Fundamentos Teóricos Para Sustenta Un Modelo Preventivo En La Ciberseguridad Financiera

Julián Esteban Acosta Castiblanco 2348364

Valentina Rojas Bohórquez 234748

Director del Proyecto José Alexander Cely Ramírez

Negocios Internacionales

Universidad Santo Tomas Seccional Tunja

6 de abril de 2026

Dedicatoria

Dedico este trabajo principalmente a mi familia, por su apoyo incondicional, comprensión y motivación constante a lo largo de este proceso académico. Su confianza en mis capacidades y sus palabras de aliento han sido fundamentales para alcanzar esta meta.

Este logro también representa el resultado del esfuerzo, la perseverancia y el compromiso invertidos durante esta etapa de aprendizaje, y simboliza un paso importante hacia nuevos desafíos y oportunidades.

Julián Esteban Acosta Castiblaco

Dedico este trabajo a mis padres, a mis hermanas y a las personas que han estado a mi lado en cada etapa de este camino, brindándome apoyo, comprensión y motivación para seguir adelante.

Su confianza en mí ha sido una de las mayores razones para no rendirme y continuar luchando por mis metas. También dedico este trabajo a mi compañero de tesis, con quien compartí este proceso lleno de aprendizaje, esfuerzo y dedicación.

Valentina Rojas Bohórquez

Agradecimientos

Expreso mi más sincero agradecimiento a todas las personas que hicieron posible la realización de este trabajo de investigación.

En primer lugar, agradezco a mi director(a) de tesis por su orientación, acompañamiento y valiosos aportes durante el desarrollo de esta investigación. Su conocimiento, experiencia y disposición fueron fundamentales para la culminación de este proyecto.

Asimismo, agradezco a los docentes que hicieron parte de mi formación académica, quienes a través de sus enseñanzas contribuyeron significativamente al desarrollo de mis conocimientos y habilidades profesionales.

Finalmente, agradezco a todas aquellas personas que directa o indirectamente brindaron su apoyo y colaboración en el desarrollo de esta investigación.

Julián Esteban Acosta Castiblanco

Le doy gracias a Dios por la experiencia brindada dentro de la universidad, expreso mi más sincero agradecimiento al director de tesis por su orientación, conocimientos y acompañamiento durante el desarrollo de esta investigación.

A la universidad y al programa académico, por brindarnos las herramientas y el espacio para desarrollar nuestras capacidades profesionales y académicos, de la misma manera a los docentes que me acompañaron a lo largo de mi formación y ser fuente de inspiración. También a mis padres por darme la oportunidad de estudiar y seguir cumpliendo mis metas.

Valentina Rojas Bohórquez

Tabla de contenido

Glosario

Phishing: Técnica de fraude informático que consiste en engañar a los usuarios mediante correos electrónicos, mensajes o sitios web falsos con el fin de obtener información confidencial, especialmente datos bancarios.

Ransomware: Tipo de ataque cibernético en el que un software malicioso bloquea el acceso a un sistema o a la información hasta que se pague un rescate.

Fraude transaccional: Actividad ilícita que consiste en manipular operaciones financieras digitales para obtener beneficios económicos de forma ilegal.

Sistemas adaptativos: Modelos tecnológicos capaces de ajustarse automáticamente a cambios en los datos o en el entorno, permitiendo mejorar la detección de amenazas en tiempo real.

Inteligencia artificial: Conjunto de técnicas computacionales que permiten a los sistemas imitar procesos de aprendizaje, razonamiento y toma de decisiones para resolver problemas complejos.

Gestión del riesgo operativo: Proceso mediante el cual las organizaciones identifican, analizan y controlan riesgos derivados de fallas en procesos, personas, tecnología o eventos externos.

Anomalía transaccional: Comportamiento inusual en una operación financiera que puede indicar fraude, error o intento de ataque cibernético.

Resumen

La presente investigación analiza los fundamentos teóricos que sustentan un modelo preventivo en la ciberseguridad financiera, con el propósito de comprender cómo los enfoques conceptuales del Big Data, el aprendizaje automático y la gestión del riesgo tecnológico permiten fortalecer la anticipación de amenazas en el sistema financiero. El estudio se desarrolló bajo un enfoque cualitativo de tipo documental, mediante la revisión sistemática de literatura científica reciente y normativa colombiana relacionada con seguridad digital y riesgo operativo.

Los resultados evidencian que el aumento de la digitalización financiera ha incrementado la complejidad de los ataques cibernéticos, lo que limita la efectividad de los modelos tradicionales de seguridad. Investigaciones recientes señalan que el uso de inteligencia artificial y análisis masivo de datos permite detectar patrones anómalos y mejorar la capacidad de respuesta frente a amenazas emergentes (Alrafi & Mishra, 2024). En este sentido, los fundamentos teóricos revisados demuestran que los modelos preventivos deben basarse en sistemas adaptativos, análisis en tiempo real y cumplimiento normativo, con el fin de garantizar la estabilidad y la confianza en los entornos financieros digitales.

Se concluye que la integración de estos enfoques proporciona el sustento conceptual necesario para el desarrollo de modelos preventivos orientados a la anticipación del riesgo, contribuyendo al fortalecimiento de la ciberseguridad en el contexto financiero colombiano

Palabras Clave: Ciberseguridad financiera, Big Data, aprendizaje automático, modelo preventivo.

Abstract

This study analyzes the theoretical foundations underpinning a preventive model in financial cybersecurity, with the aim of understanding how conceptual approaches to big data, machine learning, and technological risk management can enhance the anticipation of threats in the financial system. The study was conducted using a qualitative, documentary approach, involving a systematic review of recent scientific literature and Colombian regulations related to digital security and operational risk.

The results show that the rise of financial digitization has increased the complexity of cyberattacks, limiting the effectiveness of traditional security models. Recent research indicates that the use of artificial intelligence and big data analytics enables the detection of anomalous patterns and improves the ability to respond to emerging threats(Alrafi & Mishra, 2024). In this regard, the reviewed theoretical foundations demonstrate that preventive models must be based on adaptive systems, real-time analysis, and regulatory compliance in order to ensure stability and trust in digital financial environments.

It is concluded that the integration of these approaches provides the conceptual foundation necessary for the development of preventive models aimed at risk anticipation, thereby contributing to the strengthening of cybersecurity in the Colombian financial sector.

Keywords: Financial cybersecurity, big data, machine learning, preventive model

1. Introducción

En esta investigación se analiza los fundamentos teóricos de la ciberseguridad financiera desde el enfoque del Big Data y el aprendizaje automático. Su propósito es comprender cómo estas tecnologías pueden contribuir a la estructuración de un modelo preventivo capaz de anticipar riesgos y amenazas digitales en el sistema financiero. A partir de una revisión documental de literatura científica y normativa colombiana, se busca establecer una base conceptual que permita fortalecer las estrategias de protección frente a ciberataques en el contexto financiero colombiano.

1.1 Planteamiento del Problema

En Colombia, la digitalización del sistema financiero ha impulsado un crecimiento acelerado de los servicios electrónicos. El uso de aplicaciones móviles, las transacciones en línea y los pagos digitales se ha generalizado. Actualmente, miles de transacciones por minuto evidencian la transformación tecnológica del sector bancario, orientada a la eficiencia y a la accesibilidad digital. Sin embargo, esta evolución plantea retos significativos en materia de seguridad informática(Vega, 2025).

Según (Vega, 2025) el avance del entorno digital ha coincidido con un aumento alarmante de ciberataques dirigidos al sector financiero. Datos de la Superintendencia Financiera y reportes especializados indican que entre enero y julio de 2025 se registraron 27.000 millones de intentos de ataques cibernéticos contra establecimientos bancarios, lo que representa un crecimiento del 69 % respecto al mismo periodo del año anterior. Las entidades financieras en Colombia enfrentan aproximadamente 94 ciberataques por segundo, lo que evidencia la magnitud y frecuencia de las amenazas, entre las cuales la suplantación de identidad, la vulneración de cuentas y el fraude tecnológico son las más reportadas Estos ataques no solo representan un riesgo operacional para las instituciones, sino que también afectan directamente a los usuarios. En promedio, alrededor de 1.000 colombianos son víctimas diarias de robo de datos personales asociados a transacciones financieras, y solo en el tercer trimestre de 2025 los bancos recibieron más de **240.000** quejas por fraudes tecnológicos**.**

A nivel nacional, se estima que en los últimos periodos el sistema financiero enfrentó 36.000 millones de intentos de ciberataque en un año, equivalentes a 98 millones diarios. Estas amenazas aumentan no solo en frecuencia, sino también en sofisticación, impulsadas por técnicas avanzadas de ingeniería social, la explotación de vulnerabilidades y el robo automatizado de credenciales (Forbes, 2025).

