Trabajo de Grado
Opción Seminario Diplomado

Aplicación de big data para la detección y prevención de ciber amenazas en el sector bancario colombiano

Corporación Universitaria Remington
Facultad de Ingeniería
Ingeniería de Sistemas

Juan Esteban Rodríguez Murillo

Tutor:
Juan Pablo Vélez Uribe

Opción de Trabajo de Grado Seminario
Colombia
2025

Tabla de Contenido

1. **Dedicatoria 4**
2. **Agradecimientos 5**
3. **Resumen 6**
4. **Palabras clave 7**
5. **Marco Conceptual 7**
    - **5.1. Big Data: definición y características 7**
    - **5.2. Ciberseguridad: concepto y alcance 8**
    - **5.3. Intersección entre Big Data y Ciberseguridad 9**
    - **5.4. Big Data y normatividad en Colombia 9**
    - **5.5. Relevancia del uso de Big Data en la ciberseguridad bancaria 10**
6. **Marco Contextual 10**
    - **6.1. Panorama digital y transformación del sector bancario en Colombia 10**
    - **6.2. Amenazas cibernéticas y desafíos de seguridad en la banca colombiana …. 11**
    - **6.3. Regulación, normatividad y marco institucional 11**
    - **6.4. Integración de Big Data en estrategias de ciberseguridad 12**
    - **6.5. Pertinencia del estudio en el contexto actual 12**
7. **Objetivo General 13**
8. **Objetivos Específicos 13**
9. **Desarrollo e Implementación del Aprendizaje 14**
    - **9.1. Contexto de aplicación 14**
    - **9.2. Herramientas y tecnologías propuestas 14**
    - **9.3. Tipos de ciberataques más frecuentes en el sector bancario 15**

9.4. Metodología propuesta 16

9.5. Resultados esperados 17

9.6. Beneficios esperados 20

9.7. Limitaciones potenciales y retos 20

10. Conclusiones 21

11. Recomendaciones Finales 23

12. Referencias 25

1. Dedicatoria

A mis padres, por su amor incondicional, su dedicación constante y por transmitirme, a través de su ejemplo, los valores de la honestidad, la perseverancia y el esfuerzo. Su apoyo ha sido un pilar fundamental en mi formación académica y personal.

A mis familiares, por su acompañamiento, por las palabras de aliento en los momentos difíciles y por compartir conmigo la satisfacción de cada avance alcanzado. Su respaldo, aun en la distancia, ha sido un estímulo invaluable para continuar.

A mi gata, cuya presencia silenciosa y compañía constante han sido un alivio en las extensas jornadas de estudio, recordándome la importancia de las pausas y brindándome tranquilidad en medio de las exigencias académicas.

Este logro representa el esfuerzo conjunto de todos ustedes, pues sin su amor, compañía y apoyo inquebrantable, este objetivo no habría sido posible.

2. Agradecimientos

A mis padres, por su apoyo, guía y confianza absoluta a lo largo de este proceso, inculcándome la disciplina y la determinación necesarias para alcanzar mis metas.

A mis familiares, por su constante motivación, por impulsarme a perseverar y por celebrar cada logro como propio.

A la **Corporación Universitaria Remington**, por proporcionarme los recursos académicos, las oportunidades de aprendizaje y el entorno formativo que contribuyeron de manera significativa a mi desarrollo profesional y a la realización de este trabajo de grado.

Al tutor de grado, **Juan Pablo Uribe**, por su acompañamiento, dedicación y compromiso en la orientación de este proyecto, cuyas observaciones y recomendaciones fueron decisivas para la calidad y solidez de los resultados presentados.

3. Resumen

El sector bancario colombiano ha experimentado en la última década una transformación significativa debido a la digitalización de sus servicios, el uso masivo de canales electrónicos y la creciente adopción de herramientas tecnológicas por parte de los clientes. Este avance ha generado un volumen exponencial de datos, tanto transaccionales como comportamentales, que pueden ser aprovechados mediante técnicas de Big Data para mejorar la eficiencia operativa, la toma de decisiones y, de manera especial, la ciberseguridad.

En paralelo, la banca se ha convertido en uno de los sectores más atacados por la ciberdelincuencia en Colombia, enfrentando amenazas como el fraude electrónico, phishing, malware, robo de credenciales y ataques a la infraestructura tecnológica. Estas amenazas no solo provocan pérdidas económicas considerables, sino que también afectan la confianza de los clientes y la reputación de las entidades.

El presente trabajo tiene como objetivo analizar cómo la implementación de herramientas y metodologías de Big Data puede contribuir a la detección temprana y prevención de ciberataques en el sector bancario colombiano. Se revisan conceptos clave de Big Data, sus componentes tecnológicos (almacenamiento masivo, procesamiento distribuido, analítica avanzada, machine learning) y su integración con sistemas de seguridad informática. Asimismo, se examinan casos de éxito internacionales y nacionales que evidencian la efectividad de estas soluciones.

