JSTRI
JOURNAL OF SCIENTIFIC AND TECHNOLOGICAL RESEARCH INDUSTRIAL

Journal of Scientific and Technological Research Industrial
ISSNe: 2961-211X

PROF-JSTRI-V-00
Vol. 7 N.º 1
(January - June, 2026)

Modelos predictivos de IA y su relación con la protección contra amenazas persistentes avanzadas del sistema bancario

AI Predictive Models and Their Relationship with Protection Against Advanced Persistent Threats in the Banking System

Héctor Martín Espinoza Villavicencio
Universidad Nacional Federico Villarreal, Perú
2022032322@unfv.edu.pe

Resumen

El objetivo fue determinar la relación entre los modelos predictivos de inteligencia artificial y la protección contra amenazas persistentes avanzadas (APTs) en el sistema bancario de Lima en 2024. Se realizó un análisis de fuentes secundarias sobre los modelos predictivos de IA que detectan amenazas persistentes en ciberseguridad como el malware. Se aplicó una encuesta a una muestra de 79 empleados de instituciones bancarias en Lima. La investigación, es de carácter no experimental, cuantitativo y transversal. Los resultados mostraron un mejor rendimiento de los sistemas de seguridad en el sector bancario tras la implementación de los modelos predictivos en áreas como la detección, mitigación y prevención de APT, fortaleciendo la ciberseguridad en un entorno crítico. Estos hallazgos resaltan la utilidad de los modelos para representar con mayor seguridad tras los ataques dirigidos a las entidades financieras. La encuesta evidencio que la mayoría de participantes considera que los modelos predictivos de IA contribuyen a la protección contra (APTs) y optimizar la solución de problemas, lo cual indica una tendencia favorable hacia la implementación de herramientas basados en IA en el sistema bancario. La aplicación de los modelos de IA predictiva mejora la resiliencia del sistema bancario frente a los ataques APT, ya que su capacidad para optimizar los procesos mejora la resistencia y tiene un efecto en la evolución de la protección contra los ataques APT, otorgándoles adaptabilidad a nuevas amenazas a medida que mejoran y se vuelven más sofisticados.

Palabras claves: algoritmos inteligentes, amenazas persistentes avanzadas, aprendizaje automático, ciberseguridad, inteligencia artificial, modelos predictivos.

Abstract

The objective was to determine the relationship between artificial intelligence predictive models and protection against advanced persistent threats (APTs) in the Lima banking system in 2024. A secondary source analysis was conducted on AI predictive models that detect persistent cybersecurity threats such as malware. A survey was administered to a sample of 79 employees from banking institutions in Lima. The research is non experimental, quantitative, and cross-sectional. The results showed improved security system performance in the banking sector following the implementation of predictive models in areas such as APT detection, mitigation, and prevention, strengthening cybersecurity in a critical environment. These findings highlight the models' usefulness in more accurately predicting the impact of attacks on financial institutions. The survey revealed that the majority of participants believe AI predictive models contribute to protection against APTs and optimize problem-solving, indicating a favorable trend toward the implementation of AI-based tools in the banking system. The application of predictive AI models improves the resilience of the banking system against APT attacks, as their ability to optimize processes enhances resistance and has an effect on the evolution of protection against APT attacks, giving them adaptability to new threats as they improve and become more sophisticated.

Keywords: advanced persistent threats, artificial intelligence, cybersecurity, intelligent algorithms, machine learning, predictive models.

OPEN ACCESS

Publicado: 2026-03-27
Aceptado: 2026-03-23
Recibido: 2026-02-13

Open Access
Article scientific
https://doi.org/10.47422/jstri.v7i1.74

Introducción

La rápida proliferación que ha vivido la red y la hiperconectividad de dispositivos han generado un entorno digital potente, pero, a su vez, el mismo se antoja extremadamente frágil ante el continuo ataque de las ciberamenazas informáticas. En ese sentido, las APT (Amenazas Persistentes Avanzadas) destacan aproximadamente por su nivel de sofisticación técnica, así como por su capacidad inusual de sortear los perímetros de seguridad tradicionales de manera sostenida. Este tipo de ataque pone en barbarie la integridad de la información y representa un riesgo fundamental para la privacidad de las personas e incluso para la estabilidad de las grandes organizaciones.

La inteligencia artificial (IA) predictiva, en contraposición a este reto que nos plantea la revolución digital, se erige como una alternativa necesaria y disruptiva. Basándose en arquitecturas de machine learning y deep learning, estas funcionalidades habilitan el procesamiento de flujos masivos de datos en tiempo real, identificando anomalías que fácilmente se escaparían del ojo humano. Como señala Melo (2022), la principal ventaja competitiva de la IA predictiva consiste en la orientación proactiva de la misma; a diferencia de los enfoques reactivos, la IA predictiva permite anticipar vulnerabilidades, así como la posibilidad de un cambio adaptativo ante un agresor inclemente. La yuxtaposición de heurística conductual y de inteligencia de amenazas incrementa la precisión; de esta forma, mejora notablemente la defensa del usuario final. No obstante, que esta misma eficiencia no es la última ni la máxima, dado que la sofisticación de los ataques avanza y se desarrolla con esa misma rapidez, poniendo por tanto a prueba la solidez de la dicha tecnología en terrenos a veces poco previsibles.

En el escenario particular de Lima, la integración de la inteligencia artificial en las entidades bancarias ha provocado una metamorfosis en la administración de datos y la seguridad de los activos financieros. No obstante, esta evolución tecnológica genera importantes preocupaciones en materia de ciberseguridad, como el uso de estas herramientas no solo como herramienta de defensa, sino también como un nuevo vector de ataque. En particular, la IA generativa ha permitido un marcado aumento en la sofisticación de ataques de ingeniería social como el phishing y los deepfakes, que engañan a los usuarios y comprometen datos críticos. Bajo esta premisa, Pardiñas (2020) señala que las investigaciones actuales muestran un incremento del 60 % en las ofensivas de phishing potenciadas por IA, sumándose a los récords de vulnerabilidad reportados en otros mercados (BBVA, 2025). Esta situación de fragilidad digital obliga a priorizar la adopción de modelos predictivos que permitan anticiparse y neutralizar las amenazas persistentes avanzadas en un entorno de riesgos constantes.

Desde otra perspectiva, la utilización masiva de este tipo de tecnologías también revela el dilema de la privacidad. Así lo plantean Madrid (2024) enfatizando que el entrenamiento de modelos de alto rendimiento requiere de volúmenes muy elevados de información, lo que incrementa las vulneraciones de información sensible. En el caso del Perú, donde la normativa de protección de datos aún tiene un nivel de maduración bajo, la falta de regulaciones podría terminar provocando un uso poco ético de la tecnología al tiempo que se infringe la transparencia y la rendición de cuentas, dos elementos centrales en el sector financiero.