Aunque las entidades han incrementado la inversión en ciberseguridad, adoptando mejores prácticas de gestión de riesgos y tecnologías más robustas, las técnicas tradicionales de protección presentan limitaciones ante la escala y la complejidad de las amenazas actuales. Frecuentemente, los mecanismos de defensa son reactivos y carecen de capacidades predictivas avanzadas, lo que dificulta la identificación temprana de patrones anómalos antes de que se materialicen en pérdidas o vulneraciones. En este contexto, las tecnologías de Big Data y aprendizaje automático pueden transformar la gestión de la ciberseguridad financiera al permitir el análisis en tiempo real de grandes volúmenes de datos transaccionales, la detección de patrones sospechosos y la construcción de modelos predictivos para anticipar ataques. Sin embargo, persiste una brecha entre el uso de estas tecnologías y el desarrollo de un modelo teórico y aplicado que las integre de manera estructurada en los procesos de seguridad de las entidades financieras colombianas.

Pregunta de Investigación

¿Cómo los fundamentos teóricos sustentan un modelo preventivo en la ciberseguridad financiera?

1.2 Objetivos

1.1.1 Objetivo general

- Analizar los fundamentos teóricos del Big Data y el aprendizaje automático para estructurar una propuesta conceptual de modelo de ciberseguridad financiera aplicable al contexto colombiano.

1.1.2 Objetivos específicos

- Describir el panorama actual de las amenazas cibernéticas en el sistema financiero y su impacto en los mercados digitales
- Examinar los aportes teóricos del Big Data y del aprendizaje automático en la detección de fraudes financiero.
- Identificar los componentes tecnológicos y organizacionales necesarios para integrar herramientas preventivas en la ciberseguridad financiera.

1.1.3. Justificación

El crecimiento acelerado de los servicios financieros digitales ha incrementado la exposición a riesgos cibernéticos, convirtiendo la ciberseguridad en un elemento estratégico para la estabilidad económica y la confianza de los usuarios. En este contexto, resulta pertinente analizar desde un enfoque teórico cómo puede estructurarse un modelo preventivo en ciberseguridad financiera, integrando aportes conceptuales del Big Data y el aprendizaje automático, sin llegar a su implementación práctica.

La importancia del estudio radica en la necesidad de fortalecer las bases conceptuales que orienten futuras estrategias de prevención en el sector financiero colombiano. Actualmente, existe abundante literatura sobre detección de fraudes y análisis de datos, pero se requiere una integración teórica que articule estos elementos dentro de un enfoque preventivo estructurado. Los principales beneficiarios de esta investigación son la comunidad académica, al contar con un marco teórico organizado sobre ciberseguridad financiera; las entidades del sector financiero, que podrán utilizar este análisis como referencia para el diseño de estrategias preventivas; y los usuarios del sistema financiero, quienes se verían indirectamente favorecidos por el fortalecimiento de prácticas de seguridad digital.

El impacto esperado es principalmente académico, al aportar una sistematización conceptual actualizada sobre modelos preventivos en ciberseguridad financiera. Asimismo, el estudio puede generar impacto empresarial y social al servir como base para futuras aplicaciones que contribuyan a reducir riesgos cibernéticos y fortalecer la confianza en los entornos financieros digitale

2. Marco Referencial

2.1. Estado del arte

El sector de los servicios financieros ha experimentado un crecimiento acelerado en los últimos años, impulsado por la adopción masiva de tecnologías digitales y la demanda de servicios financieros más accesibles y eficientes, siendo un factor clave de este cambio la pandemia. Sin embargo, este avance ha generado nuevos retos en materia de ciberseguridad, ya que los sistemas digitales bancarios se han convertido en objetivos prioritarios para los ciberdelincuentes.

De tal manera, el malware financiero representa una amenaza crítica para la seguridad de las plataformas digitales bancarias. Según (Shehab et al., 2024), detalla cómo este tipo de software malicioso está diseñado específicamente para atacar sistemas financieros, con el objetivo de robar credenciales, interceptar transacciones y sustraer fondos. Los ciberdelincuentes utilizan técnicas avanzadas, como troyanos bancarios y phishing dirigido, que se adaptan rápidamente a los mecanismos de defensa existentes. Además, la investigación señala que la detección y mitigación del malware financiero requiere la integración de tecnologías emergentes, como la inteligencia artificial y el aprendizaje automático, que permiten identificar patrones anómalos y responder de forma proactiva a las amenazas. En esta línea (Akhtar & Feng, 2022a), resaltan que las soluciones tradicionales basadas en firmas resultan insuficientes frente a la complejidad del malware moderno, por lo que proponen el uso de modelos híbridos de aprendizaje profund**o**, como CNN-LSTM, capaces de detectar comportamientos anómalos en tiempo real con una precisión del 99%. Estas tecnologías, apoyadas en inteligencia artificial y aprendizaje automático, permiten identificar patrones de ataque ocultos como lo son (polimorfismo y metamorfismo) y mejorar la respuesta proactiva ante amenazas financieras emergentes, fortaleciendo así la ciberseguridad en los entornos bancarios digitales.

Por ello, (Aslan et al., 2023) proponen la adopción de soluciones innovadoras basadas en aprendizaje automático (ML), aprendizaje profundo (DL), big data y blockchain, con el fin de anticipar y mitigar las amenazas en tiempo real. En consonancia con esta visión (Mohamed, 2025) profundizan en el potencial de la inteligencia artificial aplicada a la ciberseguridad, sosteniendo que los modelos de ML y DL no solo permiten detectar patrones anómalos o ataques desconocidos, sino que también pueden adaptarse y aprender del comportamiento de los atacantes, fortaleciendo así las estrategias de defensa.

En este mismo contexto, los correos electrónicos spam emergen como una de las herramientas más utilizados para la propagación de estas amenazas, incluyendo phishing y malware dirigido a usuarios financieros individuales y organizacionales. De acuerdo con (Jáñez-Martino et al., 2025)se propone un enfoque basado en procesamiento de lenguaje natural (NLP) para extraer 56 características de correos spam agrupadas en cabeceras, texto, adjuntos, URLs y protocolos, clasificándolos según su riesgo potencial en ciberseguridad. Utilizando modelos de machine learning como Random Forest, los autores logran una precisión alta (F1-Score de 0.914) en la distinción entre correos de bajo y alto riesgo, lo que facilita alertas tempranas y análisis por expertos en ciberseguridad. Asimismo, (Y. Chen et al., 2025) exploran cómo el Deep learning combinado con NLP, mejora la detección de phishing en el sector financiero, reduciendo falsos positivos y adaptándose a campañas evolucionadas. Para reforzar esta teoría, un estudio sistemático reciente analiza la aplicación de deep learning en la detección de fraude financiero, revisando 108 publicaciones entre 2019 y 2024 para demostrar cómo los modelos DL, integrados con NLP, elevan la precisión en la identificación de patrones anómalos en correos phishing y transacciones, enfatizando la necesidad de procesar características como texto, URLs y protocolos para mitigar efectivamente la propagación de amenazas cibernéticas en el sector financiero.

De la misma forma (Gupta, 2025), propone que la protección de la infraestructura tecnológica y la información sensible en la banca digital requiere la implementación de estrategias de seguridad robustas que abarquen desde controles de acceso y autenticación multifactor, hasta sistemas de monitoreo continuo y detección temprana de amenazas. La complejidad y sofisticación de los ataques actuales obligan a las instituciones financieras a mantenerse en constante actualización para proteger la confidencialidad, integridad y

disponibilidad de sus servicios. En ese sentido, estudios como el de (Kuzior et al., 2022) confirman el impacto creciente de los ciberataques en el sector financiero, donde este representa el 22.4% de todos los ataques globales, con un costo promedio de USD 5.97 millones por incidente. Utilizando datos de tendencias informativas, por ejemplo: consultas en Google Trends sobre ataques a sistemas informáticos, redes y nubes, donde se proponen modelos de suavizado exponencial para pronosticar tendencias de ciberataques, lo que permite a las instituciones anticipar riesgos y fortalecer sus estrategias de detección temprana.

Como se menciona en los artículos anteriores, los ataques cibernéticos han aumentado, lo que hace que las empresas y bancos busquen soluciones. En particular, las redes sociales han emergido como un vector crítico de riesgo en la ciberseguridad financiera, ya que los atacantes las utilizan para propagar malware, realizar phishing dirigido, explotar vulnerabilidades derivadas de la interacción de usuarios con plataformas digitales para obtener datos sensibles o comprometer sistemas financieros. Según un estudio reciente, las redes sociales no solo facilitan ataques sofisticados como la difusión de desinformación que erosiona la confianza en las instituciones financieras, sino que también sirven como canales para la distribución de enlaces maliciosos y la recopilación de datos personales a través de perfiles falsos o publicidad engañosa(Hossain, 2025). Para mitigar estos riesgos, las instituciones están adoptando estrategias avanzadas, como el uso de inteligencia artificial para monitorear actividades sospechosas en redes sociales, el análisis de patrones de comportamiento en tiempo real y la implementación de sistemas de microsegmentación para limitar el acceso no autorizado a datos sensibles. Por ejemplo, en Brasil, un país líder en la adopción de tecnologías financieras en América Latina, importantes empresas y bancos están implementando soluciones como Cisco ISE para control de acceso y Cisco Trustsec para microsegmentación, lo que mejora la visibilidad y control de las redes, mitigando riesgos internos y externos. Complementando esto, otro análisis destaca cómo las mejores prácticas en la gestión de riesgos en redes sociales, incluyendo campañas de concienciación, marcos regulatorios robustos y el uso de herramientas de detección de amenazas en tiempo real, son esenciales para contrarrestar amenazas cibernéticas en el sector financiero(Pinheiro Santana et al., 2025).

