# Inteligencia Artificial Aplicada a la Prevención de Fraudes en el Sector Bancario

## Resumen Ejecutivo

El panorama del fraude financiero ha experimentado una transformación radical, evolucionando desde incidentes aislados hacia ataques coordinados y de alta sofisticación tecnológica. Los métodos de defensa tradicionales, fundamentados en sistemas de reglas estáticas, han demostrado ser insuficientes para contrarrestar estas amenazas dinámicas, que a menudo son impulsadas por la misma Inteligencia Artificial (IA) que las instituciones buscan emplear para su protección.1 En este contexto, la adopción de la IA ha dejado de ser una opción innovadora para convertirse en un imperativo estratégico, esencial para la resiliencia, competitividad y supervivencia de las entidades financieras modernas.4

Este informe presenta un análisis exhaustivo sobre la aplicación de la IA en la prevención de fraudes, detallando cómo un arsenal de tecnologías avanzadas —que incluye *Machine Learning* (ML), *Deep Learning* (DL) y Procesamiento del Lenguaje Natural (NLP)— faculta a los bancos para transitar de una postura meramente reactiva a una estrategia proactiva y predictiva. La IA introduce capacidades de análisis de transacciones en tiempo real, reconocimiento de patrones complejos y un aprendizaje adaptativo continuo que resultan inalcanzables para los métodos manuales o basados en reglas predefinidas.4

Para una institución como Scotiabank, la implementación estratégica de estas tecnologías se traduce en beneficios tangibles y multifacéticos. En primer lugar, una reducción drástica de las pérdidas financieras directas ocasionadas por el fraude. En segundo lugar, una mejora sustancial en la eficiencia operativa, lograda a través de la automatización de tareas de monitoreo y una disminución significativa en la tasa de "falsos positivos", lo que optimiza el uso de recursos humanos. Finalmente, y de manera crucial, se produce un fortalecimiento de la confianza del cliente, transformando la seguridad de un requisito operativo a un potente diferenciador de marca en un mercado competitivo.9

Con base en el análisis presentado, se recomienda a Scotiabank Perú adoptar un enfoque estructurado y por fases para la implementación de la IA. Este proceso debe iniciarse con una evaluación rigurosa de la calidad y disponibilidad de sus datos, seguida de la definición de casos de uso críticos y de alto impacto. Es fundamental acompañar la inversión tecnológica con una estrategia de desarrollo de talento interno, capacitando a los equipos para colaborar con estas nuevas herramientas. Asimismo, se debe establecer un marco de gobernanza de IA robusto que aborde proactivamente los riesgos de sesgos algorítmicos y garantice la explicabilidad de los modelos (XAI). Este marco debe estar en plena conformidad con el emergente panorama regulatorio peruano, en particular con la Ley N° 31814 y su reglamento, que sientan las bases para un uso responsable y ético de la IA en el país.9

## Introducción: El Nuevo Paradigma en la Prevención de Fraudes

El sector financiero global se enfrenta a una era de desafíos sin precedentes en materia de seguridad. El fraude ha mutado de actos oportunistas a operaciones industriales, coordinadas y tecnológicamente avanzadas. Los defraudadores modernos ya no solo explotan vulnerabilidades; las crean y las escalan utilizando un arsenal de herramientas sofisticadas. La IA generativa, por ejemplo, les permite crear correos electrónicos de *phishing* y mensajes de ingeniería social hiperrealistas, personalizados y a gran escala, que son casi indistinguibles de las comunicaciones legítimas.4 La tecnología

*deepfake* se utiliza para suplantar la identidad de clientes en procesos de verificación por voz o video, mientras que la velocidad de los sistemas de pagos en tiempo real es explotada para ejecutar fraudes y lavar dinero antes de que los sistemas de seguridad tradicionales puedan reaccionar.16 El impacto de esta evolución trasciende las pérdidas financieras directas; erosiona la confianza del cliente, daña la reputación de la marca y, como señalan algunos análisis, puede tener repercusiones macroeconómicas medibles.4

Frente a esta amenaza dinámica, los sistemas de prevención de fraude heredados, basados en reglas estáticas, han quedado obsoletos. Estos sistemas operan bajo una lógica predefinida y rígida, como marcar para revisión manual todas las transacciones que superen un determinado umbral monetario o que se originen en una geografía específica. Si bien fueron efectivos en un entorno más simple, hoy presentan dos debilidades críticas. Primero, generan un volumen abrumador de "falsos positivos", es decir, alertas sobre transacciones perfectamente legítimas que casualmente cumplen con una regla.18 Esto no solo consume una cantidad desproporcionada de recursos de los analistas de fraude, quienes deben investigar manualmente cada alerta, sino que también degrada severamente la experiencia del cliente al bloquear o retrasar sus transacciones legítimas.3 Segundo, y más importante, son incapaces por diseño de detectar patrones de fraude nuevos o sutiles que no se ajustan a las reglas predefinidas. Los defraudadores modernos son conscientes de estos umbrales y diseñan sus ataques para operar "bajo el radar", utilizando múltiples transacciones pequeñas o tácticas novedosas que los sistemas basados en reglas no pueden reconocer.1

En este contexto, la Inteligencia Artificial no es simplemente una mejora incremental, sino un cambio de paradigma fundamental en la defensa contra el fraude. La IA permite a las instituciones financieras pasar de una postura de *detección* reactiva a una de *prevención* proactiva y predictiva.4 En lugar de analizar el fraude después de que ha ocurrido, los sistemas de IA evalúan el riesgo en tiempo real, en el momento en que se inicia una transacción, para anticipar y bloquear las amenazas antes de que se materialicen y causen pérdidas.3 La capacidad de aprendizaje continuo (

*machine learning*) es el núcleo de esta transformación. A diferencia de las reglas estáticas que deben ser actualizadas manualmente, los modelos de IA aprenden de cada nueva transacción, adaptando y refinando constantemente su comprensión de lo que constituye un comportamiento normal versus uno fraudulento. Esto permite que las defensas del banco evolucionen dinámicamente, a la misma velocidad que las tácticas de los defraudadores.9

La situación actual puede describirse como una "carrera armamentista" tecnológica. Los sistemas de defensa tradicionales son análogos a construir un muro más alto, mientras que los defraudadores ya han desarrollado formas de volar sobre él. La IA proporciona un escudo dinámico y adaptable. Sin embargo, los atacantes también están adoptando IA, especialmente herramientas generativas, para crear ataques más sofisticados y personalizados.4 Esto establece un ciclo continuo de escalada: las defensas de IA mejoradas obligan a los defraudadores a desarrollar ataques de IA más avanzados, lo que a su vez exige defensas aún más robustas. Para una institución como Scotiabank, esto implica que la inversión en IA no puede ser un proyecto con un inicio y un fin definidos. Debe concebirse como el desarrollo de una capacidad estratégica continua, con recursos permanentemente dedicados a la investigación, el monitoreo y la actualización de los modelos para no ceder terreno en esta contienda tecnológica. La prevención del fraude se transforma así en una función de inteligencia y contrainteligencia, donde la agilidad y la capacidad de adaptación son las claves para mantener la ventaja.

La siguiente tabla resume las diferencias fundamentales entre los enfoques tradicionales y los basados en IA, ilustrando por qué la transición es un imperativo estratégico.

| Característica | Sistemas Basados en Reglas (Tradicionales) | Sistemas Basados en IA (Modernos) |
| --- | --- | --- |
| **Lógica de Detección** | Estática y predefinida (Ej. "SI monto > , ENTONCES alerta").1 | Dinámica y contextual. Aprende patrones complejos a partir de datos históricos y en tiempo real.4 |
| **Adaptabilidad** | Baja. Requiere actualización manual de reglas para cada nueva táctica de fraude.18 | Alta. Los modelos de *machine learning* se reentrenan y adaptan continuamente a nuevas amenazas.9 |
| **Tasa de Falsos Positivos** | Alta. Genera muchas alertas para transacciones legítimas que activan reglas rígidas.18 | Baja. El análisis contextual reduce significativamente las alertas innecesarias, mejorando la experiencia del cliente.10 |
| **Escalabilidad** | Limitada. La revisión manual de alertas se vuelve insostenible con el aumento del volumen de transacciones.3 | Alta. Capaz de analizar millones de transacciones en milisegundos, escalando con el negocio.9 |
| **Detección de Fraude Nuevo** | Ineficaz. Solo puede detectar patrones para los que ha sido explícitamente programado.1 | Eficaz. El aprendizaje no supervisado puede identificar anomalías y tipos de fraude nunca antes vistos.7 |
| **Mantenimiento** | Intensivo en mano de obra. Requiere que los analistas revisen y ajusten constantemente las reglas.19 | Automatizado. Los modelos se reentrenan y ajustan con nuevos datos, aunque requieren supervisión experta.23 |

## El Arsenal Tecnológico de la IA contra el Fraude

Para comprender el impacto transformador de la Inteligencia Artificial en la prevención de fraudes, es esencial desglosar las tecnologías fundamentales que componen este arsenal. Cada una de estas herramientas aborda el problema desde un ángulo diferente, y su verdadero poder reside en su capacidad para operar de manera sinérgica, creando un sistema de defensa multicapa y robusto.