En relación con este escenario, Molina (2025) plantea el vínculo fundamental entre el empleo de esquemas predictivos sustentados en inteligencia artificial (IA) y el incremento en la efectividad de las defensas contra ataques dirigidos de alta persistencia. A través de un examen detallado de las variables, la incorporación de la IA en las estrategias de ciberseguridad podría generar un cambio sustancial en la capacidad del sistema para la detección temprana y la respuesta ágil ante amenazas digitales, lo que permitiría establecer un marco de protección integral y avanzado para salvaguardar los activos en red. Con este propósito, la investigación examina pilares críticos de la seguridad informática, tales como los mecanismos de identificación y bloqueo de intrusiones, la solidez de las infraestructuras digitales y la dinámica con la que las medidas de amparo se actualizan y adaptan frente a nuevos desafíos.

Sarker (2022) también presenta un enfoque de tipo multidimensional si se analiza cómo ha afectado la IA a sectores como el financiero, el sanitario, la industria 4.0, entre otros. El autor considera que la automatización mediante sistemas inteligentes y el procesamiento del lenguaje natural ha permitido alcanzar cotas de eficiencia extraordinarias, aunque deberá advertir que para que estos modelos lleguen a ser realmente "inteligentes" requieren formaciones continuas con base en un conocimiento del dominio específico. A pesar de la potencia algorítmica que se puede alcanzar, el humano se convierte en el eje gravitacional del sistema. Tal como destacan De La Hoz Suárez et al. (2024), la destreza técnica y la experiencia del personal son las únicas determinantes para ser capaces de evaluar, corregir y guiar el desarrollo de estos modelos. Y en lo que se refiere a ciberseguridad, este trabajo conjunto entre humano e IA en tareas como el planeamiento de respuestas ante incidentes o el mantenimiento preventivo se erige verdaderamente como lo que garantiza la continuidad de la actividad y una gestión de amenazas

eficaz. Con lo cual, la tecnología se consideraría insuficiente por sí sola si no existe el juicio de expertos que posibilite que estas capacidades sean aprovechadas (Kalogiannidis et al., 2024).

Ciertamente la reducción de la superficie de ataque es drástica mediante la automatización y la inteligencia en las amenazas aunque esta cualidad depende tanto de la calidad de la entrada como de un mantenimiento intensivo para evitar falsos positivos, Duan et al. (2025) refuerzan esta posición afirmando que el éxito operativo requiere estrictas políticas de supervisión; Hua, Xi (2025) apuntan que sin ética también serían capaces de favorecer sesgos o discriminación predictiva, lo que indica que su uso debe ser razonable y controlado.

Por otra parte, la gestión de la privacidad en la era del big data sigue siendo una asignatura pendiente. La sobreexposición de datos personales en las plataformas digitales supone riesgos desmesurados tal como sugieren Ren et al. (2026), quienes hacen hincapié en la existencia de vacíos en la legislación, hasta incluso en marcos jurídicos muy desarrollados como es el caso del de la Unión Europea respecto a la automatización y/o contratos inteligentes. Por tanto, urge y se hace necesario promover la transparencia algorítmica real.

Siguiendo con la eficiencia operativa, Sifuentes (2024) identifica que la IA dentro de los flujos de trabajo contemporáneos ha hecho el camino a favor, la integración de forma estratégica de esta IA no solo permite mejorar las operaciones, sino que brinda un diagnóstico superior a las organizaciones que afecta directamente la experiencia del usuario. Pero esta tasa de crecimiento no es automática, bien en su estudio Hussain et al. (2025) explican que depende de marcos de gobernanza de privacidad de la información, así como una inversión relativamente fuerte en infraestructuras de datos especializados. Esta vez, el resultado también incluye el soporte técnico y la defensa digital, y con las herramientas automatizadas se pueden recortar drásticamente los tiempos de respuesta en su caso de una violación de seguridad e, incluso recortar en gastos operativos mediante una toma de decisiones más sutil y efectiva (Lewis, 2026; Olasehinde et al., 2026).

Las necesidades de datos mencionadas anteriormente aún persisten en esta región, lo que también ha aumentado la complejidad de la implementación debido a la falta de confianza de la población debido a la limitada regulación y conocimiento sobre el tema. La desconfianza en la toma de decisiones automatizada y la preocupación por la privacidad de los usuarios son algunas de las principales barreras para la implementación que deben abordarse para garantizar un funcionamiento eficaz y seguro (Yang et al., 2025). Incluso en el caso de un buen rendimiento y la provisión de beneficios en diferentes niveles, esta misma cautela se percibe por parte de los trabajadores humanos, quienes podrían no considerar el algoritmo tan capaz o confiable como ellos mismos, temiendo consecuencias como una disminución de la calidad o la sustitución del componente humano en general. Una planificación inadecuada también podría generar vulnerabilidades y desigualdades que podrían poner en riesgo la seguridad y la privacidad de los usuarios.

Método

La investigación se desarrolló bajo un enfoque cuantitativo y corresponde a un estudio de tipo básico con diseño no experimental y corte transversal. Este tipo de diseño permitió observar y analizar las variables de estudio sin intervenir directamente en su comportamiento. La muestra estuvo conformada por 79 trabajadores pertenecientes a distintas instituciones bancarias ubicadas en la ciudad de Lima. Los participantes fueron seleccionados con el propósito de conocer su percepción respecto al uso de modelos predictivos de inteligencia artificial en la protección frente a amenazas persistentes avanzadas.

Como instrumento de recolección de datos, se diseñó un cuestionario estructurado que permite medir la percepción técnica sobre la eficacia de la IA frente a amenazas avanzadas. La robustez métrica del instrumento fue validada mediante el juicio de expertos y un análisis de consistencia interna. En este sentido, se obtuvo un coeficiente del 0,908 para Alfa de Cronbach tras evaluar 23 elementos clave. Al superar el umbral crítico de 0,7, se confirma que la herramienta posee una fiabilidad y validez estadística óptimas para sustentar las inferencias de la investigación.

Procedimientos

El proceso analítico se estructuró en tres fases secuenciales. En la etapa inicial, se procesaron las frecuencias de la información recolectada para obtener una radiografía clara sobre la distribución de las variables. Este paso descriptivo permitió identificar la variabilidad en cada dimensión estudiada antes de proceder a análisis más complejos.

En la segunda fase, Se empleó el software SPSS (v. 25) con el fin de realizar una prueba de correlación de Spearman. Dado que se buscaba identificar la fuerza y dirección de las conexiones entre las dimensiones de la IA y la protección de redes, este método no paramétrico resultó el más adecuado para validar las hipótesis planteadas. Finalmente, en la tercera etapa, se procedió a la discusión e interpretación teórica de los datos. Aquí, los resultados cuantitativos se contrastaron con los objetivos de la investigación para ofrecer respuestas fundamentadas a las interrogantes que dieron origen al estudio.

Resultados

Examen de los sistemas de predicción basados en IA

El panorama tecnológico reciente ha sido testigo de la aparición de modelos predictivos cada vez más sofisticados. En este sentido, la Tabla 1 ofrece una visión comparativa que detalla tanto las fortalezas como las limitaciones de estas herramientas en el contexto de la ciberseguridad actual.