La metodología utilizada se basa en una revisión bibliográfica y documental de informes emitidos por organismos como Asobancaria, MinTIC, CSIRT Financiero y empresas de ciberseguridad, así como en el análisis de tendencias y herramientas aplicadas en el contexto colombiano.

Como resultado, se identifica que el uso de Big Data permite el monitoreo en tiempo real de grandes volúmenes de transacciones, el reconocimiento de patrones anómalos y la predicción de comportamientos fraudulentos antes de que generen pérdidas significativas. Además, se plantea un modelo conceptual que integra análisis predictivo, inteligencia artificial y automatización de alertas para fortalecer la protección de las entidades bancarias.

Finalmente, se concluye que la combinación de Big Data y ciberseguridad representa una estrategia esencial para el presente y futuro de la banca en Colombia, siempre que vaya acompañada de inversión en infraestructura tecnológica, capacitación del personal y cumplimiento de las normativas de protección de datos vigentes.

4. Palabras clave

Big Data, Ciberseguridad, Sector Bancario, Colombia, Análisis Predictivo, Fraude Financiero.

5. Marco Conceptual

5.1. Big Data: definición y características

El concepto de *Big Data* hace referencia al tratamiento y análisis de grandes volúmenes de datos que, por su complejidad, no pueden ser gestionados eficazmente con herramientas tradicionales. De acuerdo con Mayer-Schönberger y Cukier (2013), *Big Data* no se limita únicamente a la cantidad de datos, sino también a su diversidad, velocidad y capacidad de generar valor a partir de su análisis. Las conocidas “5V” volumen, velocidad, variedad, veracidad y valor representan los pilares de este paradigma tecnológico. En el sector bancario, esta tecnología permite procesar información transaccional en tiempo real, detectar patrones de fraude y comprender mejor el comportamiento del cliente. La correcta implementación de *Big*

Data no solo mejora la toma de decisiones estratégicas, sino que también proporciona una ventaja competitiva en mercados altamente digitalizados.

Tabla 1. Las 5V del Big Data

Dimensión	Descripción
Volumen	Grandes cantidades de datos generados por múltiples fuentes.
Velocidad	Rapidez con la que se crean, procesan y analizan los datos.
Variedad	Diversidad de formatos: estructurados, semiestructurados y no estructurados.
Veracidad	Grado de fiabilidad y precisión de los datos.
Valor	Potencial de los datos para generar beneficios y ventajas competitivas.
Fuente: Adaptado de Mayer-Schönberger y Cukier (2013).	

5.2. Ciberseguridad: concepto y alcance

La ciberseguridad engloba las prácticas, políticas y herramientas diseñadas para proteger redes, sistemas y datos frente a amenazas digitales. Según el Instituto Nacional de Estándares y Tecnología de Estados Unidos (NIST, 2018), su objetivo es garantizar la confidencialidad, integridad y disponibilidad de la información. En el sector bancario, estas funciones son críticas debido a la naturaleza sensible de los datos que gestionan las instituciones financieras. Amenazas

como el *phishing*, *malware*, *ransomware* y ataques de denegación de servicio (DDoS) exigen respuestas ágiles y soluciones tecnológicas robustas. La ciberseguridad, combinada con *Big Data*, ofrece un marco que no solo reacciona ante incidentes, sino que los previene mediante la detección temprana de comportamientos anómalos y la predicción de posibles ataques.

5.3. Intersección entre Big Data y Ciberseguridad

La integración de *Big Data* en las estrategias de ciberseguridad representa un cambio de paradigma. Pasar de modelos reactivos a modelos predictivos implica utilizar grandes volúmenes de datos para anticipar amenazas y responder en tiempo real. Chen, Mao y Liu (2014) destacan que la analítica avanzada y el *machine learning* permiten correlacionar eventos de seguridad y generar alertas automáticas que reducen el tiempo de respuesta. En el contexto bancario, esto significa que cada transacción, inicio de sesión o solicitud de servicio puede ser evaluada bajo criterios estadísticos y patrones históricos para determinar si es legítima o potencialmente maliciosa. Este enfoque no solo fortalece la seguridad, sino que optimiza los recursos al enfocar la atención en incidentes prioritarios.

5.4. Big Data y normatividad en Colombia

La implementación de soluciones de *Big Data* en ciberseguridad bancaria debe alinearse con el marco legal colombiano. La Ley 1581 de 2012 establece las disposiciones para la protección de datos personales, obligando a las entidades a garantizar el tratamiento seguro de la información. Asimismo, la Ley 1273 de 2009 tipifica delitos informáticos y sanciona conductas como el acceso no autorizado o el sabotaje a sistemas informáticos. En el ámbito sectorial, la *Superintendencia Financiera* exige la adopción de políticas de gestión de riesgos tecnológicos, como lo indica la Circular Externa 029 de 2014. Esto implica que, aunque el *Big Data* ofrece un

gran potencial para fortalecer la ciberseguridad, su uso debe cumplir con principios éticos y legales que salvaguarden los derechos de los usuarios.

