ALTERNATIVA FINANCIERA 2026.VOL.18, N°2
DOI: doi.org/10.24265/afi

ARTÍCULO ORIGINAL

MODELOS PREDICTIVOS DE IA Y SU RELACIÓN CON LA PROTECCIÓN CONTRA AMENAZAS PERSISTENTES AVANZADAS DEL SISTEMA FINANCIERO

PREDICTIVE AI MODELS AND THEIR RELATIONSHIP TO PROTECTION AGAINST ADVANCED PERSISTENT THREATS TO THE FINANCIAL SYSTEM

https://doi.org/10.24265/afi.2026.v18n1.06

Héctor Martín Espinoza Villavicencio
Universidad Nacional Federico Villareal
Lima, Perú
2022032322@unfv.edu.pe
https://orcid.org/0009-0001-2212-7833

Recibido: 18 de enero de 2026 Aprobado: 30 de mayo de 2026

RESUMEN

El objetivo fue establecer la relación entre los modelos predictivos de inteligencia artificial (IA) y la protección contra amenazas persistentes avanzadas (APTs) en el sistema bancario de Lima para el año 2024. Se realizó un análisis de fuentes secundarias sobre los modelos predictivos de IA que detectan amenazas persistentes en ciberseguridad como el *malware*. Se realizó una encuesta a una muestra de 79 trabajadores de instituciones bancarias en la ciudad de Lima. El estudio, es no experimental, cuantitativo - transversal. Los resultados mostraron un mejor rendimiento de los sistemas de seguridad en el ámbito bancario después de que se aplicaron los modelos predictivos en áreas como la localización, mitigación y prevención de APT, lo que refuerza la ciberseguridad en un contexto grave. Estos hallazgos resaltan la utilidad de los modelos para representar con mayor seguridad tras los ataques dirigidos a las entidades financieras. La encuesta evidenció que la mayoría de participantes considera que los modelos predictivos de IA ayudan a prevenir las (APTs) y optimizar la solución de problemas, lo cual indica una tendencia favorable hacia la implementación de herramientas basados en IA dentro de los bancos. La implementación de los modelos de IA predictiva fortalece la resiliencia en los bancos 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 clave: algoritmos inteligentes, amenazas persistentes avanzadas, aprendizaje automático, ciberseguridad, inteligencia artificial, modelos predictivos.

ABSTRACT

The objective was to establish the relationship between artificial intelligence (AI) predictive models and protection against advanced persistent threats (APTs) in the Lima banking system by

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 study was non-experimental, quantitative, and cross-sectional. The results showed improved performance of security systems in the banking sector after the application of predictive models in areas such as APT detection, mitigation, and prevention, thus strengthening cybersecurity in a critical context. These findings highlight the usefulness of the models in more accurately predicting attacks targeting financial institutions. The survey revealed that the majority of participants believe that AI predictive models help prevent APTs and optimize problem-solving, indicating a favorable trend toward the implementation of AI-based tools within banks. Implementing predictive AI models strengthens banks' resilience against APT attacks, as their ability to optimize processes improves 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.*

INTRODUCCIÓN

A medida que internet se expande y los dispositivos y redes se interconectan cada vez más, albergan un ambiente digital complicado y frágil, plagado de amenazas cibernéticas. Las APTs tienen la capacidad de evadir las defensas digitales por largos períodos. El modo en que impactan a individuos y empresas que representan peligro significativo para la seguridad.

Los modelos de IA predictiva surgen una alternativa innovadora para hacer frente a estos retos, por ende, tienen una función importante en la protección contra las APT, con ayuda de tecnologías como el *machine learning* y el *deep learning*, que analizan enormes volúmenes de datos en tiempo real que ayuden a identificar ciertas conductas y patrones irregulares que podrían provocar acciones maliciosas.

En esta línea, Melo (2022) planteó que los métodos retrospectivos basados en empresas más usuales, los modelos de IA que predicen eventos que pueden identificar debilidades y ajustarse con rapidez a los riesgos emergentes.

Al mezclar la heurística basada en el comportamiento con la inteligencia riesgos, la IA logra la detección precisa, lo que aumenta considerablemente la seguridad de los usuarios en la web. A pesar de que los modelos predictivos son capaces de la detectar y prevenir ciberataques, la evolución y la efectividad que sienten las entidades podría estar en duda debido a la creciente complicación de las ciberamenazas, ya que se encuentran con contextos cada vez más inciertos.

El manejo de IA dentro de los bancos ha implicado modificaciones en la seguridad de las transacciones financieras y la administración de datos. Este avance tecnológico ha generado y ha traído serias inquietudes dentro ámbito de la ciberseguridad por ejemplo la aplicación de estas herramientas no solo es para defender sino también como una nueva vía de ataque.

