueden ser desplegados con menores costos y sin necesidad de una infraestructura tan compleja (Lenko, 2021).

Cada una de estas tecnologías presenta ventajas y desventajas que deben ser evaluadas cuidadosamente en el contexto de las Fuerzas Armadas peruanas. La decisión de adoptar una tecnología específica debe considerar no solo su efectividad en mejorar la seguridad, sino también su costo, la complejidad en su instalación y mantenimiento, y la capacidad del personal para operar eficientemente. Este artículo tiene como objetivo analizar los sistemas de seguridad más óptimos para las Fuerzas Armadas del Perú, evaluando su efectividad, factibilidad económica y operativa. A través de una comparación detallada de las distintas tecnologías disponibles, se busca proporcionar una guía informada para la modernización de los sistemas de seguridad en las bases militares del país.

II. MATERIAL Y MÉTODOS

Con el objetivo de identificar y evaluar los sistemas de seguridad óptimos para las Fuerzas Armadas, se llevó a cabo una revisión exhaustiva de la literatura existente mediante una estrategia de búsqueda sistemática. Este enfoque permitió obtener una visión integral de las tecnologías más avanzadas en el ámbito de la seguridad, la inteligencia artificial (IA) y el reconocimiento facial, relevantes para la modernización de los sistemas de seguridad en contextos militares.

La búsqueda de la literatura se realizó en bases de datos académicas de reconocido prestigio, tales como SciELO, ScienceDirect, IEEE Xplore y SpringerLink. Estas plataformas fueron seleccionadas debido a su amplia cobertura de artículos científicos y tecnológicos en los campos de la seguridad, la IA y el reconocimiento facial. Se utilizaron combinaciones de términos clave específicas, tales como "sistemas de seguridad peatonal," "reconocimiento facial," "inteligencia artificial" y "fuerzas armadas," para garantizar la identificación de estudios relevantes y actuales relacionados con el tema de investigación.

El proceso de selección de los artículos incluyó una revisión rigurosa de los títulos, resúmenes y palabras clave, con el fin de asegurar la relevancia de cada fuente en relación con el objetivo del estudio. Para mantener un enfoque actualizado, se priorizaron los artículos publicados entre 2015 y 2023, lo que permitió asegurar la inclusión de investigaciones recientes y relevantes en el campo de estudio. Se excluyeron aquellos artículos que no presentaban un enfoque claro en la aplicación de tecnologías avanzadas de seguridad, como la IA y el reconocimiento facial, en contextos militares, o que no abordaban específicamente la optimización de los sistemas de seguridad en bases militares.

El análisis final incluyó un total de 70 artículos que fueron seleccionados para un análisis detallado. Estos estudios proporcionaron una base sólida para la evaluación de las ventajas, desafíos y limitaciones de los sistemas de seguridad peatonal en entornos militares, y permitieron realizar una comparación crítica entre diversas tecnologías y enfoques utilizados en la protección de instalaciones militares. Este enfoque metodológico garantiza que el análisis presentado en este artículo esté basado en la evidencia más actual y relevante, ofreciendo una evaluación integral y fundamentada de las opciones tecnológicas disponibles para mejorar la seguridad en las Fuerzas Armadas.

Este proceso sistemático asegura la objetividad y validez de los hallazgos, permitiendo obtener conclusiones informadas y útiles para la optimización de los sistemas de seguridad en el contexto específico de las Fuerzas Armadas del Perú.

DESARROLLO TEORICO

El Entorno Tecnológico en la Seguridad Militar

En el contexto actual de transformación digital, las fuerzas armadas enfrentan desafíos cada vez más complejos en la protección de sus instalaciones, personal y recursos estratégicos. La seguridad militar ha trascendido el uso exclusivo de barreras físicas y la vigilancia humana, integrando tecnologías avanzadas como la inteligencia artificial (IA), la biometría y la computación en la nube como componentes esenciales para la defensa y la soberanía nacional. Estas herramientas no solo optimizan los procesos de vigilancia y control de acceso, sino que también permiten una gestión más eficiente y segura de los datos, así como una respuesta más ágil y precisa frente a amenazas emergentes (Douzis et al., 2018).

En este marco, el concepto de vigilancia tecnológica se ha consolidado como un elemento clave para la seguridad de las fuerzas armadas. La vigilancia tecnológica implica la

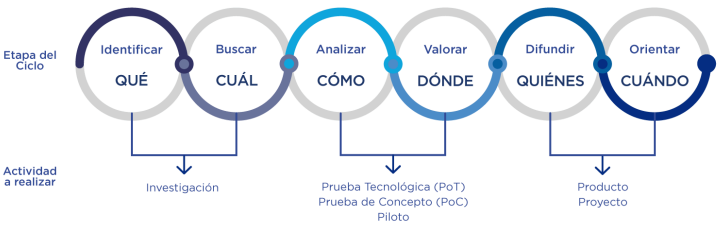
monitorización constante del entorno tecnológico y de posibles amenazas, permitiendo a las instituciones militares anticiparse y responder proactivamente a innovaciones que podrían comprometer su operatividad. Este enfoque no solo facilita la identificación de nuevas tecnologías y sistemas de armamento avanzados, sino también de tácticas emergentes en ciberseguridad que podrían poner en riesgo la seguridad nacional.