Tabla 1

Comparativa de los principales modelos predictivos de Inteligencia Artificial

Modelo Predictivo	Principales Técnicas	Ventajas	Desventajas
Redes Neuronales Artificiales (ANNs)	Aprendizaje profundo mediante arquitecturas convolucionales y recurrentes.	Gran eficacia identificando irregularidades sofisticadas.	Elevado consumo de recursos. computacional.
		Capacidad de aprendizaje automático	Opacidad en su funcionamiento interno.
Random Forest (Bosques Aleatorios)	Basado en múltiples diagramas de decisión.	Interpretabilidad, robustez ante datos desbalanceados.	Más lento en grandes volúmenes de datos. Puede sobre ajustarse.
Support Vector Machines (SVM)	Algoritmos de clasificación por soporte vectorial.	Precisión en clasificación binaria y detección de anomalías.	Ineficiente en grandes volúmenes de datos. Difícil ajuste de hiperparámetros.
Gradient Boosting (XGBoost, LightGBM, CatBoost)	Algoritmos de boosting para optimización	Alta precisión, rapidez en entrenamiento y predicción.	Puede ser difícil de ajustar en problemas muy complejos.
Análisis de Comportamiento del Usuario (UEBA)	Mecanismos para identificar irregularidades (ADS).	Detección en tiempo real de actividades inusuales.	Riesgo de errores frecuentes ante un ajuste deficiente.
Sistemas de Detección de Anomalías (ADS)	Esquemas de aprendizaje autónomo basados en agrupamiento y codificación.	Buen desempeño en detección de estructuras de datos no identificadas previamente.	Necesita bases de datos extensas para asegurar su exactitud.
Modelos generativos de confrontación (GANs).	Modelos generativos para detectar ataques adversariales	Capacidad para hallar intrusiones complejas creadas mediante inteligencia artificial.	Complejidad en el aprendizaje y gran demanda de recursos.

Evaluación de peligros digitales dirigidos (APT) en la banca

Al examinar la Tabla 2, queda en evidencia una tendencia preocupante: el incremento sostenido de los incidentes por APT en los últimos seis años. Lo que antes representaba una fracción menor del total de ciberataques, hoy muestra un peso porcentual cada vez más alto. Este crecimiento no es casual; señala que las amenazas están mutando hacia un modelo de ataque mucho más dirigido, silencioso y, por ende, más complejo de neutralizar para las entidades financieras.

Tabla 2

Evolución de incidentes APT registrados en entidades financieras entre 2018 y 2023

Año	Cantidad de eventos registrados	Proporción de ataques APT respecto al total de delitos informáticos (%).
2018	150	25%
2019	185	28%
2020	210	30%
2021	240	32%

2022	300	35%
2023	350	37%

Por otro lado, la Figura 1 permite visualizar la gravedad del problema desde una perspectiva económica. El impacto financiero de las APT ha seguido una trayectoria ascendente, alcanzando un punto de quiebre en 2023, año en el que los costos totales por este tipo de brechas superaron la barrera de los mil millones de dólares. Este salto pone de manifiesto que el daño no es solo operativo, sino que pone en riesgo la solvencia y la estabilidad financiera del sector.

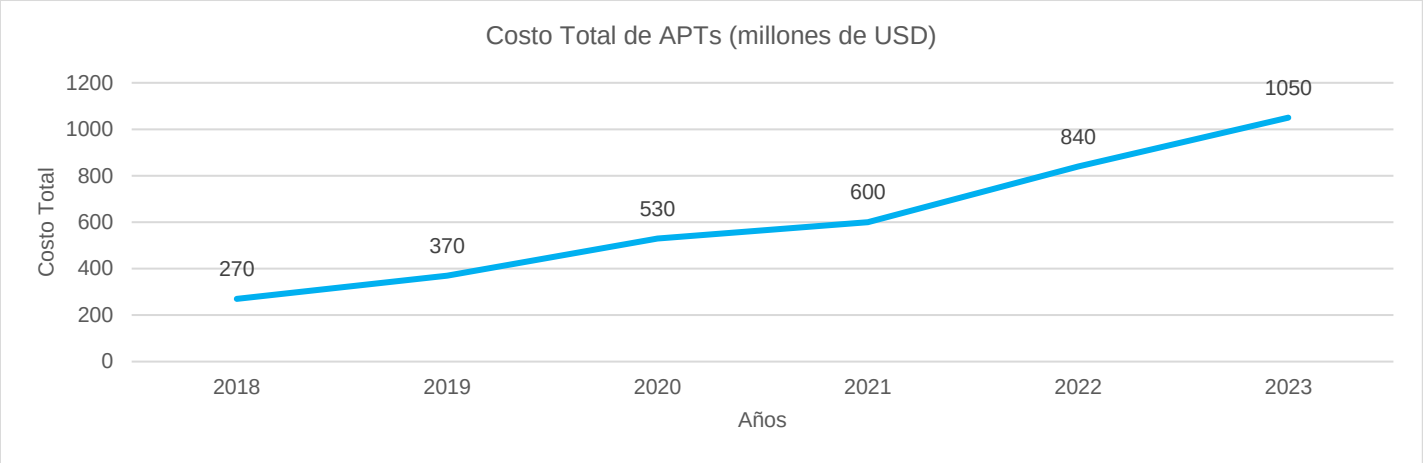

Figura 1. *Escalada del impacto financiero por ataques APT en la banca (2018-2023)*

Nota. La figura muestra el impacto financiero obtenido del estudio cuantitativo sobre los riesgos APT. Construido con datos del sector bancario.

Tabla 3

Tipología de las modalidades APT en la banca de Perú durante 2024

Categoría de amenaza identificada	Incidencia proyectada	Descripción
Sustracción de activos bancarios	48	Extracción encubierta de datos sensibles como registros de usuarios y credenciales.
Desplazamiento interno	35	Propagación por la infraestructura financiera para comprometer equipos adicionales.
Suplantación dirigida	52	Mensajería fraudulenta enviada a directivos o técnicos para obtener el ingreso original.
Intrusión vía suministros	21	Vulneración de socios tecnológicos para infiltrarse en las instituciones.
Empleo de software malicioso a medida	39	Desarrollo de código dañino diseñado exclusivamente para la banca local.
Presencia extendida	27	Permanencia invisible en la red por periodos superiores a un trimestre.
Comandos y Control Remoto (C2)	32	Empleo de infraestructura remota para la gestión de equipos internos.

Capacidad de resistencia por áreas técnicas

En la Figura 2 se presenta un diagnóstico de la resiliencia ante las APT desglosada por cada componente técnico del sistema. Esta evaluación visual es fundamental, ya que actúa como una hoja de ruta para la alta gerencia. Identificar con precisión qué áreas poseen una buena capacidad técnica y cuáles presentan debilidades permite priorizar la inversión de recursos de manera estratégica, fortaleciendo los eslabones más vulnerables antes de que sean explotados por atacantes externos.

Figura 2. *Evaluación del Nivel de fortaleza institucional frente a amenazas dirigidas.*

Nota. La ilustración muestra un esquema radial sobre la capacidad de recuperación ante ataques APT. Esta representación se adaptó de la propuesta del estudio de Hassanzadeh et al. (2023) sobre el fortalecimiento de redes mediante la automatización de conmutadores.

