Análisis de la aplicación de la inteligencia artificial asociados a la ciberseguridad en el sector financiero

Carlos Rafael Maestre Márquez

Asesor

Hernando José Peña Hidalgo,

Universidad Nacional Abierta y a Distancia – UNAD

Escuela de Ciencias Básicas, Tecnología e Ingeniería – ECBTI

Especialización en Seguridad Informática

2025

Dedicatoria

Este trabajo va dedicado primero a Dios, quien me dio la sabiduría e inteligencia para recorrer todo el camino hasta este momento, siempre llevándome de la mano e iluminándome en los momentos donde no encontraba soluciones. A mi esposa y mis hijos, fuentes de mi inspiración y anhelos de superación, quienes con su apoyo me ayudaron a salir adelante en los momentos en que todo se ponía más difícil, siempre con una palabra de aliento y motivación. A mis padres por el apoyo y la confianza y a esas personas que siempre tuvieron un buen concejo y aportaron su granito de arena con una idea para continuar.

Agradecimientos

Agradezco a Dios que me da la sabiduría para afrontar cada momento de mi vida, a mi familia, fuente de inspiración, a la universidad por abrirme las puertas, a los tutores que se brindaron para poder comprender cada tema, a los compañeros con los cuales realice muchos trabajos colaborativos y a esas personas que siempre se acercaron para brindarme su apoyo y asesoría en diversas situaciones.

Resumen

La IA está transformando el sector financiero de muchas maneras, con su evolución los ciberataques son más complejos y el uso de la inteligencia artificial ayuda a los analistas de seguridad para que puedan anticipar las amenazas y por medio de esta monografía se analizan los avances y beneficios de la implementación de inteligencia artificial para la ciberseguridad en el sector financiero, validando que su importancia se centra en que la inteligencia artificial está mejorando el conocimiento y capacidad para comprender las amenazas de seguridad cibernética y el riesgo cibernético, con una capacidad de razonamiento y análisis de relaciones entre distintos elementos que nos permite identificar amenazas de manera más rápida y eficiente.

***Palabras claves**:* Análisis predictivo, Aprendizaje Automático, Ciberseguridad, Detección de Amenazas, Inteligencia Artificial, Prevención del Fraude, Protección de Datos Financieros, Sector Financiero.

Abstract

AI is transforming the financial sector in many ways, with its evolution cyberattacks are more complex and the use of artificial intelligence helps security analysts to anticipate threats and through this monograph the advances and benefits of the implementation of artificial intelligence for cybersecurity in the financial sector are analyzed, validating that its importance focuses on the fact that artificial intelligence is improving knowledge and capacity to understand cybersecurity threats and cyber risk, with a capacity for reasoning and analysis of relationships between different elements that allows us to identify threats more quickly and efficiently.

Keywords: Artificial Intelligence, Cybersecurity, Financial Data Protection, Financial Sector, Fraud Prevention, Machine Learning, Predictive Analytics, Threat Detection.

Tabla de Contenido

Tabla de Ilustraciones

Lista de Tablas

Listado de Apéndices

Glosario

Ciberdelincuencia

uso ilegal de la tecnología informática para causar daño o destrucción a sistemas informáticos, dispositivos electrónicos y redes de Internet.

Ciberseguridad

Conjunto de medidas que se toman para proteger los sistemas informáticos, las redes y los datos de los ataques cibernéticos.

Fraude

Delito Que involucra el uso de engaño o medios ilegales para obtener algo de valor, como dinero, bienes o servicios.

Inteligencia Artificial

Campo de la informática que se enfoca en crear máquinas que puedan pensar y actuar de forma inteligente.

Machine Learning

Subcampo de la inteligencia artificial que se enfoca en desarrollar sistemas que pueden aprender a partir de datos y mejorar su desempeño con el tiempo.

Ransomware

Tipo De Malware que bloquea el acceso a los datos de una víctima y exige un pago para desbloquearlos. Es una amenaza importante para la ciberseguridad, ya que puede causar daños significativos a las empresas y los individuos.

Phishing

Una Técnica de ingeniería social usada por los delincuentes para engañar a las víctimas para que les proporcionen información personal o financiera haciéndose pasar por personas o entidades de confianza.

Tecnología Financiera (FINTECH)

Uso de la tecnología para mejorar los servicios financieros. A menudo se basa en la inteligencia artificial para automatizar tareas y brindar a los clientes una mejor experiencia.

Transacciones Fraudulentas

Actividades ilegales que involucran la manipulación de transacciones financieras para obtener un beneficio personal

Técnicas De Análisis De Datos

PROceso de recopilar, limpiar, analizar e interpretar datos para obtener información valiosa.

Introducción

La tecnología está transformando la era digital a través de cambios constantes, destacándose actualmente la implementación de la inteligencia artificial en diversas operaciones, modificando sustancialmente la eficiencia y eficacia en los procesos, desafiando la ciberseguridad en las operaciones, debido a la complejidad de las nuevas y avanzadas amenazas, lo que está demandando innovación en la implementación de estrategias que permitan mantener la integridad, confidencialidad y disponibilidad de la información.

El sector financiero es muy atractivo para los ciber atacantes y en el año 2022 quedo demostrado, cuando se revelo por parte de la consultora Cybersecurity Ventures que este sector tuvo pérdidas ese año de 6.000 millones de dólares a nivel mundial.

La inteligencia artificial está revolucionando todos los ámbitos a nivel global y el sector financiero no es la excepción, ya que esta industria ha adoptado dicha innovación para optimizar sus sistemas de seguridad cibernética, destacándose en la detección de patrones de datos sospechosos que contribuyen a la prevención de ciberataques y a una respuesta más eficaz y eficiente ante los mismos, destacando que, si bien la inteligencia artificial es utilizada en el sector financiero para prevenir, mitigar y gestionar riesgos, también es empleada de manera crítica por ciberdelincuentes para fines maliciosos.

Es importante generar un análisis de la aplicación de la inteligencia artificial asociada a la ciberseguridad en el sector financiero, a través de la revisión de fuentes confiables, especializadas que permitan contextualizar el poder que tiene el uso de la inteligencia artificial en las empresas.

Planteamiento del Problema

Antecedentes del Problema

En el actual entorno digital, el sector financiero se ha convertido en un objetivo principal de los ciberdelincuentes gracias a la cantidad de datos confidenciales y transacciones financieras que manejan, todo esto debido a la creciente sofisticación de los ataques cibernéticos, por ello las instituciones financieras han buscado soluciones más avanzadas para protegerse contra estas amenazas, siendo una de estas soluciones la aplicación de la inteligencia artificial, que ha demostrado ser una herramienta prometedora en la detección y prevención de ataques cibernéticos; sin embargo, su implementación en el sector financiero plantea desafíos y problemas únicos, como la falta de comprensión y conocimiento sobre cómo la IA puede ser utilizada de manera efectiva para fortalecer la ciberseguridad en casos como la detección de fraude y las vulnerabilidades en los sistemas de seguridad.

Kaspersky destaca, que la Inteligencia Artificial no es una solución infalible; a pesar de sus capacidades avanzadas, todavía existen vulnerabilidades y debilidades que pueden ser explotadas por los atacantes, ya que un estudio realizado por esta firma de seguridad cibernética reveló que el 53% de las organizaciones financieras han experimentado al menos un incidente de seguridad relacionado con la IA en los últimos dos años (Kaspersky, 2022).

El *New York Times*, menciona que uno de los problemas de ciberseguridad en el sector financiero asociado a la IA es el ataque al Banco de Bangladesh en 2016, donde los delincuentes utilizaron malware para infiltrarse en el sistema del banco y robaron 81 millones, describiendo que el ataque fue posible debido a la falta de medidas de seguridad adecuadas y la falta de capacitación en el uso de la IA para detectar y prevenir este tipo de ataques (New York Times, 2017). En 2019, Capital One, una de las mayores instituciones financieras de Estados Unidos,

sufrió un ciberataque que comprometió la información personal de más de 100 millones de clientes; esto se debió a que el atacante explotó una vulnerabilidad en el sistema de seguridad de la nube de Amazon Web Services y utilizó la inteligencia artificial para escanear y recopilar información (New York Times, 2019).

Formulación del Problema

¿Cuál es el impacto de la aplicación de inteligencia artificial en la ciberseguridad en las organizaciones del sector financiero colombiano?

Justificación

El avance de la tecnología por medio de su transformación digital ha llegado con grandes beneficios al sector financiero, pero también han traído consigo nuevos desafíos en términos de ciberseguridad, por ello el uso de la IA en este medio se ha vuelto muy importante para proteger los sistemas y datos sensibles de las instituciones financieras, teniendo como objetivo principal identificar y mitigar las amenazas cibernéticas de manera más eficiente y efectiva. Para lograr esto, es esencial conocer las herramientas de IA utilizados en el sector financiero, examinar su uso para la ciberseguridad y proponer recomendaciones que usen aplicaciones como mecanismos de ciberseguridad inteligentes.

Es indispensable identificar los sistemas de IA utilizados en el sector financiero, los cuales pueden incluir algoritmos de aprendizaje autónomo para el análisis de grandes cantidades de datos que permitan la detección de patrones y anomalías, también el sistemas de ingresos no autorizados basados en Inteligencia Artificial que monitorean la red en busca de actividades sospechosas y sistemas de análisis de comportamiento que identifican actividades fraudulentas, ya que al comprender cómo funcionan estos sistemas, es posible evaluar su efectividad y determinar cualquier vulnerabilidad potencial, además, es importante examinar el uso de la IA en el sector financiero ya que el análisis de la aplicación de la inteligencia artificial en la ciberseguridad permitirá proponer recomendaciones al sector en cuanto a los mecanismos de ciberseguridad inteligentes que pueden usar para permitir el aseguramiento de los activos de información (Kaspersky, 2022; New York Times, 2019).

Objetivos

Objetivo General

Analizar el impacto de la aplicación de la inteligencia artificial asociado a la ciberseguridad en el sector financiero a través de una revisión de fuentes documentales especializadas con el fin de contextualizar a las empresas del poder global y competitivo que estas tecnologías generan.

Objetivos Específicos

Identificar el impacto del uso de la inteligencia artificial en el sector financiero para conocer sus implicaciones en caso de un incidente de ciberseguridad, basado en el estudio de fuentes documentales

Examinar casos del sector financiero que emplean inteligencia artificial, mediante consulta en fuentes especializadas, para identificar vulnerabilidades, amenazas y riesgos más recurrentes en este contexto.

Proponer recomendaciones que permitan adoptar soluciones de inteligencia artificial a partir de la revisión de casos de estudio exitosos para el fortalecimiento de la ciberseguridad en entidades del sector financiero colombiano

Marco Referencial

Marco Teórico

Inteligencia Artificial, Inspiración para la Ciberseguridad

En el mundo moderno las tecnologías de la información y la comunicación son partes de la cotidianidad y el entorno, pero sin lugar a duda, la inteligencia artificial ha venido a transformarlo todo; su llegada causa tanto impacto que conforme se investiga y estudia son más las innovaciones y experimentos que se hacen entorno a ella.

Como lo señala Muñoz Fonseca et al., (2021) "Originalmente la Inteligencia Artificial se construyó en base a conocimientos y teorías existentes en otras áreas del conocimiento, algunas de las principales fuentes de inspiración que nutrieron esta área son las ciencias de la computación, la filosofía, lingüística, matemáticas y la psicología, donde cada una de estas ciencias contribuyó no solamente con los conocimientos desarrollados en ellas, sino con sus herramientas y experiencias también; contribuyendo así a la gestación y desarrollo de esta nueva área del conocimiento."

"La inteligencia artificial, se ha dedicado al estudio y el análisis del comportamiento humano, para simular las actividades intelectuales que el hombre realiza, por medio de equipos electrónicos con el fin de igualar o mejorar las actividades que normalmente el hombre realiza, por este motivo la IA no es limitada como los programas de un computador convencional, si no que va mucho más allá, y se enfoca en tres puntos de vista: El primero es hacer dispositivos capaces de pensar, lo que se conoce como IA fuerte, el segundo es la simulación de datos mentales, sin ser datos de un cerebro humano, lo que se conoce como IA débil y el tercero los que creen que existe un juicio de verdad y la IA no tiene acceso a estos. La IA abarca muchas

disciplinas lo que la hace fascinante, ya que permite a matemáticos, filósofos, biólogos y físicos entre otros, enfocarse en el cerebro y la conciencia." (Muñoz Fonseca et al., 2021).

La IA ha transformado significativamente el mundo y la ciberseguridad no ha sido ajena a esta evolución y es que desde la incorporación de las redes de telecomunicaciones en la vida cotidiana, el internet se ha consolidado como el principal medio para establecer contacto con personas en todo el mundo, sin embargo, este entorno también ha propiciado la aparición de mecanismos que transgreden normas y leyes, facilitando el aumento de los delitos informáticos y atrayendo a individuos que buscan obtener beneficios económicos mediante actividades ilícitas, por lo que "Es necesario crear sistemas de IA seguros y justos para reducir el esfuerzos para resolver los problemas generados por los ciberdelincuentes" (Delgado, Gutiérrez & Cardona, 2021).

Según Delgado, Gutiérrez & Cardona, (2021) para desarrollar, validar y desplegar sistemas de IA, se han recopilado una serie de aspectos que se deben tener en cuenta: **Privacidad**: mantener la privacidad de los datos.

Equidad. no discriminar ni favorecer injustamente ciertas personas o grupos.

Trazabilidad. analizar cómo se tomó una decisión, especialmente si hubo un fallo.

Robustez: funcionar correctamente incluso en condiciones imprevistas o con datos que no ha visto antes.

Fiabilidad. ser consistente, confiable y sus resultados estables.

Causalidad. entender qué factores influyen directamente en la decisión del modelo y no solo qué datos están correlacionados.