La incorporación de tecnologías como la IA y el reconocimiento facial en la seguridad militar no se limita a la detección y prevención de intrusiones físicas. Estos sistemas permiten un análisis en tiempo real de grandes volúmenes de datos, lo que incrementa significativamente la capacidad de respuesta ante ataques cibernéticos y amenazas físicas. La ciberdefensa, por su parte, se ha convertido en un pilar fundamental para proteger infraestructuras críticas, datos sensibles y redes de comunicación estratégicas, asegurando la integridad operativa de las fuerzas armadas frente a adversarios que emplean tácticas cibernéticas sofisticadas.

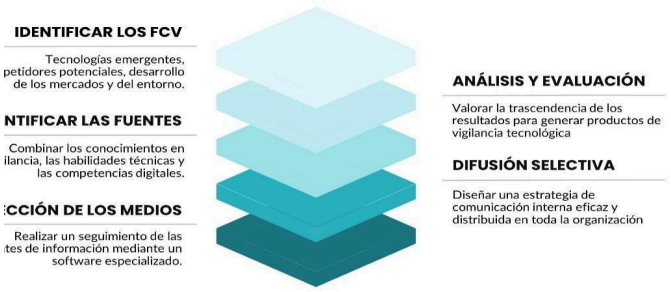
Asimismo, la vigilancia tecnológica no se restringe únicamente al ámbito defensivo, sino que también abarca la evaluación y adopción de tecnologías que puedan mejorar la eficiencia operativa y la protección de infraestructuras críticas. Este enfoque proactivo garantiza que las fuerzas armadas mantengan una ventaja competitiva en un entorno geopolítico caracterizado por la rápida evolución tecnológica. La capacidad de adaptarse e integrar innovaciones tecnológicas en sus estrategias de defensa permite a las instituciones militares no solo responder a amenazas inmediatas, sino también fortalecer su postura frente a desafíos futuros.

En conclusión, el entorno tecnológico actual exige que las fuerzas armadas adopten un enfoque integral y dinámico en la gestión de la seguridad, combinando herramientas avanzadas de vigilancia y análisis con estrategias de ciberdefensa robustas. La vigilancia tecnológica, al facilitar la anticipación de amenazas y la implementación de soluciones innovadoras, se posiciona como un componente esencial para garantizar la seguridad y la soberanía nacional en la era digital.

Gráfico 1: Fases de la Vigilancia Tecnológica



.



Fuente: Lisa Institute, Guía Práctica

Estrategias de Vigilancia Tecnológica en el Ámbito Militar

Según el Lisa Institute (2023), la implementación de la vigilancia tecnológica requiere el desarrollo de estrategias específicas que permitan probar, evaluar y ejecutar productos tecnológicos de manera eficiente. Este proceso se estructura en fases secuenciales que aseguran la integración adecuada de nuevas tecnologías en los entornos institucionales. Las fuerzas armadas, como instituciones estratégicas, están particularmente sujetas a este tipo de normativas y procedimientos, dado que la incorporación de tecnologías avanzadas puede tener implicancias significativas en la seguridad nacional y en la operatividad de sus sistemas.

El enfoque metodológico propuesto por el Lisa Institute se organiza en torno a cuatro ejes fundamentales que guían la implementación y gestión de la vigilancia tecnológica:

- Eje Tecnológico: Centrado en la identificación, evaluación y adopción de tecnologías emergentes que puedan ser aplicadas en la seguridad y defensa. Incluye el análisis de innovaciones en inteligencia artificial, ciberseguridad, y sistemas biométricos.
- Eje de Coordinación y Superación: Este eje promueve la colaboración interinstitucional y la capacitación continua del personal militar para asegurar una adaptación eficaz a las nuevas tecnologías.
- Eje de Información: Enfocado en la recopilación, análisis y difusión de información relevante sobre avances tecnológicos y amenazas emergentes. Este eje es esencial para la toma de decisiones informadas.

Eje de Gestión y Mejora Continua: Implica la evaluación constante de los procesos tecnológicos implementados, con el objetivo de optimizar su funcionamiento y adaptarlos a las necesidades cambiantes del entorno operativo.

Complementando este enfoque, la Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento (2023) define la vigilancia tecnológica como un proceso organizado, selectivo y sistemático, cuyo objetivo es minimizar los riesgos asociados a la adopción de nuevas tecnologías y evitar decisiones que puedan conducir a cambios abruptos o no planificados dentro de las instituciones. Este enfoque preventivo y estructurado permite a las organizaciones, incluidas las fuerzas armadas, anticiparse a posibles desafíos tecnológicos y estratégicos.

El modelo propuesto por esta agencia se representa mediante un ciclo que abarca desde el input hasta el output, describiendo subprocesos detallados que reflejan cada etapa de la vigilancia tecnológica. Estos subprocesos incluyen la identificación de necesidades tecnológicas, la evaluación de riesgos, la implementación controlada de innovaciones, y la retroalimentación continua para ajustar y mejorar los sistemas existentes.