Progreso y mejoras en la defensa frente a intrusiones prolongadas (APT)

Al observar la Figura 3, queda claro que ciertas técnicas tienen una predilección táctica dentro de los ataques APT. La prevalencia de estos métodos sugiere que los atacantes están moviendo sus piezas hacia estrategias de infiltración que explotan el eslabón más débil: la ingeniería social y las brechas de seguridad latentes en los sistemas. Esto confirma que el factor humano y los fallos de configuración siguen siendo las puertas de entrada preferidas para ataques prolongados.

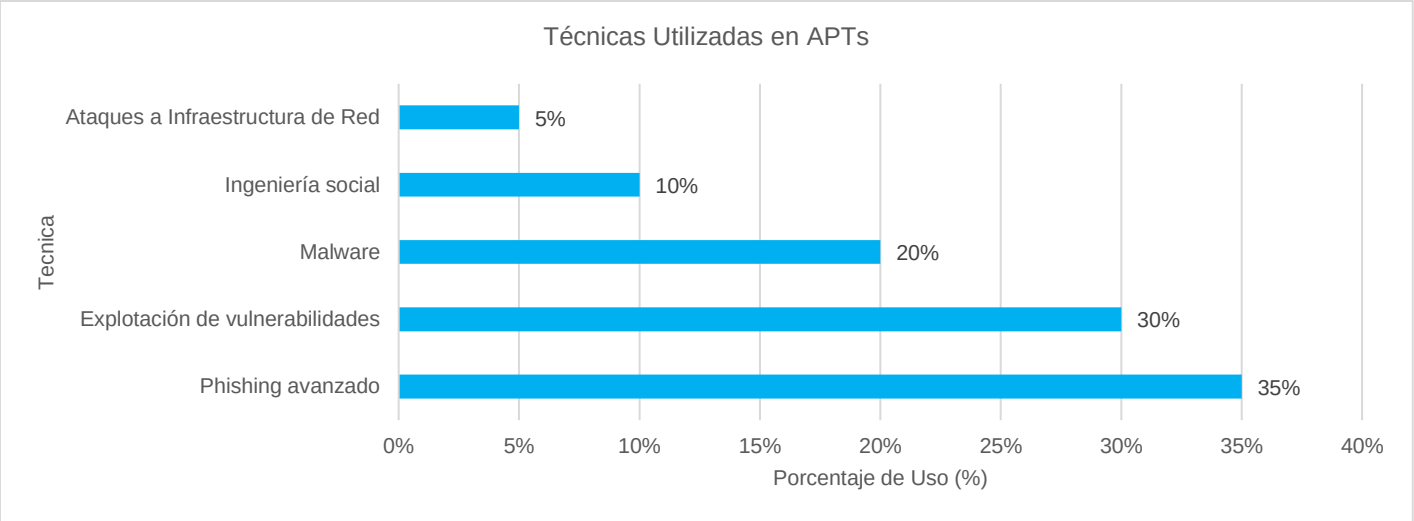

Figura 3. *Desglose de las tácticas más usadas en ataques APT financieros durante el 2023.*

Por otro lado, la Figura 4 detalla el panorama del software de seguridad en la nube que lidera el mercado bancario tanto a nivel global como en Latinoamérica. La comparativa es útil para entender cómo las instituciones financieras están migrando sus defensas hacia entornos virtualizados, adaptándose a las exigencias de escalabilidad y protección que demanda el año 2024.

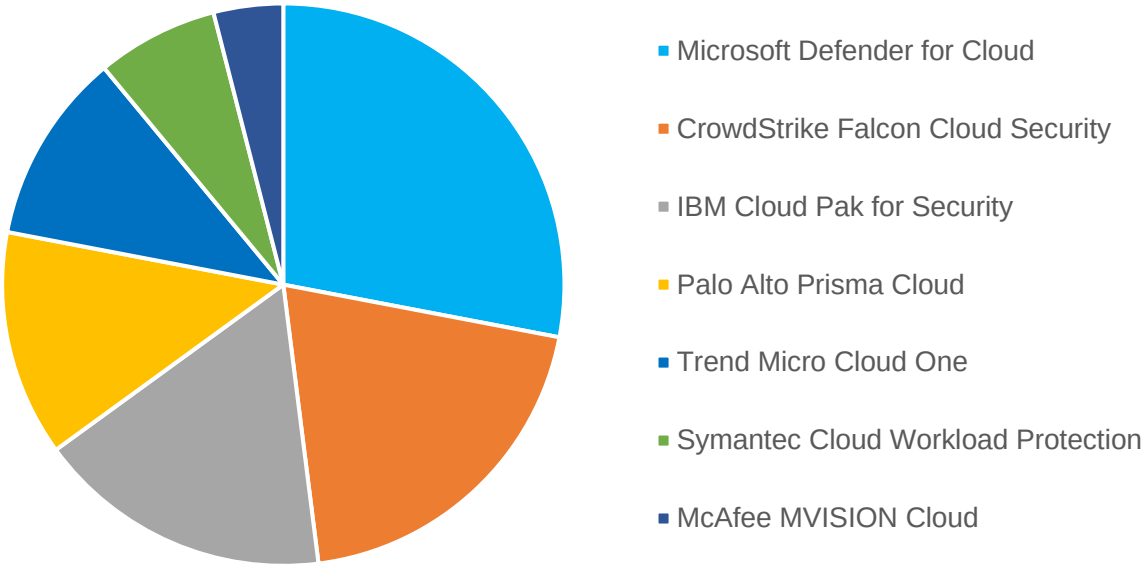

Figura 4. *Frecuencia de uso de Software de Seguridad en la Nube en la Banca (2024)*

La Tabla 4, arroja luz sobre los productos de ciberseguridad con mayor demanda por parte de la banca en el territorio peruano y a nivel latinoamericano. Se observa que la inversión no es aleatoria; las compras se concentran en soluciones diseñadas específicamente para neutralizar ataques de tipo APT, buscando herramientas que ofrezcan una protección integral y una visibilidad profunda de las amenazas antes de que el daño sea irreversible.

Tabla 4

Productos de ciberseguridad con mayor adopción en el Sector Bancario de Perú y Latinoamérica (2024)

Herramientas de protección digital	Ritmo de adquisición en el mercado
Cortafuegos de última generación (32%)	32%
Herramientas de detección y respuesta extendida	27%
Plataformas de gestión de eventos y vigilancia	19%
Sistemas de orquestación y respuesta automática	11%
Software para la prevención de fuga de información	7%
Soporte externo de monitoreo y reacción ante incidentes	4%

Tabla 5

Categorización de fabricantes por sectores

Segmento	Empresas	Atributos principales.
Referentes del mercado	Microsoft Defender, CrowdStrike Falcon	Eficacia elevada, vanguardia en inteligencia artificial y amplia presencia en el sector financiero.
Rivales directos	Soluciones como QRadar y Cortex XDR	Capacidad operativa sólida con menor enfoque en desarrollo de IA.
Estrategas creativos	Trend Micro Apex One, Symantec Endpoint	Pioneros en IA con una implementación aún limitada en entidades bancarias.
Especialistas locales	McAfee MVISION	Orientados a requerimientos puntuales con una cobertura de mercado reducida.