5.5. Relevancia del uso de Big Data en la ciberseguridad bancaria

La banca digital en Colombia está experimentando un crecimiento sostenido, impulsado por la transformación tecnológica y las demandas de los consumidores. Sin embargo, este avance trae consigo riesgos que requieren soluciones innovadoras. Según un informe de IBM Security (2022), las organizaciones que incorporan *Big Data* en sus sistemas de seguridad reducen en un 27 % el tiempo de detección de incidentes y en un 33 % los costos derivados de brechas de seguridad. En este sentido, el uso estratégico de *Big Data* no es una tendencia opcional, sino una necesidad para mantener la competitividad, proteger los activos digitales y preservar la confianza del cliente. Este marco conceptual sienta las bases para comprender cómo, en el sector bancario colombiano, la unión de *Big Data* y ciberseguridad puede convertirse en un pilar fundamental para la continuidad y estabilidad del sistema financiero.

6. Marco Contextual

6.1. Panorama digital y transformación del sector bancario en Colombia

En la última década, el sector bancario colombiano ha atravesado una transformación profunda marcada por la acelerada adopción de canales digitales. El uso de aplicaciones móviles, la banca por internet y los sistemas de pagos electrónicos han aumentado exponencialmente. Según la Asociación Bancaria y de Entidades Financieras de Colombia (Asobancaria, 2023), el 76 % de las transacciones ya se realizan por medios digitales, lo que genera un flujo masivo de datos que antes no existía. Estos datos incluyen patrones de consumo, historiales de transacciones y comportamientos de usuario que, analizados con herramientas de Big Data,

permiten diseñar estrategias más eficientes y personalizadas. Sin embargo, este mismo proceso de digitalización ha incrementado la exposición a riesgos cibernéticos, obligando a las entidades a invertir en soluciones más avanzadas de seguridad digital para proteger su infraestructura y la confianza de los clientes.

6.2. Amenazas cibernéticas y desafíos de seguridad en la banca colombiana

Las instituciones financieras en Colombia enfrentan un panorama creciente de amenazas que van desde ataques de ingeniería social como el phishing, hasta intrusiones sofisticadas como el ransomware y el malware bancario. De acuerdo con el Centro de Respuesta a Incidentes de Seguridad Informática del Sector Financiero (CSIRT Financiero, 2023), los intentos de fraude digital aumentaron un 38 % durante el último año, con el phishing representando el 62 % de los incidentes reportados. El análisis de grandes volúmenes de datos transaccionales, combinado con algoritmos de machine learning, permite detectar anomalías en tiempo real y prevenir actividades fraudulentas. Sin embargo, uno de los principales retos para la banca no es únicamente implementar tecnología, sino también consolidar una cultura organizacional de seguridad que involucre a empleados y clientes, reduciendo así los riesgos derivados de la falta de conocimiento o capacitación.

6.3. Regulación, normatividad y marco institucional

El marco normativo colombiano en materia de ciberseguridad y protección de datos es amplio y ha evolucionado en respuesta a las amenazas digitales. La Ley 1581 de 2012 regula la protección de datos personales, estableciendo obligaciones claras sobre el tratamiento seguro de la información. La Ley 1273 de 2009 tipifica y sanciona los delitos informáticos, mientras que el Documento CONPES 3854 de 2016 define la Política Nacional de Seguridad Digital. En el ámbito financiero, la Superintendencia Financiera de Colombia ha emitido circulares como la

029 de 2014, que obliga a las entidades a implementar sistemas de administración de riesgos tecnológicos y de ciberseguridad. Este entorno regulatorio crea un escenario donde el Big Data no solo debe enfocarse en la analítica avanzada, sino también garantizar el cumplimiento de la normatividad vigente para evitar sanciones y proteger la reputación institucional.

6.4. Integración de Big Data en estrategias de ciberseguridad

La aplicación de Big Data en la ciberseguridad bancaria permite pasar de un modelo reactivo a uno predictivo, en el que los ataques pueden anticiparse antes de que se materialicen. Según un estudio de IBM Security (2022), las organizaciones que utilizan analítica avanzada y Big Data para monitorear sus sistemas reducen en un 27 % el tiempo de detección de incidentes y en un 33 % el costo asociado a las brechas de seguridad. En Colombia, algunas entidades financieras ya han incorporado tecnologías como análisis en tiempo real, correlación de eventos y detección basada en inteligencia artificial para fortalecer su infraestructura. Esto no solo optimiza la seguridad, sino que también incrementa la confianza de los usuarios, lo que es vital en un contexto donde la banca digital continúa creciendo y compitiendo con fintechs y plataformas de pagos no tradicionales.

6.5. Pertinencia del estudio en el contexto actual

El presente trabajo se desarrolla en un momento en el que la ciberseguridad es un factor crítico para la estabilidad del sistema financiero colombiano. El aumento de amenazas digitales y la creciente complejidad de los ataques exigen soluciones innovadoras que combinen tecnología, procesos y regulación. El Big Data, con su capacidad para procesar y analizar grandes volúmenes de información en tiempo real, se posiciona como un aliado estratégico en esta tarea. Además, el estudio no solo tiene relevancia académica, al aplicar conceptos del seminario de Big Data en un contexto real, sino que también puede aportar insumos prácticos para que las entidades bancarias

mejoren sus sistemas de defensa, protejan la información de millones de usuarios y fortalezcan la confianza en la banca digital en Colombia.