Otra de las estrategias tomadas por las entidades bancarias es el uso de algoritmos de inteligencia artificial (IA), donde los autores(Alrafi & Mishra, 2024) explican cómo la IA y el big

TUNJA - BOYACÁ · PBX: (608) 744 0404
Campus Centro Histórico: Cll. 19 No. 11 - 64 · Campus Avenida Universitaria:
Edificio Fray Giordano Bruno, O.P.: Av. Universitaria Cll. 48 No. 1-235 este.
Edificio Santo Domingo de Guzmán: Av. Universitaria No. 45 - 202.
Santoto Services: Centro Comercial Unicentro Tunja, Local 1-106.

data (BD) están transformando la ciberseguridad en el sector financiero al automatizar el análisis de grandes volúmenes de datos, lo que permite identificar riesgos en tiempo real y fortalecer la detección de fraudes, el scoring crediticio y la protección frente a amenazas digitales. Aunque los modelos de machine learning y deep learning han demostrado eficacia en diferenciar transacciones legítimas y fraudulentas, generando mayor confianza y reduciendo pérdidas, los autores advierten sobre limitaciones como problemas de privacidad, falta de transparencia en los algoritmos, altos costos de implementación y posibles sesgos, con experimentos que mostraron una alta precisión (99%) pero tasas elevadas de falsos positivos, evidenciando la necesidad de perfeccionar los modelos. Complementando esta discusión, otro modelo propuesto por los autores (Usman et al., 2024) destaca que la efectividad en la gestión de riesgos de ciberseguridad no solo depende de las tecnologías adoptadas, sino también de las características de los auditores internos en las organizaciones financieras; a través de un marco conceptual basado en las teorías de la competencia y del comportamiento planificado, se explican factores como la ética profesional, los rasgos de personalidad, las competencias en habilidades y conocimientos, así como los mecanismos de disuasión y recompensas, que son determinantes en la capacidad de los auditores para identificar, evaluar y mitigar riesgos cibernéticos, enfatizando que, con estas cualidades y formación especializada, podrán desempeñar un rol más proactivo en la protección de la infraestructura crítica y en la generación de confianza dentro del sistema financiero, cerrando así una brecha poco explorada en la literatura sobre ciberseguridad.

La cultura desempeña un papel crucial en la adopción de soluciones de ciberseguridad y pagos digitales dentro del sistema financiero, ya que la confianza de las personas en estas tecnologías está influenciada por factores culturales y políticas financieras, lo que puede obstaculizar el progreso de los pagos digitales debido a preocupaciones sobre la seguridad de la información. Un estudio que analiza datos de 76 países entre 2011 y 2017, utilizando fuentes como Global Findex, World Bank, ITU y las dimensiones culturales de Hofstede, concluye que un mayor compromiso nacional en ciberseguridad (NCSC) fomenta significativamente el uso de pagos digitales (DPU), con un efecto moderado por dimensiones culturales como la evitación de la incertidumbre, donde un entorno sólido reduce la desconfianza y promueve la adopción de innovaciones financieras, mientras que el individualismo muestra un impacto menos claro(Krishna et al., 2023).Este efecto es más pronunciado en países con alta evitación de la

incertidumbre, donde los usuarios perciben mayores riesgos, pero políticas robustas y un enfoque en la confianza institucional ayudan a mitigar estas barreras. Además, factores como la preparación tecnológica, el desarrollo de mercados financieros y el nivel educativo de la población también resultan determinantes en este proceso, destacando la necesidad de mejorar la experiencia del usuario (UX) en pagos digitales para fomentar una adopción más amplia, especialmente en contextos como el de China, donde la percepción de facilidad de uso y utilidad influye positivamente en la actitud hacia las monedas digitales(Ma et al., 2023).

Desde otro punto de vista, un artículo describe que se centra en la adopción de servicios de pago digital en los países en desarrollo, abordando factores que impulsan o limitan su crecimiento mediante un modelo basado en la teoría unificada de aceptación y uso de tecnología (UTAUT) para analizar confianza, seguridad percibida, facilidad de uso y apoyo gubernamental. A partir de una encuesta en un contexto específico, los resultados muestran que confianza y percepción de seguridad son clave, mientras que falta de concienciación y resistencia cultural son barreras, resaltando que marcos regulatorios fortalecen la transición a economías sin efectivo (Chandra et al., 2022). Complementando, un estudio sobre pagos móviles con código QR en Bangladesh, un país en desarrollo utiliza una combinación de métodos de mínimos cuadrados parciales (PLS) y discusiones de grupos focales (FGD) para evaluar el modelo UTAUT extendido. Los hallazgos indican que la expectativa de desempeño, la expectativa de esfuerzo y la influencia social impactan positivamente la intención conductual, mientras que el autoconcepto, la autoeficacia percibida y el hábito influyen significativamente en las actitudes hacia el uso de pagos móviles QR. Además, se confirma que las actitudes positivas hacia estos pagos afectan tanto la intención conductual como el uso real, y que la intención conductual impulsa directamente la adopción de pagos QR, proporcionando implicaciones teóricas y gerenciales clave para promover economías sin efectivo en contextos similares(Islam et al., 2024).

Con todo lo anterior se puede y teniendo en cuenta las investigaciones revisadas (Shehab et al., 2024; Gupta, 2025; Kuzior et al., 2022) coinciden en que el malware financiero, el phishing y el ransomware constituyen las principales amenazas que afectan la estabilidad de los mercados de capitales y la confianza de los usuarios. Frente a ello, las soluciones tradicionales de defensa basadas en firmas resultan insuficientes ante la naturaleza dinámica y evolutiva de las amenazas modernas (Akhtar & Feng, 2022). En consecuencia, los avances más recientes en la literatura

destacan la necesidad de integrar tecnologías emergentes como la inteligencia artificial, el aprendizaje automático y el Big Data para fortalecer la detección temprana de riesgos. Modelos híbridos como CNN-LSTM y Random Forest han demostrado una alta precisión en la identificación de patrones anómalos y fraudes financieros (Aslan et al., 2023; Chen et al., 2025; Jáñez-Martino et al., 2025), optimizando la capacidad de respuesta proactiva de las instituciones. Estos enfoques, apoyados en el procesamiento de lenguaje natural y el análisis masivo de datos, permiten anticipar ataques complejos y reducir falsos positivos, consolidando una línea de investigación robusta hacia sistemas predictivos de ciberseguridad. Asimismo, los estudios señalan que el componente humano y organizacional continúa siendo un eje determinante en la gestión de riesgos cibernéticos. Factores como la ética profesional, la capacitación y las competencias de los auditores internos fortalecen las estrategias de prevención y mitigación (Usman et al., 2024). A ello se suma la influencia del contexto sociocultural y normativo, donde la confianza institucional y la preparación tecnológica inciden directamente en la adopción de pagos digitales seguros (Krishna et al., 2023; Ma et al., 2023).

Por tanto, se concluye que la evolución de la ciberseguridad en los mercados financieros demanda la creación de plataformas inteligentes integradas que aprovechen el potencial del Big Data y la inteligencia artificial para la detección temprana, análisis predictivo y respuesta automatizada frente a riesgos. Este enfoque representa no solo una innovación tecnológica, sino también una necesidad estratégica para garantizar la resiliencia, integridad y confianza del sistema financiero contemporáneo

2.2. Marco Teórico

2.2.1. Teoría Unificada de Aceptación y Uso de Tecnología

Este modelo teórico explica y predice cómo los individuos aceptan y utilizan tecnologías. La adopción tecnológica no depende de un solo factor, sino de la combinación de varios determinantes que influyen en la intención y el comportamiento de uso. Las ideas centrales son: 1. Existen constructos clave que inciden directamente en la intención de uso y, posteriormente, en el comportamiento real. 2. Factores moderadores, como la edad, el género y la experiencia, pueden modificar la fuerza de estas relaciones (Tamilmani et al., 2021).

Esta teoría se relaciona con el proyecto porque ofrece un marco teórico para comprender los factores que influyen en la adopción y uso de esa tecnología por parte de las entidades financieras y sus usuarios.

2.2.2. Teoría del Caos y Complejidad en Sistemas Financieros

La Teoría del Caos aplicada a los sistemas financieros plantea que los mercados son sistemas dinámicos complejos donde múltiples variables económicas, tecnológicas y sociales interactúan de manera no lineal, generando alta sensibilidad a las condiciones iniciales y comportamientos difíciles de predecir a largo plazo, aun cuando su estructura sea determinística. Desde esta perspectiva, fenómenos como la volatilidad, las crisis y los ciclos económicos no son anomalías aisladas, sino manifestaciones inherentes al funcionamiento del sistema. Herramientas como los modelos estocásticos, el análisis fractal y la teoría de sistemas complejos permiten identificar patrones, autosimilitudes y probabilidades de ocurrencia de determinados escenarios, reconociendo al mismo tiempo las limitaciones de enfoques tradicionales, como la hipótesis de los mercados eficientes .(Klioutchnikov et al., 2017).