La Tabla 6 muestra la caracterización de los proveedores, colocando a cada proveedor en una de las cuatro categorías del cuadrante: Líder, Competidor Desafiante, Visionarios y Jugadores de Nicho. Esta evaluación ofrece una perspectiva completa acerca de la situación actual de las soluciones de ciberseguridad con base en IA dentro del sistema bancario de Lima en el año 2024.

Tabla 6

Caracterización de los proveedores

Proveedor	Cuadrante	Puntos Fuertes	Debilidades
Microsoft Defender	Líder	Alta integración con plataformas financieras e IA de alto nivel.	Vinculación obligatoria con el entorno de Microsoft.
CrowdStrike Falcon	Líder	Detección en monitorización inmediata y exacta.	Inversión elevada frente a la competencia.
Solución SIEM de IBM	Competidor Desafiante	Potente gestión de seguridad con analítica profunda	Panel de control difícil y periodo de capacitación extenso.
Palo Alto Cortex XDR	Competidor Desafiante	Respuesta automatizada, buen soporte.	Implementación costosa.
Trend Micro Apex One	Visionario	Fuerte en protección endpoint con IA.	No es líder en respuesta a incidentes.
Symantec Endpoint Security	Visionario	Protección multicapa contra APTs.	Menos integración con bancos.
McAfee MVISION	Jugador de Nicho	Arquitectura en la nube, gestión sencilla.	No cubre todo el ciclo de seguridad.

A través de la Tabla 7, se detalla cómo los distintos proveedores son valorados basándose en su solvencia operativa y capacidad de ejecución. Esta métrica es vital para entender qué soluciones de inteligencia artificial ofrecen un blindaje real contra ataques de tipo APT dentro del ecosistema financiero limeño.

Tabla 7

Valorización de los proveedores

Proveedor/Tecnología	Completitud de Visión (X)	Capacidad de Ejecución (Y)	Categoría
Microsoft Defender ATP	9,2	9,5	Líder
CrowdStrike Falcon	9	9,3	Líder
IBM QRadar	7,5	8,7	Competidor desafiante
Plataforma de respuesta XDR de Palo Alto	7,8	8,5	Competidor desafiante
Trend Micro Apex One	8,5	7,2	Visionario
Symantec Endpoint	8,2	7	Visionario
McAfee MVISION	6,5	6,8	Jugador de dicho

El Cuadrante Mágico permite clasificar las soluciones de IA destinadas a neutralizar las APT en la banca local. Este modelo organiza a los proveedores en cuatro áreas estratégicas, evaluándolos bajo dos vectores clave: su visión tecnológica (Eje X) y su capacidad real de implementación (Eje Y).

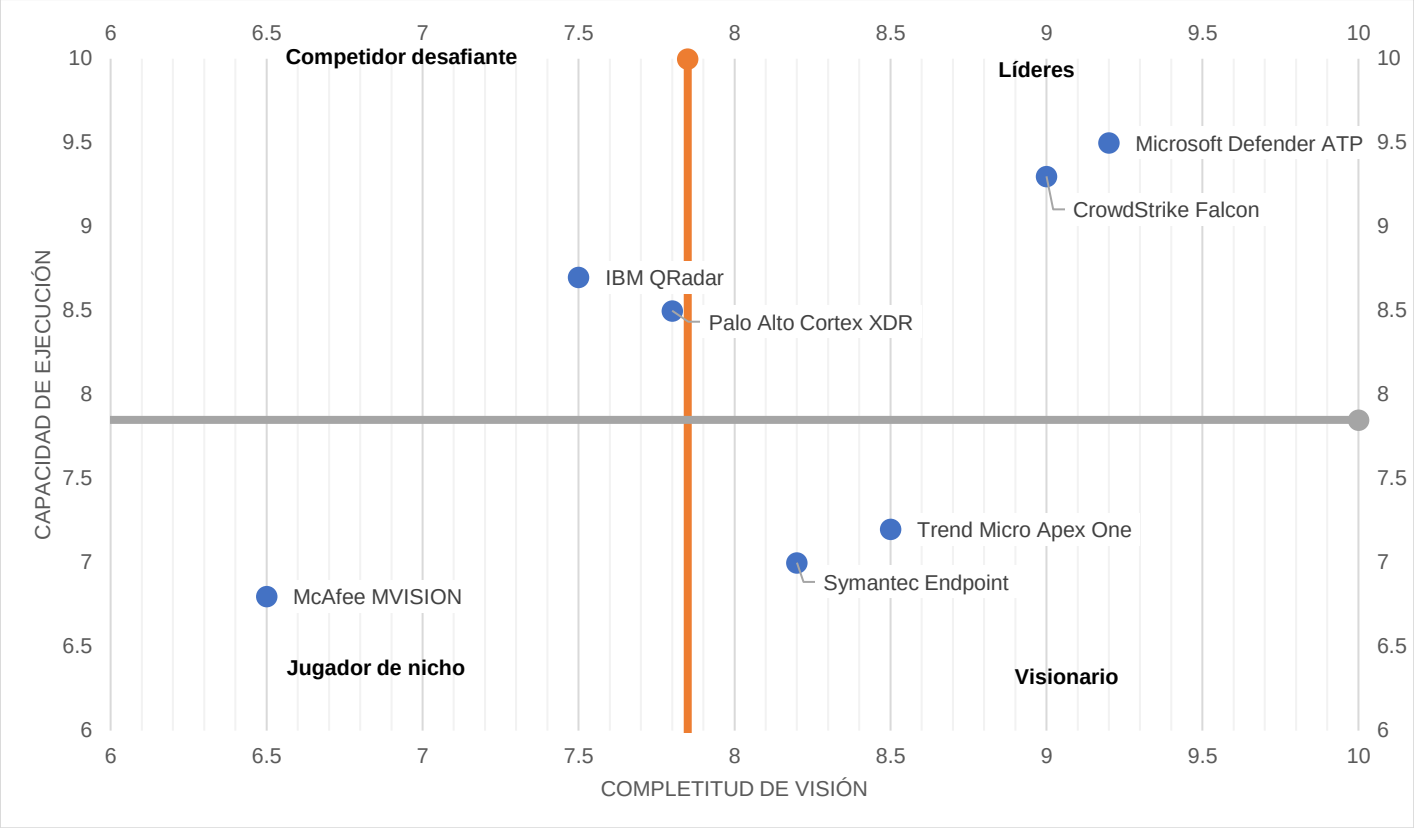

Figura 5. *Análisis de la matriz estratégica de Gartner para el periodo 2025.*

Nota. Matriz estratégica de Gartner. Adaptación basada en la investigación sobre implementación de seguridad y acceso remoto (ZTNA) realizada por Albino y Diaz (2025).

Líderes (Arriba a la derecha)

- Microsoft Defender y CrowdStrike Falcon lideran el sector gracias a su tecnología de inteligencia artificial avanzada y su eficacia demostrada contra amenazas persistentes, son las opciones más recomendadas para entidades bancarias con altas exigencias en ciberseguridad.