### 3.1. Machine Learning (ML): El Motor del Análisis Predictivo

El *Machine Learning* (ML) o aprendizaje automático es la disciplina central de la IA moderna y representa el cambio fundamental de la programación explícita al aprendizaje a partir de datos.18 En el contexto del fraude, en lugar de decirle a un sistema "una transacción es fraudulenta si cumple las condiciones A, B y C", se le proporcionan miles de ejemplos de transacciones pasadas, tanto legítimas como fraudulentas, y el algoritmo aprende por sí mismo a distinguir entre ambas.28 Este enfoque se manifiesta principalmente en dos modalidades:

* **Aprendizaje Supervisado:** Este es el método más común en la detección de fraudes. Requiere un conjunto de datos históricos donde cada transacción ha sido previamente etiquetada como "fraudulenta" o "legítima".7 El modelo de ML se entrena con estos datos para identificar los patrones y las características que se correlacionan con cada etiqueta. Por ejemplo, podría aprender que una combinación de factores como una transacción de alto valor, realizada desde una nueva ubicación, en un comercio de alto riesgo y a una hora inusual, tiene una alta probabilidad de ser fraudulenta. Una vez entrenado, el modelo puede clasificar nuevas transacciones en tiempo real con alta precisión, siendo especialmente efectivo para detectar tipos de fraude cuyos patrones ya son conocidos por la institución.7
* **Aprendizaje No Supervisado:** A diferencia del anterior, este enfoque no requiere datos etiquetados. El algoritmo recibe un gran volumen de datos de transacciones y su tarea es encontrar la estructura inherente en ellos, identificando grupos de comportamiento similar y, lo más importante, detectando "anomalías" o *outliers*, es decir, puntos de datos que se desvían significativamente del comportamiento normal.7 Esta capacidad es crucial para la ciberseguridad, ya que permite detectar esquemas de fraude completamente nuevos o "ataques de día cero" para los cuales no existen ejemplos históricos. El sistema no sabe  
  *qué* es el fraude, pero es capaz de reconocer que una transacción específica "no se parece a nada de lo que ha visto antes" y, por lo tanto, merece una investigación.7
* **Aprendizaje por Refuerzo:** Aunque su aplicación es más emergente, este tipo de aprendizaje se utiliza para optimizar las estrategias de respuesta. Un "agente" de IA aprende a tomar una secuencia de decisiones para maximizar una recompensa. En la prevención de fraudes, el agente podría decidir la mejor acción a tomar ante una alerta (bloquear la transacción, solicitar un segundo factor de autenticación o permitirla) basándose en el resultado de decisiones pasadas, aprendiendo a equilibrar la seguridad con la mínima fricción para el cliente.18

### 3.2. Deep Learning (DL): Descifrando la Complejidad Oculta

El *Deep Learning* (DL) o aprendizaje profundo es un subcampo avanzado del *Machine Learning* que utiliza redes neuronales artificiales con múltiples capas (de ahí el término "profundo"). Esta arquitectura permite a los modelos aprender representaciones de datos con múltiples niveles de abstracción, lo que les confiere una capacidad extraordinaria para identificar patrones extremadamente complejos, sutiles y no lineales en volúmenes masivos de datos (*Big Data*).2 Mientras que el ML tradicional puede encontrar correlaciones directas, el DL puede descubrir relaciones ocultas entre docenas o cientos de variables que serían invisibles para un analista humano o para algoritmos más simples.32

Algunos de los modelos de DL más relevantes para la detección de fraudes incluyen:

* **Redes Neuronales Recurrentes (RNNs) y sus variantes (LSTM, GRU):** Estos modelos están diseñados específicamente para procesar datos secuenciales, lo que los hace ideales para analizar el historial de transacciones de un cliente como una serie temporal. Una red LSTM (*Long Short-Term Memory*) o GRU (*Gated Recurrent Unit*) puede "recordar" el comportamiento de un cliente a lo largo del tiempo y detectar anomalías en la secuencia, como un cambio repentino en los patrones de gasto o una serie de acciones que no se corresponden con su comportamiento histórico.34
* **Autoencoders:** Son un tipo de red neuronal utilizada para el aprendizaje no supervisado, particularmente eficaces en la detección de anomalías.36 Un  
  *autoencoder* se compone de dos partes: un "codificador" que comprime los datos de entrada en una representación de baja dimensión, y un "decodificador" que intenta reconstruir los datos originales a partir de esa representación comprimida. El modelo se entrena exclusivamente con datos de transacciones normales y legítimas. La lógica es que el modelo aprenderá a reconstruir con gran precisión las transacciones normales. Sin embargo, cuando se le presenta una transacción fraudulenta o anómala, que tiene características que nunca ha visto antes, el modelo será incapaz de reconstruirla correctamente, generando un alto "error de reconstrucción". Este error sirve como una potente señal de alerta de fraude.38 La combinación de LSTMs con  
  *autoencoders* (*LSTM Autoencoders*) es especialmente poderosa para analizar datos de series temporales financieras.38

### 3.3. Procesamiento del Lenguaje Natural (NLP): La Defensa contra la Ingeniería Social

El Procesamiento del Lenguaje Natural (NLP) es la rama de la IA que dota a las máquinas de la capacidad de comprender, interpretar y generar lenguaje humano, tanto escrito como hablado.43 En el ámbito del fraude, su papel es fundamental para combatir las amenazas que se basan en la manipulación y el engaño, en lugar de la explotación puramente técnica.45

Sus aplicaciones clave son:

* **Detección de Phishing y Spam:** Los algoritmos de NLP analizan el contenido de correos electrónicos, SMS y mensajes de chat en busca de indicadores de fraude. Pueden identificar un lenguaje que crea una falsa sensación de urgencia ("su cuenta será bloqueada si no actúa ahora"), errores gramaticales sutiles, suplantación de remitentes y otros rasgos característicos de los ataques de ingeniería social.9
* **Análisis de Texto no Estructurado:** Una gran cantidad de información valiosa para la detección de fraudes se encuentra en datos de texto no estructurados. El NLP puede extraer y analizar información de las notas de los analistas de fraude, las descripciones de las reclamaciones de seguros, las reseñas de clientes o incluso publicaciones en redes sociales para identificar inconsistencias, sentimientos negativos o conexiones que puedan indicar una actividad fraudulenta.28
* **Chatbots de Verificación:** Los *chatbots* de servicio al cliente impulsados por IA pueden desempeñar un doble papel. Además de atender las consultas de los clientes, pueden analizar los patrones de lenguaje y el comportamiento conversacional del usuario en tiempo real. Si un usuario utiliza un lenguaje atípico, evade preguntas de seguridad o muestra patrones de conversación conocidos asociados a estafadores, el *chatbot* puede marcar la sesión como sospechosa y escalarla a un agente humano.7

### 3.4. Técnicas Analíticas Avanzadas

Más allá de los modelos fundamentales, la IA se aplica a través de técnicas analíticas específicas que potencian la prevención del fraude:

* **Análisis de Comportamiento de Usuarios y Entidades (UEBA):** Esta técnica representa un cambio de enfoque desde el análisis de eventos aislados al análisis de actores. Los sistemas UEBA recopilan y analizan datos de una amplia gama de fuentes para construir un perfil de comportamiento "normal" o una "línea base" para cada usuario y entidad (como servidores o dispositivos) en la red.49 Esta línea base incluye patrones de inicio de sesión (horarios, ubicaciones, dispositivos), aplicaciones utilizadas, volumen de datos transferidos y otros comportamientos. El sistema monitorea continuamente la actividad en tiempo real y detecta cualquier desviación significativa de esta línea base, que podría indicar una cuenta comprometida, una amenaza interna o un intento de fraude.51
* **Análisis Predictivo y Puntuación de Riesgo en Tiempo Real:** En lugar de tomar una decisión binaria (fraude/no fraude), los modelos de IA más avanzados asignan una "puntuación de riesgo" probabilística a cada transacción en milisegundos.28 Esta puntuación, que puede ir de 0 a 100, refleja la probabilidad de que la transacción sea fraudulenta. Este enfoque granular permite una gestión del riesgo mucho más flexible y eficiente. Las transacciones con puntuaciones muy bajas se aprueban automáticamente sin fricción para el cliente. Aquellas con puntuaciones intermedias pueden desencadenar una solicitud de autenticación adicional (como un código de un solo uso o una verificación biométrica). Solo las transacciones con puntuaciones muy altas se bloquean de inmediato y se escalan para una revisión humana.55
* **Análisis de Redes (Grafos):** Esta es una de las técnicas más poderosas para combatir el fraude organizado. En lugar de ver a los clientes y las transacciones como entidades aisladas, el análisis de grafos los modela como una red de nodos interconectados.2 Los nodos pueden representar clientes, cuentas, números de teléfono, direcciones de correo electrónico, dispositivos o direcciones IP. Las aristas representan las relaciones entre ellos (por ejemplo, una transacción, el uso del mismo dispositivo, o compartir una dirección). Esta perspectiva de red permite descubrir patrones de fraude coordinado que son completamente invisibles a nivel individual. Por ejemplo, puede revelar un anillo de "cuentas mula" utilizadas para el lavado de dinero al identificar un grupo de cuentas aparentemente no relacionadas que reciben fondos de una fuente común y los transfieren rápidamente a otra.28 También es fundamental para detectar fraudes de identidad sintética, al encontrar grupos de solicitudes de nuevas cuentas que comparten sutilmente algunos atributos.58

El verdadero poder de estas tecnologías no reside en su aplicación aislada, sino en su **convergencia** en un sistema de defensa unificado. Una estrategia de seguridad robusta no depende de una única herramienta, sino que orquesta una secuencia de análisis en capas. Por ejemplo, un intento de fraude podría iniciarse con un correo electrónico de *phishing*. La primera línea de defensa sería un modelo de **NLP** que analiza el texto y lo marca como sospechoso.45 Si el ataque tiene éxito y el defraudador obtiene las credenciales, intentará iniciar sesión. En este punto, un sistema

**UEBA** detectaría una anomalía, como un inicio de sesión desde una ubicación o un dispositivo nunca antes visto para ese cliente.49 A continuación, el atacante intenta realizar una transferencia de fondos. Un modelo de

**Machine Learning supervisado** compararía las características de esta transacción con miles de patrones de fraude conocidos, asignándole una alta puntuación de riesgo.28 Simultáneamente, un modelo de

**Deep Learning no supervisado**, como un *autoencoder*, detectaría que la transacción se desvía drásticamente del comportamiento histórico del cliente, generando una señal de alerta adicional por su alto error de reconstrucción.38 Finalmente, un análisis de

**grafos** podría revelar que la cuenta de destino de la transferencia está conectada a una red de cuentas previamente identificadas como mulas.57 Es la correlación de estas señales, provenientes de diferentes modelos de IA en tiempo real, lo que permite tomar una decisión de bloqueo con un altísimo grado de confianza. Por lo tanto, Scotiabank no debe aspirar a implementar "una" solución de IA, sino a construir un ecosistema de defensa inteligente y multicapa.