Explicabilidad y Transparencia. el modelo debe ser entendido por los humanos, incluso si es complejo.

Gobernanza del Dato. Se debe asegurar que los datos sean gestionados de forma lícita, eficiente y responsable.

Finalmente, la investigación se centra en el sector financiero, abordando información que brinden mecanismos que sirvan para contrarrestar los peligros que son cotidianos en internet y que afectan de algún modo u otro a un sector tan relevante como el financiero, ya que este sector contribuye al crecimiento y desarrollo económico de una ciudad, una región y una nación en general.

"El sistema financiero colombiano está conformado por los establecimientos de crédito, las entidades de servicios financieros y otras entidades financieras, las cuales, en su mayoría, se han agrupado mediante la figura de los conglomerados financieros, haciendo presencia tanto en el ámbito interno como externo, superando crisis como las de finales de la década de los noventa, lo que le ha permitido al sector fortalecerse gracias, entre otras cosas, a la regulación del gobierno nacional y de la Superintendencia Financiera de Colombia, lo que se ha reflejado en buenos indicadores de rentabilidad, riesgo y solvencia.", siendo garante de seguridad y respaldo del crédito para millones de familias, centenares de entidades privadas y por supuesto el estado en general, que son los directos beneficiados de todos sus servicios, en aras de buscar rendimientos y crecimiento económico (Muñoz Fonseca et al., 2021).

Según Delgado, Gutiérrez & Cardona (2021) el sector financiero colombiano está conformado por el Banco de la República "organismo que dirige y controla las políticas monetarias, cambiarias y crediticias del país y por instituciones avaladas por la Superintendencia Financiera de Colombia, que se encargan de captar, administrar y colocar recursos, tanto de las empresas como de las personas".

DUEÑAS, Ricardo. Describe Bancoldex, como el organismo central que siempre está garantizando la transparencia de las transacciones y la emisión del dinero en Colombia, sin embargo, en una sociedad carente de principios, valores y buenas costumbres; el sector financiero no es ajeno a sufrir con constantes ataques cibernéticos, que no solo buscan vulnerar la seguridad de estas entidades, sino también de robar grandes cantidades de dinero, por ello su inminente inclusión con la ciberseguridad es innegociable, razón por la cual en los últimos tiempos se ha caracterizado por ser uno de los sectores que más invierte en el tema, ya que el sector financiero es tal vez el más consciente en la importancia de garantizar la ciberseguridad, en gran medida por lo codiciado de su materia prima.

La IA busca reforzar la ciberseguridad, brindando garantías y resultados confiables a sus usuarios, desarrollando tanto software como sistemas con capacidades cada vez más similares a las humanas, sin tener como objetivo reemplazar la participación humana, sino complementarla, mediante una implementación eficaz que permita ofrecer beneficios significativos a entidades públicas y privadas que integran la IA en sus procesos (Delgado, Gutiérrez & Cardona, 2021).

Marco Conceptual

Inteligencia Artificial

Según Rouhiainen (2018), la Inteligencia Artificial es la capacidad que tienen las máquinas en la actualidad para usar algoritmos, que les permiten aprender de los datos y lo más importante de todo, usar los datos aprendidos para tomar decisiones como lo haría una persona, claro que existen diferencias como que los equipos basados en IA no descansan, analizan gran cantidad de información en poco tiempo y los errores son mínimos en las máquinas.

Ciberseguridad

Son un conjunto de prácticas y medidas enfocadas en la protección de los sistemas y tecnologías de información, lo que supone redes, infraestructura crítica, datos de intrusiones, ataques cibernéticos, y cualquier amenaza que provenga de internet.

Gestión de los Riesgos en la Banca Digital

Un estudio reciente encontró que la gestión de riesgos en la cooperativa no es efectiva ni eficiente, el 68% de los encuestados dijeron que los riesgos no se identifican técnicamente, y que los empleados desconocen un modelo de gestión de riesgos, lo que ha llevado a un monitoreo débil de los riesgos, donde el 76% de los trabajadores creen que la cooperativa debería crear una cultura de riesgo, ya que los objetivos estratégicos no están enfocados en la ciberseguridad (Delgado, Gutiérrez & Cardona, 2021).

Beneficios de la Implementación de las Nuevas Tecnologías

Las nuevas tecnologías son fundamentales para las instituciones financieras, ya que les permiten mejorar sus procesos, mantenerse en el mercado y responder a las necesidades de los clientes, así lo señala una encuesta donde el 90% señaló que las cooperativas que han implementado nuevas tecnologías son más eficientes y obtienen datos más rápidos, claros y en tiempo real, sin embargo, a pesar de que las cooperativas ofrecen canales virtuales, el 65% de los socios aún prefiere realizar sus operaciones en las oficinas físicas y el 35% de los socios utiliza las herramientas digitales, de los cuales el 25% lo hace por telefonía celular (Muñoz Fonseca et al., 2021).

Marco Histórico

Los primeros desarrollos de IA para la ciberseguridad se remontan a la década de 1990, teniendo como registro en 1992, que el Instituto de Tecnología de Massachusetts (MIT) desarrolló un sistema de detección de intrusiones basado en IA llamado Bayesian Intrusion Detection System, que usaba técnicas de aprendizaje automático para identificar patrones sospechosos de actividad (MIT, 1992).

En la década de 2000, la IA fue utilizada cada vez más para la ciberseguridad, a tal punto que, en 2002, la compañía Symantec lanzó su sistema de detección de intrusiones Snort, que incluía un módulo de aprendizaje automático para detectar ataques conocidos (Symantec, 2002).

En 2011, la compañía IBM lanzó su sistema de detección de intrusiones QRadar, que utilizaba técnicas de IA para detectar ataques avanzados (IBM, 2011).

En la actualidad, la IA se utiliza en una amplia gama de tareas de ciberseguridad, como lo son detectar intrusiones, prevenir ataques, responder a incidentes y proteger datos (Rouhiainen, 2018).

La relación entre el sector financiero y la seguridad informática ha evolucionado significativamente a lo largo de las últimas décadas, partiendo que, en sus inicios, la seguridad se centraba en controles físicos y procedimientos manuales, pero con el avance de las tecnologías de la información, especialmente en el ámbito financiero, se hizo evidente la necesidad de medidas más avanzadas para proteger la integridad de los datos y la confianza de los clientes (Delgado, Gutiérrez & Cardona, 2021).

El surgimiento de la banca en línea y las transacciones electrónicas introdujo nuevos desafíos y riesgos, dando paso al desarrollo de sistemas de seguridad informática más atractivos ya que las amenazas cibernéticas se volvieron más avanzadas y el sector financiero se vio

obligado a adoptar medidas más proactivas para mantener la confidencialidad, integridad y disponibilidad de la información (Muñoz Fonseca et al., 2021).

Antecedentes o Estado Actual

En el estado actual, la ciberseguridad en el sector financiero se ha convertido en una prioridad estratégica debido al aumento de la cantidad de datos y transacciones digitales que ha creado un entorno más vulnerable a las amenazas cibernéticas ya que los malware, la ingeniería social, los ataques de denegación de servicio y otros tipos de ataques cibernéticos son cada vez más sofisticados y difíciles de detectar (Delgado, Gutiérrez & Cardona, 2021).

La inteligencia artificial ha surgido como una herramienta crucial, siendo capaz de analizar grandes conjuntos de datos en tiempo real, identificar patrones anómalos y prevenir ataques antes de que ocurran, lo que le permite al sector financiero, no solo la detección de amenazas, sino también la autenticación biométrica, gestión de riesgos y la mejora general de la eficiencia operativa, permitiéndole al sector automatizar tareas, detectar amenazas y responder a incidentes de seguridad de forma rápida y oportuna (Rouhiainen, 2018).

Algunos de los principales usos de la IA en la ciberseguridad del sector financiero son los siguientes:

Detección de Intrusiones. Detectar patrones sospechosos de actividad que pueden indicar un ataque.

Prevención de Ataques. Identificar vulnerabilidades y amenazas antes de que se produzcan ataques.

Respuesta a Incidentes. Identificar y responder rápidamente a incidentes de seguridad.

Protección de Datos. Proteger los datos confidenciales de las instituciones financieras.

Marco Científico o Tecnológico

La inteligencia artificial ha revolucionado el campo de la ciberseguridad, proporcionando herramientas y técnicas más avanzadas para la detección y respuesta a amenazas ya que cuenta con la capacidad de aprender y adaptarse rápidamente a las nuevas amenazas, siendo un activo invaluable para las organizaciones financieras, que se enfrentan a un entorno cada vez más complejo y desafiante.

Las principales técnicas de IA utilizadas en la ciberseguridad son las siguientes:

Aprendizaje Automático. De acuerdo con REGO, Agustín Zubillaga; LÓPEZ, Iker Pastor; BRINGAS, Pablo García. Es una técnica que permite a los sistemas aprender de los datos sin ser programados explícitamente.

Inteligencia Artificial Basada en Reglas. De acuerdo con DÍAZ-CASILLAS, Laura; BLANCO, Fco Javier; GARIJO, Mercedes. Es una técnica que utiliza reglas predefinidas para tomar decisiones.

Procesamiento del Lenguaje Natural. De acuerdo con GELBUKH, Alexander. Es una técnica que permite a los sistemas entender y procesar el lenguaje humano.

Marco Legal

En el sector financiero, la ciberseguridad está regulada por una serie de leyes y normas, siendo la protección de los datos financieros y personales un objetivo fundamental por lo que las instituciones financieras están sujetas a requisitos estrictos, como los establecidos en la Ley de Protección de Datos y las Normativas de Ciberseguridad (Ley General de Protección de Datos Personales en Posesión de los Particulares, 2018; Ley Federal de Protección de Datos Personales en Posesión de los Particulares, 2019).

La implementación de tecnologías de inteligencia artificial también plantea cuestiones éticas y legales, especialmente en términos de privacidad y transparencia, por lo que es crucial considerar la conformidad con las regulaciones existentes y anticipar los cambios normativos que puedan surgir en respuesta a la evolución rápida de la tecnología y las amenazas cibernéticas (Reglamento (UE) 2016/679, 2016).

En el sector financiero, la ciberseguridad está regulada por una serie de leyes y regulaciones, que establecen los requisitos mínimos de seguridad que deben cumplir las instituciones financieras y algunas de las principales leyes y regulaciones de ciberseguridad en el sector financiero a nivel mundial son las siguientes:

Ley General de Protección de Datos en México. Establece los requisitos para el tratamiento de datos personales en México (Ley General de Protección de Datos Personales en Posesión de los Particulares, 2018).

Ley Federal de Protección de Datos en Estados Unidos. Establece los requisitos para el tratamiento de datos personales en Estados Unidos (Ley Federal de Protección de Datos Personales en Posesión de los Particulares, 2019).

Reglamento (UE) 2016/679. Relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos): Establece los requisitos para el tratamiento de datos personales en la Unión Europea (Reglamento (UE) 2016/679, 2016).

Diseño Metodológico

La presente revisión se desarrollará con un enfoque descriptivo - exploratorio, con el objetivo de contextualizar y comprender la información relacionada con los sistemas usados en el sector financiero y sus implicaciones en materia de ciberseguridad, además permitirá identificar las tendencias de la implementación de la Inteligencia Artificial en el sector financiero y como esta se ve implicada en la ciberseguridad.

Las fuentes de información estarán conformadas por artículos científicos, informes de algunas organizaciones financieras y otras que se especialicen en el tema de la ciberseguridad y algunos usos que se hallan presentado en el sector financiero.

La información recopilada, analizada e interpretada permitirá establecer cuáles son los principales usos y aplicabilidades de la inteligencia Artificial en el sector financiero, además de evidenciar sus implicaciones frente a incidentes y cuáles son los usos emergentes que marcan tendencia en este campo.

Uso de la Inteligencia Artificial en el Sector Financiero

La incorporación de la inteligencia artificial en el sector financiero ha desencadenado una transformación significativa en los procesos de seguridad y en la capacidad de estas entidades para protegerse frente a ciber amenazas, dado que facilita la detección de patrones y el análisis predictivo, por ello su uso en sistemas de seguridad financiera permite anticipar y responder a incidentes de manera más precisa y eficiente.

El análisis de fuentes documentadas permite presentar diversas soluciones basadas en IA implementadas en el sector financiero, enfocadas en prevenir y gestionar incidentes de ciberseguridad, que permitan explorar las capacidades de estos sistemas, destacando sus implicaciones y el impacto en la protección de los datos financieros.

Inteligencia Artificial

Es una rama de la ciencia de la computación que busca que las máquinas (hardware, software) puedan desarrollar las habilidades que son propias de los seres humanos y esta dividida en una serie de técnicas, modelos, herramientas y procedimientos que permiten a las máquinas ejecutar procesos que son propios de los seres humanos (Russell & Norvig, 2016).

La gran mayoría de aplicaciones de inteligencia artificial que existen hoy en día están basadas en el aprendizaje automático, conocido como machine learning, el cual busca que un ordenador saque conclusiones por medio de análisis estadísticos de los datos introducidos, por un proceso que automáticamente se va mejorando a medida que recibe más información en su algoritmo (Russell & Norvig, 2016).

Ciberseguridad

La ciberdelincuencia, según Gordon y Ford (2006), se refiere a cualquier actividad ilegal que se lleva a cabo a través de medios informáticos o que tiene como objetivo causar daño o destruir sistemas informáticos, dispositivos electrónicos y redes de Internet, por otro lado, el término "criminalidad informática" o cibercrimen se extiende a delitos de mayor alcance, englobando actividades como fraude, robo, chantaje, falsificación y desvío de fondos públicos, todos perpetrados a través de computadoras y redes como su medio de ejecución (Gordon & Ford, 2006).