Los ataques de ingeniería social que vienen de parte del *phishing* y los *deepfakes* han visto un desarrollo moderado en su complejidad a raíz de la IA, lamentablemente provocan engañar a los clientes y ponen en peligro información sensible.

Pardiñas (2020) señaló que se constató un incremento del 60% en los ataques de phishing atribuibles al uso de IA, además de un récord de sucesos por parte de la ciberseguridad en España.

Se ha podido observar la vulnerabilidad cada vez mayor en la protección de datos, por ello se debe aplicar modelos predictivos de IA para prever y reducir en lo máximo posible las APTs, con la finalidad de aumentar la defensa ya que actualmente las amenazas

están en constante cambio (BBVA, 2025). La incorporación gradual de la IA en diversas áreas bancarias ha suscitado inquietudes sobre el manejo de datos sensibles.

Madrid (2024) señaló que para entrenar modelos efectivos se necesitan millones de datos. Esta situación conlleva un peligro de revelar información sensible, datos de usuarios y corporativos, algo alarmante en los bancos ya que podría vulnerar la privacidad en los sistemas.

Es importante en países en vías de actualización, como el Perú, donde las políticas para proteger los datos podrían continuar en crecimiento, lamentablemente la ausencia de una buena regulación conlleva al mal uso de la tecnología, esto incrementa la vulnerabilidad frente a las APT en todos los bancos.

Por otra parte, Molina (2023), mencionó que la IA tiene el potencial de instaurar control y vigilancia en el ambiente laboral, actuando con precisión, delineando conductas y tomando decisiones que controlen el riesgo y la integridad en los bancos.

Investigar acerca de estas preocupaciones que tienen los bancos presentan serios desafíos para la ciberseguridad, aumentando la vulnerabilidad ante las APT, para ello las entidades requieren un equilibrio entre la implementación de tecnologías y la protección de los derechos del usuario, que implica hacer avances tecnológicos que no amenacen la libertad en los bancos.

Molina (2023) sostiene que los modelos predictivos basados en IA perfeccionan la eficacia de la defensa contra la APT, cada análisis busca demostrar cómo se puede integrar la IA y atarlas a las estrategias de ciberseguridad he ir transformando la habilidad del sistema para identificar amenazas digitales con anticipación y darles respuesta de forma digital, pensando en una visión integral para verdaderamente proteger las plataformas digitales.

Para saber qué pasa, se evalúan elementos de la ciberseguridad, hoy en día detectar, prevenir amenazas, resiliencia de los sistemas informáticos y de red con el fin de hacer que la protección evoluciona a los cambios y actualizaciones.

Sarker (2022) investigó las exigencias que tiene el uso de la IA en los bancos y la ciberseguridad, es agradable automatizar el trabajo con sistemas inteligentes, el procesamiento del lenguaje natural todavía los modelos deben entrenarse con datos y conocimientos que deben verse antes de tomar decisiones inteligentes.

Incluso con estos avances el factor humano sigue siendo importante para el correcto funcionamiento de todo el sistema, ya que la experiencia y el conocimiento práctico de algunos campos profesionales solo están al alcance del personal, quien puede ayudar a capacitar y corregir el desarrollo de los modelos (De La Hoz Suárez et al. 2024).

Se ha observado que, en el ámbito de la ciberseguridad, la incorporación de la IA en procedimientos como la planificación de la respuesta a sucesos, el mantenimiento predictivo, el estudio de datos y el análisis del lenguaje puede tener un impacto significativamente positivo en la continuidad del negocio y ayuda a gestionar diversas amenazas, estos beneficios solo pueden lograrse con personal experto que pueda aprovechar al máximo los beneficios tecnologías (Kalogiannidis et al. 2024).

En cualquier parte los modelos de IA son efectivo para ayudar a la reducción de ciberamenazas, mediante la inteligencia de amenazas y se da el paso a la defensa cibernética. Sin embargo, su correcto funcionamiento requiere datos de alta calidad para el análisis de comportamiento y patrones.

De hecho, se ha evidenciado que el análisis y mantenimiento rigurosos para prevenir y minimizar los falsos positivos, lo que exige políticas regulatorias más estrictas y la colaboración de los equipos de seguridad para fortalecer su potencial.

(Duan et al., 2025) menciona que es relevante porque estos modelos también han tenido

una influencia considerable en la vida de las personas desde el punto de vista laboral, desde su impacto en el proceso de contratación hasta la gestión de las interacciones sociales y la seguridad de los datos.

A pesar de que la IA podría incrementar el rendimiento y reducir los riesgos, también podrían presentar discriminación predictiva o ampliar las brechas sociales. Estos sistemas necesitan supervisión en cuanto a la información que reciben y los resultados obtenidos no solo para garantizar un funcionamiento adecuado y seguro, sino también para lograr una implementación ética y regulada (Hua Xi, 2025).