La siguiente tabla mapea cada tecnología de IA con los tipos de fraude que combate de manera más efectiva, proporcionando una guía para la priorización de su implementación.

| Tecnología de IA | Sub-Tecnología/Algoritmo Clave | Tipo de Fraude Combatido | Ejemplo de Aplicación en Scotiabank |
| --- | --- | --- | --- |
| **Machine Learning (ML)** | Aprendizaje Supervisado (Ej. Random Forest, Gradient Boosting) | Fraude de tarjeta de crédito, Fraude de pagos en línea (patrones conocidos). | Asignar una puntuación de riesgo en tiempo real a cada compra con tarjeta de crédito basada en el historial del cliente y las características de la transacción. |
|  | Aprendizaje No Supervisado (Ej. Clustering, Detección de Anomalías) | Nuevos tipos de fraude (Día Cero), Fraude de identidad sintética. | Identificar grupos de nuevas solicitudes de crédito que comparten atributos sutiles no evidentes (ej. misma imagen de perfil con ligeras variaciones). |
| **Deep Learning (DL)** | LSTM, GRU | Toma de Control de Cuentas (ATO), Fraude secuencial. | Analizar la secuencia de acciones de un usuario en la banca en línea para detectar comportamientos anómalos que indiquen un secuestro de sesión. |
|  | Autoencoders | Detección de anomalías en transacciones, Fraude en tiempo real. | Entrenar un modelo con transacciones normales para que cualquier transacción que no pueda ser "reconstruida" con precisión sea marcada como altamente sospechosa. |
| **Procesamiento del Lenguaje Natural (NLP)** | Clasificación de Texto, Análisis de Sentimiento | Phishing, Ingeniería Social, Fraude en reclamaciones. | Escanear automáticamente los correos electrónicos reportados por clientes a la dirección de *phishing* del banco para identificar campañas de ataque y extraer indicadores de compromiso. |
| **Análisis de Redes (Grafos)** | Algoritmos de Centralidad, Detección de Comunidades | Lavado de Dinero (AML), Redes de mulas, Fraude colusorio, Fraude de identidad sintética. | Visualizar y analizar el flujo de fondos entre cuentas para identificar redes de cuentas utilizadas para estratificar y mover dinero de origen ilícito. |
| **Análisis de Comportamiento (UEBA)** | Modelado de Línea Base, Detección de Desviaciones | Toma de Control de Cuentas (ATO), Fraude Interno, Amenazas Persistentes Avanzadas (APTs). | Crear un perfil de comportamiento para cada cliente y alertar si se detecta un inicio de sesión desde un país inusual seguido de un intento de transferencia a un nuevo beneficiario. |

## Aplicaciones Prácticas de la IA en la Banca

La aplicación de las tecnologías de Inteligencia Artificial descritas anteriormente no es teórica; se traduce en soluciones concretas para los desafíos de fraude más apremiantes que enfrentan las instituciones financieras como Scotiabank. Cada tipo de fraude tiene características únicas, y la IA ofrece herramientas especializadas para contrarrestar cada una de ellas de manera efectiva.

### 4.1. Fraude Transaccional

Esta es la forma más visible de fraude y el área donde la IA ha tenido uno de los impactos más inmediatos y significativos.

* **Fraude con Tarjetas de Crédito y Débito:** En cada transacción, ya sea en un punto de venta físico o en línea, los sistemas de IA analizan en milisegundos cientos de variables. Estas incluyen no solo los datos obvios como el monto, la ubicación y el tipo de comercio, sino también metadatos como la información del dispositivo, la dirección IP, la hora del día, la frecuencia de las transacciones y la comparación con el historial de gasto del cliente y de clientes con perfiles similares.19 Empresas líderes en el ecosistema de pagos, como Mastercard, han demostrado el poder de este enfoque. Mediante el uso de IA avanzada, han logrado duplicar la tasa de detección de tarjetas comprometidas y reducir los falsos positivos en las transacciones hasta en un 200%, lo que significa menos interrupciones para los clientes legítimos y una mayor seguridad general.59
* **Fraude en Pagos en Tiempo Real (RTP) y Comercio Electrónico:** La inmediatez de los pagos instantáneos y el volumen del comercio electrónico los convierten en un objetivo prioritario para los defraudadores, ya que una vez que los fondos se han movido, su recuperación es extremadamente difícil. La IA es la única tecnología capaz de operar a la velocidad requerida para tomar decisiones de riesgo en tiempo real, antes de que la transacción se complete.3 Los modelos analizan el comportamiento del cliente, la "huella digital" del dispositivo (una identificación única basada en sus características de hardware y software), la reputación del comerciante y otros factores contextuales para marcar transacciones que se desvían de los patrones históricos.7

### 4.2. Prevención del Robo de Identidad

El robo de identidad ha evolucionado de simples robos de credenciales a la creación de identidades completamente fabricadas, lo que requiere defensas más sofisticadas.

* **Toma de Control de Cuentas (Account Takeover - ATO):** En un ataque de ATO, un defraudador obtiene acceso a la cuenta legítima de un cliente. Aquí, los modelos de Análisis de Comportamiento de Usuarios y Entidades (UEBA) son la principal línea de defensa.3 Estos sistemas aprenden los patrones de comportamiento únicos de cada cliente. Una alerta se genera no por la transacción en sí, sino por las anomalías en el comportamiento que la preceden: un inicio de sesión desde una dirección IP o un dispositivo nunca antes visto, una velocidad de escritura o movimientos del ratón diferentes a los del usuario legítimo, o una navegación inusual dentro de la plataforma de banca en línea.4
* **Fraude de Identidad Sintética:** Este es uno de los tipos de fraude de más rápido crecimiento y más difíciles de detectar. Los defraudadores combinan información real (como un número de seguro social válido robado) con información fabricada (nombre, dirección) para crear una identidad completamente nueva que no pertenece a ninguna persona real.3 Estas identidades sintéticas se utilizan para solicitar créditos y luego desaparecer. Los métodos tradicionales de verificación fallan porque partes de la identidad son legítimas. Aquí es donde el Análisis de Redes (Grafos) se vuelve indispensable.46 Un sistema de IA basado en grafos puede analizar miles de solicitudes de nuevas cuentas e identificar conexiones sutiles y no obvias que delatan una red de identidades sintéticas, como múltiples solicitudes que utilizan el mismo dispositivo, la misma dirección IP, o números de teléfono secuenciales.58 Adicionalmente, la IA puede potenciar la verificación de documentos de identidad, utilizando visión por computadora para detectar alteraciones o falsificaciones que serían invisibles al ojo humano.22

### 4.3. Lucha contra el Lavado de Dinero (Anti-Money Laundering - AML)

El cumplimiento de las normativas AML es una de las mayores cargas operativas para los bancos, y la IA ofrece una oportunidad para transformar este proceso de un ejercicio de cumplimiento costoso a una función de inteligencia de riesgos eficiente.

* **Optimización del Monitoreo de Transacciones:** Los sistemas de AML tradicionales, basados en reglas, son notorios por generar una cantidad masiva de falsos positivos. Se estima que hasta el 95% de las alertas generadas no corresponden a una actividad sospechosa real, lo que obliga a los equipos de cumplimiento a invertir una enorme cantidad de tiempo y recursos en investigar transacciones benignas.62 La IA y el  
  *Machine Learning* revolucionan este proceso al introducir la priorización basada en el riesgo. En lugar de generar una alerta binaria, los modelos de IA asignan una puntuación de riesgo a cada cliente o transacción, permitiendo que los analistas enfoquen su atención en el 5% de las alertas que representan un riesgo genuino y elevado.62
* **Detección de Patrones Complejos:** Los lavadores de dinero utilizan esquemas cada vez más complejos para ocultar el origen de los fondos. Técnicas como el "smurfing" (dividir una gran suma de dinero en múltiples depósitos pequeños por debajo del umbral de reporte) o el uso de redes de empresas fantasma son difíciles de detectar con reglas simples.1 Los modelos de IA, especialmente el aprendizaje no supervisado y el análisis de grafos, pueden identificar estos patrones complejos al analizar el comportamiento de una red de cuentas en su conjunto, en lugar de transacciones individuales.2

### 4.4. Mitigación de Riesgos Internos (Fraude Interno)

El fraude no siempre proviene de actores externos. El fraude interno, perpetrado por empleados, representa un riesgo significativo y a menudo pasado por alto. La IA puede aplicar los mismos principios de UEBA utilizados para los clientes externos para monitorear la actividad de los empleados.3 Un sistema de IA puede establecer una línea base del comportamiento normal de cada empleado (sistemas a los que accede, horarios de trabajo, tipos de transacciones que procesa) y generar alertas ante desviaciones significativas. Esto podría incluir el acceso a cuentas de clientes fuera de su cartera, la modificación de registros en horarios inusuales, o la realización de transacciones que se desvían de sus funciones habituales, lo que permite una detección temprana de posibles actividades fraudulentas o maliciosas internas.19

La implementación de estas aplicaciones de IA conduce a una conclusión estratégica fundamental: la IA permite la creación de una visión unificada del riesgo del cliente. Tradicionalmente, un banco opera con sistemas aislados: uno para el fraude de tarjetas, otro para la banca en línea, y un tercero para AML.4 Esta fragmentación en "silos de datos" impide una visión holística del riesgo. Una actividad que parece de bajo riesgo en un canal puede ser una pieza clave de un esquema de fraude mayor cuando se correlaciona con datos de otros canales. Por ejemplo, un pequeño depósito en efectivo (que podría ser una señal de AML), seguido de una transferencia a una nueva cuenta desde un dispositivo inusual (potencialmente ATO), y culminando en una compra de alto valor con la tarjeta asociada (posible fraude de tarjeta), podrían ser vistos como eventos de bajo riesgo por sistemas separados. Sin embargo, una plataforma de IA unificada, alimentada por un "lago de datos" (

*data lake*) que consolida información de todas estas fuentes, reconocería la secuencia completa como un patrón de ataque coordinado y de alto riesgo.9 Por lo tanto, el éxito de la IA en Scotiabank dependerá no solo de la sofisticación de sus algoritmos, sino también de su capacidad para romper estos silos de datos internos y construir una visión 360° del riesgo de cada cliente.

## Ventajas Estratégicas y Operacionales para Scotiabank

La adopción de la Inteligencia Artificial en la prevención del fraude trasciende la mera actualización tecnológica; representa una inversión estratégica que genera valor tangible en múltiples dimensiones del negocio. Al traducir las capacidades técnicas de la IA en resultados de negocio medibles, es posible justificar y priorizar su implementación. Las ventajas se pueden agrupar en tres áreas principales: la mejora de la precisión en la detección, el aumento de la eficiencia operativa y el fortalecimiento de la posición competitiva del banco.