Detección de Fraude

Según Francés Monedero, (2020), una de las implicaciones más significativas del aprendizaje automático ML en el sector financiero es la detección de fraudes, gracias a las capacidades de análisis de grandes volúmenes de datos, dejando en evidencia que sin su implementación, la detección de fraudes se realiza mediante reglas estáticas definidas por expertos, pero estos sistemas son poco flexibles y no se adaptaban bien a nuevas estrategias de fraude, por este motivo al aplicar IA, los sistemas ahora pueden aprender y ajustarse automáticamente a nuevos patrones de comportamiento sospechoso.

Existen dos grandes enfoques en esta área, el aprendizaje supervisado y el no supervisado.

Aprendizaje Supervisado. los algoritmos son entrenados con conjuntos de datos que incluyen ejemplos etiquetados de transacciones legítimas y fraudulentas, como los árboles de decisión, redes neuronales o bosques aleatorios, que aprenden a identificar patrones característicos del fraude y pueden clasificar nuevas transacciones con alta precisión (Francés Monedero, 2020).

Aprendizaje no Supervisado. Aplica cuando no se dispone de ejemplos claramente etiquetados, como el análisis de agrupamiento o clustering, que buscan detectar anomalías al identificar desviaciones en el comportamiento habitual de los usuarios, comparando transacciones actuales con el historial del cliente para identificar actividades inusuales que puedan sugerir fraude (Francés Monedero, 2020).

Un desafío clave en este campo es el desequilibrio en los datos, ya que los casos de fraude son mucho menos frecuentes que los casos legítimos, lo que puede sesgar los modelos hacia la clasificación de transacciones como legítimas, por lo tanto, es importante que se mitigue este problema, mediante la implementación de técnicas de muestreo como el sobre muestreo (duplicación de muestras de fraude) y el submuestreo (reducción de muestras legítimas).

Predicción del Riesgo de Crédito

Según Francés Monedero, (2020), la predicción del riesgo de crédito representa una de las aplicaciones más estratégicas de la inteligencia artificial en el sector financiero, ya que permite anticipar la probabilidad de incumplimiento de los pagos por parte de los clientes, optimizando así la gestión de riesgo de las entidades crediticias.

Para abordar esta problemática, emplean técnicas de aprendizaje supervisado, donde los algoritmos se entrenan con datos históricos de clientes (entradas) y sus resultados financieros (salidas: cumplimiento o impago), donde a partir de esta información, los modelos aprenden a predecir si un nuevo solicitante presenta un perfil de riesgo elevado.

Uno de los modelos más utilizados es el scorecard de crédito, que consiste en una herramienta estructurada que evalúa distintos atributos del cliente (como edad, historial laboral, ingresos, comportamiento de pago previo) y les asigna puntuaciones, así que cuanto mayor sea la

puntuación, menor es el riesgo de impago y este scorecard está basado en técnicas como regresión logística, árboles de decisión, redes neuronales artificiales.

Existen dos tipos de scorecards:

- Application scoring: evalúa nuevos solicitantes en función de los datos que presentan en el momento de pedir el préstamo.
- Behavior scoring: utiliza el comportamiento financiero del cliente a lo largo del tiempo para ajustar dinámicamente su nivel de riesgo.

Chatbots en el Sector Financiero

Según Francés Monedero (2020), los chatbots representan una de las aplicaciones más populares y visibles de la inteligencia artificial en el sector financiero, ya que estos programas simulan conversaciones humanas a través de plataformas de mensajería o interfaces web, utilizando técnicas de procesamiento de lenguaje natural (NLP) y aprendizaje automático para entender preguntas y ofrecer respuestas contextualizadas.

En el entorno bancario, los chatbots son usados principalmente para atención al cliente, asistencia en operaciones financieras, gestión de consultas frecuentes y soporte técnico, contando con una disponibilidad 24/7 y la capacidad de escalar a miles de usuarios simultáneamente lo que la convierte en una solución efectiva para reducir costos operativos y mejorar la experiencia del usuario.

Estos sistemas pueden clasificarse en tres generaciones:

- ✓ Los primeros: Eran basados en reglas, con respuestas programadas ante frases específicas.

- ✓ Los segundos: Se desarrollaron modelos híbridos que incorporaban aprendizaje automático para mejorar sus respuestas mediante retroalimentación.
- ✓ Los terceros: Actualmente, se desarrollan chatbots impulsados exclusivamente por IA, entrenados con grandes volúmenes de datos históricos para identificar intenciones, extraer información clave del mensaje y generar respuestas óptimas basadas en el contexto de la conversación.

El backend de estos sistemas emplea algoritmos de aprendizaje supervisado y aprendizaje profundo para procesar y analizar las interacciones, mientras que el frontend se apoya en técnicas de NLP, permitiendo al chatbot interpretar el lenguaje humano de forma natural, lo que les permite resolver problemas complejos, asistir en la selección de productos financieros e incluso ejecutar operaciones como transferencias o consultas de saldo, además también se aplican como asistentes internos dentro de las instituciones financieras, ayudando a empleados con consultas frecuentes, apoyo en procesos de recursos humanos, seguimiento de tareas o análisis financieros básicos, optimizando los flujos de trabajo y reduciendo tiempos de respuesta.

Si bien estas herramientas aportan grandes beneficios, también enfrentan retos técnicos y de percepción, entre ellos, la dificultad para interpretar el lenguaje humano con total precisión y la necesidad de una estrategia clara para su implementación.

Roboadvisors en el Sector Financiero

Según Francés Monedero (2020), son plataformas digitales que utilizan algoritmos de aprendizaje automático para brindar asesoramiento financiero automatizado, analizando los datos personales y financieros del usuario para ofrecer recomendaciones personalizadas sobre

inversiones, ahorro y planificación financiera, lo que constituye en una evolución de la inteligencia artificial aplicada al servicio directo del cliente en el sector financiero.

El funcionamiento de un roboadvisor inicia con la recopilación de información a través de un cuestionario que indaga sobre aspectos como ingresos, perfil de riesgo, objetivos financieros y preferencias de inversión del cliente, para luego con base en estas variables, el sistema cree un perfil detallado que sirve como base para sus sugerencias.

Los algoritmos combinan técnicas de clasificación y análisis de datos históricos para generar carteras de inversión óptimas que se ajusten a las necesidades individuales, no solo proponiendo una estrategia inicial, sino que realizan ajustes dinámicos en tiempo real en función de la evolución del mercado y del comportamiento del usuario.

En términos de ciberseguridad, los roboadvisors presentan desafíos relevantes, ya que manejan información altamente sensible, siendo fundamental que implementen mecanismos de autenticación robusta, cifrado de datos y protocolos de seguridad que garanticen la privacidad e integridad de la información, cumpliendo con regulaciones estrictas en materia de protección de datos y transparencia algorítmica (Francés Monedero, 2020).

Análisis de Documentos en el Sector Financiero

Es una de las aplicaciones más valiosas de la inteligencia artificial en el ámbito financiero, especialmente para agilizar tareas operativas que antes requerían revisión manual exhaustiva, ya que está sustentada en algoritmos de *machine learning* diseñados para procesar, interpretar y extraer información relevante de documentos no estructurados.

Según Francés Monedero (2020), los sistemas de análisis y reconocimiento de documentos (Document Analysis and Recognition, DAR) permiten a las entidades financieras

identificar, clasificar y extraer información de contratos, informes financieros, formularios de solicitud de crédito, estados de cuenta y otros archivos, por medio de técnicas avanzadas de procesamiento de lenguaje natural (NLP) y aprendizaje profundo para ser comprendido por las máquinas.

El proceso se compone de tres fases principales:

Recopilación y Almacenamiento. Consiste en centralizar los documentos digitales en una base accesible y segura.

Preprocesamiento. Incluye la conversión de documentos escaneados a texto (OCR), limpieza de datos, normalización del contenido, eliminación de palabras irrelevantes y reducción morfológica (stemming).

Análisis Automático. Usa técnicas como la frecuencia de palabras clave (TF-IDF), análisis de sentimiento o minería de texto para extraer insights útiles para el negocio, como cláusulas contractuales críticas, términos financieros relevantes o indicadores de riesgo.

Un caso emblemático de esta aplicación es el uso de la plataforma COiN por JP Morgan, que analiza contratos financieros en segundos, lo cual permite ahorrar más de 360.000 horas de trabajo humano al año, representando un salto significativo en eficiencia y precisión (Francés Monedero, 2020),

El análisis automatizado debe cumplir con altos estándares de integridad y confidencialidad, ya que trabaja con documentos que contiene información sensible, siendo necesaria la implementación de cifrado, controles de acceso robustos y auditorías automatizadas de accesos y manipulaciones de los datos.

Es evidente que la evolución y el desarrollo de la inteligencia artificial se basan en técnicas y herramientas avanzadas que han permitido su integración en diversos campos, incluido el sector financiero, gracias a que su aplicación ofrece numerosos beneficios, como la automatización de tareas, la mejora en la eficiencia y la personalización de los servicios para los clientes, sin embargo, también presenta nuevos desafíos, particularmente para garantizar la confidencialidad de la información de los clientes.

La ciberseguridad es crucial para todas las entidades financieras ya que los delincuentes emplean herramientas como phishing, ataques DoS/DDoS y Ransomware para amenazar la seguridad de las instituciones y la privacidad de los clientes, por lo que la IA se surge como una herramienta fundamental en la lucha contra los ciberdelitos financieros, gracias a su capacidad para identificar fraudes, detectar patrones y reforzar la seguridad de la información permitiendo a las instituciones proteger sus datos y sistemas de manera más efectiva (Smith, 2023).

Uso de la Inteligencia Artificial en Casos del Sector Financiero

Resulta relevante analizar la Inteligencia Artificial en las aplicaciones actualmente empleadas por las entidades financieras, resaltando algunos de los aportes de la IA en este sector tan importante y de mucho riesgo, que permitan evidenciar las razones que hacen que su papel en la sociedad actual sea tan relevante, examinando las ventajas y desventajas asociadas que estas traen consigo (Smith, 2024).

El avance e innovación de la tecnología han dado lugar a sistemas complejos que resultan ser más inteligentes, capaces de llevar a cabo tareas avanzadas, lo que conlleva a una mayor precisión en el análisis y seguridad de la información, haciendo posible crear bases de datos sólidas, que permiten a las empresas detectar oportunidades confiables en el mercado, analizar la competencia y proporcionar información sobre las preferencias de los clientes, permitiéndoles brindar productos personalizados y al mismo tiempo, reforzar la ciberseguridad en el sector (Johnson & Lee, 2023).

Es importante destacar que, con la automatización de tareas, los tiempos de ejecución disminuyen, mejorando la calidad y eficiencia de los servicios prestados al cliente, aumentando su satisfacción, siendo este el objetivo principal de las entidades, generando así una mayor cobertura y análisis de las amenazas y riesgos que puedan surgir (Williams, 2024).

La inteligencia artificial se está expandiendo por las entidades financieras, en todas sus actividades, como lo son procesamiento, ciberseguridad, servicios, operaciones, enfocándose en la prevención de fraudes y la supervisión de actividades de lavado de dinero, con tareas de verificación y control de clientes, tanto así que, en la actualidad, es habitual que todas las

entidades cuenten con sistemas inteligentes dedicados a la asistencia y atención de clientes, con aplicaciones como Chatbots y autenticación biométrica (Davis, 2023).

Uso de las Aplicaciones de Inteligencia Artificial en Entidades Bancarias

Las entidades financieras se han dado a la tarea de desarrollar sus propias aplicaciones implementando inteligencia artificial en sus servicios, algunas de las cuales son Banco de Bogotá, BBVA, Banco Santander, CaixaBank y Bank One, que, gracias a su rentabilidad y liquidez, cuentan con la capacidad de realizar grandes inversiones en tecnología, como el desarrollo de aplicaciones con IA (García, 2023).

La mayoría de las entidades financieras tienen sucursales a nivel mundial, por lo que tienen un grado de madurez en la implementación de aplicaciones que se basan en IA dentro del sector (Martínez, 2024).

Banco de Bogotá

Para brindar una experiencia más ágil, segura e intuitiva a sus clientes, el Banco de Bogotá ha adoptado el uso de herramientas tecnológicas propias de la Inteligencia Artificial, usándola además para predecir los comportamientos de los clientes, capturando patrones que respondan a lo que necesitan de manera anticipada, como también usa reconocimiento óptico de caracteres (OCR) para obtener y almacenar información de documentos, y facilitar el proceso de digitalización (López, 2023).

Reconocimiento Facial y Biométrico

La organización adoptó medidas que le permite reconocer a individuos de manera remota al abrir sus productos digitales, reduciendo el riesgo de fraude y suplantación, al mismo tiempo que simplifica el acceso al sistema financiero en todo el territorio nacional, gracias a gestiones

realizadas por el director de Estrategia Digital y Datos del Banco de Bogotá, Alejandro Esguerra, que afirma “con la herramienta de Reconocimiento Facial los usuarios son guiados a través de una serie de pasos de validación de identidad, para que el software compruebe si coincide el rostro de la persona con su documento de identidad y por último, los datos son cruzados con una lista de riesgo financiero, lo que ha llevado al análisis de más de 600.000 rostros, permitiendo vincular más clientes, disminuyendo el riesgo de suplantación” (Esguerra, 2023).

En la actualidad, el 80% de las cuentas de ahorro nuevas y el 88% de las ventas de sus servicios crediticios son efectuados a través de canales digitales, desde su introducción en el mundo digital en 2017 y hasta la fecha, se ha distribuido más de 4,3 millones en todo el país, superando los $4,7 billones en saldo, gracias a la simplificación del acceso a productos de ahorro, financiación e inversión de forma digital (García, 2023).

El Banco de Bogotá, a medida que usa la Inteligencia Artificial, va ganando habilidades que le permiten crear nuevos productos digitales, contando con elementos esenciales de seguridad, flexibilidad, escalabilidad y disponibilidad, asegurando la entrega de un valor tangible a los clientes, lo que le permite al Banco destacarse en el sector (López, 2023).