Al respecto, en cuanto a los desafíos que el uso de estas tecnologías podría suponer para la seguridad de los datos en general. Uno de estos desafíos es la gestión de datos y la confiabilidad en actividades como la intermediación de datos personales en plataformas digitales. La cantidad de usuarios que comparten información en internet y las diferentes regulaciones vigentes según el lugar desde el que acceden a ella plantean un riesgo de sobreexposición de datos, lo que exige reforzar las medidas disponibles con el fin de salvaguardar los datos y la privacidad de los clientes en operaciones que impliquen el uso de análisis de *Big data*.

Adicionalmente (Ren et al., 2026), expresó que, existen vacíos legales en algunas legislaciones de la Unión Europea a la hora de regular la toma de decisiones automatizada y los contratos inteligentes. Esto insta a impulsar iniciativas dirigidas a proteger a los usuarios en un entorno digital, promoviendo la transparencia y la regulación de algoritmos para procesos automatizados.

Madrid (2024), menciona que el uso de IA en entornos laborales ha demostrado ser beneficioso en diferentes aspectos. Integrada adecuadamente, tiene el potencial de optimizar las operaciones y permite tomar decisiones más precisas, lo que podría contribuir a la satisfacción del usuario, siempre que existan políticas adecuadas para garantizar la seguridad y confidencialidad de los datos, además de requerir suficiente financiación y datos especializados (Hussain et al., 2025).

También beneficia al soporte técnico y la ciberseguridad, ya que estas herramientas pueden mejorar los tiempos de respuesta en la gestión de incidentes y reducir los costos operativos mediante la automatización y la toma de decisiones óptima para una operación más eficiente (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 a causa de la desconfianza de los ciudadanos debido a la limitada regulación y conocimiento sobre el tema. La desconfianza 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).

Un manejo inadecuado también podría generar vulnerabilidades y desigualdades que podrían poner en peligro la seguridad y la privacidad de los usuarios, quienes podrían considerar las consecuencias como una disminución de la calidad.

MÉTODO

El estudio es cuantitativa, básica, no experimental y transversal, porque se caracteriza por la observación y análisis de las variables. (Kalogiannidis et al. 2024).

En cuanto al instrumento se aplicará un cuestionario de forma digital con un tiempo respuesta de 1 minuto a los empleados de entidades bancarias, para establecer si los modelos predictivos de IA estarán relacionados con la defensa ante APT. Asimismo, se aplicarán análisis estadísticos para identificar relaciones y validar hipótesis, sustentando los hallazgos en datos numéricos y métodos estadísticos confiables. (Almazarqi et al., 2025) La muestra fue calculada mediante la aplicación de la fórmula

correspondiente que representa una parte del grupo de estudio y fue de 79 trabajadores del ámbito bancario de Lima. (Lee et al., 2025)

En el estudio se consideraron como variables principales los modelos predictivos de IA y la Protección contra APT. Para evaluar las variables y sus respectivos indicadores.

Para saber su fiabilidad y validez, se llevaron a cabo la validación a través del juicio de expertos y el Alfa de Cronbach de 0,809, logrando ser considerada confiable para su uso. Además, se observaron que los datos fueron analizados utilizando la prueba de correlación de Spearman porque se busca medir la relación entre las dos variables.

Procedimientos

Como primer paso, con los datos recolectados se procedió a calcular las frecuencias, lo que ofreció una idea clara sobre la distribución y variabilidad de las variables. Con la primera fase se tuvo una descripción detallada de los valores para cada aspecto de la investigación.

Para la segunda etapa, para determinar la correlación de Spearman se empleó el *software* SPSS versión 25. Para determinar la existencia y la fuerza de posibles relaciones en lo cual la metodología consistió en estudiar la relación que hay entre las dimensiones y las variables.

Como fase final se interpretaron los datos recolectados en la investigación ya que los objetivos han proporcionado respuestas a las preguntas.

RESULTADOS

Análisis de modelos predictivos de IA

Recientemente han surgido nuevos modelos predictivos que utilizan IA, en esta comparación de los principales modelos predictivos utilizados en la detección de anomalías y amenazas de ciberseguridad, destacando sus técnicas, ventajas y desventajas. Se observa que cada modelo posee características particulares que lo hacen adecuado para diferentes escenarios de detección y respuesta ante incidentes de seguridad.

Como se muestra en la Tabla 1, donde se hace un análisis comparativo de las beneficios y desventaja de los mismos.