### 5.1. Precisión y Reducción de Falsos Positivos

Una de las ventajas más impactantes de la IA es su capacidad para analizar el contexto completo de una transacción, lo que le confiere una precisión muy superior a la de los sistemas basados en reglas estáticas.4 Un sistema tradicional podría marcar una compra de alto valor realizada en el extranjero como sospechosa. Un sistema de IA, en cambio, puede correlacionar esa transacción con otros datos, como la compra de un boleto de avión a ese destino días antes o el inicio de sesión en la aplicación del banco desde una red Wi-Fi en esa misma ciudad, concluyendo que la transacción es legítima y evitando un bloqueo innecesario.10

Este aumento en la precisión tiene un impacto directo y crucial en la reducción de "falsos positivos". Minimizar las alertas sobre transacciones legítimas genera un triple beneficio:

1. **Mejora la Experiencia del Cliente:** Evitar el rechazo de transacciones válidas es fundamental para la satisfacción y retención del cliente. Un bloqueo innecesario puede generar frustración, vergüenza y, en última instancia, la pérdida del cliente.18
2. **Aumenta los Ingresos:** Cada transacción legítima que se rechaza erróneamente es una venta perdida para el comercio y una oportunidad de ingreso perdida para el banco. La IA ayuda a maximizar la aprobación de transacciones seguras.
3. **Optimiza los Recursos de los Analistas:** Al reducir el "ruido" de las alertas irrelevantes, los analistas de fraude pueden concentrar su tiempo y experiencia en investigar las amenazas genuinas y de alto riesgo, en lugar de malgastar esfuerzos en casos benignos.20 Empresas como Mastercard han reportado una reducción de falsos positivos superior al 85% gracias a la implementación de sus tecnologías de IA de última generación.68

### 5.2. Eficiencia Operativa y Escalabilidad

La IA introduce niveles de automatización y escalabilidad que son inalcanzables con procesos manuales.

* **Automatización Inteligente:** Los sistemas de IA pueden monitorear y analizar millones de transacciones de forma continua, 24 horas al día, 7 días a la semana, sin fatiga ni errores humanos.29 Tareas como la revisión inicial de alertas, la recopilación de datos para una investigación y el reporte de actividades sospechosas pueden ser automatizadas, liberando a los equipos humanos para que se dediquen a tareas de mayor valor añadido, como el análisis estratégico de nuevas tendencias de fraude o la gestión de casos complejos.4
* **Escalabilidad Masiva:** A medida que el volumen de transacciones digitales continúa su crecimiento exponencial, los equipos de revisión manual se convierten en un cuello de botella. Los sistemas de IA, por el contrario, están diseñados para escalar. Pueden procesar volúmenes de datos masivos en tiempo real, permitiendo que el banco crezca y expanda sus servicios digitales sin necesidad de aumentar proporcionalmente su equipo de prevención de fraudes.9

El impacto combinado de la automatización y la escalabilidad se traduce directamente en un aumento de la productividad del equipo de fraude, una reducción de los costos operativos y una mayor agilidad para adaptarse a las demandas del mercado.22

### 5.3. Fortalecimiento de la Confianza y Ventaja Competitiva

En el sector financiero actual, donde los productos y servicios tienden a homogeneizarse, la seguridad y la confianza del cliente se han convertido en diferenciadores competitivos clave.4 Los clientes no solo esperan que su dinero esté seguro; esperan que la seguridad sea proactiva, inteligente y que no interfiera con su experiencia de usuario.

Una estrategia de prevención de fraudes basada en IA, que opera de manera "invisible" y "sin fricciones" para el cliente legítimo, fortalece la percepción de la marca como una entidad tecnológicamente avanzada y confiable.9 Las instituciones que invierten y comunican eficazmente sus capacidades de seguridad basadas en IA no solo se protegen mejor contra las pérdidas, sino que también construyen un capital de marca que atrae y retiene a clientes de alto valor. Se posicionan como líderes en un mercado que valora cada vez más la seguridad digital, convirtiendo un centro de costos (la prevención de fraudes) en un motor de ventaja competitiva.1

En última instancia, el éxito de un programa de IA para la prevención de fraudes no debe medirse únicamente por la cantidad de fraude detenido. La verdadera medida del éxito es un equilibrio optimizado entre tres pilares fundamentales: la **Reducción del Riesgo**, la **Experiencia del Cliente** y la **Eficiencia Operativa**. Un sistema que bloquea todas las transacciones ofrece un riesgo cero, pero destruye el negocio. Un sistema que no bloquea nada ofrece una experiencia sin fricciones, pero maximiza las pérdidas por fraude. Los sistemas tradicionales basados en reglas a menudo obligan a los bancos a hacer una elección difícil entre estos dos extremos. La IA, con su capacidad de análisis contextual y puntuación de riesgo granular, permite a las instituciones financieras encontrar un punto de equilibrio óptimo: mantener tasas de detección de fraude extremadamente altas mientras se minimizan los falsos positivos y se automatizan los procesos.10 Por lo tanto, el Retorno de la Inversión (ROI) de una iniciativa de IA en Scotiabank debe evaluarse no solo en función de las pérdidas por fraude evitadas, sino también considerando la reducción en la deserción de clientes causada por falsos positivos y los ahorros de costos generados en el equipo de analistas.

## Guía de Implementación y Desafíos Críticos

La adopción de la Inteligencia Artificial para la prevención de fraudes es un viaje transformador que requiere una planificación cuidadosa, una ejecución por fases y una comprensión profunda de los desafíos inherentes. No se trata simplemente de adquirir una nueva tecnología, sino de integrar una nueva capacidad en el núcleo de las operaciones del banco.

### 6.1. Hoja de Ruta para la Adopción de IA

Una implementación exitosa puede estructurarse en las siguientes fases, asegurando un enfoque gradual que minimice los riesgos y maximice el valor en cada etapa.9

* **Fase 1: Estrategia y Evaluación de Datos (Meses 1-3)**
  + **Definir Objetivos y Alcance:** Identificar y priorizar los tipos de fraude más críticos para Scotiabank Perú (ej. fraude con tarjetas en comercio electrónico, robo de cuentas, lavado de dinero). Establecer KPIs claros para medir el éxito.
  + **Evaluar la Calidad de los Datos:** Realizar una auditoría exhaustiva de los datos históricos de transacciones, perfiles de clientes y metadatos. Evaluar su completitud, consistencia y precisión. Este es el paso más crítico, ya que la calidad del modelo de IA dependerá directamente de la calidad de los datos de entrada.
  + **Asegurar el Cumplimiento de la Privacidad:** Involucrar al equipo legal y de cumplimiento desde el inicio para garantizar que la recopilación y el uso de datos se adhieran estrictamente a la Ley de Protección de Datos Personales de Perú (N° 29733).
* **Fase 2: Selección de Socio y Prueba Piloto (Meses 4-9)**
  + **Seleccionar un Socio Tecnológico:** Buscar un proveedor con experiencia comprobada en el sector financiero, preferiblemente con conocimiento del mercado latinoamericano. Evaluar la capacidad de integración de su plataforma con los sistemas existentes de Scotiabank.
  + **Realizar una Prueba Piloto (PoC):** Implementar la solución de IA en un entorno controlado y de alcance limitado, como un canal específico (ej. la aplicación móvil) o una región geográfica. El objetivo es validar la efectividad del modelo, medir la reducción de fraudes y la tasa de falsos positivos, y ajustar los umbrales de riesgo.
  + **Recopilar Retroalimentación:** Involucrar a los analistas de fraude en la validación de las alertas generadas por la IA para recopilar su experiencia y mejorar el modelo.
* **Fase 3: Escalado y Optimización Continua (Meses 10-18)**
  + **Escalar por Etapas:** Basándose en los resultados exitosos del piloto, expandir gradualmente la solución a otros canales, productos y mercados. Ajustar los modelos a las particularidades de cada nuevo entorno.
  + **Activar Ciclos de Retroalimentación:** Establecer un proceso formal para que los resultados de las investigaciones manuales (confirmación de fraude o de falso positivo) se reincorporen al sistema. Este ciclo de retroalimentación es esencial para que los modelos de *machine learning* aprendan y mejoren continuamente.
* **Fase 4: Gobernanza, Capacitación y Monitoreo (Continuo)**
  + **Asegurar el Cumplimiento Normativo:** Verificar que la plataforma de IA genere registros de auditoría detallados y explicaciones de sus decisiones, en línea con los requisitos de la SBS y la Ley de IA de Perú.
  + **Capacitar al Equipo Humano:** Desarrollar programas de formación para que los analistas de fraude, los agentes de soporte y los equipos de cumplimiento aprendan a interpretar las alertas de la IA, a utilizar las nuevas herramientas y a colaborar eficazmente con el sistema.
  + **Monitorear y Optimizar:** Medir constantemente los KPIs definidos en la Fase 1. Ajustar los modelos periódicamente para adaptarse a las nuevas tácticas de fraude y a los cambios en el comportamiento de los clientes.

### 6.2. Desafíos Fundamentales a Superar

La implementación de la IA presenta desafíos significativos que deben ser gestionados proactivamente. Estos no son solo de naturaleza técnica, sino también organizacional, cultural y regulatoria.