Banco Santander

Mediante la aplicación del aprendizaje automático (ML), sus sistemas de seguridad cibernética tienen la capacidad de examinar patrones y aprender de ellos, previniendo así nuevos ataques similares ya que puede responder de manera rápida y eficaz al detectar los cambios, simplificando así la ciberseguridad y reduciendo costos, usando técnicas como el aprendizaje no supervisado (unsupervised learning), el cual permite detectar anomalías sin requerir datos previamente etiquetados, agrupando información similar mediante algoritmos como clustering o reducción de dimensionalidad, además, se emplean modelos de aprendizaje supervisado como

árboles de decisión, random forest y redes neuronales profundas (deep learning), especialmente útiles en la detección de fraudes o accesos indebidos.

El Banco Santander cuenta con expertos en Inteligencia Artificial, lo que le permite desarrollar sus aplicaciones y programas para usarlos en diversos ámbitos, además de asegurar una conexión fácil y personalizada con sus clientes, mejorando así la gestión del riesgo, por medio de aplicaciones como robots cognitivos que pueden detectar anormalidades en las cláusulas de los contratos

Entre los programas que está utilizando se encuentra el 'Chatbots' que les permiten a los clientes resolver inconvenientes en tiempo real y de manera segura, además de ser de mucha utilidad también para los propios empleados de la entidad ya que ofrece productos y servicios, garantizando también la seguridad en las transacciones financieras realizadas por los usuarios o la entidad (Santander Asset Management, 2018).

Aplicaciones Desarrolladas Con IA por Banco Santander

Banco de Santander no se ha quedado atrás con el auge de la IA por lo tanto empezado a implementar algunos desarrollos.

Asistentes Virtuales de Voz y Chatbots

La innovación introducida por el Banco al emplear Chatbots en el ámbito financiero se evidencia a través del Bot corporativo implementado en algunas de sus entidades, el cual está dedicado únicamente a sus empleados, brindándoles un medio seguro para consultar información relacionada con la contratación de seguros.

En el Reino Unido, ha implementado un Chatbot más avanzado a través de la aplicación móvil llamada SmartBank, que le permite a los clientes una interacción directa con el banco, ya que tiene la capacidad de hacer transferencias, seguimiento de gastos, verificación del estado

actual de la cuenta, notificación de robos y notificación de pérdidas de tarjetas para desactivarlas (Santander, 2021).

El banco tiene un asistente virtual de voz, Sherpa, que es un agente inteligente para interfaz de voz que Santander integra en su aplicación móvil, desarrollada por Anboto, una empresa vasca, que hizo posible que Sherpa se comunique con el cliente en lenguaje natural (Santander, 2021).

Autenticación Biométrica

El Banco Santander hace uso de técnicas biométricas para la preservación de la identidad de los usuarios y la protección de sus datos personales, como lo implementado por Openbank, que es un banco online del grupo Santander, el cual está comenzando a incorporar sistemas de reconocimiento de imágenes para el proceso de inscripción a dicha banca online en países como Brasil, México y España (Santander, 2022).

Las aplicaciones de Openbank, están implementando el uso de huella dactilar como método de autenticación en España, Polonia, Portugal, Brasil y Estados Unidos.

El uso de reconocimiento de voz está experimentando una expansión en México, por la implementación de VocalPassword, un sistema completamente inteligente diseñado por Nuance, con el que se usa reconocimiento de voz en lugar de ingresar contraseñas y PIN en el servicio al cliente telefónico, validando la identificación de los clientes por medio de su voz.

BBVA

Están enfocados en la ciberseguridad, identificando problemas, previendo o reconociendo patrones que permitan anticiparse al riesgo (BBVA, 2022).

Algunas aplicaciones inteligentes que introduce el banco son:

Chatbots y Asistentes Virtuales de Voz

El fondo de inversión Propel Venture Partners, de BBVA, ha introducido a Charlie en su página web corporativa para ayudar al usuario en la gestión de sus finanzas y según indican sus inversores, esta aplicación está dirigida a los millenials, generación que acostumbra a realizar la mayoría de sus gestiones online, permitiéndoles realizar transacciones de dinero por medio de aplicaciones como Facebook Messenger o Telegram, manteniendo un alto estándar de seguridad (BBVA, 2023).

BBVA e IPSoft han implantado el asistente de voz Amelia en México, el cual es capaz de comprender las emociones de los usuarios y adaptarse a ellas, de forma que atienda a las reclamaciones de los interlocutores (BBVA, 2023).

Garanti Bank del grupo BBVA ha incorporado UGI como asistente de voz en Turquía, facilitando la realización de transacciones a partir de las instrucciones indicadas por los clientes ya que es capaz de comunicarse en lenguaje natural, recibiendo el premio EFMA a la innovación debido al planteamiento multicanal que permite la comunicación cliente-asistente y por otra conecta a este último con la entidad (BBVA, 2023).

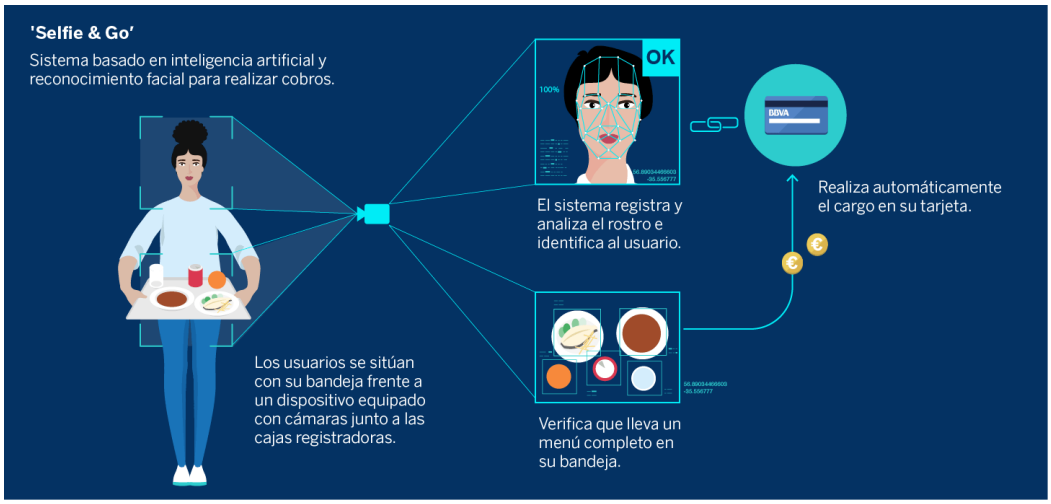
Autenticación y Biometría

Selfie&Go se trata de un sistema revolucionario, dentro del contexto financiero, tanto así que ha sido seleccionada como una de las 100 mejores ideas del año en la categoría de pagos móviles.

Esta aplicación ha sido realizada junto con la start-up Veridas y Das-Nano, de Pamplona y en la siguiente ilustración se puede evidenciar su funcionamiento (BBVA, 2023).

Figura 1

Selfie&Go



Nota. Tomado de https://www.bbva.com/es/innovacion/algoritmos-que-ven-mejor-que-los-humanos-asi-funciona-el-reconocimiento-facial- en-bbva/

Se trata de una aplicación de pago, únicamente habilitada en el restaurante Central de BBVA desde mediados de 2018, con la que los comensales pueden realizar el pago del menú diario posando unos instantes para una cámara situada al lado del cajero, que se encarga, por una parte, de visualizar el menú escogido para calcular su importe y por otra, de reconocer el rostro del cliente, que está registrado en la base de datos, permitiendo que cuando el proceso de reconocimiento esté finalizado, se realice el cobro automático, ya que la cuenta del cliente se asocia a la cara del mismo (BBVA, 2023).

Start-up en colaboración con BBVA ha permitido que los clientes nuevos accedan a la banca online empleando canales digitales, así, han creado un proyecto llamado Alta Inmediata, el cual permite a los usuarios formar parte del banco en línea mediante un reconocimiento facial a partir de una selfie (BBVA, 2023).

Una utilización adicional de la autenticación biométrica en España proviene de la colaboración entre BBVA y Samsung, creando un software llamado Samsung Pass que permite a través del iris un reconocimiento biométrico, permitiendo el acceso a la banca móvil de manera

segura sin incurrir en suplantación a los clientes, facilitando tambien la identificación mediante huella dactilar (BBVA, 2023).

CaixaBank

Tiene tecnología especializada en inteligencia artificial, como 'Chatbots', que pueden abordar las preguntas de los clientes mediante voz o texto, asistiéndolos en la búsqueda de las opciones deseadas (CaixaBank, 2023).

CaixaBank y Microsoft firmaron un acuerdo de innovación para potenciar el desarrollo y uso de la IA implementando soluciones nuevas en el sector financiero, creando entornos de trabajo sofisticados en el Metaverso (CaixaBank, 2023).

La entidad organizó su estructura directiva para reforzar su apuesta por la transformación digital, creando en 2023 una dirección específica de “Transformación Digital y Advanced Analytics”, liderada por Mariona Vicens y otra de “Pagos y Consumo” bajo el mando de Jordi Nicolau, estas áreas forman parte del comité de dirección, con el propósito de integrar soluciones basadas en inteligencia artificial en canales tanto físicos como digitales. En este marco, el banco detectó más de cien casos de uso de IA en ámbitos como seguridad, atención al cliente y eficiencia operativa (CaixaBank, 2023; Diario La República de España, 2019).

Chatbots y Asistentes Virtuales

La entidad financiera ha implementado Gina, un Chatbot creado por ImaginBank, servicio usado por el banco en sus servicios online, que usa tarjetas de crédito para fraccionar los pagos, siendo en su momento el primer Bot que hizo posible las transacciones en el sector financiero de España (CaixaBank, 2023). Tras Gina, otros Chatbots han sido desarrollados, como es el caso de Neo, un chat especializado en ofrecer servicios de asistencia y resolución de dudas de clientes vía texto y voz, permitiendo observar el estado de las cuentas bancarias desde el

smartwatch, sin la necesidad de recurrir a la aplicación móvil, ni de asistir físicamente a las sucursales (CaixaBank, 2023).

BrokerNow es una aplicación adicional dentro de CaixaBank que ofrece información sobre la bolsa y todo tipo de opciones, warrants, futuros y fondos cotizados (ETFs) de más de 25 mercados en todo el mundo, actualizados en tiempo real. Igualmente, permite enviar órdenes de compra y venta si así lo desea el usuario (CaixaBank, 2023).

Con la colaboración de IBM Watson, CaixaBank dispone de un asistente virtual que puede dar respuesta al 80% de las consultas de los gestores físicos de la entidad y está dirigido especialmente a los empleados de sus sucursales ya que dispone de una gran base de datos que recoge información tanto de clientes y servicios como de marcos normativos y legislativos, de forma que ante cualquier duda del empleado puede ofrecer respuesta en un 80% de los casos (CaixaBank, 2023).

Autenticación Biométrica

CaixaBank es pionero en la inclusión de reconocimiento facial en cajeros automáticos en España para fomentar la seguridad de los clientes, gracias a la colaboración conjunta con Fujitsu y FacePhi, desde el año 2019 (CaixaBank, 2023). No obstante, previamente al éxito obtenido con el reconocimiento facial, CaixaBank ya ofrecía servicio de identificación biométrica en lo referente al acceso a aplicaciones y consultas de los estados financieros de los clientes, además, en la actividad cotidiana de la entidad, las firmas y contrataciones se recogen bajo la firma con huella dactilar (CaixaBank, 2023).

Otra aportación de la biométrica a CaixaBank consiste en la identificación facial denominada FaceID para clientes con iPhone X (CaixaBank, 2023).

El ritmo de crecimiento tecnológico es tan acelerado que muchas herramientas apenas llegan al mercado cuando ya están siendo superadas por nuevas innovaciones y no solo eso, sino que este fenómeno se ha intensificado con la irrupción de la inteligencia artificial, que ha impulsado una evolución más vertiginosa, volviéndose esencial para afrontar los complejos desafíos actuales en materia de seguridad y eficiencia (CaixaBank, 2023).

Por todo esto se destacan las ventajas que tiene la inteligencia artificial en todas las áreas de la sociedad, por ejemplo, en el campo de las finanzas transmite seguridad cuando ingresan a los canales bancarios para realizar desde una consulta hasta una transacción, gracias a reconocimiento facial, autenticación biométrica, Chatbots y asistentes virtuales entre otros, mejorando la experiencia de los clientes, fortaleciendo la ciberseguridad, optimizando los procesos internos, lo que se traduce en que la sociedad confié en estas industrias.

Las entidades financieras han encontrado en la Inteligencia Artificial una oportunidad de mejorar su ciberseguridad y brindar soluciones rápidas y oportunas a los clientes, siendo muy importante la evolución constante en la que se encuentran, realizando alianzas con las principales compañías mundiales pioneras en el uso de la IA, para estar siempre un paso más adelante de las amenazas que surgen a diario.

Recomendaciones para la adopción de Inteligencia Artificial en el sector financiero

El sector financiero ha sido un objetivo prioritario de ataques cibernéticos debido a la cantidad de datos valiosos que maneja y es que según un informe de IBM (2021), más del 25% de los ataques cibernéticos dirigidos en 2020 se centraron en instituciones financieras, los cuales incluyeron ransomware, phishing, amenazas internas y acceso no autorizado a bases de datos financieras.

La complejidad de los ataques ha impulsado a las instituciones a adoptar mecanismos de seguridad más avanzados, integrando IA en su infraestructura para mejorar la detección y mitigación de amenazas (IBM, 2021).

La principal ventaja de la Inteligencia Artificial en la ciberseguridad es su capacidad para analizar grandes volúmenes de datos en tiempo real, identificar patrones de comportamiento inusuales y tomar decisiones basadas en modelos de predicción de riesgos, permitiendo adelantarse a los atacantes y minimizar el impacto de los incidentes de seguridad.