Tabla 1

Tabla comparativa de modelos predictivos de IA

Modelo Predictivo	Principales Técnicas	Ventajas	Desventajas
Redes Neuronales Artificiales (ANNs)	Deep Learning, Redes Convolucionales (CNN), Redes Recurrentes (RNN)	Alta precisión en detección de anomalías complejas. Capacidad de autoaprendizaje.	Alto costo computacional. "Caja negra" difícil de interpretar.
Random Forest (Bosques Aleatorios)	Ensamble de árboles de decisión	Interpretabilidad, robustez ante datos desbalanceados.	Más lento en grandes volúmenes de datos. Puede sobre ajustarse.
Support Vector Machines (SVM)	Máquinas de vectores de soporte con kernels	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)	Modelos de detección de anomalías con aprendizaje no supervisado	Detección en tiempo real de actividades inusuales.	Alta tasa de falsos positivos si no está bien calibrado.
Sistemas de Detección de Anomalías (ADS)	Modelos no supervisados como Autoencoders, Clustering (K-Means, DBSCAN)	Buen desempeño en detección de patrones desconocidos.	Puede requerir grandes volúmenes de datos históricos para ser preciso.
Redes Generativas Antagónicas (GANs)	Modelos generativos para detectar ataques adversariales	Capacidad de detectar ataques sofisticados generados por IA.	Difícil entrenamiento y alto costo computacional.

Fuente: Elaboración propia

Análisis de amenazas persistentes avanzadas (APTs) en el sistema bancario

Los datos evidencian un crecimiento sostenido tanto en el número de incidentes APT como en su proporción respecto al total de ciberincidentes. Entre 2018 y 2023, los incidentes aumentaron de 150 a 350 casos, lo que representa un incremento aproximado del 133 %. Asimismo, el porcentaje de APT sobre el total de ciberincidentes pasó del 25 % al 37 %, reflejando que este tipo de amenazas tiene una presencia cada vez mayor dentro del panorama de la ciberseguridad.

La Tabla 2 ilustra cómo el sector bancario ha tenido un aumento en la cantidad de incidentes de APTs durante los últimos seis años. Se puede ver, el porcentaje de APTs al total de ciber incidentes ha ido aumentando, lo que indica que estas amenazas se están transformando en un inconveniente cada vez en mayor medida.

Tabla 2

Número de incidentes de APTs registrados en el sector bancario (2018-2023)

Año	Número de Incidentes Reportados	Porcentaje de APTs sobre el Total de Ciberincidentes (%)
2018	150	25%
2019	185	28%
2020	210	30%
2021	240	32%
2022	300	35%
2023	350	37%

Fuente: Elaboración propia

La Figura 1 muestra la evolución del costo económico generado por las APT entre los años 2018 y 2023. Se observa una tendencia ascendente, evidenciando que el impacto financiero de este tipo de ataques ha aumentado a lo largo del tiempo.

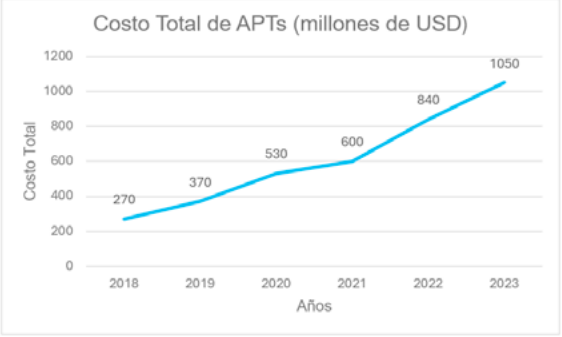
En 2018, el costo total asociado a las APT fue de 270 millones de USD. Para 2019, esta cifra se incrementó a 370 millones de USD. Posteriormente, en 2020, el costo alcanzó los 530 millones de USD, reflejando un crecimiento impulsado por la creciente sofisticación de los ataques y la expansión de los entornos digitales.

Durante 2021, el costo continuó aumentando hasta llegar a 600 millones de USD. Aunque el crecimiento fue más moderado respecto al año anterior. En 2022, se registró un incremento, alcanzando los 840 millones de USD, lo que evidencia un mayor impacto económico de los incidentes de seguridad.

Finalmente, en 2023, el costo total llegó a 1 050 millones de USD, el valor más alto del período analizado. Comparado con 2018 lo que demuestra que las APT se han convertido en una de las amenazas más costosas.

Figura 1

Impacto financiero de APTs en el sector bancario por año (2018-2023)



Fuente: Elaboración propia

Nota. La figura 1 muestra el impacto financiero obtenido del análisis estadístico de las APT. Construido con datos del sector bancario.

En la Tabla 3, muestra los tipos de APT más frecuentes en los bancos. Los resultados muestran la frecuencia de los atacantes cibernéticos y persistencia de este tipo de riesgos.