En el contexto militar, la aplicación de estas estrategias y modelos no solo facilita la integración segura de tecnologías emergentes, sino que también fortalece la capacidad de las fuerzas armadas para adaptarse a un entorno geopolítico y tecnológico en constante evolución. La vigilancia tecnológica, cuando se implementa de manera rigurosa y sistemática, se convierte en una herramienta clave para mantener la superioridad operativa y proteger la infraestructura crítica frente a amenazas tanto físicas como cibernéticas.

Gráfico 2: Etapas del Ciclo de la Vigilancia Tecnológica

Fuente: Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento, Tecnologías emergentes

Reconocimiento Facial: Precisión y Adaptabilidad en la Seguridad Militar

El reconocimiento facial se ha consolidado como una de las tecnologías más avanzadas y prometedoras en el ámbito de la seguridad militar, gracias a su capacidad para identificar individuos en tiempo real mediante el análisis detallado de patrones biométricos faciales. Esta tecnología no solo optimiza el control de acceso en instalaciones militares, sino que también refuerza la vigilancia perimetral y la protección de infraestructuras críticas, proporcionando un nivel de seguridad superior al de los métodos tradicionales (Cascone, Pero, & Proença, 2023).

La precisión de los sistemas de reconocimiento facial ha mejorado significativamente en los últimos años, alcanzando tasas de exactitud que permiten la identificación confiable de personas incluso en condiciones adversas, como baja iluminación o ángulos no convencionales. Además, la adaptabilidad de estos sistemas facilita su integración con plataformas de vigilancia existentes, permitiendo el monitoreo simultáneo de grandes volúmenes de personas sin necesidad de intervención humana constante. Esto no solo reduce la carga operativa sobre el personal de seguridad, sino que también disminuye la posibilidad de errores humanos en la identificación de potenciales amenazas.

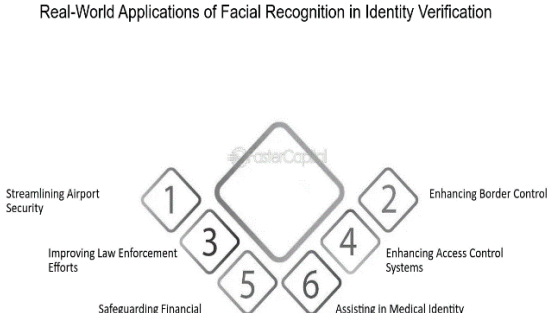
La implementación de sistemas de reconocimiento facial en las fuerzas armadas es fundamental, considerando la importancia estratégica de proteger tanto al personal militar como a las instalaciones clave. Esta tecnología no solo mejora la seguridad física, sino que también contribuye a la gestión eficiente de la información y la respuesta rápida ante situaciones de riesgo, factores cruciales en entornos militares donde la toma de decisiones oportuna es vital.

En el contexto global, el reconocimiento facial puede sofisticar los sistemas de seguridad militar en múltiples aspectos:

- Control de Acceso Automatizado: Mejora la seguridad en puntos de entrada mediante la identificación precisa de personal autorizado y la detección de intrusos en tiempo real.
- Vigilancia en Tiempo Real: Permite el monitoreo continuo de áreas estratégicas, integrándose con sistemas de cámaras para identificar comportamientos sospechosos o no autorizados.
- Gestión de Identidades: Facilita la creación de bases de datos biométricas que mejoran la administración del personal y la coordinación de operaciones.
- Respuesta Rápida a Amenazas: Acelera la identificación de posibles infiltrados o individuos buscados, optimizando la capacidad de respuesta ante amenazas internas o externas.

La siguiente ilustración (no incluida aquí) presenta de manera visual cómo el reconocimiento facial puede integrarse en diferentes niveles de la infraestructura militar, resaltando su impacto en la seguridad operativa, la eficiencia logística y la protección estratégica de las fuerzas armadas.

Gráfico 3: Roles del Reconocimiento Facial



Fuente: FasterCapital, Verificación de identidad de AAI

Importancia de Bases de Datos Robustas en Sistemas de Reconocimiento Facial

Las bases de datos desempeñan un papel fundamental en la efectividad de los sistemas de reconocimiento facial, al servir como repositorios de imágenes faciales y otros datos biométricos que los algoritmos utilizan para identificar características distintivas. Estas bases de datos permiten el entrenamiento de modelos de aprendizaje automático, facilitando la mejora continua en la precisión del reconocimiento y la reducción de errores, como falsos positivos y falsos negativos. La diversidad de los datos almacenados es igualmente crucial, ya que contribuye a mitigar sesgos algorítmicos y garantiza que el sistema funcione de manera equitativa en diferentes contextos demográficos.

Asimismo, la actualización periódica de las bases de datos es esencial para mantener la precisión del sistema, ya que la variabilidad de las características faciales a lo largo del tiempo puede afectar el rendimiento del reconocimiento. A la par, la implementación de protocolos de seguridad robustos es indispensable para proteger la privacidad de los individuos, resguardando la información biométrica de accesos no autorizados.

Durante el proceso de operación del reconocimiento facial, se generan vectores característicos de dimensiones reducidas que deben ser comparados con los datos previamente almacenados en la base de datos. Este procedimiento de cotejo es esencial para la identificación precisa de los individuos, destacando la necesidad de una estructura de datos eficiente y bien organizada (Cadena, J., Humberto, R., Flores, G., Chancúsig, J., & Guaypatín, O., 2017).