Competidores Desafiantes (Arriba a la izquierda)

- En este grupo, IBM QRadar y Palo Alto Cortex XDR demuestran un rendimiento operativo sobresaliente. No obstante, su integración de herramientas de IA aún no alcanza el nivel de sofisticación de los líderes, posicionándose como alternativas de gran valor para bancos que ya cuentan con una infraestructura tecnológica consolidada y buscan robustez funcional.

Visionarios (Abajo a la derecha)

- Trend Micro Apex One y Symantec Endpoint están marcando la pauta mediante innovaciones disruptivas en la detección de amenazas basadas en IA. Si bien todavía no gozan del respaldo masivo de los líderes del mercado, su visión tecnológica y capacidad de anticipación las sitúan como oportunidades estratégicas con un alto potencial de expansión a futuro.

Jugadores de Nicho (Abajo a la izquierda)

- Finalmente, McAfee MVISION destaca por ofrecer funcionalidades sumamente específicas. Aunque no se presenta como una solución integral para las grandes corporaciones financieras, constituye una herramienta eficaz para entidades de menor escala o aquellas que deben cubrir necesidades técnicas muy particulares.

Discusión

En consideración a la información recopilada en el presente trabajo, es posible aseverar que la implementación de modelos predictivos aplicados a IA tiene un impacto positivo y determinante sobre la protección contra las APT en el entorno bancario de Lima. Esta tecnología actúa no solo como filtro, sino que también refuerza estructuralmente las estrategias de detección, contención y respuesta ante incidentes. Al poner en relación los resultados que emanan de esta investigación y los resultados de las tesis de Iturbe, et al. (2025) podemos

observar cómo confluyen en valorar las ventajas competitivas que la IA proporciona al área de la ciberseguridad. No obstante, el análisis también destila una nota negativa: la implementación no está libre de roces, particularmente en términos de privacidad y en el tratamiento ético de los datos, ya que son puntos que requieren una gestión técnica tan rigurosa como la defensa misma.

Los Hitos relevantes de esta investigación resaltan la existencia de una relación necesaria entre la complejidad de los modelos de predicción y la posibilidad de operación a fin de desactivar las APT. Las herramientas automatizadas pasaron de ser recursos de soporte, convirtiéndose así en estructuras clave de la ciberseguridad financiera, pretendiendo llevar la detección avanzada en forma de procesamiento de patrones complejos. Lo dicho coincide con las afirmaciones de Shen et al. (2025) cuando sostiene que la conjunción Big Data más IA es la única forma útil para poder tratar la cantidad de datos que producen las bancas contemporáneas. Esta competencia de los algoritmos de poder identificar comportamientos maliciosos en tiempo real, se pueden pasar de una seguridad reactiva a una proactiva, anticipándose al atacante.

Por otra parte, se genera una discrepancia interesante al comparar la investigación de Alageel y Maffeis (2026), pues para ellos los limitantes tienen que ver con la resistencia al cambio/temor a que la automatización pueda reemplazar el capital humano. En cambio, se puede sostener que los resultados de la presente investigación permiten volcar lo expuesto a una mayor integración de los sucesos: los modelos predictivos no son, para nada, un estrés de cambio, sino más bien entrevistas que permiten que las herramientas de seguridad se desarrollen. El capital humano no es reemplazable, dado que el personal experto está dotado por la tecnología para ofrecer una rapidez en la respuesta ante las nuevas potencialidades de la amenaza, lo que sugiere que el ser humano es el eje central en el sistema de defensa.

En lo que al eje normativo y regulador se refiere, Wang et al. (2026) sugieren que la protección de datos personales no necesariamente puede tener éxito si las normas que delinean sus límites son no contundentes, ya que ello podría dar lugar a riesgos de tipo sistémico. Este trabajo, si bien también entiende la relevancia de la gobernanza, los resultados alcanzados en las entidades financieras de Lima enriquecen el acervo de evidencia empírica que suele faltar en los análisis únicamente jurídicos, lo cual puede ser una perspectiva complementaria a lo que se constata en la literatura. Ambas perspectivas coinciden en un argumento central y que comporta también cierta relevancia: potenciar y encontrar las fortalezas de la IA es la vía más corta para incrementar la resiliencia del sector financiero ante los ataques más persistentes.

Un importante punto de inflexión se constituye al considerar lo expuesto por Belali et al. (2026), quien pone de relieve la disminución de la carga de trabajo operativa gracias a la identificación de las amenazas en tiempo real. Ahora bien, nuestra investigación indaga más a fondo al expresar que, dentro del sistema bancario de Lima, el entrenamiento especializado de estas herramientas dentro del sector financiero ha permitido alcanzar especificaciones de precisión que rompen con las barreras genéricas de las cuales se da cuenta en la literatura anteriormente expuesta. La integración táctica de la IA en este espacio no solo permite avanzar en el camino de la detección, sino que se transforma en la habilidad de dar respuesta, permitiendo que la arquitectura de la seguridad avance y evolucione, a la par que la capacidad de asestar ataques complejos que hasta hace poco se consideraban incognoscibles.

Por otra parte, el trabajo realizado por Deng et al. (2026) otorga una óptica regia sobre la fusión entre el Big Data y la IA de forma que permite advertir ofensivas cibernéticas. Sus conclusiones destacan que es posible gestionar grandes flujos de información asociándose a la detección de actos maliciosos mediante algoritmos de aprendizaje automático. Esta visión está íntimamente ligada a los resultados obtenidos en el entorno del sistema bancario en Lima, donde los modelos predictivos obtuvieron una correlación positiva notable con la detección satisfactoria de las APT.

Es necesario identificar con claridad este estudio para diferenciarlo de otros antecedentes, como el de Almazarqi et al. (2025), pero en este caso se articula eminentemente en una revisión teórica vinculada a los estudios a nivel académico. A diferencia de esta investigación, nosotros hemos permitido comprobar empíricamente y de una forma más directa cómo relacionar estos modelos predictivos con las amenazas factuales que viven las entidades bancarias. El original resultado no hace otra cosa más que permitirnos confirmar la existencia de una relación significativa entre ambas variables y a la vez confirma las proyecciones de Gutta et al. (2025) que proponen la AI como un punto muy importante a tener en cuenta en la ciberseguridad financiera. Al final, parece que la inteligencia artificial se ha convertido en el factor clave para actualizar la detección de las amenazas avanzadas y por tanto reforzar la integridad y la estabilidad operativa de las entidades bancarias ante los desafíos actuales del escenario digital.

Du et al. (2025), quienes consideran la inteligencia artificial desde un enfoque relacionado con la forma de la protección de la información personal en el ámbito de la Ley N.º 29733, se lograron identificar motivos

sobresalientes en relación con la gestión de riesgos y la importancia de contar con un marco regulatorio sólido. Incluso (Abualhassan et al., 2026) presuponen que los modelos predictivos de IA y la resiliencia del sistema bancario frente a APTs, los momentos presentes exhibieron cómo estos modelos fueron útiles para la mejora de la capacidad de recuperación para el sector financiero frente a los ataques avanzados. Si bien la investigación previa se orientaba hacia el marco normativo y los dilemas éticos; la investigación del presente trabajo mostró la relación asociada entre los modelos predictivos de inteligencia artificial y la resiliencia del sistema bancario que hace frente a las amenazas persistentes. Con esto se reafirma la idea de que esos modelos podría ayudar a la anticipación y al seguimiento de los riesgos cibernéticos, conjugando las recomendaciones regulatorias que establece el estudio (Arulkumar & K, 2025).