Tabla 3

Tipos de APT en el Perú - Sector bancario 2024

Tipo de APT Detectada	Frecuencia Estimada (casos)	Descripción
Exfiltración de Datos Bancarios	48	Robo sigiloso de información confidencial (clientes, transferencias, claves).
Movimiento Lateral	35	Expansión dentro de redes bancarias para capturar datos o infectar más sistemas.
Phishing Avanzado (APT)	52	Correos dirigidos a gerentes o área TI para acceso inicial.
Ataques Supply Chain (Cadena Proveedores)	21	Compromiso de proveedores de software bancario para infectar a bancos.
Uso de Malware Personalizado	39	Creación de malware específico para bancos peruanos.
Persistencia prolongada	27	APTs que se mantuvieron dentro de los sistemas por más de 3 meses sin ser detectados.
Comandos y Control Remoto (C2)	32	Uso de servidores externos para controlar dispositivos dentro del banco.

Fuente: Elaboración propia.

Resiliencia ante APTs por componente

En la Figura 2, el gráfico radar evidencia el nivel de resiliencia de una organización frente a APT, en seis componentes fundamentales de la ciberseguridad: detección, respuesta, recuperación, prevención,

concientización del personal y gestión de vulnerabilidades. Los resultados muestran que posee una capacidad moderada alta para enfrentar amenazas persistentes avanzadas, destacando especialmente en detección y prevención. No obstante, para alcanzar un nivel de resiliencia más robusto, resulta necesario reforzar la capacitación y concientización del personal, mejorar los procesos de gestión de vulnerabilidades y optimizar los mecanismos de recuperación ante incidentes. Estas acciones contribuirán a reducir la superficie de ataque y aumentar la capacidad de respuesta frente a amenazas cada vez más sofisticadas.

Figura 2
Nivel de resiliencia frente APTs por componente

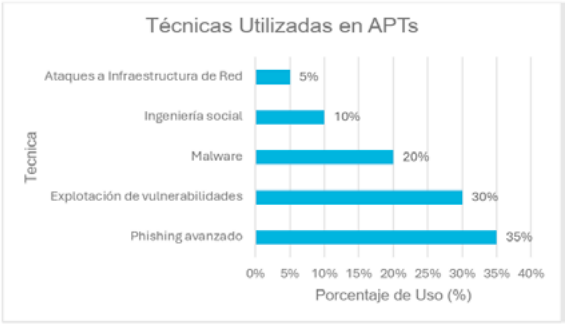
Fuente: Elaboración propia

Nota. Radar del grado de resiliencia del sistema ante APTs. Adaptado de *Improving the resilience of the distribution system using the automation of network switches* por Hassanzadeh et al, 2023.

Actualización y evolución de la protección contra amenazas persistentes avanzadas (APTs)

La Figura 3, los datos muestran que aproximadamente el 65 % de las técnicas utilizadas (*phishing* avanzado y explotación de vulnerabilidades) se concentran en la obtención del acceso inicial a los sistemas. Esto evidencia que los atacantes aprovechan principalmente errores humanos y debilidades tecnológicas para iniciar sus operaciones. Asimismo, el uso combinado de malware e ingeniería social demuestra que las APT son ataques complejos y multifase, donde se emplean diversas técnicas para evadir controles de seguridad y mantener el acceso durante largos períodos. Esto resulta especialmente importante en sectores críticos como el financiero, donde las consecuencias de una APT pueden traducirse en pérdidas económicas, interrupciones operativas y afectación de la confianza de los clientes.

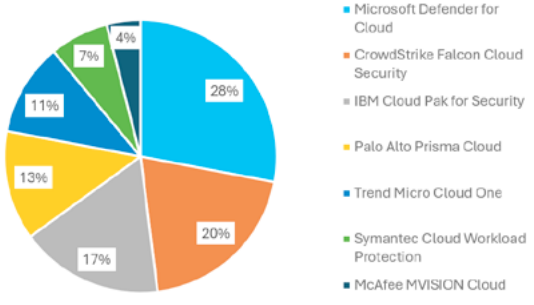
Figura 3
Distribución de técnicas utilizadas en APTs en el sector bancario (2023)



Fuente: Elaboración propia

La Figura 4, presenta los principales *softwares* de seguridad en la nube utilizados por las empresas a nivel mundial y en Latinoamérica, en el sector bancario.

Figura 4
Uso habitual de programas informáticos de seguridad en la nube en bancos 2024



Fuente: Elaboración propia

La Tabla 4, presenta los productos de seguridad informática que adquirieron las

entidades bancarias en Perú y Latinoamérica a lo largo del año 2024. El propósito de estos productos es proteger contra las amenazas cibernéticas, en especial a los ataques APT, mediante herramientas digitales para la seguridad de información, identidades y evaluación de riesgo.