Esta teoría es relevante para la presente investigación porque permite comprender que el riesgo financiero y el riesgo cibernético no se comportan de manera lineal ni predecible, especialmente en el contexto colombiano, donde la transformación digital del sistema financiero ha aumentado la interconexión entre entidades, usuarios y plataformas tecnológicas. Un incidente cibernético puede desencadenar efectos en cadena que afecten la confianza del mercado, la estabilidad operativa y la reputación institucional. En este sentido, la teoría del caos justifica conceptualmente la necesidad de implementar enfoques preventivos y sistemas adaptativos capaces de analizar grandes volúmenes de datos y detectar patrones emergentes antes de que evolucionen en crisis sistémicas. Así, el uso de Big Data y el aprendizaje automático no solo responde a una innovación tecnológica, sino también a la necesidad estructural de gestionar la complejidad inherente al sistema financiero contemporáneo.

2.2.3. Ciberseguridad y Gestión del Riesgo Financiero

La ciberseguridad en el marco de la gestión del riesgo financiero puede entenderse como el conjunto de estrategias, metodologías y herramientas tecnológicas orientadas a identificar, evaluar y mitigar amenazas digitales que puedan afectar la estabilidad, la integridad y la sostenibilidad del sistema financiero. Desde una perspectiva contemporánea, la gestión del riesgo

financiero ha evolucionado para incorporar riesgos tecnológicos y cibernéticos como parte del riesgo operacional, reconociendo que fraudes digitales, ataques informáticos y vulnerabilidades en sistemas automatizados pueden generar pérdidas económicas significativas y afectar la confianza del mercado. En esta línea, (Li et al., 2025) proponen un marco avanzado para la detección efectiva de fraude financiero basado en modelos analíticos transparentes que combinan técnicas de aprendizaje automático y programación genética, y resaltan que la gestión moderna del riesgo no solo debe enfocarse en la identificación de pérdidas pasadas, sino también en la construcción de sistemas predictivos y explicables que permitan anticipar comportamientos anómalos en entornos financieros cada vez más digitalizados.

En relación con la investigación, esta teoría adquiere especial relevancia al proporcionar un fundamento conceptual para comprender que los riesgos financieros y cibernéticos no se comportan de manera lineal ni son completamente predecibles. La digitalización del sistema financiero ha incrementado la interconexión y la velocidad de propagación de eventos adversos, lo que amplifica los efectos de pequeñas vulnerabilidades tecnológicas. Bajo este enfoque, la ciberseguridad no puede abordarse únicamente mediante esquemas reactivos, sino que requiere modelos preventivos capaces de adaptarse a entornos cambiantes y de anticipar patrones emergentes de amenaza. En la teoría del caos, al reconocer la naturaleza dinámica e incierta de los sistemas financieros, se justifica la necesidad de incorporar mecanismos de autoaprendizaje y de análisis predictivos basados en datos, que fortalecen la capacidad anticipativa del sistema financiero frente a riesgos digitales.

2.2.4. Teoría del Aprendizaje Automático

El aprendizaje automático (machine learning), subcampo de la inteligencia artificial, permite a las computadoras aprender sin programación explícita. Definido por Arthur Samuel en los años 50 como el estudio que otorga a las máquinas la capacidad de aprender por experiencia, utiliza enfoques supervisados, no supervisados y de refuerzo para procesar datos, identificar patrones o predecir resultados. Se aplica en tareas como la detección de fraudes y el procesamiento del lenguaje natural mediante modelos como redes neuronales(Brown, 2021).

Con respecto a la investigación, la creciente digitalización de los servicios bancarios y de los mercados de capitales ha generado volúmenes masivos de datos transaccionales cuya complejidad supera la capacidad de análisis de los métodos tradicionales. En este escenario, los

algoritmos de machine learning permiten identificar patrones anómalos, comportamientos atípicos y señales tempranas de posibles amenazas antes de que estas se materialicen en pérdidas económicas. Más allá de su capacidad predictiva, su relevancia radica en el carácter adaptativo y de autoaprendizaje de los sistemas, que pueden ajustarse continuamente a nuevas modalidades de fraude y de ataques digitales. De esta manera, el aprendizaje automático no solo actúa como herramienta tecnológica, sino también como fundamento conceptual de lo propuesto, al posibilitar una gestión anticipativa del riesgo basada en el análisis dinámico de datos, lo que fortalece la resiliencia del sistema financiero frente a amenazas emergentes.

Esta teoría es fundamental para esta investigación, ya que respalda la necesidad de integrar enfoques preventivos y analíticos en la ciberseguridad financiera, particularmente en Colombia, donde el crecimiento de la banca digital y los pagos electrónicos ha incrementado la exposición a fraudes y amenazas cibernéticas. La implementación de modelos transparentes de detección fortalece la gestión del riesgo al mejorar la capacidad institucional para anticipar eventos fraudulentos y reducir las pérdidas operativas.

2.2.5 Teoría de los Cinco V de Big Data

La Teoría de los Cinco V de Big Data describe las características clave de los big data: volumen (cantidad masiva de datos), velocidad (rapidez en generación y procesamiento), variedad (diversidad de tipos y fuentes de datos), valor (beneficios de insights accionables) y veracidad (precisión y credibilidad de los datos), guiando la gestión de datos para análisis predictivos y decisiones informadas en sectores como la banca, evolucionando de tres V iniciales para optimizar el procesamiento de datos estructurados y no estructurados (Robinson & Gillis, 2023).

Este aporta un sustento conceptual sobre por qué el Big Data es necesario para la estructuración de un modelo preventivo de ciberseguridad financiera. En este sentido, el Big Data no solo representa una infraestructura tecnológica, sino también el soporte estructural que permite aplicar técnicas de aprendizaje automático orientadas a la anticipación de riesgos. Así, el enfoque preventivo propuesto se fundamenta en la capacidad de integrar grandes volúmenes de datos confiables en tiempo real y de transformarlos en información estratégica para fortalecer la resiliencia y la seguridad del sistema financiero frente a amenazas cibernéticas emergente

2.2.6. Modelos Preventivos y Sistemas Adaptativos

Los modelos preventivos y los sistemas adaptativos representan un enfoque avanzado dentro de la seguridad financiera que combina aprendizaje automático y análisis en tiempo real para identificar comportamientos atípicos o anomalías antes de que se conviertan en eventos adversos. Según (Michael Rogers et al., 2025) estos modelos incorporan algoritmos que se ajustan dinámicamente a cambios en los datos y en el entorno del sistema, lo que permite que el proceso de detección evolucione conforme se actualizan los patrones de comportamiento. A diferencia de los enfoques estáticos, que dependen de reglas fijas o firmas históricas, los sistemas adaptativos utilizan técnicas de aprendizaje continuo y retroalimentación para mejorar su capacidad de predicción y responder eficazmente a nuevas tendencias de fraude u otros riesgos operacionales mediante la automatización del análisis de grandes volúmenes de información financiera.

Esta teoría es altamente relevante para esta investigación, ya que sustenta el fundamento conceptual de un modelo preventivo de ciberseguridad financiera que supera criterios reactivos al incorporar la capacidad de anticipar amenazas en tiempo real mediante sistemas adaptativos. En Colombia, donde la digitalización bancaria ha incrementado la complejidad de los datos transaccionales y la superficie de riesgo, los modelos adaptativos basados en el aprendizaje automático ofrecen una solución coherente para fortalecer la detección temprana de anomalías y fraudes. Estos modelos pueden ajustarse dinámicamente a comportamientos cambiantes sin intervención humana constante, lo cual resulta crucial para las instituciones financieras en entornos altamente volátiles.

2.3 Marco Conceptual

2.3.1. Big Data: Big Data se comprende como el manejo de conjuntos de datos extremadamente amplios, diversos y de alta velocidad que no pueden ser procesados eficazmente por las herramientas tradicionales de gestión de datos: Incluye datos estructurados, semiestructurados y no estructurados (Michael, s. f.), para la big data existen las 5V: Volumen, velocidad, variedad, veracidad y valor, donde el propósito central es extraer conocimiento accionables mediante técnicas como el análisis avanzando, el machine learning y la inteligencia artificial, convirtiendo los datos sin procesar en insumos para decisiones estratégicas(Badman & Kosinski, 2024).

2.3.2. Ciberseguridad: Puede definirse como el conjunto de prácticas, tecnologías y políticas orientadas a proteger la información, los sistemas y los dispositivos frente a amenazas digitales, ataques o accesos no autorizados. De acuerdo (Microsoft, s. f.) con "la ciberseguridad consiste en proteger los sistemas, las redes y los programas de ataques digitales", los cuales buscan "acceder, cambiar o destruir información confidencial, extorsionar a los usuarios o interrumpir los procesos normales del negocio". En esa misma línea, (Lindemulder & Kosinski, 2024) sostiene que la ciberseguridad "se centra en proteger los sistemas informáticos, las redes, los dispositivos y los datos frente a ataques, daños o accesos no autorizados", y que su objetivo es "prevenir los ciberataques o minimizar su impacto cuando se producen". Ambas perspectivas coinciden en que la ciberseguridad no solo implica la implementación de herramientas tecnológicas, sino también la creación de una estrategia integral de gestión del riesgo, que abarque personas, procesos y tecnología, para garantizar la confidencialidad, integridad y disponibilidad de la información en un entorno digital cada vez más complejo.