Gráfico 4: Relación de Base de Datos con un Vector

Fuente: Modelo de Sistema de Reconocimiento Facial para el Control de la Trata de Personas

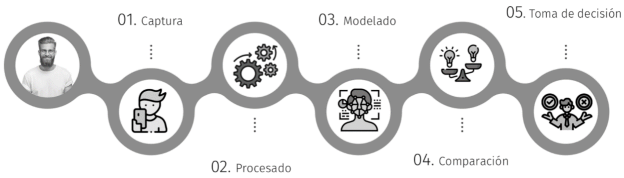
El gráfico ilustra el proceso mediante el cual una imagen presentada se compara con los rostros almacenados en la base de datos. Este procedimiento se realiza a través de sistemas como OpenFace, que permiten la extracción de características específicas y detalladas de cada rostro, facilitando así una mejora en el reconocimiento de la imagen procesada en relación con las ya registradas.

Estimaciones y Viabilidad

La implementación de sistemas de reconocimiento facial resulta viable para bases militares interesadas en modernizar sus protocolos de seguridad. Aunque la inversión inicial puede ser considerable, esta tecnología proporciona beneficios a largo plazo, destacando la precisión en la identificación y la reducción de costos operativos. Además, su capacidad de adaptarse a diversos entornos y condiciones convierte al reconocimiento facial en una solución flexible y robusta.

El proceso de reconocimiento facial comienza con un input (la imagen de entrada) y culmina con un output, que consiste en la confirmación de si la imagen ha sido reconocida o no. Este procedimiento se ejecuta mediante programas diseñados para comparar la imagen entrante con aquellas previamente procesadas y almacenadas en la base de datos.

Gráfico 5: Proceso de Reconocimiento Facial



Fuente: Mobbeel, Reconocimiento Facial

Reconocimiento Ocular: Seguridad de Alto Nivel

El reconocimiento ocular es una tecnología biométrica de alta precisión utilizada en el ámbito de la seguridad militar. Este sistema se basa en el análisis del patrón único del iris de cada individuo, proporcionando una identificación sumamente confiable, incluso en condiciones adversas. Su aplicación es especialmente valiosa en escenarios donde se requiere un máximo nivel de seguridad, como el control de acceso a áreas sensibles dentro de bases militares (Devi et al., 2022).

Factibilidad y Operatividad

Aunque la instalación de sistemas de reconocimiento ocular implica una inversión considerable en equipos especializados, su implementación es factible en entornos que demandan altos estándares de seguridad. Esta tecnología demuestra una operatividad eficiente en diversas

condiciones, consolidándose como una opción preferente en instalaciones de máxima seguridad.

Tabla 1: Ventajas y Limitaciones de los Tipos de Reconocimiento

Tecnología Biométrica	Ventajas	Limitaciones
Reconocimiento Facial	Alta precisión, integración con vigilancia, adaptable	Costo inicial elevado, preocupaciones de privacidad
Reconocimiento Ocular	Precisión extrema, fiabilidad en condiciones adversas	Costo de instalación, necesidad de equipos especializados

Fuente: Elaboración propia

Inteligencia Artificial: Automatización y Predicción

La inteligencia artificial (IA) ha emergido como un componente clave en la seguridad militar moderna, facilitando la automatización de tareas de vigilancia y la predicción de amenazas potenciales. Los sistemas impulsados por IA son capaces de procesar grandes volúmenes de datos para identificar patrones anómalos, lo que permite una respuesta proactiva ante posibles incidentes de seguridad (Makhdoom et al., 2019).

El papel de la IA en el reconocimiento facial y ocular ha evolucionado significativamente, mejorando la precisión y confiabilidad de estos sistemas. La capacidad de la IA para interpretar patrones complejos ha optimizado el rendimiento de los programas desarrollados, asegurando su funcionamiento efectivo en diversos escenarios y permitiendo la gestión de eventos en tiempo real con alta eficiencia. Sin embargo, no se pueden ignorar los riesgos éticos asociados, especialmente aquellos relacionados con la violación de la privacidad de los usuarios. Estos aspectos constituyen elementos fundamentales en el análisis del caso de estudio sobre la seguridad en el control de acceso de las Fuerzas Armadas que estamos desarrollando.

Gráfico 6: Roles de la Inteligencia Artificial en el Reconocimiento Facial

Fuente: Elaboración propia con datos de FasterCapital

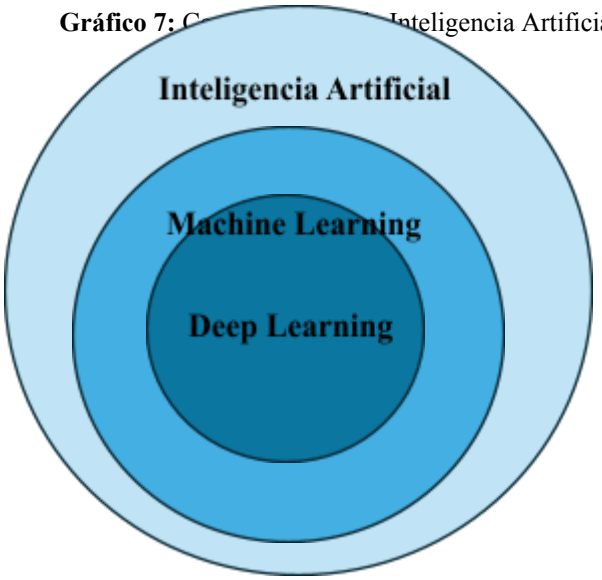
.