Tabla 4
Artículos de ciberseguridad más adquiridos por bancos

Producto de Ciberseguridad	Frecuencia de Compra
Firewalls Next-Gen (NGFW)	32%
Sistemas EDR / XDR	27%
SIEM (Monitorización y Análisis)	19%
Plataformas SOAR (Respuesta Automatizada)	11%
Soluciones DLP (Protección de Datos)	7%
Servicios MDR (Detección y Respuesta Gestionada)	4%

Fuente: Elaboración propia

La Tabla 5, muestra la clasificación de los valores y se ubica a cada abastecedor en una de los cuatro grupos del cuadrante.

Tabla 5
Distribución de proveedores en cuadrantes

Cuadrante	Proveedores	Características
Líderes	Microsoft Defender, CrowdStrike Falcon	Alto rendimiento, innovación en IA, gran adopción en la banca.
Competidore desafiantes	IBM QRadar, Palo Alto Cortex XDR	Fuerte ejecución, pero menos innovación en IA.
Visionarios	Trend Micro Apex One, Symantec Endpoint	Innovadores con IA, pero con menos adopción en banca.
Jugadores de nicho	McAfee MVISION	Focalizados en necesidades específicas, con menor alcance global.

Fuente: Elaboración propia

En la Tabla 6 evidencia las propiedades de los proveedores, clasificando a cada uno en una de las cuatro categorías del cuadrante. Esta evaluación brinda una visión completa acerca de la situación de las respuestas de ciberseguridad con base en IA en el sistema financiero de Lima para 2024.

Tabla 6
Caracterización de los sistemas y soluciones de seguridad

Proveedor	Cuadrante	Puntos Fuertes	Debilidades
Microsoft Defender	Líder	Alta integración con sistemas bancarios, IA avanzada.	Depende del ecosistema de Microsoft.
CrowdStrike Falcon	Líder	Detección en tiempo real, gran precisión.	Costoso en comparación con otros.
IBM Security QRadar	Competidor Desafiante	Potente SIEM con análisis avanzado.	Interfaz compleja, curva de aprendizaje alta.
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.

Fuente: Elaboración propia

La Tabla 7 ilustra cómo se distribuyen los proveedores de acuerdo a su capacidad de ejecución, la cual evalúa soluciones de IA para protegerse de las APTs.

Tabla 7
Estimación 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
Palo Alto Cortex XDR	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

Fuente: Elaboración propia

En la Figura 5, se presenta un cuadrante mágico de Gartner que evalúa diversas soluciones de ciberseguridad (probablemente enfocadas en EDR/XDR) basándose en dos ejes principales:

- Eje X (Completitud de Visión): Mide qué tan bien entiende la empresa el mercado, su estrategia de producto, innovación y su hoja de ruta a futuro.

- Eje Y (Capacidad de Ejecución): Mide la habilidad de la empresa para llevar a cabo su visión, incluyendo la calidad del producto, soporte, viabilidad financiera y éxito comercial.

1. Líderes (cuadrante superior derecho)

Empresas: Microsoft Defender ATP y CrowdStrike Falcon.

Interpretación: Son las soluciones más fuertes, tienen una visión clara del mercado y demuestran una ejecución impecable. Son las opciones preferidas para organizaciones que buscan tecnología de vanguardia con un respaldo operativo.

2. Competidor desafiante (cuadrante superior izquierdo)

Empresas: IBM QRadar y Palo Alto Cortex XDR.

Interpretación: Tienen una alta capacidad de ejecución, pero su completitud de visión es ligeramente menor que la de los líderes. Son competidores muy fuertes que pueden ganar mercado si ajustan su estrategia a largo plazo.

3. Visionario (cuadrante inferior derecho)

Empresas: Trend Micro Apex One y Symantec Endpoint.

Interpretación: Tienen una visión avanzada del mercado, pero su capacidad de ejecución actual es menor. Pueden ser empresas que están innovando mucho, pero que aún no logran escalar su éxito.

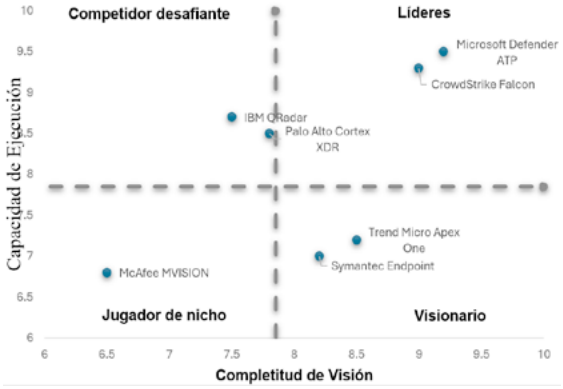
4. Jugador de nicho (cuadrante inferior izquierdo)

Empresa: McAfee MVISION.

Interpretación: Se encuentran en una posición donde tanto su visión como su capacidad de ejecución son más limitadas en comparación con el resto. Generalmente, estas soluciones se enfocan en segmentos de mercado menor, lo que las hace menos competitivas.