La inteligencia artificial (IA) en la gestión de servicios de tecnología de la información (TI) fue capaz de aumentar la eficiencia, reducir costos y mejorar la toma de decisiones, así como indican (Choudhary & Khaitan, 2026). En un contexto de importantes cambios, como la resistencia al cambio organizacional y el riesgo del reemplazo de tareas humanas, lo que puede impactar el empleo, lo que indica (Bodström & Hämäläinen, 2026). En el presente estudio estaba presente de forma análoga una relación positiva entre los modelos de predicción de la IA y la constante actualización de las estrategias de defensa contra APT. A diferencia del estudio mencionado que aborda el impacto de la IA en los servicios generales de TI en concreto, este estudio se detiene más en la aplicación relativa a la evolución de las estrategias de defensa de ciberseguridad dentro del sector bancario. Los resultados son consistentes con las conclusiones de (Lee et al., 2025), que insisten en que los modelos predictivos no son solo una mejora de los procesos, sino que también favorecieron la adaptación de manera continua de las herramientas de seguridad para las nuevas amenazas, enfatizando su importancia en un entorno cibernético con riesgo elevado.

Conclusiones

Dado lo anteriormente expuesto, se constata que la inclusión de modelos predictivos basados en IA no es solo una cuestión técnica, sino que constituye un cambio radical en lo que tiene que ver con la seguridad en el sector bancario limeño. Es decir, los bancos no dependen de muros digitales (muros de protección) estáticos, sino que otorgan al sistema la posibilidad de "comprender" y procesar volumetrías masivas de datos en tiempo real, lo que configura una diferencia abismal con respecto a la defensa convencional. Gracias a su base en el aprendizaje automático, las entidades son capaces de ir interpretando patrones de comportamiento y anomalías antes de que se hayan vuelto irreparables, es decir, de transformar una infraestructura reactivamente pura en una arquitectura inteligente que anticipa el movimiento del atacante.

Del mismo modo, el uso de estas herramientas también favorece la resistencia de la infraestructura financiera a las incursiones que son sostenidas. La IA genera la optimización de los procesos de defensa; se avanzan en la resistencia actual, además de la evolución de los mecanismos de defensa, ello es importante, porque la IA de forma continua permite que los procesos de protección sean más sofisticados conforme se va avanzando en los vectores de ataque, lo que permite una evolución de los sistemas de protección conforme a los vectores de ataque, que siempre están en cambio.

Dada la característica evasiva y el carácter que poseen las APT (amenazas persistentes avanzadas), el sector bancario requiere mecanismos de defensa que se adapten a ese carácter dinámico y, a la vez, puedan autoaprender. En este sentido, la interacción de la incorporación de modelos predictivos en los SOC (Centros de Operaciones de Seguridad) mejora enormemente el nivel de anticipación respecto de los riesgos implícitos. Esta tecnología no se limita a la detección de la intrusión en tiempo real, sino que también proyecta las vulnerabilidades que pueden aparecer en el futuro más próximo, dotando al nivel de seguridad operativa de la capacidad de anticipar las incidencias para consolidar el perímetro digital proactivamente.

Se pone de manifiesto el impacto de la inteligencia artificial de cara a disminuir los riesgos en la ciberseguridad bancaria permitiendo a las instituciones anticiparse a los ataques y fortalecer sus sistemas ante las numerosas y crecientes amenazas digitales.

Recomendaciones

Las entidades bancarias deberían centrarse en la implementación de programas de capacitación técnica especializada mientras se hace seguimiento a la idoneidad continuada de sus arquitecturas de IA; a diferencia de los enfoques puramente teóricos que se han analizado en la literatura, este trabajo demuestra que la incorporación empírica de las amenazas reales junto a los modelos predictivos constituye la clave para perfeccionar la defensa; por ello, la inversión en tecnología ha de ir acompañada de un camino de desarrollo de competencias en el capital humano para garantizar la viabilidad frente a los retos actuales.

Con todo ello, también se recomienda desarrollar protocolos específicos basados en IA que ayuden a mejorar la detección adelantada. Para verificar que estos sistemas son eficaces, es necesario programar y realizar simulacros

periódicos dirigidos a los equipos de ciberseguridad que permitan auditar la eficacia de la capacidad de respuesta real del sistema ante amenazas complejas, asegurando de este modo que las herramientas predictivas están correctamente afinadas para contrarrestar ataques de alta persistencia.

Se aconseja a las áreas de infraestructura tecnológica de las entidades financieras reforzar la resiliencia del sistema frente a las APT, garantizando la implementación de herramientas que permitan el monitoreo y la mitigación continua de los riesgos.

Resulta apropiado establecer calendarios de actualización de los modelos predictivos de IA contra amenazas con carácter más sofisticado, la actualización de las mejoras se guarda alineada a las tendencias globales de innovación tecnológica y futuras APT.

Referencias Bibliográficas

Abualhassan, Z., Hassan, E., Husni, D., Alothman, B., Shehata, N., Trabelsi, M., Shyha, I., Jaradat, S., & Al-Dubai, A. (2026). Malware recognition using novel convolutional neural network with residual connections. International Journal Of Machine Learning And Cybernetics, 17(3). https://doi.org/10.1007/s13042-025-02815-6

Alageel, A., & Maffeis, S. (2026). Investigation of advanced persistent threats network-based tactics, techniques and procedures. Computer Networks, 278, 112069. https://doi.org/10.1016/j.comnet.2026.112069

Almazarqi, H. A., Woodyard, M., & Marnerides, A. K. (2025). BotPro: Data-driven tracking & profiling of IoT botnets in the wild. Computers & Security, 162, 104778. https://doi.org/10.1016/j.cose.2025.104778

Arulkumar, D., & K, K. (2025). Metastack-aptnet: An ensemble deep learning framework for advanced persistent threat detection and mitigation in cyber-physical systems using blockchain technology. Computers & Electrical Engineering, 130, 110838. https://doi.org/10.1016/j.compeleceng.2025.110838

Banco Bilbao Vizcaya Argentaria S.A. ”BBVA ”. (2025, 10 de septiembre). La IA, en los dos lados de la ciberseguridad: aliada y amenaza en el mundo digital. BBVA. https://www.bbva.com/es/innovacion/la-ia-en-los-dos-lados-de-la-ciberseguridad-aliada-y-amenaza-en-el-mundo-digital/

Belali, F., Essetty, A., Bah, S., Wafi, I. E., & Daghouri, A. (2026). Design of a resilient multi-layered security framework for satellite communications. International Journal Of Information Security, 25(2). https://doi.org/10.1007/s10207-025-01184-z