Aprendizaje de Máquina

El aprendizaje de máquina se basa en el uso de algoritmos, los cuales constituyen una secuencia de pasos diseñados para resolver problemas específicos. Estos algoritmos procesan datos numéricos como entrada y generan una respuesta o acción como salida. Diversos tipos de algoritmos pueden emplearse para codificar instrucciones que permiten la creación y automatización de modelos de reconocimiento, facilitando su entrenamiento y mejora continua a través de prácticas repetidas.

Es fundamental comprender las diferencias entre los dos enfoques principales dentro del ámbito de la inteligencia artificial: el Machine Learning tradicional y el Deep Learning. Mientras que el primero se enfoca en algoritmos que requieren intervención humana para la selección de características relevantes, el Deep Learning utiliza redes neuronales profundas que permiten el aprendizaje autónomo de patrones complejos, optimizando así el rendimiento en tareas como el reconocimiento facial y ocular.

Gráfico 7: C[illegible]nteligencia Artificial



Fuente: Elaboración propia

Tabla 2: Diferencias entre Machine Learning y Deep Learning

Aspecto	Machine Learning	Deep Learning
Datos	Funciona con menos datos	Requiere grandes volúmenes de datos
Intervención Humana	Necesita que humanos definan características	Aprende características automáticamente
Estructura	Utiliza algoritmos más simples como SVM o árboles de decisión	Usa redes neuronales profundas (CNN, RNN)
Hardware	Puede funcionar con CPUs	Necesita GPUs o TPUs para procesar
Tiempo de Entrenamiento	Rápido en comparación	Puede ser muy lento
Precisión	Puede ser menos preciso en tareas complejas	Muy preciso en tareas complejas, pero requiere más recursos

Fuente: Elaboración Propia

Redes Neuronales

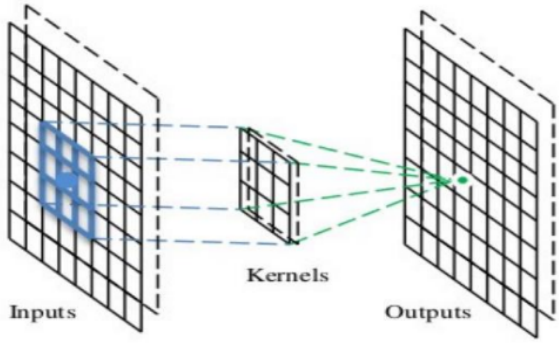
En el reconocimiento facial, el Deep Learning es ampliamente utilizado debido a la eficacia de las redes neuronales profundas, especialmente las redes neuronales convolucionales (Convolutional Neural Networks, CNNs), en el análisis de imágenes. Estas redes tienen la capacidad de aprender automáticamente las características más relevantes de los rostros, como la textura, las formas y los patrones faciales, sin la necesidad de programación explícita por parte de un ingeniero.

Redes Neuronales Convolucionales (CNNs)

Las CNNs son un tipo especializado de red neuronal diseñado para el procesamiento de datos visuales. Se emplean en sistemas de reconocimiento facial porque permiten un análisis detallado de las imágenes, identificando patrones complejos como la estructura geométrica y la textura del rostro. Estas redes son especialmente eficaces en la detección de rostros bajo diversas condiciones, incluyendo variaciones de iluminación, ángulos y expresiones faciales. Además, facilitan la verificación e identificación de personas mediante la comparación de imágenes faciales con bases de datos de rostros previamente registrados.

Como se muestra en la figura, las redes convolucionales trabajan con matrices bidimensionales aplicando filtros o kernels sobre las imágenes. Estos filtros actúan como máscaras que extraen características específicas, permitiendo obtener resultados precisos en el reconocimiento facial.

Gráfico 8: Filtración de una imagen



Fuente: Deep Learning: Redes convolucionales

Implementación y Eficiencia

La integración de la inteligencia artificial (IA) en los sistemas de seguridad militar no solo optimiza la vigilancia, sino que también disminuye la carga operativa al reducir la necesidad de intervención humana. La IA puede incorporarse en infraestructuras de seguridad ya existentes, facilitando una adopción fluida y generando un impacto significativo en la efectividad de las operaciones de seguridad.

Sistemas de Seguridad en la Nube: Flexibilidad y Escalabilidad

La computación en la nube está transformando la gestión de datos en el ámbito de la seguridad militar. Estos sistemas permiten almacenar y procesar grandes volúmenes de información de forma centralizada, lo que facilita la monitorización en tiempo real y la actualización constante de datos. La flexibilidad que ofrece esta tecnología supera a la de los sistemas tradicionales, permitiendo a las fuerzas armadas escalar sus operaciones de seguridad según las necesidades específicas del momento (Mohammed et al., 2023).