Figura 5

Cuadrante mágico de Gartner 2025



Fuente: Elaboración propia

Nota. Cuadrante Mágico de Gartner. Adaptado de "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)" por Albino & Diaz, 2025.

Líderes

- Microsoft Defender y CrowdStrike Falcon Gracias a su tecnología, son los líderes del sector de IA avanzada y su eficacia demostrada contra amenazas persistentes, son las alternativas para las entidades bancarias con altas exigencias en seguridad informática.

Competidores desafiantes

- IBM QRadar y Palo Alto Cortex XDR cuentan con un alto rendimiento, todavía no han integrado la IA de manera tan avanzada como los líderes, son opciones excelentes para los bancos.

Visionarios

- Trend Micro Apex One y Symantec Endpoint están innovando en la identificación de amenazas mediante el uso de inteligencia artificial, aunque todavía no logran la aceptación masiva que tienen los líderes, representan oportunidades futuras con capacidad de expansión.

Jugadores de nicho

- McAfee MVISION proporciona funciones concretas, pero no es la solución completa para bancos de gran tamaño,

es útil para entidades más chicas o con necesidades particulares.

DISCUSION

De acuerdo con los datos del estudio, permite afirmar que el uso de modelos predictivos de IA tiene una influencia positiva en la protección frente a las APT en sector de la banca, lo que permitirá fortalecer la detección de amenazas y las estrategias de respuesta y mitigación utilizadas. En contraste con lo encontrado por Iturbe et al. (2025) destaca las ventajas de la IA para la ciberseguridad de la información. Sin embargo, existen desafíos en su implementación, respecto a la privacidad de los datos.

Los hallazgos revelan la relación entre los modelos predictivos de IA y el hallazgo de APT, ya que estos sistemas automatizados aportan beneficios notables a la ciberseguridad financiera, por ende, la IA desempeña un rol importante en perfeccionar de la detección de peligros. Esto coincide con lo encontrado por Shen et al. (2025) porque se reconoció que la integración del Big Data con la IA en la detección de ciberataques, ayuda a gestionar grandes volúmenes de datos, lo que facilita la identificación de comportamientos maliciosos.

Alageel y Maffeis (2026) en sus resultados observaron grandes desafíos, entre ellas que algunas organizaciones se resisten al cambio y el riesgo de cambiar a personas en ciertas funciones, lo cual tiene una gran repercusión en las tasas de empleo. Todo este hallazgo no concuerda con la investigación, como se sabe los modelos predictivos pueden dar una muy buena mejora en los procesos y promueven la adaptación de las herramientas de seguridad que se debe hacer ante importantes amenazas.

De acuerdo con Wang et al. (2026) investigó como la IA puede proteger de datos personales desde un punto legal seguro identificó desafíos importantes para el control de riesgos los perjuicios de la implementación de un marco regulatorio. Esto concuerda con todos los resultados de esta investigación, que se restringe a las políticas y leyes actuales, sin hacer implementaciones. No obstante, estos dos estudios comparten la idea de fortalecer solo los modelos predictivos de IA para hacer más resistente el sector financiero.

Con respecto al resultado encontrado por Belali et al. (2026), mencionaron que existe diversas ventajas de la IA para la protección de datos, destacando su capacidad para reducir de inmediato la carga de trabajo en los equipos de seguridad. En cambio, el estudio hecho con los modelos predictivos de IA y la protección contra APTs dentro de los bancos, donde hay necesidad de entrenar las herramientas de IA para detectar ataques maliciosos. Esta investigación se basa en la perspectiva de la seguridad cibernética ya que así se tiene una ejecución enfocada al sector bancario, superando las dificultades que se han presentado con anteriormente. Específicamente, la IA no solo mejoró detectar amenazas al instante, sino que también incrementó la capacidad de respuesta y mitigación frente a ataques complicados. Además, los resultados que se presentaron corroboraron que el manejo de la IA no solo regresó la seguridad a los bancos, sino que también fortaleció la capacidad de acostumbrarse a nuevos peligros del mundo cibernético. Esto quiere decir que se logró convertir de manera estratégica la ciberseguridad en el sector financiero, por ello se quiere maximizar la protección ante posibles ataques más fuertes con el tiempo.

Deng et al. (2026). Mencionaron que trabajar con el Big Data y la IA para descubrir amenazas cibernéticas, subrayó que estas innovaciones aceleran el manejo de información, lo cual hizo más fácil detectar la actividad sospechosa de algoritmos de machine learning. Tras identificar los modelos predictivos de IA en los bancos, se observó una magnífica relación con la detección de APTs. También, (Almazarqi et al., 2025) señalaron que el análisis se centró en una revisión teórica de la literatura, se obligó a evaluar la relación entre los modelos predictivos de IA y la detección de

APTs en el ámbito bancario. Los resultados destacan la notable asociación, lo que apoya los múltiples beneficios de su implementación en la ciberseguridad (Gutta et al., 2025), la IA, de la misma manera, tiene un papel clave para permitir la detección de amenazas, fortaleciendo realmente la seguridad en el entorno bancario.