* **Calidad de los Datos e Infraestructura:** El axioma "basura entra, basura sale" es especialmente cierto para la IA. Los modelos de *machine learning* son tan buenos como los datos con los que se entrenan. Datos incompletos, inconsistentes o que contienen sesgos históricos producirán modelos ineficaces o, peor aún, discriminatorios.4 Además, los sistemas de IA requieren una infraestructura tecnológica robusta, generalmente basada en la nube, con la capacidad de procesar grandes volúmenes de datos (  
  *Big Data*) en tiempo real y con baja latencia. Esto puede requerir una inversión significativa en la modernización de la infraestructura existente.5
* **Talento y Supervisión Humana:** Existe una escasez global de profesionales con las habilidades necesarias para desarrollar, implementar y gestionar sistemas de IA, como científicos de datos e ingenieros de *machine learning*.12 Es crucial entender que la IA no reemplaza a los analistas de fraude, sino que aumenta sus capacidades. La intuición, la experiencia y el juicio crítico de un experto humano siguen siendo indispensables para investigar casos complejos, gestionar excepciones que el modelo no comprende y tomar la decisión final en situaciones de alto riesgo. La IA es una herramienta para potenciar al experto, no para sustituirlo.4
* **Integración con Sistemas Heredados (*Legacy Systems*):** La mayoría de los bancos operan con una combinación de sistemas modernos y sistemas *core* heredados que pueden tener décadas de antigüedad. Integrar una nueva plataforma de IA con esta infraestructura compleja puede ser un desafío técnico significativo, requiriendo APIs robustas y un esfuerzo considerable de ingeniería.4
* **Ética y Sesgos Algorítmicos:** Este es uno de los riesgos más serios. Si los datos históricos utilizados para entrenar un modelo reflejan sesgos sociales existentes (por ejemplo, si ciertos grupos demográficos han sido históricamente objeto de un mayor escrutinio), el modelo de IA puede aprender y amplificar estos sesgos. Esto podría llevar a que el sistema marque injustamente las transacciones de ciertos grupos de clientes con más frecuencia que otros, resultando en discriminación algorítmica y un grave riesgo reputacional y legal.7
* **El Problema de la "Caja Negra" y la IA Explicable (XAI):** Muchos de los modelos de IA más potentes, especialmente los de *Deep Learning*, funcionan como "cajas negras": proporcionan una predicción (ej. "esta transacción es 85% probable de ser fraude"), pero no pueden explicar fácilmente *por qué* llegaron a esa conclusión. Esta opacidad es un problema importante para la auditoría interna, la validación de modelos y el cumplimiento regulatorio.83 La  
  **IA Explicable (XAI)** es un campo emergente que desarrolla técnicas (como LIME y SHAP) para proporcionar transparencia e interpretabilidad a las decisiones de los modelos, mostrando qué factores influyeron más en una predicción determinada.2
* **Marco Regulatorio en Perú:** La implementación de IA en Scotiabank Perú debe navegar un marco regulatorio específico y en evolución. La **Ley N° 31814 (Ley que promueve el uso de la IA)** y su reglamento, aprobado en septiembre de 2025, es la pieza central.86 Esta ley clasifica los sistemas de IA en el sector financiero como de "alto riesgo", lo que implica requisitos estrictos de  
  **supervisión humana, transparencia algorítmica y la existencia de mecanismos de auditoría y reclamación**.13 Además, todo tratamiento de datos debe cumplir con la  
  **Ley de Protección de Datos Personales (N° 29733)**, que exige consentimiento informado y respeto a los principios de finalidad y proporcionalidad.89 Finalmente, la  
  **Superintendencia de Banca, Seguros y AFP (SBS)** juega un rol crucial en la supervisión y se espera que emita normativas más específicas para la gestión de riesgos derivados del uso de modelos de IA en el sector.91

La superación de estos desafíos requiere una visión que vaya más allá de la tecnología. La implementación exitosa de la IA depende de una transformación organizacional y cultural. Un banco puede adquirir la plataforma de IA más avanzada, pero si sus datos son de mala calidad, el proyecto fracasará.11 Si los analistas de fraude no confían en el sistema o no están capacitados para interpretar sus resultados, la tecnología será infrautilizada.9 Si los departamentos de TI, Fraude, Cumplimiento y Negocio no colaboran para romper los silos de datos y procesos, la IA no podrá alcanzar su máximo potencial.67 Por lo tanto, el proyecto de IA en Scotiabank debe ser liderado por un equipo multifuncional que entienda que el éxito depende tanto de la gestión del cambio organizacional como de la excelencia técnica.

La siguiente tabla resume el marco regulatorio clave en Perú, proporcionando una guía de cumplimiento esencial para la gerencia.

| Normativa | Entidad Reguladora Principal | Requisito Clave para IA en Banca | Implicación para Scotiabank |
| --- | --- | --- | --- |
| **Ley N° 31814 y su Reglamento** | Presidencia del Consejo de Ministros (PCM) - Secretaría de Gobierno y Transformación Digital | Clasificación de sistemas de IA en finanzas como de "alto riesgo". Exigencia de supervisión humana, transparencia algorítmica y auditorías.13 | Implementar soluciones de IA Explicable (XAI). Mantener un "humano en el ciclo" para decisiones críticas. Documentar rigurosamente el funcionamiento de los modelos para auditorías. |
| **Ley de Protección de Datos Personales (N° 29733)** | Autoridad Nacional de Protección de Datos Personales (ANPD) | Cumplimiento de los principios de legalidad, consentimiento, finalidad, proporcionalidad y seguridad en todo tratamiento de datos personales.89 | Asegurar que los datos de los clientes utilizados para entrenar modelos de IA sean anonimizados o se cuente con el consentimiento explícito e informado. Diseñar sistemas con "privacidad por diseño". |
| **Regulación de la SBS** | Superintendencia de Banca, Seguros y AFP (SBS) | Supervisión de la gestión de riesgos derivados del uso de modelos. Lucha contra el lavado de activos y financiamiento del terrorismo (LAFT).91 | Validar los modelos de IA según los estándares de gestión de riesgos de la SBS. Asegurar que los sistemas de IA para AML sean efectivos y sus resultados puedan ser reportados a la UIF-Perú. |

## El Futuro de la Lucha contra el Fraude: Tendencias Emergentes

La evolución de la Inteligencia Artificial es constante, y la vanguardia de la tecnología de hoy se convertirá en el estándar de mañana. Para que Scotiabank mantenga una postura de liderazgo en la prevención de fraudes, es crucial no solo implementar las tecnologías actuales, sino también comprender y prepararse para las tendencias emergentes que definirán el futuro de la ciberseguridad financiera.

### 7.1. IA Generativa: Un Arma de Doble Filo

La IA generativa, popularizada por modelos como ChatGPT y las Redes Generativas Adversarias (GANs), presenta tanto una oportunidad monumental como una amenaza creciente.

* **Oportunidad: Creación de Datos Sintéticos:** Uno de los mayores desafíos en el entrenamiento de modelos de IA para la detección de fraudes es la escasez de datos de fraude reales. Por naturaleza, las transacciones fraudulentas son eventos raros en comparación con las legítimas (un problema conocido como "desbalance de clases"). Esto dificulta que los modelos aprendan a reconocerlas eficazmente. La IA generativa, y en particular las GANs, ofrece una solución poderosa: la **generación de datos sintéticos**.93 Una GAN consta de dos redes neuronales que compiten entre sí: un "generador" que crea datos falsos (ej. transacciones fraudulentas sintéticas) y un "discriminador" que intenta distinguir los datos falsos de los reales. A través de este proceso adversarial, el generador aprende a crear datos sintéticos extremadamente realistas.95 Estos datos pueden usarse para aumentar los conjuntos de entrenamiento, permitiendo que los modelos de detección de fraude se entrenen en una variedad mucho mayor de escenarios fraudulentos, mejorando su robustez y precisión sin comprometer la privacidad de los datos de clientes reales.74
* **Amenaza: Sofisticación de los Ataques:** El mismo poder de la IA generativa está siendo explotado por los defraudadores. Ya se están utilizando para generar textos de *phishing* personalizados y gramaticalmente perfectos, crear *deepfakes* de voz para engañar a los centros de atención al cliente y a los clientes en estafas de ingeniería social, y producir imágenes y videos falsos para crear identidades sintéticas convincentes. Esta tendencia obliga a las instituciones financieras a desarrollar defensas de IA aún más avanzadas, capaces de detectar estas manipulaciones sutiles.14

### 7.2. Aprendizaje Federado (Federated Learning): Hacia una Defensa Colectiva

El fraude, especialmente el crimen organizado, no opera dentro de los límites de una sola institución financiera. Las redes de lavado de dinero y los anillos de fraude de identidad sintética a menudo abarcan múltiples bancos. Sin embargo, la colaboración entre bancos ha sido históricamente limitada por las regulaciones de privacidad y la confidencialidad comercial.

* **Concepto:** El Aprendizaje Federado es un enfoque de *machine learning* que permite entrenar un modelo de IA de forma colaborativa en datos descentralizados, sin que los datos brutos abandonen nunca los servidores seguros de cada institución participante.99 El proceso funciona de la siguiente manera: un modelo de IA global se envía a cada banco participante. Cada banco entrena este modelo localmente con sus propios datos de transacciones. Luego, en lugar de enviar los datos de vuelta, solo se envían las actualizaciones del modelo (los "aprendizajes" o parámetros, de forma anónima y agregada) a un servidor central. Este servidor combina las actualizaciones de todos los participantes para crear una versión mejorada del modelo global, que luego se distribuye de nuevo a los bancos. Este ciclo se repite, mejorando continuamente el modelo con la inteligencia colectiva de todo el ecosistema.101
* **Potencial:** Esta técnica tiene el potencial de revolucionar la prevención del fraude. Un modelo entrenado con los patrones de fraude y comportamiento de todo el sistema bancario peruano sería exponencialmente más poderoso y preciso que un modelo entrenado únicamente con los datos de Scotiabank. Permitiría detectar redes de fraude que operan a través de múltiples instituciones con una eficacia sin precedentes, creando una defensa colectiva contra amenazas compartidas.99

### 7.3. Ataques Adversariales: La Carrera Armamentista de la IA

A medida que los sistemas de detección de fraudes basados en IA se vuelven más comunes, los atacantes han comenzado a desarrollar técnicas para engañarlos activamente.

* **Concepto:** Un ataque adversarial consiste en crear "ejemplos adversariales", que son entradas de datos (por ejemplo, los detalles de una transacción) que han sido modificadas de forma muy sutil e intencionada. Estas modificaciones son a menudo imperceptibles para un ser humano, pero están diseñadas específicamente para explotar las debilidades de un modelo de *machine learning* y hacer que clasifique erróneamente una transacción fraudulenta como legítima.102 Es el equivalente digital de un camuflaje diseñado para ser invisible a los sensores de la IA.
* **Implicación:** La existencia de ataques adversariales significa que ya no es suficiente que un modelo de IA sea simplemente "preciso" en un conjunto de datos de prueba. También debe ser **robusto** y **resiliente** a la manipulación deliberada. Esto ha dado lugar a un nuevo campo de investigación en ciberseguridad de la IA, centrado en el "entrenamiento adversarial". Esta técnica consiste en entrenar los modelos de detección de fraude no solo con datos normales y fraudulentos, sino también con ejemplos adversariales generados artificialmente. Al "vacunar" al modelo contra este tipo de ataques durante su entrenamiento, se aumenta su capacidad para resistir intentos de engaño en un entorno de producción real.102

Estas tendencias emergentes pintan un cuadro claro del futuro de la prevención del fraude. No se tratará de encontrar un único modelo de IA "perfecto", sino de construir un ecosistema de defensa que sea ágil, colaborativo y resiliente. La IA generativa resolverá el problema de la escasez de datos de entrenamiento, pero al mismo tiempo creará amenazas más sofisticadas. El Aprendizaje Federado abordará el problema de los silos de datos entre instituciones, permitiendo una visión de riesgo a nivel de todo el sistema financiero. Y la amenaza de los Ataques Adversariales subraya que la defensa debe ser un proceso continuo de adaptación y fortalecimiento, no un estado estático.