Respuesta a Incidentes en el Sector Financiero Mediante Inteligencia Artificial

El sector financiero, debido a su naturaleza crítica y la cantidad de datos sensibles que maneja, enfrenta continuamente amenazas cibernéticas de alta complejidad, por ello, garantizar una respuesta eficaz a los incidentes se ha convertido en una prioridad estratégica y es donde emerge la IA como una herramienta esencial para transformar los procesos de gestión de incidentes, no solo haciéndolos más rápidos y precisos, sino también más predictivos y adaptativos, siendo uno de sus principales aportes la capacidad para realizar análisis de eventos en tiempo real, a diferencia de los sistemas tradicionales de detección que dependen en gran

medida de reglas predefinidas y análisis manual, lo que va quedando obsoleto debido a los ataques avanzados y persistentes.

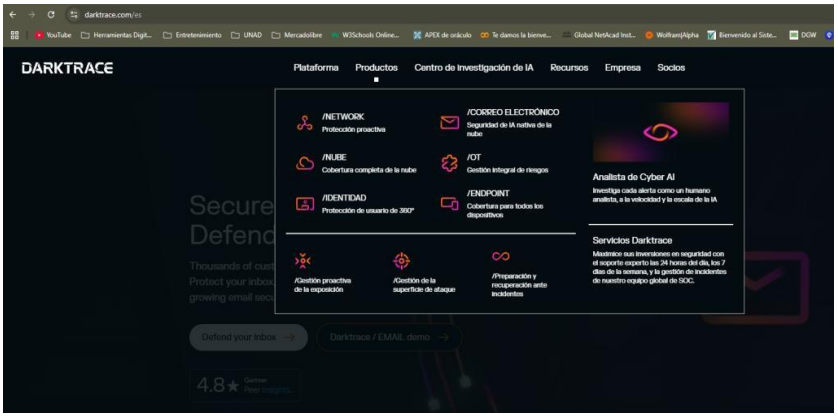
Algunas de las aplicaciones que están dando un salto de calidad y que pueden ayudar grandemente a las entidades financieras a mejorar su ciberseguridad aplicando la IA son Darktrace, SAS Fraud Management, IBM OpenPages y Plataformas de análisis de comportamiento.

Darktrace

Es una plataforma que se ha consolidado como una de las soluciones más innovadoras del mercado al adoptar un enfoque autónomo basado en el análisis del comportamiento, con una tecnología de sistema inmunológico digital que permite identificar desviaciones respecto a la actividad normal dentro de una red, facilitando una defensa adaptativa y proactiva frente a ataques sofisticados, tanto internos como externos, destacando su tecnología de análisis de comportamiento que es aplicada a múltiples vectores de ataque, incluyendo redes corporativas, servicios en la nube y plataformas de correo electrónico. Estas bondades son apreciadas en la siguiente ilustración.

Figura 2

Darktrace



Nota. Tomado de. https://www.darktrace.com/es

Esta herramienta proporciona una protección integral frente a incidentes complejos como accesos no autorizados, movimientos laterales y exfiltración de datos (Darktrace, 2023).

Un sistema Inmunológico Digital

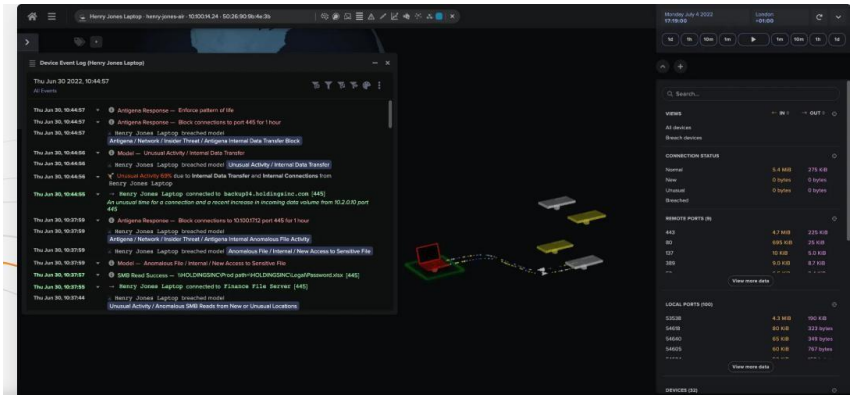
Darktrace utiliza un enfoque innovador conocido como "sistema inmunológico digital". Inspirado en el funcionamiento del sistema inmunológico humano, este enfoque permite a la herramienta aprender y adaptarse a los patrones normales de comportamiento dentro de una infraestructura tecnológica, al establecer un perfil base de "normalidad", identifica de manera autónoma cualquier desviación o anomalía que pueda ser indicativa de una amenaza, como intentos de intrusión, movimientos laterales no autorizados o exfiltración de datos.

Detección Proactiva en Tiempo Real

Uno de los principales diferenciadores de Darktrace es su capacidad para operar en tiempo real, analizando grandes volúmenes de datos mientras monitorea múltiples vectores de ataque, incluyendo correos electrónicos, redes internas y conexiones a la nube, lo que le permite identificar amenazas antes de que puedan causar un daño significativo. En la siguiente ilustración se muestra su interfaz gráfica.

FIGURA 3

Identificación de Amenazas



Nota. Tomado de https://www.darktrace.com/es/products/detect

Un ejemplo de su intervención es si un atacante intenta acceder a un sistema protegido mediante credenciales comprometidas, la herramienta no solo detecta el acceso anómalo, sino que también genera una alerta inmediata y en algunos casos, puede tomar medidas automáticas para aislar el dispositivo afectado.

Impacto En La Ciberseguridad Financiera

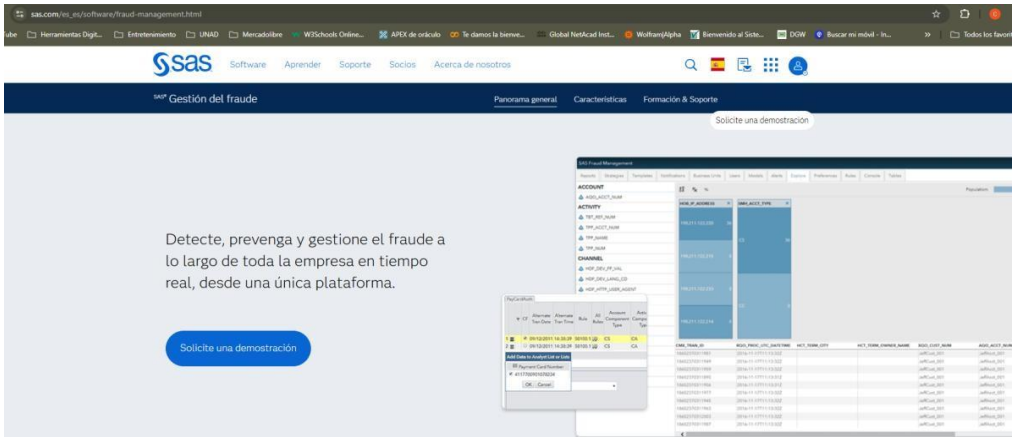
El sector financiero es uno de los más vulnerables a los ciberataques, debido al valor de los datos que maneja y la alta frecuencia de las transacciones, por ello es recomendable el uso de esta herramienta que ofrece una ventaja competitiva al permitir que estas instituciones sean proactivas en lugar de reactivas frente a los incidentes de seguridad.

SAS Fraud Management

Está basada en técnicas de análisis predictivo, minería de datos y machine learning, permitiendo a las organizaciones detectar, prevenir y mitigar fraudes en tiempo real, transformando la manera en que se enfrentan a estos desafíos. A continuación, se observa la página principal y lo que ofrece.

Figura 4

SAS



Nota. Tomado de https://www.sas.com/es_es/software/fraud-management.html

Una de sus grandes ventajas es la capacidad para conectar eventos aparentemente aislados, permitiéndole descubrir fraudes organizados o sofisticados que podrían pasar desapercibidos si se analizaran de forma puntual o sin contexto.

Un Enfoque Predictivo para un Problema Complejo

Se diferencia de los métodos tradicionales de detección de fraudes al adoptar un enfoque predictivo, ya que no depende únicamente de reglas predefinidas, si no que utiliza algoritmos de aprendizaje automático que analizan patrones históricos y contextuales para identificar comportamientos sospechosos (SAS, 2023).

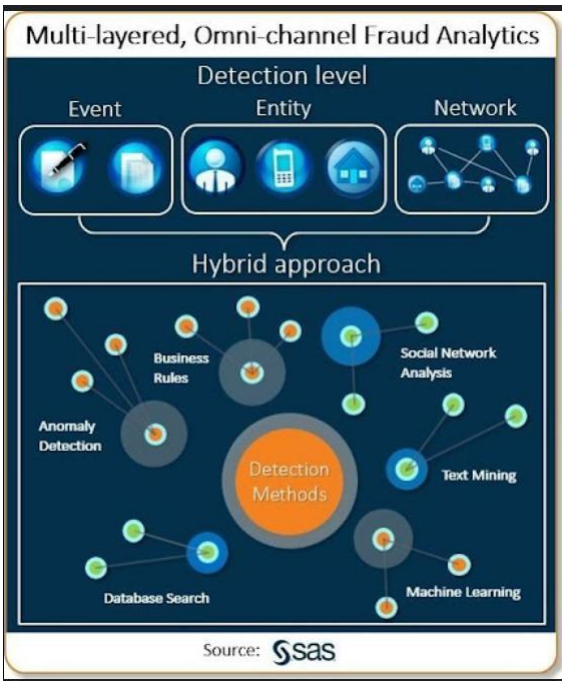
Detección Avanzada de Patrones

Una de las fortalezas de esta aplicación es su capacidad para identificar patrones complejos de fraude que podrían pasar desapercibidos con enfoques convencionales, ya que, mediante el uso de minería de datos, la herramienta conecta eventos aparentemente aislados y los asocia con actividades fraudulentas organizadas, como el uso de identidades falsas.

SAS permite construir perfiles de comportamiento tanto a nivel individual (clientes, empleados) como colectivo (segmentos de usuarios), lo que facilita la identificación de desviaciones en tiempo real, además el sistema incorpora un motor de detección híbrido, que combina reglas de negocio tradicionales con modelos predictivos basados en inteligencia artificial, asegurando un equilibrio entre precisión, cobertura normativa y capacidad de adaptación frente a nuevos vectores de fraude. Como se visualiza en la siguiente ilustración.

Figura 5

Detección de Fraudes



Nota. Tomado de http://bswan.org/sas_holistic_fraud_solutions.asp

Adicionalmente, ofrece herramientas de visualización y análisis que facilitan la comprensión de las relaciones entre eventos, permitiendo a los analistas de fraude justificar las decisiones tomadas, siendo fundamental para los procesos de auditoría, cumplimiento regulatorio y fortalecimiento de la confianza institucional (SAS, 2023).

Impacto en el Sector Financiero

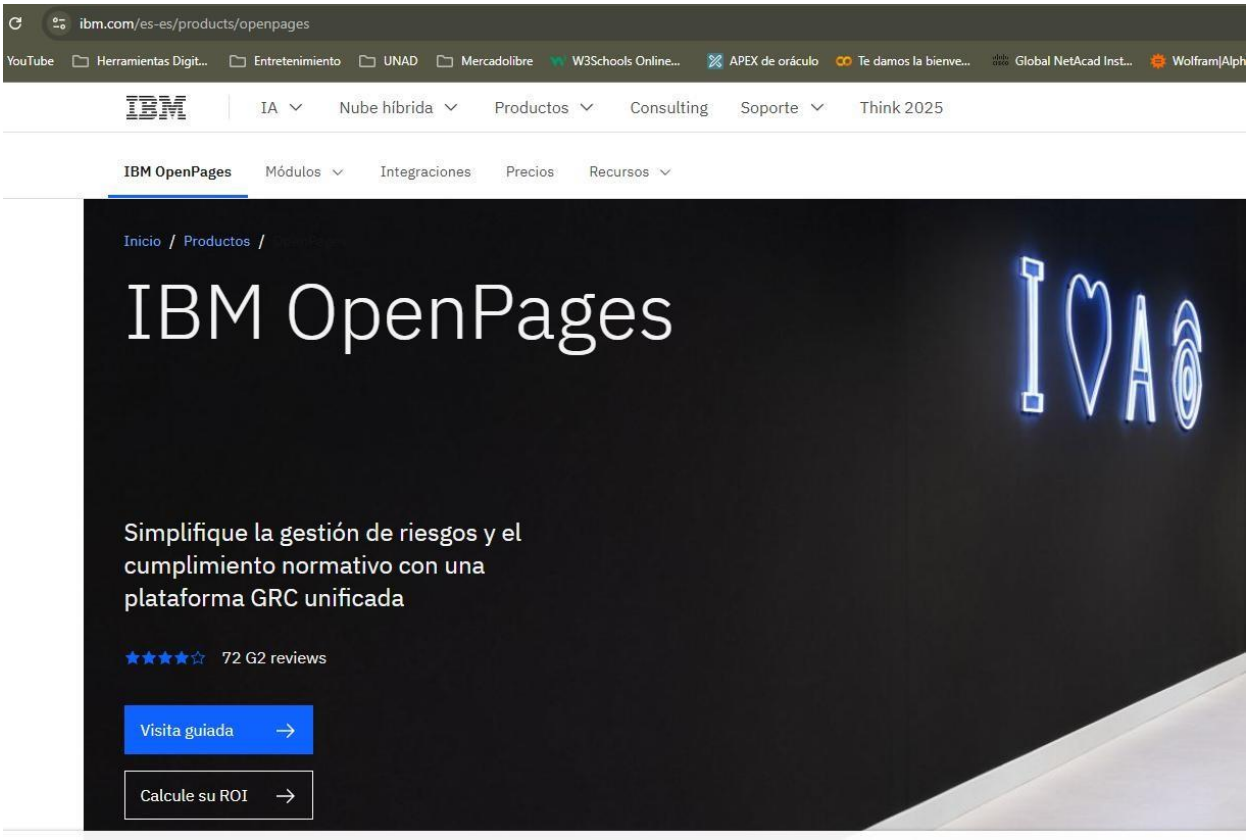
Esta herramienta puede transformar la forma en que las instituciones detectan, previenen y gestionan el fraude en entornos altamente transaccionales, gracias a su capacidad para identificar patrones complejos de comportamiento y anticipar actividades sospechosas en tiempo real, reduciendo significativamente las pérdidas económicas, también fortalece los procesos internos de control y auditoría, contribuyendo directamente a la construcción de una cultura organizacional orientada a la prevención proactiva del fraude.