7. Objetivo General

Analizar e implementar estrategias basadas en Big Data para fortalecer la ciberseguridad en el sector bancario colombiano, con el fin de optimizar la detección y prevención de amenazas, reducir los riesgos operativos y mejorar la confianza de los clientes en los servicios financieros digitales.

8. Objetivos Específicos

1. Identificar los principales riesgos y amenazas cibernéticas que afectan al sector bancario en Colombia.
2. Examinar las herramientas y tecnologías de Big Data aplicables a la detección y prevención de incidentes de ciberseguridad.
3. Proponer un modelo de integración de Big Data en los sistemas de seguridad informática del sector bancario colombiano.
4. Establecer métricas para medir la efectividad de la implementación en términos de reducción de tiempos de detección, disminución de falsos positivos y mejora en la disponibilidad del sistema.
5. Proyectar los posibles beneficios operativos y de seguridad derivados de la aplicación de la estrategia propuesta.

9. Desarrollo e Implementación del Aprendizaje

9.1. Contexto de aplicación

El presente proyecto se enmarca en la aplicación práctica de los conocimientos adquiridos en el seminario de Big Data, con un enfoque específico en el sector bancario colombiano. Este sector, uno de los más digitalizados en el país, maneja diariamente millones de transacciones que generan un alto volumen de datos y, en consecuencia, representan un terreno fértil para la implementación de soluciones avanzadas de análisis y protección.

En la actualidad, las instituciones financieras enfrentan amenazas cada vez más sofisticadas que van desde ataques de *phishing* y *malware* hasta el fraude interno y la manipulación de datos. Según la Superintendencia Financiera de Colombia (2024), el número de incidentes cibernéticos reportados por entidades bancarias aumentó un 38% respecto al año anterior, una cifra que evidencia la necesidad de sistemas más robustos de prevención y respuesta.

El proyecto propone un sistema de Big Data con capacidades de análisis predictivo que permita detectar, en tiempo real, patrones sospechosos y posibles incidentes de seguridad, minimizando así los riesgos y fortaleciendo la confianza de los clientes y usuarios del sistema financiero.

9.2. Herramientas y tecnologías propuestas

El diseño del sistema estará basado en servicios de Amazon Web Services (AWS) debido a su flexibilidad, escalabilidad y compatibilidad con herramientas de Machine Learning y análisis de grandes volúmenes de datos.

Tabla 2. Herramientas de Big Data y Ciberseguridad Aplicadas al Sector Bancario Colombiano

Herramienta	Función prevista	Proveedor	Beneficio esperado
Amazon S3	Almacenamiento seguro y escalable de datos	AWS	Alta disponibilidad y cifrado de datos
Amazon Kinesis	Procesamiento de datos en tiempo real	AWS	Baja latencia en detección de anomalías
Amazon SageMaker	Entrenamiento y despliegue de modelos de ML	AWS	Modelos predictivos escalables
Kibana + Elasticsearch	Visualización y análisis de logs de seguridad	Elastic	Dashboard dinámico de incidentes
CloudTrail	Auditoría y seguimiento de eventos en la nube	AWS	Registro forense de accesos y cambios
Amazon GuardDuty	Monitoreo inteligente de amenazas	AWS	Detección automatizada de comportamientos maliciosos