El sistema de prevención de fraudes ideal del futuro probablemente combinará estas tres tendencias: utilizará el **Aprendizaje Federado** para entrenar un modelo base robusto con la inteligencia colectiva de la industria; este modelo será continuamente validado y mejorado con **datos sintéticos** generados por IA para simular las últimas tácticas de fraude; y estará construido desde cero con técnicas de **entrenamiento adversarial** para ser resistente a la manipulación. Para Scotiabank, esto significa que la estrategia a largo plazo debe incluir la exploración activa de estas fronteras tecnológicas, ya sea a través de pruebas de concepto internas o participando en consorcios de la industria. El liderazgo en la prevención de fraudes del mañana se definirá por la capacidad de dominar estas capacidades emergentes.

## Recomendaciones Estratégicas para Scotiabank Perú

Basado en el análisis exhaustivo de las capacidades de la Inteligencia Artificial, el panorama actual del fraude, los desafíos de implementación y las tendencias futuras, se presenta el siguiente conjunto de recomendaciones estratégicas diseñadas para guiar a Scotiabank Perú en la adopción de una postura de liderazgo en la prevención de fraudes impulsada por IA.

1. Establecer una Gobernanza de IA Centralizada y Multifuncional:  
   La implementación de la IA no es un proyecto exclusivamente tecnológico; es una transformación empresarial. Se recomienda la creación de un Centro de Excelencia de IA (CoE). Este equipo debe ser multifuncional, integrando a líderes y expertos de las áreas de Prevención de Fraude, Riesgos, Tecnología de la Información (TI), Cumplimiento Normativo, Legal y las unidades de negocio. Las responsabilidades de este CoE incluirían: definir la estrategia de IA del banco, supervisar la implementación de proyectos, establecer políticas de gobernanza de datos, gestionar los riesgos éticos y de sesgo, y asegurar la alineación continua con los objetivos estratégicos de Scotiabank.
2. Iniciar con un Caso de Uso de Alto Impacto y Alcance Definido:  
   En lugar de intentar una transformación a gran escala desde el principio, se aconseja adoptar un enfoque ágil y comenzar con un proyecto piloto enfocado en un área de alto impacto y riesgo conocido. El análisis del sector financiero peruano sugiere que el fraude en transacciones de comercio electrónico (sin tarjeta presente) es un punto de partida ideal debido a su alta vulnerabilidad.106 La implementación de un modelo de  
   *Machine Learning* para la puntuación de riesgo en tiempo real en este canal permitiría obtener resultados medibles rápidamente, generar aprendizajes valiosos sobre el proceso de implementación y demostrar el valor de la tecnología a los *stakeholders* internos, facilitando la aprobación de futuras inversiones.
3. Priorizar la Calidad y Gobernanza de los Datos como Proyecto Fundacional:  
   Ninguna iniciativa de IA puede tener éxito sin una base de datos sólida. Se recomienda encarecidamente que, antes de la implementación de cualquier modelo, se lleve a cabo una auditoría exhaustiva de los activos de datos del banco, incluyendo datos transaccionales, de comportamiento del cliente y metadatos de dispositivos. Es crucial invertir en herramientas y procesos para la limpieza, normalización, enriquecimiento e integración de datos. Establecer un marco de gobernanza de datos claro, que defina la propiedad, los estándares de calidad y los controles de acceso, es el cimiento indispensable sobre el cual se construirán todas las capacidades futuras de IA.11
4. Desarrollar un Plan de Talento Híbrido: Capacitación Interna y Contratación Estratégica:  
   El éxito a largo plazo dependerá del talento humano. Se propone un enfoque híbrido. Por un lado, lanzar programas de capacitación y recualificación (upskilling) para los analistas de fraude y los equipos de riesgo actuales. El objetivo no es convertirlos en científicos de datos, sino en "consumidores inteligentes" de IA, capaces de interpretar los resultados de los modelos, colaborar con los sistemas y aplicar su juicio experto.12 Por otro lado, realizar contrataciones estratégicas de talento especializado en ciencia de datos, ingeniería de  
   *Machine Learning* y análisis de grafos, preferiblemente con experiencia en el sector financiero, para liderar el desarrollo técnico.12
5. Exigir y Priorizar la IA Explicable (XAI) desde el Diseño:  
   Dada la naturaleza de "alto riesgo" de los sistemas de IA en finanzas según el marco regulatorio peruano (Ley 31814) y la necesidad de validación por parte de la auditoría interna y la SBS, la explicabilidad no es una opción, sino un requisito.13 Al evaluar y seleccionar socios tecnológicos o al desarrollar modelos internos, Scotiabank debe exigir que las soluciones incorporen capacidades de  
   **IA Explicable (XAI)**. Esto significa que el sistema debe ser capaz de proporcionar una justificación clara y comprensible de por qué una transacción fue marcada como fraudulenta, identificando los factores de riesgo que más influyeron en la decisión. Esta transparencia es fundamental para el cumplimiento normativo, la gestión de riesgos y la generación de confianza en la tecnología.2
6. Liderar la Exploración de la Colaboración Sectorial a través del Aprendizaje Federado:  
   Para abordar las redes de fraude que operan a través de múltiples instituciones, Scotiabank Perú tiene la oportunidad de posicionarse como un líder innovador en el mercado. Se recomienda iniciar conversaciones proactivas con otras instituciones financieras líderes en el país, así como con la Asociación de Bancos del Perú (ASBANC) y la propia SBS, para explorar la viabilidad de un consorcio de Aprendizaje Federado. Liderar una iniciativa piloto para entrenar un modelo de detección de fraude colaborativo, que respete la privacidad de los datos de cada entidad, no solo proporcionaría a Scotiabank acceso a un modelo mucho más potente, sino que también establecería un nuevo estándar de seguridad para todo el ecosistema financiero peruano.

## Apéndice: Casos de Estudio Relevantes

El análisis de casos de éxito de líderes de la industria y de iniciativas locales proporciona una perspectiva práctica sobre la implementación y el impacto de la Inteligencia Artificial en la prevención del fraude.

* Mastercard: Liderazgo a través de la IA Integral  
  Mastercard ha integrado la IA en el núcleo de su estrategia de seguridad con su plataforma Decision Intelligence. Este sistema analiza cientos de puntos de datos por transacción en tiempo real, incluyendo el comportamiento del titular de la tarjeta, el dispositivo y el comercio, para generar una puntuación de riesgo precisa.107 La implementación de esta tecnología ha permitido a la compañía reducir los "falsos positivos" (transacciones legítimas rechazadas) en un 50%, mejorando significativamente la experiencia del cliente.107 Más recientemente, Mastercard ha incorporado  
  **IA generativa y análisis de grafos** para identificar proactivamente tarjetas de crédito comprometidas que se venden en la *dark web*, incluso antes de que se utilicen para cometer fraude, duplicando la tasa de detección previa.59 Su nueva tecnología, Decision Intelligence Pro, promete aumentar las tasas de detección de fraude en un promedio del 20% y reducir los falsos positivos en más de un 85%.68
* Visa: Inversión Masiva en Seguridad Predictiva  
  Visa ha invertido más de $12 mil millones en los últimos cinco años en tecnología para prevenir el fraude, con la IA como pilar central.110 Sus soluciones  
  **Visa Advanced Authorization (VAA)** y **Visa Protect** utilizan modelos de *deep learning* para analizar más de 500 atributos de riesgo en cada transacción en menos de 50 milisegundos.111 Se estima que esta tecnología ayuda a prevenir más de $26 mil millones en fraudes anualmente a nivel global.111 En América Latina, Visa ha demostrado su capacidad de adaptación al colaborar con COELSA en Argentina para personalizar su solución Visa Protect para el ecosistema de Pagos en Tiempo Real (RTP) de ese país, demostrando la viabilidad de implementar estas tecnologías avanzadas en el contexto regional.112
* BBVA: Enfoque Global y Fomento de la Innovación Interna  
  BBVA ha adoptado un enfoque estratégico y global para la lucha contra el crimen financiero, creando una unidad especializada denominada Financial Crime Prevention. En México, la aplicación de IA ha sido clave para reducir los intentos de fraude con tarjetas a niveles significativamente por debajo del promedio de América Latina (0.054% frente al 0.13% regional).113 Además de implementar soluciones tecnológicas, BBVA fomenta activamente la innovación interna a través de iniciativas como la competición "BBVA Bot Talent", donde los propios empleados proponen y desarrollan casos de uso para la IA, incluyendo herramientas para que los agentes de ciberseguridad puedan detectar si un mensaje de  
  *phishing* es fraudulento.114
* Santander: IA como Motor de Eficiencia y Estrategia Futura  
  Banco Santander ha cuantificado el impacto de la IA en su eficiencia operativa, reportando ahorros superiores a 200 millones de euros en 2024 gracias a diversas iniciativas de IA, incluyendo la detección de fraude.115 La entidad está acelerando su transformación digital con el objetivo de convertirse en un "banco nativo en IA", y para ello ha firmado un acuerdo estratégico con OpenAI, la empresa detrás de ChatGPT. Este movimiento subraya la visión de Santander de integrar la IA no solo como una herramienta de defensa, sino como el núcleo de sus operaciones futuras, desde el riesgo de crédito hasta el marketing.117
* **Casos en América Latina y Perú: Potencial y Desafíos**
  + **Nubank:** La *fintech* brasileña, uno de los bancos digitales más grandes del mundo con presencia en México y Colombia, es un caso de éxito emblemático del uso de la IA en América Latina. Utiliza algoritmos de IA desde su concepción para analizar millones de transacciones en tiempo real, no solo para detectar fraudes, sino también para personalizar la experiencia del cliente y realizar evaluaciones de crédito más inclusivas.118
  + **Prototipo en un Banco Peruano:** Un trabajo de suficiencia profesional de 2020 detalla la aplicación de un prototipo de detección de fraudes con tarjetas de crédito en un banco peruano, enfocado en el canal de comercio electrónico.106 Utilizando el algoritmo de  
    *Machine Learning* **Random Forest**, el modelo inicial alcanzó una precisión del 48.10% con una tasa de falsos positivos de 4.35. Aunque estos resultados iniciales son modestos, el estudio destaca el potencial de la tecnología y subraya un punto crítico: la precisión de los modelos mejora progresivamente a medida que se alimentan con un mayor volumen de datos transaccionales. Este caso local sirve como una valiosa lección sobre la importancia de comenzar, recopilar datos y refinar los modelos de forma iterativa.106