Estabilidad y Mantenimiento

Aunque la migración a sistemas basados en la nube implica una inversión inicial considerable en infraestructura y medidas de ciberseguridad, los beneficios a largo plazo son notables. Estos incluyen una reducción en los costos operativos y una mayor capacidad de respuesta frente a amenazas emergentes. La escalabilidad de estos sistemas resulta especialmente útil en entornos militares, donde la adaptación rápida a nuevos desafíos es esencial.

Tabla 3: Estimaciones y Comparaciones de Sistemas de Seguridad

Tecnología	Estimaciones de Viabilidad	Nivel de Seguridad Ofrecido	Requerimientos de Mantenimiento
Reconocimiento Facial	Alta, viable en múltiples entornos	Alta	Medio
Reconocimiento Ocular	Media-Alta, ideal para alta seguridad	Muy Alta	Alto
Seguridad Basada en la Nube	Alta, excelente para escalabilidad	Alta	Bajo-Medio
Inteligencia Artificial (IA)	Alta, adaptable y eficiente	Muy Alta	Bajo-Medio

Fuente: Elaboración propia

Importancia de la Seguridad Militar en el Entorno Tecnológico Actual

La adopción de tecnologías avanzadas es fundamental para la protección de instalaciones militares en un contexto global cada vez más complejo. La combinación de sistemas biométricos, inteligencia artificial y computación en la nube constituye un enfoque integral para la seguridad, que no solo incrementa la precisión y eficiencia, sino que también facilita la adaptación rápida a nuevas amenazas. En un mundo donde la información y la tecnología son tan estratégicas como la fuerza física, es imperativo que las fuerzas armadas dispongan de las herramientas más avanzadas para mantener su ventaja competitiva (Enge et al., 2022).

El desarrollo de un entorno de seguridad tecnológicamente avanzado no representa únicamente una inversión en infraestructura, sino también en la resiliencia y capacidad de respuesta de las fuerzas armadas. La protección de información crítica, el control del acceso a áreas sensibles y la capacidad de anticipar amenazas antes de que se materialicen son elementos esenciales para la defensa nacional en el siglo XXI.

DISCUSIÓN

La seguridad en las instalaciones militares representa un pilar fundamental para la protección nacional, especialmente en un entorno global donde las amenazas cibernéticas y físicas evolucionan con rapidez. Este artículo ha explorado diversas tecnologías emergentes, como el reconocimiento facial, ocular y los sistemas de autenticación biométrica multimodal, todas con un gran potencial para fortalecer la seguridad en las bases militares peruanas.

El reconocimiento facial ha demostrado ser una herramienta eficaz en el control de acceso debido a su capacidad para procesar grandes volúmenes de datos en tiempo real. No obstante, surgen preocupaciones en torno a la privacidad y el elevado costo inicial de su implementación. Aunque se destaca su precisión y velocidad, es crucial considerar cómo estas tecnologías pueden integrarse en infraestructuras existentes sin comprometer la confidencialidad del personal militar. En contraste, el reconocimiento ocular, aunque más costoso y especializado, ofrece una precisión superior en entornos que requieren seguridad extrema, como las áreas restringidas de las bases. A diferencia del reconocimiento facial, este sistema es menos susceptible a errores provocados por factores ambientales, como la iluminación o las posiciones faciales, lo que lo convierte en una opción fiable para situaciones críticas. Sin embargo, su alto costo limita su adopción masiva en todas las instalaciones.

La computación en la nube emerge como una tecnología que, aunque proporciona escalabilidad y flexibilidad, introduce riesgos vinculados a la dependencia de la infraestructura de internet y a posibles vulnerabilidades cibernéticas. Esta consideración es esencial, ya que cualquier interrupción en la conectividad podría comprometer la seguridad de las instalaciones. Por lo tanto, su implementación debe evaluarse en función de la solidez de la infraestructura tecnológica del país y la capacidad de las Fuerzas Armadas para mitigar estos riesgos.

El uso de inteligencia artificial (IA) en los sistemas de seguridad evidencia su capacidad para automatizar procesos y predecir amenazas de manera eficaz. Sin embargo, la dependencia de grandes volúmenes de datos para entrenar los modelos de IA plantea desafíos operativos y de mantenimiento, así como la necesidad de garantizar que los datos utilizados no introduzcan sesgos en los sistemas de identificación. Estos factores deben ser cuidadosamente considerados para evitar vulnerabilidades en los procesos automatizados.

A lo largo del análisis, se ha subrayado que, aunque estas tecnologías representan una mejora significativa respecto a los métodos de seguridad tradicionales, cada una conlleva desafíos económicos y logísticos que deben ser evaluados antes de su adopción. La viabilidad de estas soluciones dependerá del presupuesto disponible, la complejidad de su integración con los sistemas actuales y la capacitación del personal militar para operarlas de manera eficiente.

La modernización de los sistemas de seguridad en las Fuerzas Armadas del Perú es fundamental para enfrentar las amenazas contemporáneas y proteger eficazmente sus instalaciones. Las tecnologías emergentes, como el reconocimiento facial, ocular, la biometría multimodal y los sistemas basados en la nube, ofrecen soluciones robustas y adaptables que pueden mejorar significativamente la eficiencia y efectividad de la seguridad militar.