IBM OpenPages

Es una plataforma empresarial de gestión de riesgos, cumplimiento normativo y gobernanza, diseñada para ayudar a las organizaciones a identificar, evaluar y mitigar riesgos operacionales, regulatorios y financieros de forma integral. En la siguiente ilustración se puede ver su página principal, la cual ofrece una visita guiada para que la comunidad conozca sus capacidades.

Figura 6

IBM OpenPages



Nota. Tomado de https://www.ibm.com/es-es/products/openpages

Impulsada por inteligencia artificial y analítica avanzada, esta solución permite automatizar procesos clave de control y monitoreo, facilitando la toma de decisiones informadas y alineadas con los objetivos estratégicos de la organización, lo que la convierte en una

herramienta poderosa para transformar la gestión de riesgos en una actividad predictiva, proactiva y estratégicamente alineada con los objetivos organizacionales (IBM, 2021)

Una Plataforma Integral de Gestión de Riesgos

Fue diseñada para ofrecer una visión holística de los riesgos que enfrentan las organizaciones, con una capacidad para integrar la gestión de riesgos operativos y regulatorios permitiendo a las organizaciones y porque no a las instituciones financieras tener una comprensión profunda de su exposición al riesgo y así tomar decisiones informadas para mitigar posibles amenazas, a diferencia de las soluciones tradicionales, que tienden a tratar los riesgos de forma aislada o fragmentada, mientras la IA trae consigo nuevos avances que permite afrontar los desafíos de ciberseguridad de una forma nunca antes imaginada.

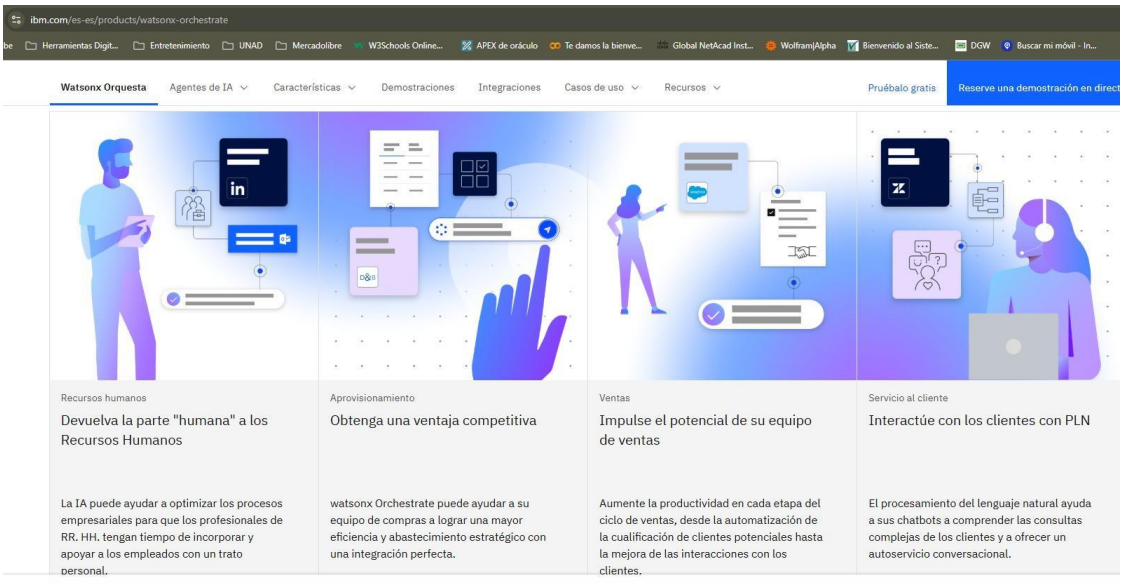
Capacidades Predictivas Basadas en IA

Una de las funcionalidades más destacadas de IBM OpenPages es su capacidad para incorporar modelos predictivos basados en inteligencia artificial, los cuales permiten anticipar riesgos antes de que se materialicen, mediante el uso de algoritmos de machine learning, analizando grandes volúmenes de datos estructurados y no estructurados provenientes de múltiples fuentes internas y externas, detectando patrones y tendencias que podrían indicar eventos de riesgo emergentes.

Esta capacidad predictiva mejora significativamente la toma de decisiones, ya que permite a las organizaciones actuar proactivamente ante posibles incumplimientos regulatorios y vulnerabilidades operativas. En la siguiente ilustración es posible conocer algunas de las herramientas con las que cuenta la aplicación.

Figura 7

Capacidad Predictiva



Fuente: *https://www.ibm.com/es-es/products/watsonx-orchestrate*

Al integrar los análisis con flujos de trabajo automatizados, facilita una gestión dinámica, eficiente y basada en datos, alineando la gestión del riesgo con los objetivos estratégicos del negocio.

Cumplimiento Normativo Y Alineación Estratégica

En toda gran organización, el cumplimiento normativo es una prioridad constante debido a la gran cantidad de regulaciones y leyes que deben cumplirse, por este motivo IBM OpenPages no solo facilita la gestión de riesgos, sino que ayuda a las organizaciones a cumplir las normativas vigentes mediante el seguimiento continuo de los cambios regulatorios, ya que proporciona un marco de cumplimiento alineado con las normas, asegurando el cumplimiento con todos los requisitos legales y regulatorios aplicables, además, al integrar estos aspectos regulatorios dentro del proceso de gestión de riesgos, ayuda a las organizaciones a evitar

sanciones y multas por incumplimiento, reduciendo significativamente los riesgos legales y reputacionales (IBM, 2021)

Impacto en el Sector Financiero

La implementación de IBM OpenPages en el sector financiero permitirá a las instituciones gestionar los riesgos de una manera ágil y segura, ya que ahora tienen acceso a herramientas de IA que no solo mejoran la eficacia en la identificación y mitigación de riesgos, sino que también optimizan los recursos internos, permitiéndoles un cumplimiento normativo más riguroso, mejorando su capacidad de resiliencia frente a crisis inesperadas.

Behavioral Analytics Suite de Splunk

Es una plataforma de análisis de comportamiento que emplea IA para detectar patrones anómalos en el comportamiento de usuarios y dispositivos, ayudando a la identificación, prevención y mitigación de amenazas antes de que causen daños significativos como se puede ver en la siguiente ilustración (Splunk, 2022).

Figura 8

Splunk

Nota. Tomado de. *https://www.splunk.com/en_us/blog/learn/behavioral-analytics.html*

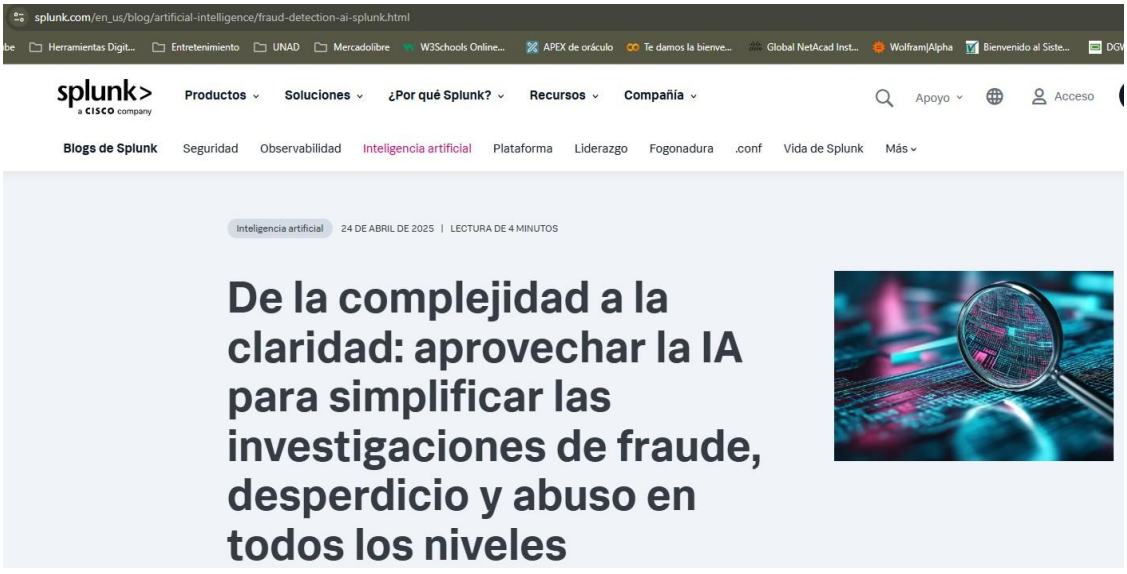
A diferencia de los enfoques tradicionales basados en reglas estáticas, esta suite se adapta dinámicamente al entorno, permitiéndole anticiparse a las actividades maliciosas como accesos no autorizados, robo de credenciales o movimientos laterales, antes de que causen daños significativos.

El Análisis de Comportamiento Como Base de la Detección de Amenazas

Está basado en la premisa de que los patrones de comportamiento de los usuarios y dispositivos son, en su mayoría, predecibles y consistentes, sin embargo, cuando ocurren desviaciones significativas de estos patrones normales, puede ser indicativo de actividades maliciosas, como el robo de credenciales, acceso no autorizado o exfiltración de datos y es donde el aplicativo aprovecha esta premisa mediante el uso de algoritmos de aprendizaje automático para crear un perfil de "normalidad" para cada usuario y dispositivo dentro de la red, como lo describe la siguiente ilustración (Splunk, 2022).

Figura 9

Aprovechamiento de la IA



Nota. Tomado de. https://www.splunk.com/en_us/blog/artificial-intelligence/fraud-detection-ai-splunk.html

El uso de la IA en el sector financiero colombiano se presenta como una estrategia crucial para fortalecer la ciberseguridad en un entorno cada vez más digitalizado y vulnerable, es por ello que las herramientas analizadas, como Darktrace, SAS Fraud Management, IBM OpenPages y Behavioral Analytics Suite de Splunk, evidencian que la adopción de tecnologías basadas en IA no solo mejoran la capacidad de detección y respuesta ante incidentes, sino que también transforman la gestión de riesgos y previenen actividades fraudulentas con una precisión sin precedentes.

Una de las principales fortalezas de estas soluciones es su capacidad para procesar grandes volúmenes de datos en tiempo real y adaptarse dinámicamente a las amenazas emergentes.

Darktrace ofrecen un enfoque proactivo para la detección de amenazas internas y externas, permitiendo a las instituciones financieras anticiparse a los atacantes.

SAS Fraud Management destaca en la identificación de patrones complejos de fraude, garantizando no solo la protección de activos, sino también la confianza de los clientes, un factor esencial en este sector.

Plataformas como IBM OpenPages integran capacidades predictivas y normativas, ofreciendo a las organizaciones una gestión de riesgos holística que no solo identifica vulnerabilidades, sino que también facilita el cumplimiento regulatorio y reduce la exposición a sanciones legales.

Behavioral Analytics Suite de Splunk proporciona una capa adicional de seguridad al analizar patrones de comportamiento para detectar accesos no autorizados o actividades maliciosas, fortaleciendo la protección contra amenazas internas y externas.

Características Principales de Cada Herramienta Propuesta

Nota: A continuación, se presenta una comparación de las principales características, capacidades y recomendaciones estratégicas asociadas a cada una de las herramientas basadas en inteligencia artificial analizadas en este capítulo.

Tabla 1

Características Principales

Herramienta	Utilidad Principal	Capacidades destacadas	Recomendación estratégica
Darktrace	Detección temprana de amenazas internas y externas en tiempo real	- Sistema inmunológico digital basado en IA - Autoaprendizaje de comportamiento - Respuesta autónoma ante incidentes	Ideal para instituciones que requieren vigilancia continua y respuesta automatizada frente a amenazas avanzadas
SAS Fraud Management	Prevención y detección de fraudes financieros complejos	- Análisis predictivo con machine learning - Detección de patrones no evidentes - Supervisión multicanal en tiempo real	Recomendado para entidades que manejan altos volúmenes de transacciones y necesitan protección contra fraude organizado
IBM OpenPages	Gestión integral de riesgos y cumplimiento normativo	- Capacidad predictiva con IA - Integración de riesgos operativos, regulatorios y financieros - Automatización de flujos de trabajo	Aporta a la gobernanza y cumplimiento regulatorio; ideal para entidades con marcos de riesgo robustos o en expansión

Behavioral Analytics (Splunk)	Detección de amenazas basadas en comportamiento y análisis contextualizado	- Modelos de perfilado dinámico - Identificación de accesos inusuales - Correlación de eventos sospechosos	Recomendado para complementar herramientas de monitoreo tradicionales, aumentando la detección de amenazas internas y sutiles

Nota. La tabla describe la utilidad principal de cada herramienta, así como sus capacidades y recomendaciones estratégicas para cada implementación.

El estudio de las herramientas Darktrace, SAS Fraud Management, IBM OpenPages y Splunk Behavioral Analytics Suite demuestran que el impacto de la IA en la ciberseguridad financiera es evidente ya que permiten a las instituciones ser más ágiles, resilientes y seguras frente a un panorama de amenazas en constante evolución, sin embargo, su implementación requiere no solo una inversión tecnológica, sino también un cambio cultural dentro de las organizaciones, donde la capacitación del personal y la integración con sistemas existentes sean prioridades estratégicas.