Bodström, T., & Hämäläinen, T. (2026). Raw binary data usage with deep learning for advanced persistent threat attacks early stage detection. International Journal Of Machine Learning And Cybernetics, 17(2). https://doi.org/10.1007/s13042-025-02853-0

Choudhary, N., & Khaitan, V. (2026). Dependability Analysis of Cloud-Based VoIP Under an Advanced Persistent Threat Attack: A Semi-Markov Approach. Transactions On Emerging Telecommunications Technologies, 37(2). https://doi.org/10.1002/ett.70353

De la Hoz Suárez, B. A., Moran, I. F. L., Tete, A. E. M., & De la Hoz Suárez, A. I. (2024). Inteligencia artificial como estrategia para gestionar los procesos de auditoría financiera. Revista Estrategia Organizacional, 13(1), 57-72. https://doi.org/10.22490/25392786.7818

Deng, X., Li, P., Wang, C., Wang, R., Liu, Y., Han, W., & Tian, Z. (2026). A Stackelberg game based deception defense strategy against APT under resource constraints. Science China Information Sciences, 69(3). https://doi.org/10.1007/s11432-025-4530-7

Du, Y., Ren, W., Li, W., Wang, M., Wang, W., Zhang, H., & Xia, M. (2025). GA-ConvE: An APT attack prediction method based on combination of graph attention network and 2D convolution. Neural Networks, 195, 108216. https://doi.org/10.1016/j.neunet.2025.108216

Duan, L., Wen, M., & Xiong, Y. (2025). MLDSJ: a multi-level feature joint attribution method for APT group based on threat intelligence. EURASIP Journal On Information Security, 2026(1). https://doi.org/10.1186/s13635-025-00222-6

Enrique, D. M. L., & Samuel, A. H. E. (2025, 22 junio). Implementación de una Solución de Seguridad para el Filtrado Web y el Acceso Remoto Seguro a Aplicaciones Empresariales mediante el uso de Zero Trust Network Access (ZTNA). http://hdl.handle.net/10757/685827

Gutta, A., S, S., M, N., Shetty, Y. A., C, D., G, A., & Kamwa, I. (2025). A security-centric SCADA framework for wind energy systems using enhanced network segmentation and rogue traffic visualization. Results In Engineering, 29, 108535. https://doi.org/10.1016/j.rineng.2025.108535

Hassanzadeh, E., Hajiabadi, M. E., Samadi, M., & Lotfi, H. (2023). Improving the resilience of the distribution system using the automation of network switches. The Journal Of Engineering, 2023(2). https://doi.org/10.1049/tje2.12238

Hua, B., & Xi, H. (2025). A privacy preserving intrusion detection framework for IIoT in 6G networks using homomorphic encryption and graph neural networks. Scientific Reports, 16(1), 2297. https://doi.org/10.1038/s41598-025-32087-7

Hussain, N., Li, S., Hussain, A., Ullah, Z., & Jamjoom, M. (2025). Quantum-aware secure blockchain intrusion detection system for industrial IoT networks. Scientific Reports, 16(1), 2265. https://doi.org/10.1038/s41598-025-31985-0

Iturbe, E., Dalamagkas, C., Radoglou-Grammatikis, P., Rios, E., & Toledo, N. (2025). A pattern-aware LSTM-based approach for APT detection leveraging a realistic dataset for critical infrastructure security. Future Generation Computer Systems, 178, 108308. https://doi.org/10.1016/j.future.2025.108308

Kalogiannidis, S., Patitsa, C., & Chalaris, M. (2024). The Integration of Artificial Intelligence in Business Communication Channels: Opportunities and Challenges. WSEAS TRANSACTIONS ON BUSINESS AND ECONOMICS, 21, 1922-1944. https://doi.org/10.37394/23207.2024.21.157

Lee, S., Seo, H., Heo, H., Wang, A., Shin, S., & Kim, J. (2025). SecTracer: A framework for uncovering the root causes of network intrusions via security provenance. Computers & Security, 161, 104760. https://doi.org/10.1016/j.cose.2025.104760

Lewis, A. (2026). The Red Queen of cyberspace: The persistence of advanced persistent threats (APTs) explained through co-evolution. Technology In Society, 86, 103238. https://doi.org/10.1016/j.techsoc.2026.103238

Madrid, J. (2024). El impacto de la Inteligencia Artificial en la protección de datos personales y el acceso a la información. https://www.ucm.es/eg/file/el-impacto-de-la-inteligencia-artificial-en-protecci%C3%93n-de-datos-personales-y-acceso-a-la-informaci%C3%93n?ver.

Melo, V. (2022). Inteligencia artificial, desinformación y protección de datos personales. In Itinere. Revista Digital de Estudios Humanísticos de la Universidad FASTA, 12(1),26–37. https://revistas.ufasta.edu.ar/index.php/initinere/article/view/234/pdf_174

Molina, O. (2023). Inteligencia artificial, Bigdata y Derecho a la protección de datos de las personas trabajadoras. Revista de Estudios Jurídico Laborales y de Seguridad Social (REJLSS), 6, 89-117. https://revistas.uma.es/index.php/REJLSS/article/view/16225/16626

Olasehinde, D. O., Bamisile, O., Ejiyi, C. J., Zhang, G., Cai, D., Li, J., Wei, L., & Huang, Q. (2026). Cybersecurity in cyber-physical power systems: analyzing vulnerabilities, threats, and control structures. Cluster Computing, 29(3). https://doi.org/10.1007/s10586-025-05894-w

Pardiñas, S. (2020). Inteligencia Artificial: un estudio de su impacto en la sociedad. https://ruc.udc.es/rest/api/core/bitstreams/e6401877-6b89-4b3c-9c51-0e8e5ec26224/content

Ren, W., Zhao, L., & Li, W. (2026b). A knowledge extrapolation model for attack inference based on graph attention networks and relation mapping. Knowledge And Information Systems, 68(1). https://doi.org/10.1007/s10115-025-02669-y

Sarker, I. H. (2022). AI-Based Modeling: Techniques, Applications and Research Issues Towards Automation, Intelligent and Smart Systems. SN Computer Science, 3(2), 158. https://doi.org/10.1007/s42979-022-01043-x

Shen, J., Li, F., Hashemi, M., & Fang, H. (2025). Resilient and Robust Controller Design in Large-Scale Multi-Agent Industrial Cyber-Physical Systems. Journal Of Dynamic Systems Measurement And Control, 148(3). https://doi.org/10.1115/1.4070173

Wang, H., Chen, W., Li, L., Pu, H., & Zhang, Y. (2026). Dinspector: Dual factor graph attention mechanism for Advanced Persistent Threat detection. Engineering Applications Of Artificial Intelligence, 167, 113861. https://doi.org/10.1016/j.engappai.2026.113861

Yang, L., Ye, A., Liu, Y., Lu, W., & Huang, C. (2025). LLM-APTDS: A high-precision advanced persistent threat detection system for imbalanced data based on large language models with strong interpretabilit. Future Generation Computer Systems, 178, 108315. https://doi.org/10.1016/j.future.2025.108315

CORRESPONDENCIA:

Héctor Martín Espinoza Villavicencio

2022032322@unfv.edu.pe