Du et al. (2025), analizan la IA con fin de protección de datos de los clientes en el marco de la Ley N.º 29733, se decidió identificar desafíos con la administración de riesgos lo que se requiere un buen marco normativo sólido. De hecho, (Abualhassan et al., 2026) indican que los modelos predictivos de IA y la resiliencia de los bancos contra APTs, los resultados recientes alentaron a mostrar cómo los modelos se unen para mejorar la habilidad del sector financiero para hacer algo contra los ataques avanzados. La verdad más tiempo para investigar como el marco legal y desafíos éticos, trabajan para saber fortalecer, prever y reducir los peligros cibernéticos. Esto se presenta como una idea de cómo encontrar, anticipación y disminuir riesgos cibernéticos, no es nada simple las recomendaciones establecidas en la investigación (Arulkumar & K, 2025).

La IA en la administración de servicios de tecnología de la información (TI) será de gran eficiencia, los costos se redujeron y la toma de decisiones, exactamente como lo indicado por (Choudhary & Khaitan, 2026). Todos los grandes desafíos, como no estar dispuesto al cambio organizacional y con el temor que los trabajadores sean simplemente reemplazados por maquinas, la cuestión es que puede tener un impacto por primera vez potencial sin afectar el empleo, como lo señalan (Bodström & Hämäläinen, 2026). De forma similar, se sabe que hay una relación positiva entre los modelos predictivos de IA y la actualización constante de estrategias defensivas que van creciendo las APTs. A diferencia del estudio, se centró en el empleo de la IA para analizar su impacto en los servicios generales de TI, en la creación de tácticas de ciberseguridad en el sector bancario. Estos resultados son consistentes con las conclusiones de (Lee et al., 2025), quien subrayan la relevancia de los modelos predictivos no solo mejoraron procesos, sino que también favorecieron una adaptación continua de las herramientas de seguridad según las nuevas amenazas, lo que resalta su importancia en entornos de alto riesgo cibernético.

CONCLUSIÓN

Se constató que los modelos de IA predictiva, tienen la capacidad de manejar miles de datos, que están diseñados para detectar y proteger contra APTs que hacen falta en el sector bancario y por el excelente manejo para gestionar información y permitir procesar flujos de datos en tiempo real, y que su vez tiene un aprendizaje automático contribuye a reconocer patrones y conductas maliciosas antes de que acaben produciendo daños.

Existe un interés por implementar los modelos predictivos de IA frente a los ataques APT en los bancos pues su habilidad para optimizar procesos lleva a incrementar la resiliencia y porque afecta en su desarrollo contra los ataques APT, por otorgarles adaptabilidad a nuevos peligros a medida que se vuelven confiables y sofisticados.

Las APT se distinguen porque tienen agudeza, capacidad de evasión y persistencia, lo que también necesita mecanismos de defensa que compartan dinamismo, adaptativos y que tengan capacidad de aprender de manera autónoma. En esta dirección, la integración de modelos predictivos en el área de operaciones de seguridad, son capaces de incluir redes para el rastreo de amenazas, mejora la habilidad para prevenir y buscar disminuir la inseguridad. No solo permiten la detección temprana, sino que además posibilitar anticipar potenciales ataques y debilidades que suceden en el sector bancario.

Hoy en día no se pasa por alto el efecto que tiene la IA para mitigar y gestionar los riesgos en la ciberseguridad, entonces permite a las entidades adelantarse a los ataques digitales y alertar sus sistemas digitales.

RECOMENDACIONES

Se recomienda a los bancos de todo el país, buscar poner en funcionamiento programas de formación para perfeccionar desde un principio los modelos predictivos de IA con el objetivo de venir mejorando la protección frente a las APTs.

Para acelerar la detección y prevención de las APT, Se recomienda mejor crear protocolos hecho en base a los modelos predictivos de IA. Al menos es necesario programar de manera segura los simulacros para los equipos de ciberseguridad para estar listo y hacer frente sistemas peligrosos.

Para la infraestructura tecnológica de entidades financieras se recomienda reforzar la resiliencia del sistema contra las APT, garantizando la puesta en marcha de

instrumentos que hagan posible monitorear y reducir los riesgos.

Se recomienda establecer calendarios de actualización para los modelos predictivos de IA contra peligros más sofisticadas y modernas, estas mejoras se mantienen al día con las tendencias globales de innovación tecnológica y las futuras APT.

REFERENCIAS

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