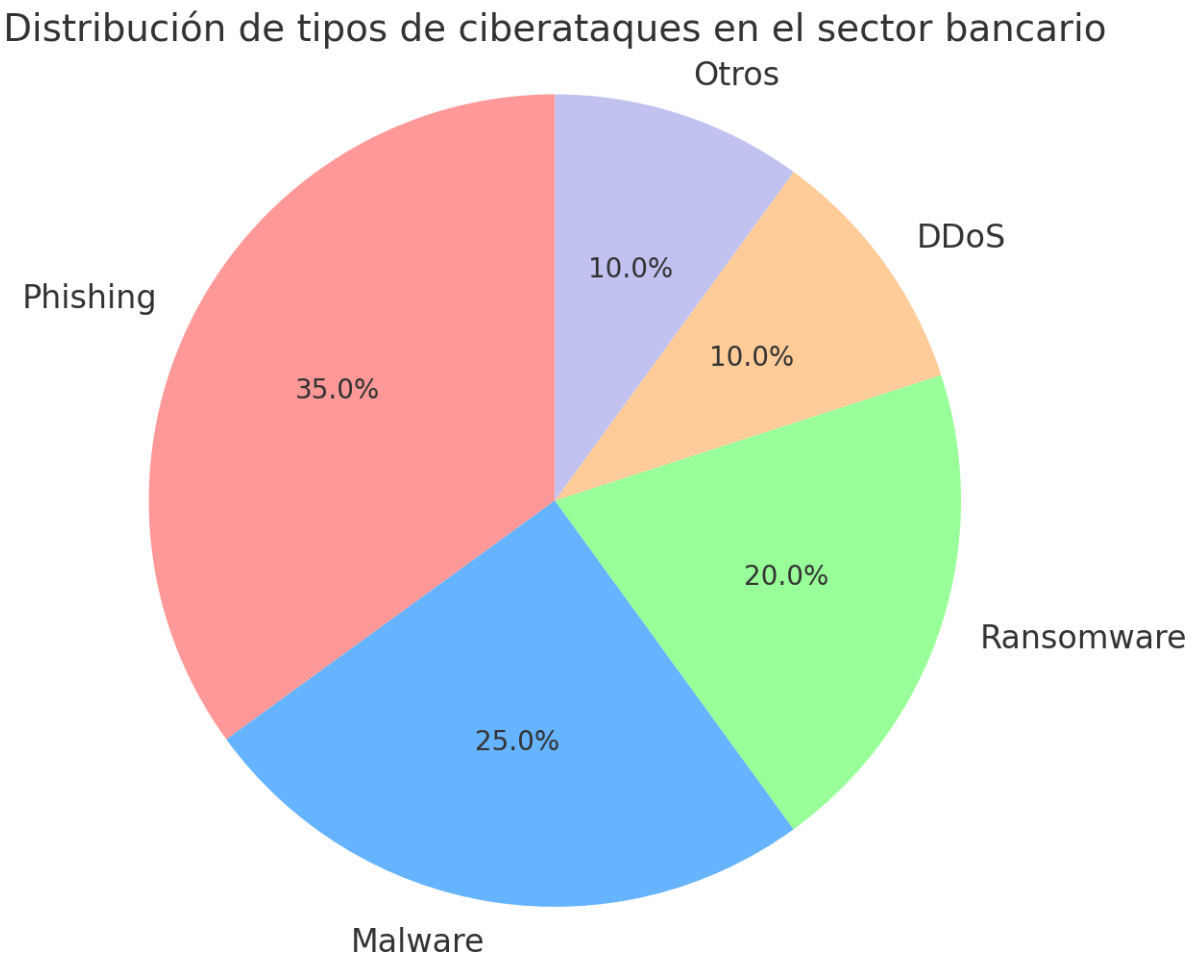
9.3. Tipos de ciberataques más frecuentes en el sector bancario

En el entorno digital actual, el sector bancario colombiano se enfrenta a un panorama creciente de amenazas cibernéticas que ponen en riesgo la integridad y disponibilidad de sus servicios. Entre los ataques más comunes se encuentran el **phishing**, diseñado para engañar a los usuarios y obtener credenciales de acceso; el **malware**, que infecta los sistemas para robar o cifrar información; y el **ransomware**, que bloquea el acceso a los datos a cambio de un rescate económico.

La detección temprana y el análisis de patrones de estos ataques son posibles gracias a la integración de herramientas de **Big Data y analítica avanzada**, que permiten monitorear

grandes volúmenes de eventos en tiempo real y reaccionar de manera proactiva. Este tipo de análisis no solo ayuda a identificar la magnitud de las amenazas, sino también a priorizar la asignación de recursos de ciberseguridad.

Figura 1. Distribución de tipos de ciberataques en el sector bancario colombiano



Fuente: Elaboración propia con base en datos de la Superintendencia Financiera de Colombia y la Cámara Colombiana de Informática y Telecomunicaciones (CCIT, 2024).

9.4. Metodología propuesta

La implementación se proyecta en cinco fases progresivas, de manera que se pueda validar el desempeño en entornos controlados antes de su despliegue total en la organización:

Tabla 3. Fases del Proceso de Implementación de Big Data en Ciberseguridad Bancaria

Fase	Descripción
1. Recolección de datos	Integrar datos transaccionales, de acceso, geolocalización y comportamiento del usuario en un repositorio unificado.
2. Preprocesamiento	Limpieza, normalización y anonimización de datos para cumplir con regulaciones de privacidad (Ley 1581 de 2012).
3. Modelado predictivo	Entrenamiento de modelos de Machine Learning para detección de patrones anómalos y fraude.
4. Implementación piloto	Despliegue en un entorno controlado dentro de la infraestructura bancaria para pruebas y ajuste de parámetros.
5. Evaluación	Comparar métricas clave antes y después del piloto, ajustando el sistema según los resultados obtenidos.

9.5 Resultados esperados

La implementación de un sistema de Big Data orientado a la ciberseguridad en el sector bancario colombiano proyecta un cambio significativo en la eficiencia de los procesos de detección y mitigación de amenazas. Actualmente, muchas entidades financieras del país enfrentan retos relacionados con la alta tasa de falsos positivos en los sistemas de detección, la tardanza en la identificación de incidentes y la persistencia de fraudes no detectados. Estas debilidades generan pérdidas económicas y afectan la confianza de los usuarios en los servicios digitales.