2.3.3. Malware Financiero: Se puede definir como una categoría de software malicioso específicamente diseñada para atacar activos, canales y usuarios del sector financiero con el fin de robar credenciales, interceptar transacciones o vaciar cuentas; en términos generales Microsoft señala que "El malware es un programa o archivo que está diseñado para dañar específicamente o interrumpir un sistema", y cuando ese propósito se orienta a obtener beneficio económico o acceso a información bancaria hablamos de malware financiero (Microsoft, 2026). IBM, que estudia y mitiga estas amenazas en entornos bancarios, describe esfuerzos para "detectar y prevenir infecciones de malware financiero y ataques de phishing", subrayando que sus técnicas incluyen troyanos bancarios, overlays remotos y otras variantes móviles que se ocultan o interceptan comunicaciones para evitar la detección (IBM, 2024).

2.3.4. El Machine Learning: una rama de la inteligencia artificial que se centra en el desarrollo de algoritmos y modelos que permiten a las computadoras aprender y tomar decisiones sin necesidad de ser programadas explícitamente para cada tarea. Según (M. Chen, 2024), el machine learning utiliza datos y algoritmos para imitar la forma en que los humanos aprenden, mejorando progresivamente su precisión a medida que procesa más información. Por su parte, (Daniel, 2021) destaca que este enfoque se basa en identificar patrones en los datos para realizar predicciones o tomar decisiones, utilizando técnicas estadísticas y computacionales.

2.3.5. El Deep Learning: es una subdisciplina del machine learning que emplea redes neuronales artificiales con múltiples capas para analizar datos complejos y extraer patrones de alto nivel. Según (Domínguez, 2023), el deep learning es el "corazón" de muchas aplicaciones de inteligencia artificial, ya que permite a los sistemas procesar grandes volúmenes de datos no estructurados, como imágenes o audio, imitando el funcionamiento del cerebro humano. Además (Bergmann, 2025) añade que estas redes neuronales profundas aprenden características directamente de los datos, eliminando la necesidad de preprocesamiento manual, y son especialmente efectivas en tareas como reconocimiento facial, traducción automática y conducción autónoma.

2.4. Marco Normativo

2.4.1. ley 1581 de 2012:

La Ley 1581 de 2012 establece el régimen general de protección de datos personales en Colombia y regula el tratamiento de la información que identifique o pueda identificar a personas naturales. Esta norma desarrolla el derecho fundamental al hábeas data y define principios rectores, como la legalidad, la finalidad, la libertad, la veracidad, la transparencia, el acceso y la seguridad, que deben observarse por todas las entidades que recolecten, almacenen o procesen datos personales. Asimismo, impone obligaciones a los responsables y encargados del tratamiento, exigiendo la adopción de medidas técnicas, humanas y administrativas que garanticen la protección de la información frente a accesos no autorizados, pérdida o uso indebido(Congreso de Colombia, 2012).

Esta ley es especialmente relevante para esta investigación, dado que los modelos preventivos basados en Big Data y en aprendizaje automático requieren procesar grandes volúmenes de datos financieros, muchos de ellos personales o sensibles. Por tanto, cualquier propuesta teórica para fortalecer la ciberseguridad financiera debe considerar no solo la eficacia tecnológica, sino también el cumplimiento de los principios de protección de datos establecidos en la normativa colombiana. La implementación de sistemas adaptativos y predictivos debe garantizar la confidencialidad, la trazabilidad y la seguridad de la información, protegiendo los derechos de los titulares y la responsabilidad institucional de las entidades financieras

2.4.2. Ley 1273 de 2009

La Ley 1273 de 2009 introdujo modificaciones al Código Penal colombiano con el propósito de tipificar y sancionar los delitos informáticos, reconociendo la información y los datos digitales como bienes jurídicamente protegidos. Esta norma establece conductas punibles como el acceso abusivo a sistemas informáticos, la interceptación ilícita de datos, el daño informático, la utilización de software malicioso, la suplantación de identidad y la transferencia no consentida de activos, entre otras. Con ello, el legislador colombiano respondió al incremento de los riesgos asociados al uso de las tecnologías de la información, fortaleciendo el marco legal para proteger la confidencialidad, la integridad y la disponibilidad de la información digital en el territorio nacional (Congreso de Colombia, 2009).

En el contexto del sector financiero colombiano, esta ley adquiere especial relevancia, ya que las entidades bancarias y de servicios financieros operan mediante plataformas tecnológicas altamente interconectadas, lo que incrementa su exposición a ataques cibernéticos. La tipificación de delitos como el acceso abusivo o la manipulación fraudulenta de datos justifica la necesidad de implementar mecanismos preventivos de ciberseguridad que permitan anticipar y mitigar riesgos antes de que se materialicen en conductas penalizadas. En consecuencia, el enfoque teórico del modelo preventivo de ciberseguridad financiera se alinea con el deber institucional de prevenir hechos que constituyen infracciones penales en el ordenamiento jurídico colombiano.

2.4.3 Gestión del Riesgo Operativo (SARO)

El sistema **SARO** en Colombia es una normativa establecida por la Superintendencia Financiera de Colombia, mediante la Circular Externa 048 de 2006 y sus modificaciones (049 de 2006, 041 de 2007 y 025 de 2020), que obliga a las entidades vigiladas a gestionar de forma estructurada y continua los riesgos operativos. Este sistema busca que las organizaciones identifiquen, midan, monitoreen y controlen los riesgos derivados de fallas en procesos internos, tecnología, recursos humanos o eventos externos, con el fin de mitigar pérdidas financieras y daños reputacionales, así como de asegurar la continuidad operativa y la eficiencia de sus operaciones. El SARO exige implementar políticas, procedimientos, controles internos y planes de contingencia para garantizar una gestión integral del riesgo y fortalecer la estabilidad del sistema financiero colombiano(Solutions, 2024).

Los lineamientos del SARO son fundamentales para justificar un enfoque preventivo en ciberseguridad financiera, ya que la normativa exige que las entidades consideren, en sus procesos de riesgo operativo, no solo eventos tradicionales, sino también aquellos derivados del uso de tecnología y sistemas de información. La incorporación de análisis predictivos basados en Big Data y en el aprendizaje automático en la gestión del riesgo responde directamente a esta obligación regulatoria de anticipar, controlar y monitorear las vulnerabilidades tecnológicas.

2.4.4. Lineamientos de Riesgo Tecnológico

Según (MinTic, 2025) los lineamientos de riesgo tecnológico establecen directrices para identificar, evaluar y mitigar amenazas que puedan afectar los activos de información y los sistemas tecnológicos, con el propósito de garantizar la continuidad operativa y fortalecer la confianza digital. Estos lineamientos contemplan la valoración y clasificación de activos físicos y digitales, la identificación de amenazas y vulnerabilidades, la implementación de controles de seguridad y la aplicación de estrategias de tratamiento del riesgo como aceptar, transferir, evitar o reducir impactos. Asimismo, promueven el cumplimiento del ciclo PHVA (Planear, Hacer, Verificar y Actuar), el monitoreo continuo de la infraestructura tecnológica y el establecimiento de planes de contingencia. En Colombia, estas directrices se articulan con la política de Gobierno Digital del Ministerio de Tecnologías de la Información y las Comunicaciones, orientadas a proteger la información institucional, la infraestructura crítica y los datos de los ciudadanos, tanto en entidades públicas como en privadas.

Desde la investigación, los lineamientos sobre riesgo tecnológico reafirman la importancia de desarrollar un enfoque preventivo en ciberseguridad financiera, ya que los riesgos derivados de la tecnología no pueden gestionarse únicamente de forma reactiva. La inclusión de mecanismos de análisis predictivo, como los basados en Big Data y en el aprendizaje automático, permite avanzar hacia una gestión anticipativa alineada con la regulación vigente, al facilitar la identificación temprana de vulnerabilidades y patrones anómalos.

3. Metodología

Esta investigación adopta un enfoque cualitativo teórico-conceptual, orientado a analizar los fundamentos académicos y normativos que sustentan un modelo preventivo de ciberseguridad financiera, sin incluir la implementación empírica ni el desarrollo tecnológico. Este enfoque permite interpretar y sistematizar los aportes de la literatura científica reciente, la normativa colombiana y los documentos técnicos especializados, con el fin de estructurar una propuesta conceptual aplicable al contexto colombiano.

El estudio es descriptivo y analítico, orientado a caracterizar el panorama actual de las amenazas cibernéticas en el sistema financiero y a examinar los fundamentos teóricos del Big Data, del aprendizaje automático y de los modelos adaptativos en la gestión del riesgo. Posee un diseño documental basado exclusivamente en la revisión y el análisis de fuentes secundarias académicas y normativas publicadas entre 2022 y 2025, priorizando la actualidad y la pertinencia (Ver Anexo1).