Conclusiones

A lo largo de los años la inteligencia artificial se ha convertido en una parte integral del sector financiero y se utiliza en varios sistemas para mejorar la eficiencia, toma de decisiones y la seguridad, en cuanto a las implicaciones en caso de un incidente de seguridad, es importante tener en cuenta que ningún sistema es completamente infalible, por lo tanto también pueden estar expuestos a riesgos de seguridad, como ataques cibernéticos o manipulación de datos, siendo fundamental implementar medidas de seguridad robustas, como el cifrado de datos, autenticación de usuarios y monitorización constante, para proteger estos sistemas y mitigar los posibles riesgos.

La IA desempeña un papel fundamental en el sector financiero, pero también presenta riesgos significativos en caso de un incidente de seguridad, lo que lleva a realizar auditorías y pruebas de seguridad regularmente, además de implementar planes de contingencia en caso de incidentes cibernéticos para mitigar estos riesgos.

Al analizar el uso de la IA por parte de entidades como Banco de Bogotá, Banco Santander, BBVA y CaixaBank, se destacó cómo estas instituciones han adoptado tecnologías avanzadas como la autenticación biométrica, reconocimiento facial, chatbots y asistentes virtuales, optimizando la seguridad de las transacciones y los datos, además de mejorar significativamente la experiencia de los clientes al ofrecer servicios más rápidos, personalizados y seguros, pero esto no se detiene aquí y se debe seguir identificando los nuevos avances tecnológicos que van surgiendo, ya que estos permiten proponer y adoptar recomendaciones específicas basadas en casos de éxito para potenciar aún más la ciberseguridad en el sector financiero colombiano, como pueden ser el uso de herramientas como Darktrace, SAS Fraud Management, IBM OpenPages y Splunk Behavioral Analytics Suite que ejemplifican cómo la IA

puede detectar patrones anómalos en tiempo real, prevenir fraudes complejos y gestionar riesgos de manera integral, demostrando que la inteligencia artificial no solo responde a incidentes de seguridad, sino que también permite a las instituciones ser proactivas y resilientes frente a amenazas emergentes.

La inteligencia artificial se presenta como una solución transformadora que va más allá de la mera automatización, consolidándose como un aliado estratégico para la sostenibilidad y competitividad del sector financiero, aclarando que su implementación debe ser cuidadosamente gestionada, priorizando la seguridad de los sistemas, la capacitación del personal y la creación de marcos regulatorios y éticos que aseguren su uso responsable, por ello las entidades financieras que adopten la IA de manera estratégica no solo estarán mejor preparadas para enfrentar los desafíos del futuro digital, sino que también fortalecerán su posición en un mercado cada vez más exigente, garantizando la protección de sus activos, la confianza de sus clientes y el cumplimiento de sus objetivos organizacionales.

Recomendaciones

La adopción de soluciones basadas en Inteligencia Artificial representa una estrategia clave para fortalecer la ciberseguridad en el sector financiero colombiano por ello las plataformas analizadas en este capítulo Darktrace, SAS Fraud Management, IBM OpenPages y Behavioral Analytics Suite de Splunk, permiten observar un cambio de paradigma: de la defensa reactiva basada en reglas estáticas, hacia sistemas proactivos y adaptativos que emplean análisis de comportamiento, aprendizaje automático y capacidades predictivas, ya que estas herramientas no solo detectan patrones anómalos en tiempo real, sino que también automatizan respuestas ante incidentes, integrando múltiples fuentes de datos.

No obstante, la implementación de estas tecnologías no debe abordarse como una solución aislada o puramente técnica, ya que su efectividad está condicionada por factores organizacionales, tales como la cultura institucional frente a la innovación, la capacidad de integración con infraestructuras existentes, la madurez en gestión de riesgos y la disponibilidad de personal capacitado para interpretar y operar los sistemas inteligentes.

Por tanto, es recomendable que las entidades financieras adopten un enfoque gradual y estratégico para la incorporación de soluciones de IA en sus esquemas de ciberseguridad, sustentando su adopción con diagnósticos previos de capacidades tecnológicas, evaluaciones de costo - beneficio, gestión del cambio organizacional y la consolidación de un gobierno corporativo que entienda la ciberseguridad como una función transversal al negocio, no solo como una responsabilidad técnica.

El valor de la IA radica en complementar la capacidad de análisis y respuesta de los equipos de seguridad, dotándolos de herramientas avanzadas que les permitan actuar con anticipación, precisión y resiliencia frente a un entorno de amenazas cada vez más dinámico, así

que la implementación responsable, informada y estratégica de estas tecnologías constituye no solo una recomendación, sino una necesidad urgente para la sostenibilidad y competitividad del sistema financiero actual.

Referencias

Aldea Torres, C. (2020). Impacto de la Inteligencia Artificial en el sistema financiero. https://repositorio.comillas.edu/xmlui/handle/11531/37543

Al-Hammadi, Y., & Aickelin, U. (2008, March). Detecting bots based on keylogging activities. In 2008 Third International Conference on Availability, Reliability and Security (pp. 896-902). Piscataway, NJ: IEEE. https://ieeexplore.ieee.org/abstract/document/4529439

Autor o entidad responsable. (2016). Ventajas de usar la huella dactilar. Recuperado de https://blog.caixabank.es/blogcaixabank/smartphones-ventajas-de-usar-la-huella-dactilar/

Baccala, M., Curran, C., Garret, D., Likens, S., Rao, A., Ruggles, A., & Shehab, M. (2018). 2018 AI predictions. PwC. https://www.thomsonreuters.com/en/reports/2018-ai-predictions.html

Banco de Bogotá. (2022, septiembre 21). Innovación con Inteligencia Artificial del Banco de Bogotá permite mayor acceso a los colombianos al sistema financiero. https://saladeprensa.bancodebogota.com/2022/09/21/innovacion-con-inteligencia-artificial-del-banco-de-bogota-permite-mayor-acceso-a-los-colombianos-al-sistema-financiero/

Banco de Pagos Internacionales. (2018). Innovative technology in financial supervision (suptech) – The experience of early users, FSI Insights on policy implementation, n.º 9. https://cris.maastrichtuniversity.nl/en/publications/innovative-technology-in-financial-supervision-suptech-the-experi

BBVA. (2018). “Robo-advisors”: Qué son y por qué hay que tenerlos en cuenta a la hora de invertir. BBVA. https://cutt.ly/mtGttEA

BBVA. (2018). BBVA automatiza los servicios de atención al cliente con la tecnología de inteligencia artificial de IPSoft. https://www.bbva.com/es/innovacion/bbva-automatiza-servicios-atencion-cliente-tecnologia-inteligencia-artificial-ipsoft/

BBVA. (2018). Inteligencia Artificial y Big Data aplicados al negocio bancario. https://www.bbvaapimarket.com/es/mundo-api/inteligencia-artificial-y-big-data-aplicados-al-negocio-bancario/

BBVA. (2019). Los 'pagos por la cara' de BBVA, entre las ideas más innovadoras del año. BBVA. https://www.bbva.com/es/los-pagos-por-la-cara-de-bbva-entre-las-ideas-mas-innovadoras/

BBVA. (2020). Creando la experiencia global de Blue, el asistente virtual de BBVA. https://www.bbva.com/es/creando-la-experiencia-global-de-blue-el-asistente-virtual-de-bbva/

BBVA. (2020). Garantía BBVA, ahora también en WhatsApp. https://www.bbva.com/es/innovacion/garanti-bbva-ahora-tambien-en-whatsapp/

BBVA. (2023). BBVA colabora con más de 20 'startups' en su área de innovación abierta. https://www.bbva.com/es/innovacion/bbva-colabora-con-mas-de-20-startups-en-su-area-de-innovacion-abierta/

Buchanan, B. (2020, febrero 2). How North Korean Hackers Rob Banks Around the World. Wired. https://cutt.ly/Xt7SvUb

Bughin, J., Seong, J., Manyika, J., Chui, M., & Joshi, R. (2018). Notes from the AI frontier: Modeling the global economic impact of AI. McKinsey Global Institute. https://www.mckinsey.com/featured-insights/artificial-intelligence/notes-from-the-ai-frontier-modeling-the-impact-of-ai-on-the-world-economy

CaixaBank. (2019). Los cajeros con reconocimiento facial de CaixaBank, mejor proyecto tecnológico del año según The Banker. https://www.caixabank.com/comunicacion/noticia/los-cajeros-con-reconocimiento-facial-de-caixabank-mejor-proyecto-tecnologico-del-ano-segun-the-banker_es.html?id=41844

CaixaBank. (2020). CaixaBank se alía con los servicios de IBM para acelerar la transformación y la innovación en la nube en la industria de servicios financieros. https://www.caixabank.com/comunicacion/noticia/caixabank-teams-with-ibm-services-to-accelerate-cloud-transformation-and-innovation-in-the-financial-services-industry_es.html?id=42296

CaixaBank. (2022). El 'Chatbot' de CaixaBank ya conversa con uno de cada tres clientes de banca digital. https://www.caixabank.com/comunicacion/noticia/el-chatbot-de-caixabank-ya-conversa-con-uno-de-cada-tres-clientes-de-banca-digital_es.html?id=43753

CaixaBank. (2023). Descubre todo lo que puedes hacer con CaixaBankNow, tu banca digital. https://www.caixabank.es/particular/bancadistancia/caixabanknow_es.html

CaixaBank. (2023). La nueva forma de invertir en bolsa*. https://www.caixabank.es/particular/inversion/ocean-broker/app-brokernow.html#:~:text=Ocean%20Br%C3%B3ker%20app%20es%20la,actualidad%20financiera%20en%20un%20instante

Castillo, J., et al. (2022). Artificial Intelligence in Cybersecurity. Journal of Cybersecurity Research. http://scielo.senescyt.gob.ec/scielo.php?pid=S1390-76972022000200057&script=sci_arttext

Cheng, C., Kung, H. T., & Tan, K. S. (2002). Use of spectral analysis in defense against DoS attacks. IEEE GLOBECOM 2002, 3(3), 2143-2148. https://ieeexplore.ieee.org/abstract/document/1189011

Chui, M., Harryson, M., Manyika, J., Roberts, R., Chung, R., Heteren, A. van, & Nel, P. (2018). Notes from the AI frontier Applying AI for social good. McKinsey Global Institute. https://www.mckinsey.com/featured-insights/artificial-intelligence/applying-artificial-intelligence-for-social-good

Danielsson, J., Macrae, R., & Uthemann, A. (2017). Artificial intelligence, financial risk management and systemic risk. Systemic Risk Centre Special Papers, n.º 13. https://www.sciencedirect.com/science/article/pii/S0378426621002466

Darktrace. (2023). AI Solutions for Cyber Threat Detection. Darktrace Research Reports. https://www.darktrace.com/es

Delgado, L. D., Gil, O. M., Gutiérrez, M. P., & Cardona, C. P. (2019). Diseño de un sistema de clasificación de riesgos para proyectos financiados a través de plataformas digitales bajo la modalidad del crowdfunding financiero. Revista Espacios, 40 (11). https://www.revistaespacios.com/a19v40n11/19401115.html

Díaz-Casillas, L., Blanco, F. J., & Garijo, M. (2010). Sistema basado en reglas para la validación del despliegue de servicios. Inteligencia Artificial. Revista Iberoamericana de Inteligencia Artificial, 14(47), 54-70. https://www.researchgate.net/publication/220071759_Sistema_basado_en_reglas_para_la_validacion_del_despliegue_de_servicios

Fernández Bedoya, A. (2019). Inteligencia artificial en los servicios financieros. Boletín económico/Banco de España. https://www.bde.es/f/webbde/SES/Secciones/Publicaciones/InformesBoletinesRevistas/ArticulosAnaliticos/19/T2/descargar/Fich/be1902-art7.pdf

Fernández, A. (2019). Inteligencia artificial en los servicios financieros. https://core.ac.uk/download/pdf/322617455.pdf

Fernández-Villaverde, J., & Sanches, D. (2019). ¿Puede funcionar la competencia monetaria? Revista de Economía Monetaria, 106, 1-15. https://www.sciencedirect.com/science/article/abs/pii/S0304393219301217

Fernández-Villaverde, J., Hurtado, S., & Nuño, G. (2019). Financial Frictions and the Wealth Distribution. mimeo. https://onlinelibrary.wiley.com/doi/abs/10.3982/ECTA18180

Francés Monedero, T. (2020). Impacto del machine learning en el sistema financiero. https://repositorio.comillas.edu/xmlui/handle/11531/42692

García-Uribe, S. (2018). The effects of tax changes on economic activity: A narrative approach to frequent anticipations. Documentos de Trabajo, n.º 1828, Banco de España. https://academic.oup.com/ej/article-abstract/133/650/706/6697752?login=false

Gelbukh, A. (2010). Procesamiento de lenguaje natural y sus aplicaciones. Komputer Sapiens, 1, 6-11. https://www.academia.edu/download/30768432/Procesamiento_de_lenguaje_natural_y_sus_aplicaciones.pdf

Ghirelli, C., Pérez, J. J., & Urtasun, A. (2019). A new economic policy uncertainty index for Spain. Documentos de Trabajo, n.º 1906, Banco de España. https://www.sciencedirect.com/science/article/abs/pii/S0165176519301806

Gil, M., Pérez, J. J., Sánchez, A. J., & Urtasun, A. (2018). Nowcasting private consumption: Traditional indicators, uncertainty measures, credit cards and some internet data. Documentos de Trabajo, n.º 1842, Banco de España. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3299575

Goldman, D. (2012, septiembre 28). Major banks hit with biggest cyberattacks in history. https://money.cnn.com/2012/09/27/technology/bank-cyberattacks/index.html