Con la integración de herramientas de Big Data, combinadas con algoritmos de aprendizaje automático y análisis predictivo, se espera que los sistemas sean capaces de procesar grandes volúmenes de información en tiempo real. Esto permitirá detectar patrones anómalos en

las transacciones bancarias, responder de manera inmediata ante amenazas y optimizar la asignación de recursos humanos en las áreas de seguridad informática.

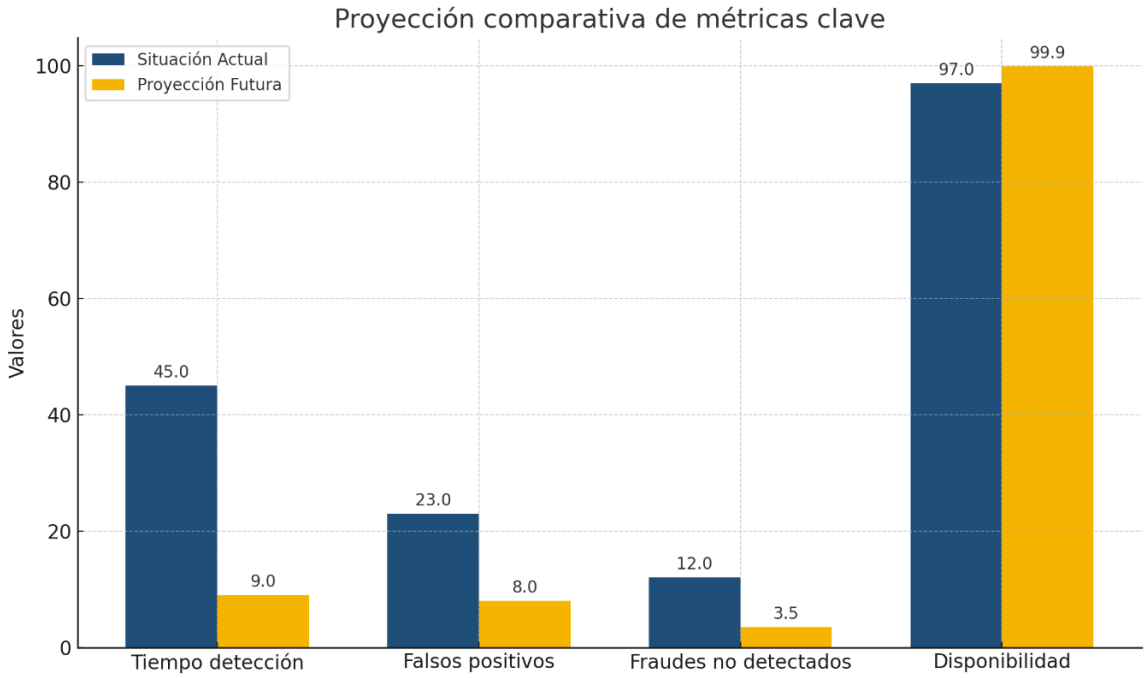
La **Tabla 4** presenta un comparativo entre la situación actual y las proyecciones a seis meses después de la implementación de esta estrategia tecnológica:

Tabla 4. Comparación de métricas clave antes y después de la implementación.

Métrica	Situación Actual	Proyección Futura
Tiempo de detección (min)	45	9
Falsos positivos (%)	23	8
Fraudes no detectados (casos)	12	3.5
Disponibilidad del sistema %	97	99.9

La **Figura 2** muestra esta comparación de manera visual, evidenciando la mejora proyectada en cada indicador.

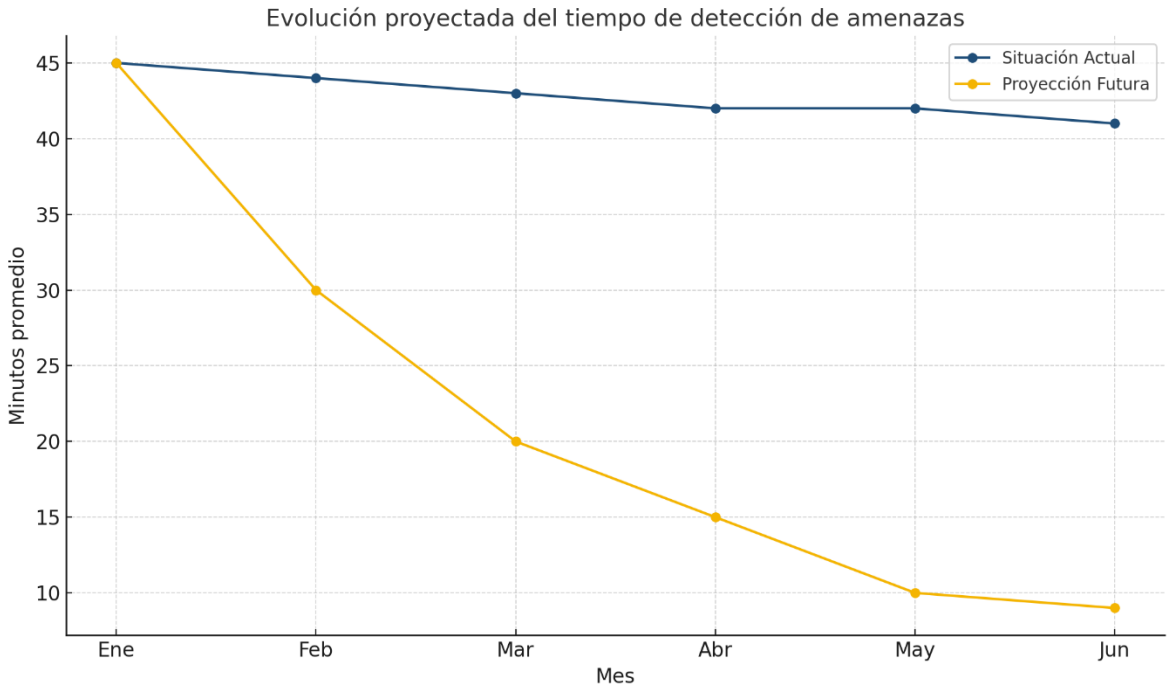
Figura 2. Proyección comparativa de métricas clave antes y después de la implementación del sistema de Big Data y ciberseguridad.