3.1. Técnicas de Recolección de Información

La técnica principal utilizada es la revisión documental sistematizada, mediante la cual se recopilaron y seleccionaron artículos científicos indexados en bases de datos como Scopus y ScienceDirect, así como documentos oficiales del marco normativo colombiano (Ley 1273 de 2009, Ley 1581 de 2012, lineamientos de riesgo tecnológico y SARO).

- Para garantizar rigor académico, se aplicaron criterios de inclusión como:
- Publicaciones de no más de cinco años.
- Estudios relacionados con la ciberseguridad financiera, Big Data, aprendizaje automático y modelos predictivos.
- Artículos con enfoque en el sector financiero o en la gestión del riesgo tecnológico.

La información recopilada se organizó en matrices de análisis documental, lo que permitió clasificar los aportes en categorías temáticas previamente definidas.

3.2. Técnicas de Análisis de la Información

El análisis se realizó mediante análisis de contenido cualitativo, el cual permitió identificar conceptos clave, enfoques teóricos recurrentes y tendencias investigativas relacionadas con la ciberseguridad financiera preventiva.

Se empleó una estrategia de categorización temática, organizando la información en ejes como:

- Amenazas y vulnerabilidades en el sistema financiero.
- Modelos predictivos basados en inteligencia artificial.
- Sistemas adaptativos y aprendizaje automático.
- Marco normativo colombiano en materia de datos y delitos informáticos.

Se aplicó un análisis deductivo–integrador, articulando los hallazgos teóricos con el contexto colombiano, con el fin de estructurar una propuesta conceptual coherente y fundamentada. Este proceso permitió relacionar las teorías del aprendizaje automático, Big Data, modelos adaptativos y teoría del caos con la necesidad de un enfoque preventivo en la gestión del riesgo financiero digital.

3.3. Justificación del Diseño Metodológico

El diseño metodológico es coherente con el objetivo general y se centra en analizar los fundamentos teóricos, sin desarrollar un modelo aplicado ni experimental. El énfasis está en la construcción conceptual, la sistematización académica y la integración de enfoques interdisciplinarios que sirvan de base para futuras investigaciones empíricas o desarrollos tecnológicos en el sector financiero colombiano.

4. Desarrollo y resultados.

Describir el panorama actual de las amenazas cibernéticas en el sistema financiero permitió evidenciar que el avance de la digitalización ha incrementado significativamente la exposición a riesgos informáticos, debido al uso intensivo de plataformas electrónicas, sistemas interconectados y servicios financieros en línea. La expansión de la banca digital y de los medios de pago electrónicos ha generado nuevas vulnerabilidades que son aprovechadas por los ciberdelincuentes para acceder a información confidencial, alterar transacciones y afectar la estabilidad de los mercados digitales. Esta situación ha convertido al sector financiero en uno de los principales objetivos de los ataques cibernéticos, debido al alto valor económico de los datos que administra y a la necesidad de mantener la continuidad de sus operaciones.

En los estudios revisados se observa que las amenazas más frecuentes en el entorno financiero son el malware, el phishing, el ransomware y el fraude en transacciones electrónicas, los cuales impactan tanto a las entidades como a los usuarios. (Shehab et al., 2024) señalan que el malware financiero se utiliza para interceptar credenciales y manipular operaciones bancarias, generando pérdidas económicas y afectando la confianza en los servicios digitales. De igual manera, (Jáñez-Martino et al., 2025) explican que los ataques de phishing han evolucionado mediante el uso de automatización y procesamiento de lenguaje natural, lo que permite crear mensajes más convincentes y dificulta su detección por parte de los sistemas tradicionales. Estos resultados muestran que las amenazas actuales presentan un alto grado de adaptación, lo que incrementa la complejidad del entorno digital financiero.

A medida que se profundiza en el análisis del problema, se hace necesario examinar los fundamentos teóricos que permiten comprender cómo las nuevas tecnologías pueden contribuir a la prevención del fraude. La revisión de literatura demuestra que los modelos tradicionales de seguridad presentan limitaciones frente a amenazas dinámicas, debido a que se basan en reglas previamente definidas y en la identificación de patrones conocidos.(Akhtar & Feng, 2022b)explican que los sistemas basados en firmas solo pueden reconocer ataques previamente registrados, lo que reduce su efectividad frente a fraudes novedosos o malware que modifica constantemente su estructura para evitar ser detectado. Esta situación ha impulsado el desarrollo de enfoques más avanzados orientados a anticipar los riesgos mediante el análisis de grandes volúmenes de información.

En este contexto, el aprendizaje automático se presenta como una herramienta fundamental para mejorar la detección de fraudes financieros, debido a su capacidad para analizar datos en tiempo real e identificar comportamientos anómalos. (Alrafi & Mishra, 2024) demuestran que los modelos basados en redes neuronales permiten detectar transacciones sospechosas con altos niveles de precisión, fortaleciendo los sistemas de seguridad y reduciendo la probabilidad de pérdidas económicas. De manera similar, (Y. Chen et al., 2025) señalan que los algoritmos de clasificación permiten diferenciar operaciones legítimas de posibles fraudes mediante el análisis de patrones de comportamiento, lo que mejora la capacidad de respuesta de las instituciones financieras.

De forma complementaria, el Big Data se reconoce como un soporte esencial para la prevención del fraude, ya que permite procesar grandes cantidades de información provenientes de múltiples fuentes. (Robinson & Gillis, 2023) explican que las características de volumen, velocidad, variedad, veracidad y valor permiten transformar los datos en información útil para la toma de decisiones, facilitando la detección temprana de amenazas. Gracias a estas capacidades, las entidades financieras pueden anticipar riesgos y aplicar modelos predictivos que fortalecen la seguridad en los mercados digitales.

A partir de estos fundamentos, resulta necesario identificar los componentes que hacen posible la integración de herramientas predictivas dentro de la ciberseguridad financiera. El análisis documental permitió determinar que la prevención del fraude requiere la combinación de elementos tecnológicos, normativos y organizacionales que permitan responder de manera oportuna a los riesgos del entorno digital. Entre los componentes más relevantes se encuentran los sistemas adaptativos, los modelos de análisis de datos, el cumplimiento regulatorio y la gestión institucional del riesgo.

Los estudios revisados indican que los sistemas adaptativos constituyen uno de los principales elementos para mejorar la seguridad, ya que permiten ajustar los parámetros de detección según el comportamiento de los datos. (Michael Rogers et al., 2025) señalan que estos modelos utilizan aprendizaje continuo, lo que les permite reconocer nuevas formas de ataque y responder con mayor rapidez frente a amenazas desconocidas, fortaleciendo la estabilidad del sistema financiero.

De igual manera, la revisión normativa evidencia que la regulación vigente exige a las entidades financieras implementar mecanismos orientados a la protección de la información y al control del riesgo tecnológico. La (Congreso de Colombia, 2012) establece la obligación de garantizar la seguridad de los datos personales, mientras que el sistema de administración del riesgo operativo exige identificar, medir y controlar los riesgos derivados del uso de tecnología. Estas disposiciones muestran que la prevención no solo responde a una necesidad técnica, sino también a un requerimiento legal orientado a asegurar la estabilidad del sistema financiero.

Finalmente, también se identificó que el factor humano constituye un componente esencial en la efectividad de los modelos preventivos, debido a que la correcta aplicación de los procedimientos depende de la formación y la experiencia del personal encargado de la seguridad. (Usman et al., 2024) destacan que la capacitación permanente y el conocimiento especializado permiten reducir errores y mejorar la respuesta ante incidentes, lo que demuestra que la ciberseguridad financiera debe abordarse desde un enfoque integral que incluya tecnología, normativa y gestión organizacional.

La estructura del modelo se divide en cuatro pasos:

1. Regulación y gobernanza:

En este paso se busca ajustar el modelo al contexto colombiano, teniendo en cuenta leyes importantes como la protección de datos (Ley 1581), la seguridad de la información recolectada y la gestión del riesgo operativo. Además, se considera el cumplimiento del marco normativo del sistema financiero en Colombia, con el fin de construir un modelo más realista y aplicable al país.

2. Big Data (Datos):

Se recolectan datos y se organiza la información a través de las transacciones financieras y los datos de los usuarios, incluyendo información básica como la identificación y la edad. También se consideran los logs del sistema, es decir, el historial técnico, los intentos de inicio de sesión, errores del sistema, direcciones IP sospechosas y accesos inusuales. Gracias a esta información se obtiene el comportamiento digital del usuario. Asimismo, los datos externos, como redes y ubicación, permiten generar una base de datos masiva y en tiempo real.

3. Machine Learning (Aprendizaje automático):

En esta etapa se busca detectar y predecir amenazas mediante la transformación de los datos recolectados utilizando algoritmos de detección de fraude, identificación de patrones

anómalos, modelos predictivos y clasificación de riesgos. De esta manera, se pretende anticipar los ataques antes de que ocurran.