González, G. (2023, septiembre 4). Encriptado homomórfico: La tecnología que permite almacenar y calcular datos sensibles en la nube sin comprometer la privacidad. BBVA. https://www.bbva.com/es/innovacion/encriptado-homomorfico-la-tecnologia-que-permite-almacenar-y-calcular-datos-sensibles-en-la-nube-sin-comprometer-la-privacidad/

Gordon, S., & Ford, R. (2006). On the definition and classification of cybercrime. Journal in Computer Virology, 2 (1), 13-20. https://link.springer.com/article/10.1007/s11416-006-0015-z

Grupo BBVA. (2020). BBVA aplica la tecnología de reconocimiento facial en sus oficinas en España. https://www.bbva.com/es/biometria-con-machine-learning-cada-vez-mas-inteligente-y-segura-para-acceder-a-tu-banco/

Grupo BBVA. (2023). BBVA es el banco europeo con la mayor presencia internacional, según el ranking BrandZ™ Global 2023. https://www.bbva.com/es/bbva-es-el-banco-europeo-con-la-mayor-presencia-internacional-segun-el-ranking-brandz-global-2023/

HSBC. (2021). Fraud Detection in Banking. HSBC White Paper. https://www.hsbc.com/-/files/hsbc/investors/hsbc-results/2021/annual/pdfs/hsbc-holdings-plc/220222-risk-review-2021-ara.pdf

IBM. (2021). State of Financial Security. IBM Security Insights. https://www.ibm.com/think/x-force/whats-new-2021-cost-of-a-data-breach-report

IBM. (2021). The Role of AI in Risk Management. IBM Research. https://www.ibm.com/think/insights/ai-risk-management

Instituto Español de Ciberseguridad. (2022). Guía sobre ciberseguridad en la banca digital. https://www.incibe.es/protege-tu-empresa/blog/guia-ciberseguridad-banca-digital

IPSoft. (2018). Amelia, la asistente virtual de BBVA. https://cutt.ly/mtGttEA

Jones, C., Lee, D., Phan, L., Han, J., Kim, J., & Wu, D. (2017). Artificial intelligence applications in retail financial services. IBM Institute for Business Value. https://www.ibm.com/downloads/cas/WERWEKBG

Kao, J., & Reidy, S. (2019). Consumer Finance Monitor. https://www.consumerfinancemonitor.com/

KPMG. (2017). The Pulse of Fintech Q2 2017. https://assets.kpmg/content/dam/kpmg/xx/pdf/2017/08/pulse-of-fintech-q2-2017.pdf

KPMG. (2018). The Pulse of Fintech Q3 2018. https://assets.kpmg/content/dam/kpmg/xx/pdf/2018/10/pulse-of-fintech-q3-2018.pdf

KPMG. (2020). The Pulse of Fintech Q1 2020. https://assets.kpmg/content/dam/kpmg/xx/pdf/2020/05/pulse-of-fintech-q1-2020.pdf

Kroenke, D. M., & Boyle, R. J. (2021). Experiencing MIS (8a ed.). Pearson.

La educación en la era de la inteligencia artificial. https://doi.org/10.18421/TEM131-42

Larson, S. (2019, septiembre 23). Google enfrenta nueva demanda por violar la privacidad de los usuarios con su asistente de voz. CNN Business. https://cnnespanol.cnn.com/2019/09/23/google-demanda-privacidad-asistente-voz/

Microsoft. (2022). Threat Intelligence with AI. Microsoft Security Report. https://www.microsoft.com/en-us/security/security-insider/intelligence-reports/microsoft-digital-defense-report-2022

Nonbank Financials, Fintech, and Innovation. https://home.treasury.gov/system/files/136/A-Financial-System-That-Creates-Economic-Opportunities-Nonbank-Financials-Fintech-and-Innovation.pdf

OECD. (2017). Financial Stability, Financial Services and Technology: New Approaches to Financial Regulation. https://www.oecd.org/finance/New-Approaches-to-Financial-Regulation.pdf

OECD. (2020). Digital disruption in banking and its impact on competition. https://www.oecd.org/finance/Digital-Disruption-in-Banking-and-its-Impact-on-Competition.pdf

OECD. (2020). OECD Business and Finance Outlook 2020: Sustainable and Resilient Finance. https://www.oecd.org/daf/OECD-Business-and-Finance-Outlook-2020.pdf

OECD. (2020). The impact of AI on the labour market: What do we know so far?. https://www.oecd.org/ai/The-impact-of-AI-on-the-labour-market.pdf

OECD. (2021). AI in Business and Finance: Opportunities and Challenges for Asia and the Pacific. https://www.oecd.org/finance/AI-in-Business-and-Finance-Asia-Pacific.pdf

PwC. (2018). Global FinTech Report 2018. https://www.pwc.com/gx/en/industries/financial-services/assets/pwc-global-fintech-report-2018.pdf

PwC. (2019). Succeeding in the new digital economy: The big shift to AI and automation. https://www.pwc.com/gx/en/issues/reports/succeeding-in-the-new-digital-economy.pdf

Sánchez, D. (2019). Modelización de la economía española: Proyecciones de mediano plazo. Documentos de Trabajo, n.º 1911, Banco de España. https://www.bde.es/f/webbde/SES/Secciones/Publicaciones/PublicacionesSeriadas/DocumentosOcasionales/20/Fich/do2011.pdf

Sociedad para la Gestión de Activos Procedentes de la Reestructuración Bancaria. (2020). Estrategia de transformación digital de Sareb. https://www.sareb.es/es/conocenos/transformacion-digital

Splunk. (2022). Behavioral Analytics and Threat Detection. Splunk Insights. https://www.splunk.com/en_us/products/enterprise-security.html

Symantec. (2021). AI and Threat Intelligence. Symantec Security Insights. https://www.security.com/threat-intelligence

The Economist Intelligence Unit. (2018). The critical role of infrastructure for the adoption of digital finance in developing countries. https://www.eiu.com/n/The-critical-role-of-infrastructure-for-the-adoption-of-digital-finance-in-developing-countries/

The European Banking Authority. (2018). EBA Report on the impact of Fintech on incumbent credit institutions' business models. https://www.eba.europa.eu/eba-report-on-the-impact-of-fintech-on-incumbent-credit-institutions-business-models

The Institute of International Finance. (2018). Machine learning in the finance industry: Taking the pulse. https://www.iif.com/publication/fintech/machine-learning-finance-industry-taking-pulse

The World Bank. (2020). Digital financial services. https://www.worldbank.org/en/topic/financialinclusion/brief/digital-financial-services

U.N. Secretary-General's High-Level Panel on Digital Cooperation. (2019). The Age of Digital Interdependence. https://www.un.org/en/pdfs/DigitalCooperation-report-for-web.pdf

U.S. Department of the Treasury. (2020). A Financial System That Creates Economic Opportunities. https://home.treasury.gov/sites/default/files/2018-07/Nonbank%20Financials%20EO%20-%20Fact-Sheet%20FINAL.PDF

Unión Europea. (2021). Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales ya la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) (Texto pertinente a efectos del EEE). https://travesia.mcu.es/bitstream/10421/9133/1/Regla_UE_679_2016.pdf

Vilches, M. (2020). La regulación del crowdfunding: una visión comparada. Revista de Derecho Financiero, 7 (1), 97-123. https://dialnet.unirioja.es/servlet/articulo?codigo=8328964

Villanueva, J. A., & Mora, P. (2021). Evolución y desafíos del fintech en México: un análisis del sector. Revista de Economía Mexicana, 13 (25), 67-83. https://www.scielo.org.mx/scielo.php?pid=S1665-53462021000500010&script=sci_abstract

Villanueva, J. A., Mora, P., & De la Fuente, S. (2019). El impacto de la digitalización en la banca tradicional: Oportunidades y retos. Documentos de Trabajo, n.º 1912, Banco de España. https://repositorio.comillas.edu/rest/bitstreams/507662/retrieve

Weigend, A. (2016). Data for the People: How to Make Our Post-Privacy Economy Work for You. Basic Books. https://books.google.es/books?hl=es&lr=&id=pKtVDgAAQBAJ&oi=fnd&pg=PT7&dq=Weigend,+A.+(2016).+Data+for+the+People:+How+to+Make+Our+Post-Privacy+Economy+Work+for+You.+Basic+Books.+&ots=VdFHK8sSSz&sig=5OTrx2E98F1UQW2Y8bvLwfTJgvo

World Bank Group. (2020). Digital Financial Services. https://www.worldbank.org/en/topic/financialinclusion/brief/digital-financial-services

World Economic Forum. (2017). The future of financial infrastructure: An ambitious look at how blockchain can reshape financial services. https://www.weforum.org/reports/the-future-of-financial-infrastructure-an-ambitious-look-at-how-blockchain-can-reshape-financial-services

World Economic Forum. (2018). Innovative technology in financial services: The regulatory response. https://www.weforum.org/reports/innovative-technology-in-financial-services-the-regulatory-response

World Economic Forum. (2020). The impact of the COVID-19 crisis on the fintech sector. https://www.weforum.org/reports/the-impact-of-the-covid-19-crisis-on-the-fintech-sector

World Economic Forum. (2021). Fintech and the Global Economy: Fostering Growth and Inclusion. https://www.weforum.org/reports/fintech-and-the-global-economy-fostering-growth-and-inclusion

Apéndices

Apéndice A

Formato RAE

Fecha de Realización: 30/05/2025
Título: Análisis de la aplicación de la inteligencia artificial asociada a la ciberseguridad en empresas financieras seleccionadas
Autor: MAESTRE, Carlos
Palabras Claves: aprendizaje automático, ciberseguridad, inteligencia artificial, prevención del fraude, sector financiero.
Descripción: Esta monografía analiza el impacto de la IA aplicada a la ciberseguridad dentro del sector financiero, considerando sus beneficios, desafíos y riesgos asociados, desarrollando una revisión documental centrada en cómo las entidades bancarias utilizan tecnologías basadas en IA como aprendizaje automático, procesamiento de lenguaje natural y autenticación biométrica para detectar amenazas, prevenir fraudes y gestionar incidentes de seguridad, incluyendo casos reales de entidades como Banco de Bogotá, BBVA, Banco Santander y CaixaBank y he examinado soluciones como Darktrace, SAS Fraud Management, IBM OpenPages y Behavioral Analytics Suite de Splunk, con el objetivo de brindar recomendaciones estratégicas para la adopción de la IA como mecanismo robusto de protección ante ciberataques, bajo un enfoque predictivo y proactivo.
Fuentes: Banco de Bogotá. (2022, septiembre 21). Innovación con Inteligencia Artificial del Banco de Bogotá permite mayor acceso a los colombianos al sistema financiero.

https://saladeprensa.bancodebogota.com/2022/09/21/innovacion-con-inteligencia-artificial-del-banco-de-bogota-permite-mayor-acceso-a-los-colombianos-al-sistema-financiero/

BBVA. (2018). BBVA automatiza los servicios de atención al cliente con la tecnología de inteligencia artificial de IPSoft. https://www.bbva.com/es/innovacion/bbva-automatiza-servicios-atencion-cliente-tecnologia-inteligencia-artificial-ipsoft/

CaixaBank. (2022). El 'Chatbot' de CaixaBank ya conversa con uno de cada tres clientes de banca digital. https://www.caixabank.com/comunicacion/noticia/el-chatbot-de-caixabank-ya-conversa-con-uno-de-cada-tres-clientes-de-banca-digital_es.html?id=43753

Darktrace. (2023). AI Solutions for Cyber Threat Detection. Darktrace Research Reports. https://www.darktrace.com/es

HSBC. (2021). Fraud Detection in Banking. HSBC White Paper. https://www.hsbc.com/-/files/hsbc/investors/hsbc-results/2021/annual/pdfs/hsbc-holdings-plc/220222-risk-review-2021-ara.pdf

IBM. (2021). The Role of AI in Risk Management. IBM Research. https://www.ibm.com/think/insights/ai-risk-management

Splunk. (2022). Behavioral Analytics and Threat Detection. Splunk Insights. https://www.splunk.com/en_us/products/enterprise-security.html

Contenido del documento:

Metodología:

Empleé un enfoque cualitativo, de tipo descriptivo y exploratorio, mediante la revisión fuentes documentales como artículos científicos e informes institucionales, seleccionando casos de aplicación práctica en bancos reconocidos para evidenciar los beneficios y retos del uso de IA en la ciberseguridad, analizando las herramientas empleadas, su funcionalidad y su impacto en la protección de activos digitales.

Conceptos nuevos:

Reconocimiento óptico de caracteres (OCR): Tecnología utilizada para convertir texto impreso o manuscrito en datos digitales, optimizando procesos de digitalización documental en entidades financieras.

Scorecard de crédito: Herramienta analítica basada en algoritmos que asigna puntuaciones de riesgo crediticio a los usuarios mediante variables como edad, ingresos y comportamiento financiero.

Procesamiento de lenguaje natural (NLP): Subcampo de la inteligencia artificial que permite a los sistemas comprender, interpretar y generar lenguaje humano, clave para el funcionamiento de chatbots bancarios.

Conclusiones:

El uso de inteligencia artificial en la ciberseguridad del sector financiero ha demostrado ser una herramienta esencial para anticipar, detectar y mitigar amenazas, ya que permite mejorar la eficiencia, personalización y toma de decisiones, destacando que su implementación requiere medidas robustas de protección y monitoreo continuo, ya que los ciberdelincuentes también usan la IA a su favor, por tal motivo deben complementarse con controles técnicos, auditorías y estrategias de contingencia.

Hay que reconocer que las entidades bancarias analizadas evidencian avances significativos en su adaptación tecnológica, lo cual les proporciona una ventaja competitiva y fortalece la confianza del cliente y pienso que la adopción de IA debe ir acompañada de un cambio cultural y organizacional que garantice su uso ético, transparente y conforme a las normativas vigentes.
AUTOR: Carlos Rafael Maestre Márquez