No obstante, estas innovaciones presentan desafíos relacionados con costos, implementación y protección de la privacidad. Su adopción debe ser planificada y gradual, evaluando cuidadosamente su viabilidad operativa y financiera dentro del contexto nacional. El reconocimiento facial, por su adaptabilidad y velocidad, puede constituir una solución intermedia, mientras que el reconocimiento ocular se reserva para áreas que demanden un nivel de seguridad extremo.

En última instancia, una estrategia integral que combine estas tecnologías con una infraestructura de ciberseguridad robusta permitirá a las Fuerzas Armadas peruanas fortalecer sus capacidades defensivas y mantenerse a la vanguardia frente a las amenazas actuales. El éxito radicará en equilibrar la adopción de nuevas tecnologías con las limitaciones presupuestarias y logísticas, asegurando una implementación efectiva y sostenible a largo plazo. .

CONCLUSIÓN

La integración de tecnologías emergentes como la inteligencia artificial, el aprendizaje automático y las redes neuronales convolucionales representa un avance significativo en la seguridad militar, ya que permiten un análisis más preciso y eficiente de datos biométricos, mejorando el control de acceso y la vigilancia en tiempo real.

El reconocimiento facial y ocular, junto con la biometría multimodal, ofrecen diferentes niveles de precisión y adaptabilidad según el entorno, siendo el reconocimiento ocular más fiable en áreas de alta seguridad, mientras que el reconocimiento facial es más versátil para aplicaciones masivas, aunque presenta desafíos en términos de privacidad y costos de implementación.

La computación en la nube proporciona flexibilidad y escalabilidad en la gestión de la seguridad militar, facilitando el almacenamiento y procesamiento de grandes volúmenes de datos. Sin embargo, esta tecnología también introduce riesgos cibernéticos que requieren inversiones en infraestructura de ciberseguridad para garantizar la protección de información crítica.

La adopción de inteligencia artificial en sistemas de seguridad no solo automatiza procesos y reduce la intervención humana, sino que también plantea desafíos relacionados con el sesgo en los datos y los costos operativos de mantenimiento, lo que hace necesaria una evaluación continua de su impacto en la eficiencia y la equidad del sistema.

Para garantizar una implementación efectiva y sostenible de estas tecnologías en las Fuerzas Armadas del Perú, es fundamental un enfoque estratégico que equilibre los beneficios tecnológicos con las limitaciones presupuestarias y logísticas, asegurando la formación adecuada del personal y la adaptación de las infraestructuras existentes para maximizar la efectividad y minimizar los riesgos asociados. .

AGRADECIMIENTOS

A la EOFAP por sus laboratorios y asesores teóricos y a la PUCP por sus asesores metodológicos y estadísticos para la realización de esta investigación.

REFEREBCIAS

[1] Agarkar, A. A., Karyakarte, M., Chavhan, G., Patil, M., Talware, R., & Kulkarni, L. (2024). Blockchain aware decentralized identity management and access control system. Measurement: Sensors, 31, 101032. https://doi.org/10.1016/j.measen.2024.101032

[2] Alahi, A., Vandergheynst, P., Bierlaire, M., & Kunt, M. (2010). Cascade of descriptors to detect and track objects across any network of cameras. Computer Vision and Image Understanding, 114(6), 624-640. https://doi.org/10.1016/j.cviu.2010.01.004

[3]

[4] Alejandra, M.-O. D. (2016). Re-identificación de personas a través de sus características soft-biométricas en un entorno multi-cámara de video-vigilancia. Ingeniería, Investigación y Tecnología, 17(2), 257-271. https://doi.org/10.1016/j.riit.2016.06.010

[5] Andreadis, G., Fourtounis, G., & Bouzakis, K.-D. (2015). Collaborative design in the era of cloud computing. Advances in Engineering Software, 81, 66-72. https://doi.org/10.1016/j.advengsoft.2014.11.002

[6] Antonolpoulos, F., Petrakis, E. G. M., Sotiriadis, S., & Bessis, N. (2018). A physical access control system on the cloud. Procedia Computer Science, 130, 318-325. https://doi.org/10.1016/j.procs.2018.04.045

[7] Bakshi, S., Sa, P. K., & Majhi, B. (2015). A novel phase-intensive local pattern for periocular recognition under visible spectrum. Biocybernetics and Biomedical Engineering, 35(1), 30-44. https://doi.org/10.1016/j.bbe.2014.05.003

[8] Barbu, T. (2014). Pedestrian detection and tracking using temporal differencing and HOG features. Computers & Electrical Engineering, 40(4), 1072-1079. https://doi.org/10.1016/j.compeleceng.2013.12.004

[9] Beretta, E., Voto, C., & Rozera, E. (2024). Decoding faces: Misalignments of gender identification in automated systems. Journal of Responsible Technology, 19, 100089. https://doi.org/10.1016/j.jrt.2024.100089

[10] Brown, T., et al. (2023). Counteracting cyber attacks on military systems. Journal of Cybersecurity, 12(3), 45-67. https://doi.org/10.6789/jcs.2023.012