4. Respuesta inteligente:

En este paso se propone actuar de forma automática mediante el bloqueo de transacciones sospechosas, el envío de alertas en tiempo real, el ajuste dinámico de reglas y el aprendizaje continuo. De esta forma, la capa adaptativa no solo responde ante incidentes, sino que fortalece progresivamente la capacidad preventiva del sistema.

5. Conclusiones y Recomendaciones

El desarrollo de la investigación permitió establecer que los fundamentos teóricos analizados proporcionan un sustento conceptual suficiente para estructurar un modelo preventivo en la ciberseguridad financiera. A partir de la revisión documental, se evidenció que la complejidad del entorno digital financiero exige enfoques que no se limiten a reaccionar ante los ataques, sino que permitan anticipar comportamientos de riesgo mediante el análisis continuo de la información y la adaptación del sistema frente a nuevas amenazas.

De acuerdo con los hallazgos, las teorías relacionadas con el Big Data, el aprendizaje automático y los sistemas adaptativos explican de manera coherente cómo es posible fortalecer la seguridad financiera a través de la capacidad de procesar datos en tiempo real, reconocer patrones irregulares y generar respuestas automatizadas. Esto demuestra que el sustento teórico no solo describe el problema de la ciberseguridad, sino que también orienta la construcción de modelos preventivos capaces de ajustarse a entornos digitales cambiantes.

De igual manera, el análisis realizado permitió comprobar que la prevención en la ciberseguridad financiera debe entenderse como un proceso integral en el que intervienen factores tecnológicos, normativos y organizacionales. La evidencia encontrada muestra que el cumplimiento del marco legal, la gestión del riesgo operativo y la capacitación del personal son elementos que complementan el uso de herramientas predictivas, lo que confirma que la seguridad no depende exclusivamente de la tecnología, sino de la articulación de múltiples componentes dentro de la organización.

En relación con la pregunta de investigación, se concluye que los fundamentos teóricos sí sustentan la formulación de un modelo preventivo en la ciberseguridad financiera, debido a que explican la necesidad de utilizar sistemas capaces de aprender, adaptarse y anticipar amenazas en contextos de alta digitalización. La integración conceptual de estos enfoques permite proponer una estructura lógica para la prevención del riesgo, alineada con las exigencias actuales del sistema financiero colombiano.

Finalmente, la investigación aporta una base teórica organizada que puede servir como referencia para futuros estudios orientados al diseño aplicado de modelos de ciberseguridad preventiva. En este sentido, se considera pertinente que nuevas investigaciones desarrollen pruebas empíricas o implementaciones tecnológicas que permitan validar el funcionamiento de estos modelos en escenarios reales, con el fin de fortalecer la protección de la información y la confianza en los servicios financieros digitales.

6. Referencias

Akhtar, M. S., & Feng, T. (2022a). Detection of Malware by Deep Learning as CNN-LSTM Machine Learning Techniques in Real Time. *Symmetry*, *14*(11). Scopus. https://doi.org/10.3390/sym14112308

Akhtar, M. S., & Feng, T. (2022b). Detection of Malware by Deep Learning as CNN-LSTM Machine Learning Techniques in Real Time. *Symmetry*, *14*(11). Scopus. https://doi.org/10.3390/sym14112308

Alrafi, H. S., & Mishra, S. (2024). The impact of AI-based cyber security on the banking and financial sectors. *Journal of Cybersecurity and Information Management*, *14*(1), 8-19. https://doi.org/10.54216/JCIM.140101

Aslan, Ö., Aktuğ, S. S., Ozkan-Okay, M., Yilmaz, A. A., & Akin, E. (2023). A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions. *Electronics (Switzerland)*, *12*(6). Scopus. https://doi.org/10.3390/electronics12061333

Badman, A., & Kosinski, M. (2024, noviembre 18). *¿Qué es el big data? | IBM*. https://www.ibm.com/es-es/think/topics/big-data

Bergmann, D. (2025, septiembre 15). *What Is Deep Learning? | IBM*. https://www.ibm.com/think/topics/deep-learning

Brown, S. (2021, abril 21). *Machine learning, explained | MIT Sloan*. https://mitsloan.mit.edu/ideas-made-to-matter/machine-learning-explained

Chandra, N. A., Ramli, K., Ratna, A. A. P., & Gunawan, T. S. (2022). Information Security Risk Assessment Using Situational Awareness Frameworks and Application Tools. *Risks*, *10*(8). https://doi.org/10.3390/risks10080165

Chen, M. (2024, noviembre 25). *Desmitificando el aprendizaje automático: Una guía completa*. https://www.oracle.com/latam/artificial-intelligence/machine-learning/what-is-machine-learning/

Chen, Y., Zhao, C., Xu, Y., Nie, C., & Zhang, Y. (2025). Deep Learning in Financial Fraud Detection: Innovations, Challenges, and Applications. *Data Science and Management*. https://doi.org/10.1016/j.dsm.2025.08.002

Congreso de Colombia. (2009). *Ley 1273 de 2009—Gestor Normativo*. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34492

Congreso de Colombia. (2012). *Ley 1581 de 2012—Gestor Normativo*. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

Daniel. (2021, diciembre 13). Machine Learning: Definición, funcionamiento, usos. *DataScientest*. https://datascientest.com/es/machine-learning-definicion-funcionamiento-usos

Domínguez, S. (2023). *Deep Learning: El corazón de la inteligencia artificial | OpenWebinars*. OpenWebinars.net. https://openwebinars.net/blog/deep-learning-el-corazon-de-la-inteligencia-artificial/

Forbes, S. (2025, octubre 20). *Colombia registró 98 millones de ataques cibernéticos al día en 2024*. https://forbes.co/2025/10/20/tecnologia/colombia-registro-98-millones-de-ataques-ciberneticos-al-dia-en-2024

Gupta, S. (2025). Hacking the System: A Deep Dive into the World of E-Banking Crime. En G. Kaur, T. Choudhury, & S. Balamurugan (Eds.), *The Techno-Legal Dynamics of Cyber Crimes in Industry 5.0* (pp. 121-148). wiley. https://doi.org/10.1002/9781394242177.ch7

Hossain, M. I. (2025). *Exploring the Impact of Social Media on Cyber security Threats and Mitigation Strategies*. 1-21.

IBM. (2024, mayo 16). *IBM Trusteer Rapport | Malware and Phishing Attacks*. https://www.ibm.com/products/trusteer-rapport

Islam, M., Tamanna, A. K., & Islam, S. (2024). The path to cashless transaction: A study of user intention and attitudes towards quick response mobile payments. *Heliyon*, *10*(15), e35302. https://doi.org/10.1016/j.heliyon.2024.e35302

Jáñez-Martino, F., Alaiz-Rodríguez, R., González-Castro, V., Fidalgo, E., & Alegre, E. (2025). Spam email classification based on cybersecurity potential risk using natural language processing. *Knowledge-Based Systems*, *310*. https://doi.org/10.1016/j.knosys.2024.112939

Klioutchnikov, I., Sigova, M., & Beizerov, N. (2017). Chaos Theory in Finance. *Procedia Computer Science*, *119*, 368-375. https://doi.org/https://doi.org/10.1016/j.procs.2017.11.196

Krishna, B., Krishnan, S., & Sebastian, M. P. (2023). Examining the Relationship between National Cybersecurity Commitment, Culture, and Digital Payment Usage: An Institutional Trust Theory Perspective. *Information Systems Frontiers*, *25*(5), 1713-1741. https://doi.org/10.1007/s10796-022-10280-7

Kuzior, A., Brożek, P., Kuzmenko, O., Yarovenko, H., & Vasilyeva, T. (2022). Countering Cybercrime Risks in Financial Institutions: Forecasting Information Trends. *Journal of Risk and Financial Management*, *15*(12). https://doi.org/10.3390/jrfm15120613

Li, W., Liu, X., Su, J., & Cui, T. (2025). Advancing financial risk management: A transparent framework for effective fraud detection. *Finance Research Letters*, *75*, 106865. https://doi.org/10.1016/j.frl.2025.106865

Lindemulder, G., & Kosinski, M. (2024, agosto 12). *¿Qué es la ciberseguridad? | IBM*. https://www.ibm.com/es-es/think/topics/cybersecurity

Ma, C., Wu, J., Sun, H., Zhou, X., & Sun, X. (2023). Enhancing user experience in digital payments: A hybrid approach using SEM and neural networks. *Finance Research Letters*, *58*, 104376. https://doi.org/10.1016/j.frl.2023.104376

Michael, C. (s. f.). *Big Data, grandes posibilidades: Cómo extraer el máximo valor*. Recuperado 13 de octubre de 2025, de https://www.oracle.com/latam/big-data/what-is-big-data/

Michael Rogers, Ahmad Ahmady, Setayesh Khasehtarash, & Annachiara Ronca. (2025, octubre 7). *Adaptive machine learning models for anomaly detection in real-time financial control | Request PDF*. ResearchGate. https://www.researchgate.net/publication/395802052_Adaptive_machine_learning_models_for_anomaly_detection_in_real-time_financial_control

Microsoft. (s. f.). *¿Qué es la ciberseguridad? - Soporte técnico de Microsoft*. Recuperado 13 de octubre de 2025, de https://support.microsoft.com/es-es/topic/-qu%C3%A9-es-la-ciberseguridad-8b6efd59-41ff-4743-87c8-0850a352a390