#### Obras citadas

1. Aplicaciones prácticas de Inteligencia Artificial para detectar fraudes, prevenir lavado de dinero y evaluar riesgos crediticios en el sector bancario panameño - PwC, fecha de acceso: octubre 2, 2025, <https://www.pwc.com/ia/es/publicaciones/perspectivas-pwc/aplicaciones-practicas-de-inteligencia-artificial.html>
2. Estrategias de IA para la Detección y Prevención del Fraude - Asociación ICPF, fecha de acceso: octubre 2, 2025, <https://asociacionicpf.org/noticias/estrategias-de-ia-para-la-deteccion-y-prevencion-del-fraude/>
3. Así se aplica la IA en la detección de fraudes en el sector bancario - Forbes España, fecha de acceso: octubre 2, 2025, <https://forbes.es/tecnologia/699969/asi-se-aplica-la-ia-en-la-deteccion-de-fraudes-en-el-sector-bancario/>
4. ¿Qué capacidades aporta la Inteligencia Artificial en la lucha contra ..., fecha de acceso: octubre 2, 2025, <https://latinia.com/es/resources/inteligencia-artificial-para-prevenir-fraude-bancario>
5. La IA como herramienta en la prevención del fraude financiero - OpenExpo Europe, fecha de acceso: octubre 2, 2025, <https://openexpoeurope.com/es/la-ia-como-herramienta-en-la-prevencion-del-fraude-financiero/>
6. IA para la Detección de Fraudes | Caso de Uso - NVIDIA, fecha de acceso: octubre 2, 2025, <https://www.nvidia.com/es-la/use-cases/ai-for-fraud-detection/>
7. Detección del fraude con IA en el sector bancario - IBM, fecha de acceso: octubre 2, 2025, <https://www.ibm.com/es-es/think/topics/ai-fraud-detection-in-banking>
8. The 5 benefits of financial fraud detection with AI - Adviters, fecha de acceso: octubre 2, 2025, <https://adviters.com/sp/finance/financial-fraud-detection-with-artificial-intelligence/>
9. Prevención de fraude: cómo proteger la operación financiera con IA - Topaz, fecha de acceso: octubre 2, 2025, <https://www.topazevolution.com/es/blog/prevencion-de-fraude-bancario>
10. El rol de la inteligencia artificial (IA) en la detección de fraude - FinTech México, fecha de acceso: octubre 2, 2025, <https://www.fintechmexico.org/notices/el-rol-de-la-inteligencia-artificial-ia-en-la-deteccion-de-fraude-estadisticas-y-aplicaciones-claves>
11. AI Data Quality | Econ One Data Analytics, fecha de acceso: octubre 2, 2025, <https://econone.com/es/data-analytics/resources/blogs/ai-data-quality/>
12. La banca, a la cola en el uso de IA para la gestión del talento, fecha de acceso: octubre 2, 2025, <https://www.rrhhdigital.com/secciones/actualidad/779859/la-banca-a-la-cola-en-el-uso-de-ia-para-la-gestion-del-talento/>
13. La Inteligencia Artificial para el otorgamiento de créditos: ¿inclusión ..., fecha de acceso: octubre 2, 2025, <https://tytl.com.pe/la-inteligencia-artificial-para-el-otorgamiento-de-creditos-inclusion-o-exclusion-financiera/>
14. Tendencias de Fraude con IA 2025: Los Bancos Contraatacan | Feedzai, fecha de acceso: octubre 2, 2025, <https://www.feedzai.com/es/pressrelease/tendencias-de-fraude-con-ia-2025/>
15. Identifica cómo la IA es usada para hacer fraudes digitales | Blog | Scotiabank México, fecha de acceso: octubre 2, 2025, <https://www.scotiabank.com.mx/blog/para-ti-identifica-como-la-ia-es-usada-para-hacer-fraudes-digitales>
16. Suplantación de identidad con IA: cómo protegerte del fraude - Mitek Systems, fecha de acceso: octubre 2, 2025, <https://www.miteksystems.com/es/blog/fraude-digital-inteligencia-artificial-generativa>
17. Riesgos de Seguridad de la Inteligencia Artificial, fecha de acceso: octubre 2, 2025, <https://dpss.lacounty.gov/es/resources/awareness/cybersecurity-awareness/artificial-intelligence.html>
18. Una guía sobre machine learning y detección de fraude - Vass Company, fecha de acceso: octubre 2, 2025, <https://vasscompany.com/es/insights/blogs-articles/deteccion-fraude-machine-learning/>
19. El papel de la auditoría interna en la detección del fraude mediante IA - Wolters Kluwer, fecha de acceso: octubre 2, 2025, <https://www.wolterskluwer.com/es/expert-insights/internal-audits-role-ai-fraud-detection>
20. Cómo la IA reduce los falsos positivos en la detección de fraudes - Inaza, fecha de acceso: octubre 2, 2025, <https://www.inaza.com/es/blog/how-ai-reduces-false-positives-in-fraud-detection>
21. La nueva era de la ciberseguridad: cómo la IA ayudará a la ... - BBVA, fecha de acceso: octubre 2, 2025, <https://www.bbva.com/es/innovacion/la-nueva-era-de-la-ciberseguridad-como-la-ia-ayudara-a-la-prevencion-del-fraude-en-2025/>
22. Cómo la Inteligencia Artificial permite evitar fraudes financieros - Embat, fecha de acceso: octubre 2, 2025, <https://www.embat.io/blog/como-la-inteligencia-artificial-permite-evitar-fraudes-financieros>
23. Prevención de fraude: cómo proteger la operación financiera con IA - Topaz, fecha de acceso: octubre 2, 2025, <https://www.topazevolution.com/es/blog/prevencion-de-fraude-bancario?hsLang=es>
24. Detección de fraude con IA en la banca - IBM, fecha de acceso: octubre 2, 2025, <https://www.ibm.com/mx-es/think/topics/ai-fraud-detection-in-banking>
25. Los piratas informáticos utilizan la IA para facilitar el robo de identidad - Forbes España, fecha de acceso: octubre 2, 2025, <https://forbes.es/tecnologia/757724/los-piratas-informaticos-utilizan-la-ia-para-facilitar-el-robo-de-identidad/>
26. Cómo la IA transforma la detección de fraude en tiempo real - Truora Blog, fecha de acceso: octubre 2, 2025, <https://blog.truora.com/es/c%C3%B3mo-la-ia-transforma-la-detecci%C3%B3n-de-fraude-en-tiempo-real>
27. Fraud Detection with Machine Learning | FICO, fecha de acceso: octubre 2, 2025, <https://www.fico.com/es/glossary/fraud-detection-machine-learning>
28. Guía sobre detección de fraude con machine learning - Stripe, fecha de acceso: octubre 2, 2025, <https://stripe.com/es/resources/more/how-machine-learning-works-for-payment-fraud-detection-and-prevention>
29. Machine learning para detectar el fraude: Cómo usarlo - SEON, fecha de acceso: octubre 2, 2025, <https://seon.io/es/recursos/machine-learning-para-detectar-fraude/>
30. Estudio de la prevención y detección de fraudes financieros a través de técnicas de aprendizaje automático - Revistas PUC-SP, fecha de acceso: octubre 2, 2025, <https://revistas.pucsp.br/index.php/CAFI/article/download/58372/42906/200547>
31. Advancing fraud detection through deep learning: A comprehensive review - WJAETS, fecha de acceso: octubre 2, 2025, <https://wjaets.com/sites/default/files/WJAETS-2024-0332.pdf>
32. Deep Learning Techniques for Financial Fraud Detection - ResearchGate, fecha de acceso: octubre 2, 2025, <https://www.researchgate.net/publication/359264071_Deep_Learning_Techniques_for_Financial_Fraud_Detection>
33. How AI Detects Financial Fraud: A Review of Emerging Deep Learning Methods - OSF, fecha de acceso: octubre 2, 2025, <https://osf.io/5yjm4_v1/download/?format=pdf>
34. Year-over-Year Developments in Financial Fraud Detection via Deep Learning: A Systematic Literature Review - arXiv, fecha de acceso: octubre 2, 2025, <https://arxiv.org/html/2502.00201v2>
35. (PDF) Deep Learning for Credit Card Fraud Detection: A Review of ..., fecha de acceso: octubre 2, 2025, <https://www.researchgate.net/publication/382187222_Deep_Learning_for_Credit_Card_Fraud_Detection_A_Review_of_Algorithms_Challenges_and_Solutions>
36. Credit Card Fraud Detection with Deep Learning Techniques - ResearchGate, fecha de acceso: octubre 2, 2025, <https://www.researchgate.net/publication/388459328_Credit_Card_Fraud_Detection_with_Deep_Learning_Techniques>
37. Credit Card Fraud Detection based on Deep Learning Models | Mesopotamian Journal of Computer Science, fecha de acceso: octubre 2, 2025, <https://mesopotamian.press/journals/index.php/cs/article/view/666>
38. Anomaly Detection in Time Series Data using LSTM Autoencoders ..., fecha de acceso: octubre 2, 2025, <https://medium.com/@zhonghong9998/anomaly-detection-in-time-series-data-using-lstm-autoencoders-51fd14946fa3>
39. Credit Card Fraud Detection: A Deep Learning Approach - arXiv, fecha de acceso: octubre 2, 2025, <https://arxiv.org/html/2409.13406v1>
40. Algoritmos de detección de anomalías con redes profundas. Revisión para detección de fraudes bancarios - Redalyc, fecha de acceso: octubre 2, 2025, <https://www.redalyc.org/journal/3783/378370462015/html/>
41. LSTM AutoEncoder for Finance Anomaly Detection - Kaggle, fecha de acceso: octubre 2, 2025, <https://www.kaggle.com/code/hughiephan/lstm-autoencoder-for-finance-anomaly-detection>
42. Anomaly Prediction Based On LSTM And Autoencoders Using Federated Learning In Financial Transactions- Survey | International Journal of Environmental Sciences, fecha de acceso: octubre 2, 2025, <https://theaspd.com/index.php/ijes/article/view/2674>
43. Comprender el procesamiento del lenguaje natural: una guía - SAP, fecha de acceso: octubre 2, 2025, <https://www.sap.com/spain/resources/what-is-natural-language-processing>
44. ¿Qué es el PLN (procesamiento del lenguaje natural)? - IBM, fecha de acceso: octubre 2, 2025, <https://www.ibm.com/es-es/think/topics/natural-language-processing>