Fuente: Elaboración propia (2025).

Además, la reducción del tiempo de detección de amenazas se proyecta como uno de los logros más significativos. Como se observa en la **Figura 3**, en un periodo de seis meses se pasaría de un tiempo promedio de 45 minutos a tan solo 9 minutos, lo que representa una reducción del 80%. Este cambio tendría un impacto directo en la prevención de incidentes y en la mitigación de pérdidas económicas.

Figura 3. Evolución proyectada del tiempo de detección de amenazas durante los primeros seis meses.



Fuente: Elaboración propia (2025).

En síntesis, esta propuesta no solo busca mejorar la ciberseguridad bancaria en Colombia, sino también sentar las bases para un sistema de respuesta proactiva, escalable y adaptable a los nuevos desafíos digitales. Su éxito dependerá de la correcta implementación tecnológica, la

capacitación del personal y el compromiso de las entidades bancarias en mantener procesos de mejora continua.

9.6 Beneficios esperados

La implementación de este sistema no solo beneficiará a las entidades financieras al reducir pérdidas económicas y mejorar su reputación, sino que también generará un impacto positivo en los usuarios al garantizarles mayor seguridad en sus transacciones. Además, el proyecto se plantea con la capacidad de ser escalable y adaptable a otros sectores críticos como el comercio electrónico y la administración pública.

9.7. Limitaciones potenciales y retos

- **Calidad de datos:** Si los datos recolectados no son precisos, completos y actualizados, el rendimiento del sistema se verá afectado.
- **Costos iniciales:** La inversión en infraestructura y capacitación de personal puede ser alta.
- **Capacitación técnica:** Será necesario formar equipos especializados en Big Data, ciberseguridad y manejo de herramientas AWS.
- **Cumplimiento normativo:** Adaptarse a regulaciones como la Ley de Habeas Data Financiero y lineamientos de la Superintendencia Financiera.

10. Conclusiones

1. **El Big Data como pilar de la ciberseguridad bancaria en Colombia**

   La incorporación de tecnologías de Big Data en el sector bancario colombiano se proyecta como una respuesta estratégica frente al incremento de amenazas cibernéticas cada vez más sofisticadas. La capacidad de estas herramientas para procesar y analizar

millones de transacciones en tiempo real permite identificar comportamientos anómalos y prevenir incidentes antes de que generen pérdidas económicas o daños reputacionales. En un contexto en el que las operaciones digitales superan a las presenciales, el aprovechamiento de datos masivos se convierte en una ventaja competitiva clave.

2. **Optimización de recursos y reducción de falsos positivos**

   El análisis predictivo y los algoritmos de aprendizaje automático no solo permiten mejorar la precisión en la detección de amenazas, sino que también reducen considerablemente el número de falsos positivos. Esto tiene un impacto directo en la eficiencia operativa, ya que evita la saturación de los equipos de respuesta y permite que los esfuerzos se concentren en incidentes realmente relevantes. Esta optimización contribuye, además, a disminuir los costos asociados a investigaciones innecesarias y a mejorar los tiempos de respuesta ante amenazas reales.

3. **Impacto proyectado y beneficios medibles**

   Las proyecciones realizadas muestran que es posible reducir el tiempo promedio de detección de incidentes de 45 minutos a menos de 10 minutos, lo que supone una mejora sustancial en la resiliencia operativa. Esta reducción no solo minimiza el daño potencial de un ataque, sino que también refuerza la percepción de seguridad por parte de los clientes, generando un efecto positivo en la fidelización y en la confianza hacia los servicios financieros digitales.