Microsoft. (2026). *Protéjase del malware y la suplantación de identidad (phishing)—Soporte técnico de Microsoft*. https://support.microsoft.com/es-es/topic/prot%C3%A9jase-del-malware-y-la-suplantaci%C3%B3n-de-identidad-phishing-c1c0c2cf-7e80-4805-8b7e-81aa48610b44

MinTic. (2025, abril 21). *Lineamientos del Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Públicas*. https://gobiernodigital.mintic.gov.co/692/articles-401774_recurso_1.pdf

Mohamed, N. (2025). Artificial intelligence and machine learning in cybersecurity: A deep dive into state-of-the-art techniques and future paradigms. *Knowledge and Information Systems*, *67*(8), 6969-7055. Scopus. https://doi.org/10.1007/s10115-025-02429-y

Pinheiro Santana, M., Cezar Amate, F., & Dos Santos, C. E. (2025). Preventing social engineering attacks: A case study of a financial scam in Brazil. *International Journal of Circuit, Computing and Networking*, *6*, 1-6. https://doi.org/10.33545/27075923.2025.v6.i2a.93

Robinson, S., & Gillis, A. S. (2023, noviembre 17). *What are the 5 V's of Big Data? | Definition TechTarget*. Search Data Management. https://www.techtarget.com/searchdatamanagement/definition/5-Vs-of-big-data

Shehab, R., S.alismail, A., Almaiah, M. A., Alkhdour, T., Alwadi, B. M., & Alrawad, M. (2024). Assessment of Cybersecurity Risks and threats on Banking and Financial Services. *Journal of Internet Services and Information Security*, *14*(3), 167-190. https://doi.org/10.58346/JISIS.2024.I3.010

Solutions, G. (2024, octubre 3). Norma SARO | Sistema de Administración del Riesgo Operativo en Colombia. *GlobalSuite Solutions*. https://www.globalsuitesolutions.com/es/norma-saro-sistema-administracion-riesgo-operativo-colombia/

Tamilmani, K., Rana, N. P., Wamba, S. F., & Dwivedi, R. (2021). The extended Unified Theory of Acceptance and Use of Technology (UTAUT2): A systematic literature review and theory evaluation. *International Journal of Information Management*, *57*, 102269. https://doi.org/10.1016/j.ijinfomgt.2020.102269

Usman, A., Che-Ahmad, A., & Abdulmalik, S. O. (2024). THE ROLE OF INTERNAL AUDITORS CHARACTERISTICS IN CYBERSECURITY RISK ASSESSMENT IN

FINANCIAL-BASED BUSINESS ORGANISATIONS: A CONCEPTUAL REVIEW. *Revista de Gestao Social e Ambiental*, *18*(6). https://doi.org/10.24857/rgsa.v18n6-008

Vega, J. P. (2025, noviembre 8). *En Colombia se registran 94 ciberataques al sistema financiero por segundo; a julio crecieron 69 %*. https://www.valoraanalitik.com/colombia-ciberataques-sistema-financiero/

7. Anexos

Anexo 1. Matriz de Análisis documental

Tabla 1

Fase metodológica	**Paso**	**Descripción del procedimiento**	**Herramientas / criterios**	**Resultado esperado**
1. Definición del enfoque	Enfoque cualitativo documental	La investigación se desarrolló bajo un enfoque cualitativo de tipo teórico-conceptual, orientado al análisis de literatura científica, normativa colombiana y documentos técnicos relacionados con la ciberseguridad financiera.	Diseño documental, análisis teórico	Base conceptual para el modelo preventivo
2. Revisión sistemática de literatura	Planeación de la búsqueda	Se realizó una revisión sistemática de literatura con el fin de identificar investigaciones recientes sobre ciberseguridad financiera, Big Data, machine learning y gestión del riesgo tecnológico.	Método de revisión sistemática	Selección organizada de fuentes
3. Construcción	Definición de palabras clave	Se construyeron fórmulas de búsqueda	Operadores booleanos	Resultados más precisos

de fórmulas de búsqueda		combinando términos en inglés y español como: cybersecurity, financial cybersecurity, machine learning, big data, fraud detection, financial risk, cyber risk, banking security.	(AND, OR, NOT)	en bases de datos
4. Selección de bases de datos	Búsqueda en bases indexadas	La búsqueda se realizó en bases de datos académicas reconocidas para garantizar rigor científico	Scopus, ScienceDirect	Artículos científicos indexados
5. Criterio de idioma	Filtrado por idioma	Se priorizaron artículos en idioma inglés debido a que la mayor producción científica sobre ciberseguridad y machine learning se encuentra en este idioma.	Inglés principalmente	Mayor calidad académica
6. Ventana de tiempo	Criterio temporal	Se estableció una ventana de publicación de cinco años para asegurar actualidad teórica.	2020 – 2025	Literatura actualizada
7. Excepción normativa	Inclusión de leyes fuera del rango	Se incluyeron normas colombianas sin límite	Ley 1273 de 2009, Ley 1581	Marco normativo completo

		de fecha debido a su vigencia jurídica.	de 2012, SARO, MinTIC	
8. Criterios de exclusión	Eliminación de artículos no pertinentes	Se excluyeron documentos que no estuvieran relacionados con el sector financiero, ciberseguridad, Big Data o modelos predictivos.	Revisión de resumen y palabras clave	Depuración de resultados
9. Criterio de validez científica	Selección de artículos citados	Se priorizaron artículos que hubieran sido citados en otras investigaciones académicas, con el fin de garantizar mayor validez, relevancia científica y reconocimiento dentro de la comunidad investigativa	Número de citas, indexación, relevancia	Mayor confiabilidad teórica
10. Selección final de documentos	Validación de pertinencia	Se seleccionaron únicamente artículos que aportaran fundamentos teóricos, modelos conceptuales o evidencia sobre ciberseguridad financiera preventiva.	Lectura completa	Base teórica sólida

12. Análisis de contenido	Interpretación cualitativa	Se realizó análisis de contenido cualitativo para identificar categorías como amenazas, modelos predictivos, Big Data, aprendizaje automático y normativa.	Categorización temática	Identificación de patrones teóricos
13. Integración teórica	Relación entre conceptos	Se integraron los hallazgos para estructurar un enfoque teórico de modelo preventivo en ciberseguridad financiera aplicable al contexto colombiano.	Análisis deductivo	Construcción del modelo conceptual
14. Validación conceptual	Coherencia con objetivos	Se verificó que los resultados teóricos respondieran al objetivo general y a los objetivos específicos de la investigación.	Revisión metodológica	Consistencia del estudio

Anexo 2. Cronograma

Actividad	Mes 2	Mes 4	Mes 6	Mes 8	Mes 10	Mes 12	Mes 14
Revisión inicial de literatura sobre ciberseguridad financiera	X						
Recolección de artículos científicos y normativa	X	X					
Análisis del panorama de amenazas cibernéticas en el sistema financiero (Objetivo específico 1)	X	X					
Análisis teórico del Big Data y aprendizaje automático (Objetivo específico 2)		X					
Identificación de componentes tecnológicos y organizacionales del modelo (Objetivo específico 3)		X					
Elaboración del marco teórico y conceptual		X	X	X			
Desarrollo de metodología y análisis documental		X	X	X			
Elaboración del documento final de investigación			X	X	X		
Revisión del director y correcciones				X	X		
Entrega del anteproyecto corregido					X		
Revisión por jurados						X	
Ajustes finales y entrega definitiva						X	X

Anexo 2. Presupuesto

Tipo de recurso	Recurso	Descripción	Justificación	Valor estimado (COP)
Humano	Investigadores (estudiantes)	Estudiantes responsables de la búsqueda de información, análisis de literatura y elaboración del documento de investigación.	Son quienes desarrollan el proyecto y realizan el análisis.	No Aplica
Humano	Director de tesis	Docente encargado de orientar el proceso metodológico y académico de la investigación.	Garantiza la coherencia metodológica, la calidad académica y el cumplimiento de los objetivos del estudio.	No aplica
Tecnológico	Computador personal	Equipo utilizado para la búsqueda de información, redacción del documento y organización de la información.	Permite acceder a bases de datos académicas y desarrollar el documento final de la investigación.	$0 (recurso propio)
Tecnológico	Software de ofimática	Programas como Word y Excel utilizados para redactar el documento y organizar la información	Facilita la elaboración del documento, tablas, matrices de análisis	$0 (licencia institucional o personal)

			y presentación del proyecto.	
Tecnológico	Acceso a internet	Conexión utilizada para consultar artículos científicos, libros y normativa relacionada con la investigación.	Permite el acceso a bases de datos académicas y fuentes bibliográficas necesarias para el desarrollo del estudio.	$120.000
Financiero	Papelería	Hojas, carpetas y materiales para organizar la información del proyecto.	Facilita la organización y revisión del material de investigación.	$40.000
Financiero	Transporte	Desplazamientos para reuniones con el director o actividades relacionadas con la investigación.	Permite asistir a asesorías académicas o trámites institucionales relacionados con el proyecto	$100.000