[11] Carlaw, S. (2020). Impact on biometrics of Covid-19. Biometric Technology Today, 2020(4), 8-9. https://doi.org/10.1016/S0969-4765(20)30050-3

[12] Cascone, L., Pero, C., & Proença, H. (2023). Visual and textual explainability for a biometric verification system based on piecewise facial attribute analysis. Image and Vision Computing, 132, 104645. https://doi.org/10.1016/j.imavis.2023.104645

[13] Castrillón-Santana, M., Lorenzo-Navarro, J., & Ramón-Balmaseda, E. (2016). On using periocular biometric for gender classification in the wild. Pattern Recognition Letters, 82, 181-189. https://doi.org/10.1016/j.patrec.2015.09.014

[14] Dalal, N., & Triggs, B. (2005, June 20-25). Histograms of oriented gradients for human detection. In 2005 IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR'05).

[15] Devi, R. M., Keerthika, P., Suresh, P., Sarangi, P. P., Sangeetha, M., Sagana, C., & Devendran, K. (2022). Retina biometrics for personal authentication. In P. P. Sarangi, M. Panda, S. Mishra, B. S. P. Mishra, & B. Majhi (Eds.), Machine Learning for Biometrics (pp. 87-104). Academic Press. https://doi.org/10.1016/B978-0-323-85209-8.00005-5

[16] Douzis, K., Sotiriadis, S., Petrakis, E. G. M., & Amza, C. (2018). Modular and generic IoT management on the cloud. Future Generation Computer Systems, 78, 369-378. https://doi.org/10.1016/j.future.2016.05.041

[17] Díaz, V. (2014). Legal challenges of biometric immigration control systems. Mexican Law Review, 7(1), 3-30. https://doi.org/10.1016/S1870-0578(16)30006-3

[18] Edwards, M., & Garcia, T. (2023). Enhancing military security through AI and blockchain. Journal of Information Warfare, 18(1), 55-70.

https://www.journalofinformationwarfare.com/enhancing-military-security-ai-blockchain

[19] Enge, A., Satybaldy, A., & Nowostawski, M. (2022). An offline mobile access control system based on self-sovereign identity standards. Computer Networks, 219, 109434. https://doi.org/10.1016/j.comnet.2022.109434

[20] Evans, R., & Martin, G. (2023). The strategic impact of blockchain on military supply chains. Journal of Defense Logistics, 5(3), 32-46. https://www.taylorandfrancis.com/journals/defenselogistics/blockchain-military-supply-chains

[21] Gosselin, P. H., Precioso, F., & Philipp-Foliguet, S. (2011). Incremental kernel learning for active image retrieval without global dictionaries. Pattern Recognition, 44(10), 2244-2254. https://doi.org/10.1016/j.patcog.2010.12.006

[22] H.R, V. K., & M, M. (2023). A novel hybrid biometric software application for facial recognition considering uncontrollable environmental conditions. Healthcare Analytics, 3, 100156. https://doi.org/10.1016/j.health.2023.100156

[23] Harris, J., & Lee, Y. (2023). Defense technologies and their impact on national security. Journal of Security and Defense, 25(2), 60-75. https://www.taylorandfrancis.com/journals/defense-technology-impact

[24] Hernandez, M., & Lopez, C. (2022). The evolution of military cybersecurity: Trends and strategies. Journal of Cyber Warfare, 6(4), 121-135. https://www.journalofcyberwarfare.org/JCW-evolution-military-cybersecurity

[25] Hiran, K. K., & Dadhich, M. (2024). Predicting the core determinants of cloud-edge computing adoption (CECA) for sustainable development in the higher education institutions of Africa: A high order SEM-ANN analytical approach. Technological Forecasting and Social Change, 199, 122979. https://doi.org/10.1016/j.techfore.2023.122979

[26] Mitchell, H., & Stone, P. (2022). AI in military operations: Ethical considerations and strategic implications. Journal of Military Ethics, 13(4), 34-48. https://www.tandfonline.com/doi/abs/10.1080/15027570.2022.1954487

[27] Patel, N., & Kumar, V. (2023). Blockchain in military applications: Challenges and opportunities. Journal of Military Information Technology, 11(3), 18-31. https://militarytechnologyjournal.org/blockchain-military-applications

[28] Rodriguez, S. (2023). Emerging technologies and their influence on modern warfare. International Journal of Military Studies, 22(2), 89-104. https://journals.sagepub.com/doi/full/10.1177/0885066621146527

[29] Smith, E. (2022). Cyber threats and military defense: An overview. Institute for Security Studies. https://www.iss.org/cyber-threats-overview

[30] Thompson, E., & Black, H. (2022). The role of AI in modern military strategy. Defense and Security Review, 30(4), 89-103. https://www.defenseandsecurityreview.com/journal/role-of-ai-military-strategy

[31] Thompson, R., & Garcia, M. (2023). Blockchain integration in military communications: A review. Cybersecurity & Defense, 19(2), 45-59. https://cyberdefense.org/publications/blockchain-integration-military-communications

[32] Williams, H., et al. (2023). Blockchain and the future of military security. Defense Technology Journal, 27(2), 76-89.

.