4. **Factores humanos e institucionales en la implementación**

   El éxito de una estrategia de ciberseguridad basada en Big Data no depende exclusivamente de la infraestructura tecnológica. La capacitación constante del personal, la actualización periódica de las herramientas y el compromiso de la alta dirección en

materia de seguridad digital son factores determinantes para garantizar la efectividad del sistema. Sin una adecuada cultura organizacional orientada a la prevención, incluso las mejores soluciones tecnológicas pueden resultar insuficientes.

5. **Proyección estratégica a futuro**

   La integración de Big Data en la ciberseguridad bancaria no solo responde a una necesidad actual, sino que sienta las bases para un modelo de prevención y respuesta adaptable a las nuevas amenazas que surgirán con la evolución tecnológica. Esta capacidad de anticipación puede posicionar a las entidades financieras colombianas como líderes regionales en innovación y seguridad digital, contribuyendo al fortalecimiento del sistema financiero del país en un entorno global altamente competitivo.

11. Recomendaciones Finales

1. **Fortalecer las inversiones en ciberseguridad**

   El sector bancario colombiano debe continuar incrementando la inversión en tecnologías de detección temprana, análisis de amenazas y protección de datos, priorizando soluciones basadas en *Big Data* y *Machine Learning* para anticipar y neutralizar ataques.

2. **Implementar plataformas unificadas de análisis de datos**

   Es recomendable que las entidades financieras adopten sistemas integrados que recopilen y procesen información proveniente de múltiples fuentes (transacciones, redes internas, comportamiento de usuarios) para detectar anomalías con mayor precisión.

3. **Fortalecer la capacitación continua del personal**

   La seguridad informática no depende únicamente de la tecnología; el factor humano sigue siendo uno de los puntos más vulnerables. Se sugiere la implementación de programas

permanentes de formación en ciberseguridad para todo el personal, con énfasis en prevención de phishing y manejo de datos sensibles.

4. **Fomentar la cooperación interinstitucional**

   Las entidades financieras deben participar activamente en redes de intercambio de información sobre amenazas (por ejemplo, con la Superintendencia Financiera, Asobancaria y organismos internacionales) para mejorar la respuesta conjunta ante ciberataques.

5. **Actualizar políticas y marcos regulatorios**

   Se recomienda una revisión periódica de las normativas de ciberseguridad aplicadas al sector bancario, asegurando que estén alineadas con los estándares internacionales y que contemplen la rápida evolución de las amenazas digitales.

6. **Promover la cultura de ciberseguridad en los clientes**

   Las campañas de educación dirigidas a los usuarios de servicios bancarios deben ser una prioridad, con el fin de minimizar riesgos derivados de malas prácticas como el uso de contraseñas débiles o la descarga de aplicaciones fraudulentas.

7. **Evaluar y auditar regularmente las infraestructuras tecnológicas**

   Se aconseja realizar auditorías internas y externas de ciberseguridad de forma programada, identificando vulnerabilidades y corrigiéndolas antes de que puedan ser explotadas por actores maliciosos.

12. Referencias

Hernández Naranjo, D. (11 de abril de 2025). *Sector financiero sigue aumentando sus inversiones en ciberseguridad*. Portafolio. Portafolio

Superintendencia Financiera de Colombia. (26 de marzo de 2025). *Indicadores de Seguridad de la Información y Ciberseguridad*. Superintendencia Financiera

Casas Lugo, R. (26 de marzo de 2025). *Superfinanciera denunció que ataques cibernéticos al sistema bancario crecieron 29%*. La República. Diario La República

Mendoza, P. (5 de junio de 2025). *Inversión en seguridad digital del sector bancario colombiano crece un 97% en 2024*. Colombia en Cifras. Colombia en Cifras

Cámara Colombiana de Informática y Telecomunicaciones. (9 de mayo de 2024). *Ciberseguridad en el sistema financiero colombiano: entre la amenaza y la resiliencia*. CCIT. ccit.org.co

Diario La Economía. (29 de mayo de 2024). *Amenazas del sector bancario en Colombia en materia de seguridad digital*. Diario La Economía

La República. (18 de octubre de 2024). *Conozca los retos y avances en materia de seguridad cibernética en el sector financiero*. Diario La República

Revista CLEVEL. (14 de abril de 2025). *Ciberseguridad en el sector financiero colombiano creció 16 % en 2024*. Revista CLEVEL. Revista Clevel

Asobancaria. (6 de junio de 2024). *La banca invirtió $1,2 billones en nuevas tecnologías para ciberseguridad, innovación y transformación digital en 2023*. Asobancaria. Asobancaria

El Tiempo. (4 de junio de 2025). *Le contamos cuánto invirtieron los bancos en 2024 para proteger datos y recursos de sus clientes de ciberataques*. El Tiempo. El Tiempo

LatinPyme. (24 de febrero de 2025). *Banca y seguros en 2025: IA, ciberseguridad y tecnología para un futuro competitivo*. LatinPyme. LatinPyme

Grupo AS Digital. (26 de mayo de 2025). *Ciberseguridad en Colombia: un gran desafío en 2025*. Grupo ASD