45. ¿Qué es PNL o procesamiento del lenguaje natural? | Proofpoint ES, fecha de acceso: octubre 2, 2025, <https://www.proofpoint.com/es/threat-reference/natural-language-processing>
46. Riesgos de la Inteligencia Artificial: fraudes y robo de identidad, fecha de acceso: octubre 2, 2025, <https://blog.bancolombia.com/tendencias/riesgos-inteligencia-artificial/>
47. Procesamiento de lenguaje natural en la detección de fraudes en facturas del municipio de Sao Paulo (parte 1) | Centro Interamericano de Administraciones Tributarias, fecha de acceso: octubre 2, 2025, <https://www.ciat.org/ciatblog-procesamiento-de-lenguaje-natural-en-la-deteccion-de-fraudes-en-facturas-del-municipio-de-sao-paulo-parte-1/>
48. El papel del procesamiento del lenguaje natural (PLN) en la detección y prevención del fraude en seguros | Shaip, fecha de acceso: octubre 2, 2025, <https://es.shaip.com/blog/nlp-in-insurance-fraud-detection/>
49. ¿Qué es el análisis de comportamiento de usuarios y entidades ..., fecha de acceso: octubre 2, 2025, <https://www.microsoft.com/es-es/security/business/security-101/what-is-user-entity-behavior-analytics-ueba>
50. Qué es el análisis del comportamiento del usuario (UBA) - IBM, fecha de acceso: octubre 2, 2025, <https://www.ibm.com/es-es/topics/user-behavior-analytics>
51. Desarrollos de IA en la Detección de Fraude: Más Allá de los Algoritmos - XofoSol, fecha de acceso: octubre 2, 2025, <https://xofosol.com/posts/desarrollos-ia-deteccion-fraude>
52. Analisis de comportamiento de usuarios – VirtualSecure.cl, fecha de acceso: octubre 2, 2025, <https://virtualsecure.cl/analisis-de-comportamiento-de-usuarios/>
53. Analítica de Usuario (UEBA): Descubre qué es y cómo funciona - A3Sec, fecha de acceso: octubre 2, 2025, <https://a3sec.com/blog/ueba-que-es-y-como-funciona>
54. Detección de fraude ¿Cómo usar el aprendizaje automático (IA) en bancos y fintechs?, fecha de acceso: octubre 2, 2025, <https://uflow.biz/blog/deteccion-de-fraude-usar-el-aprendizaje-automatico-ia-en-bancos-fintechs/>
55. 6 buenas prácticas para prevenir el fraude financiero utilizando Inteligencia Artificial, fecha de acceso: octubre 2, 2025, <https://blog.fintechamericas.co/6-buenas-practicas-para-prevenir-el-fraude-financiero-utilizando-inteligencia-artificial>
56. Leveraging Predictive Analytics for Fraud Detection and Prevention, fecha de acceso: octubre 2, 2025, <https://www.tookitaki.com/compliance-hub/leveraging-predictive-analytics-for-fraud-detection-and-prevention>
57. ¿Qué es el análisis del fraude? Técnicas, flujos de trabajo y ..., fecha de acceso: octubre 2, 2025, <https://www.datacamp.com/es/blog/fraud-analytics>
58. Detección y prevención del fraude en banca y FinTech - Innowise, fecha de acceso: octubre 2, 2025, <https://innowise.com/es/blog/financial-fraud-detection-software/>
59. Mastercard acelera la detección del fraude en tarjetas gracias a la tecnología IA Generativa, fecha de acceso: octubre 2, 2025, <https://www.mastercard.com/news/latin-america/es/sala-de-prensa/comunicados-de-prensa/pr-es/2024/mayo/mastercard-acelera-la-deteccion-del-fraude-en-tarjetas-gracias-a-la-tecnologia-ia-generativa/>
60. Detección de fraude | Machine Learning | Amazon Web Services, fecha de acceso: octubre 2, 2025, <https://aws.amazon.com/es/ai/use-cases/fraud-detection/>
61. Cómo evitar el robo de identidad con el uso de Inteligencia Artificial - NAAT.TECH, fecha de acceso: octubre 2, 2025, <https://www.naat.tech/blog/uso-de-inteligencia-artificial-para-reducir-el-robo-de-identidad>
62. IA contra el lavado de dinero | Google Cloud, fecha de acceso: octubre 2, 2025, <https://cloud.google.com/anti-money-laundering-ai?hl=es-419>
63. Inteligencia artificial (IA): el nuevo aliado de los bancos en la lucha contra el lavado de activos | - Cumplo360, fecha de acceso: octubre 2, 2025, <https://cumplo360.com/es/ia-en-plaft/>
64. Machine Learning y su rol en la detección de fraudes y cumplimiento contra el lavado de dinero - InfoSol, fecha de acceso: octubre 2, 2025, <https://infosol.com.mx/machine-learning-y-su-rol-en-la-deteccion-de-fraudes-y-cumplimiento-contra-el-lavado-de-dinero/>
65. Descripción general de la IA contra el lavado de dinero | Anti Money Laundering AI, fecha de acceso: octubre 2, 2025, <https://cloud.google.com/financial-services/anti-money-laundering/docs/concepts/overview?hl=es-419>
66. Prevención de fraudes y lavado de dinero: ¿cómo hacerlo con IA? - Topaz, fecha de acceso: octubre 2, 2025, <https://www.topazevolution.com/es/blog/prevencion-y-lavado-de-dinero>
67. Prevención de Fraude con IA para Bancos y Fintechs de América Latina 2025, fecha de acceso: octubre 2, 2025, <https://www.galileo-ft.com/es/blog/prevencion-fraude-ia-bancos-fintechs-america-latina/>
68. Mastercard supercharges consumer protection with gen-AI, fecha de acceso: octubre 2, 2025, <https://www.mastercard.com/news/press/2024/february/mastercard-supercharges-consumer-protection-with-gen-ai/>
69. IA en la detección de fraudes: Cómo proteger a tu negocio (2025) - Darwin Blog, fecha de acceso: octubre 2, 2025, <https://blog.getdarwin.ai/es/deteccion-de-fraudes>
70. 7 beneficios de la IA en seguridad financiera - Blog Nu Mexico, fecha de acceso: octubre 2, 2025, <https://blog.nu.com.mx/seguridad-en-linea/consejos-de-seguridade/beneficios-ia-seguridad-financiera/>
71. IA en detección de fraudes: cómo prevenir riesgos en empresas y finanzas - aggity, fecha de acceso: octubre 2, 2025, <https://aggity.com/ia-en-deteccion-de-fraudes-financieros/>
72. Avances en el uso de inteligencia artificial para la mejora del control y la detección de fraudes en organizacionesAdvances in the use of artificial intelligence to improve control and fraud detection in organizations - ResearchGate, fecha de acceso: octubre 2, 2025, <https://www.researchgate.net/publication/384574957_Avances_en_el_uso_de_inteligencia_artificial_para_la_mejora_del_control_y_la_deteccion_de_fraudes_en_organizacionesAdvances_in_the_use_of_artificial_intelligence_to_improve_control_and_fraud_detection>
73. IA en el Sector Financiero: Beneficios, Innovación y Seguridad - Bambu Mobile, fecha de acceso: octubre 2, 2025, <https://bambu-mobile.com/ia-en-el-sector-financiero/>
74. Cómo la IA puede ayudar en la prevención del fraude | Cognizant ..., fecha de acceso: octubre 2, 2025, <https://www.cognizant.com/es/es/insights/blog/articles/como-la-ia-puede-ayudar-en-la-prevencion-del-fraude>
75. Datos preparados para la IA: claves para captar su valor - Gartner, fecha de acceso: octubre 2, 2025, <https://www.gartner.es/es/articulos/datos-preparados-para-la-ia>
76. ¿Qué es la inteligencia artificial (IA) en finanzas? - IBM, fecha de acceso: octubre 2, 2025, <https://www.ibm.com/es-es/think/topics/artificial-intelligence-finance>
77. Soluciones de IA para Industrias Financieras - NVIDIA, fecha de acceso: octubre 2, 2025, <https://www.nvidia.com/es-la/industries/finance/>
78. Inteligencia Artificial en la Banca: Una Perspectiva Integral para 2024 | Latinia, fecha de acceso: octubre 2, 2025, <https://latinia.com/es/resources/inteligencia-artificial-banca-perspectiva-integral-2024>
79. IA en el sector bancario - IBM, fecha de acceso: octubre 2, 2025, <https://www.ibm.com/mx-es/think/topics/ai-in-banking>
80. Revista de Estabilidad Financiera n.º 47 - Otoño 2024. La inteligencia artificial en el sistema financiero: implicaciones y av - Banco de España, fecha de acceso: octubre 2, 2025, <https://www.bde.es/f/webbe/GAP/Secciones/Publicaciones/InformesBoletinesRevistas/RevistaEstabilidadFinanciera/24/1_REF47_Artificial.pdf>
81. Riesgos de sesgo y discriminación en Inteligencia Artificial (IA) - BDO, fecha de acceso: octubre 2, 2025, <https://www.bdo.es/es-es/blogs-es/coordenadas-bdo/riesgos-de-sesgo-y-discriminacion-en-inteligencia-artificial-(ia)>
82. ¿Qué es el sesgo algorítmico? | IBM, fecha de acceso: octubre 2, 2025, <https://www.ibm.com/mx-es/think/topics/algorithmic-bias>
83. IA Explicable (XAI): Cómo Confiar en la IA en 2025 - Blog de Bismart, fecha de acceso: octubre 2, 2025, <https://blog.bismart.com/ia-explicable-confianza-empresarial>
84. ¿Qué es la IA explicable (XAI)? | IBM, fecha de acceso: octubre 2, 2025, <https://www.ibm.com/mx-es/think/topics/explainable-ai>
85. IA explicable (XAI): Hacer transparentes las decisiones sobre IA, fecha de acceso: octubre 2, 2025, <https://focalx.ai/es/inteligencia-artificial-es/ia-explicable-xai-hacer-transparentes-las-decisiones-sobre-ia/>
86. Ley N.° 31814 - Normas y documentos legales - Congreso de la ..., fecha de acceso: octubre 2, 2025, <https://www.gob.pe/institucion/congreso-de-la-republica/normas-legales/4565760-31814>
87. Gobierno aprobó el Reglamento de la Ley que promueve el uso de la Inteligencia Artificial, fecha de acceso: octubre 2, 2025, <https://www.gob.pe/institucion/pcm/noticias/1243553-gobierno-aprobo-el-reglamento-de-la-ley-que-promueve-el-uso-de-la-inteligencia-artificial>
88. Perú reglamenta el uso de la IA, para promover el desarrollo ..., fecha de acceso: octubre 2, 2025, <https://www.swissinfo.ch/spa/per%C3%BA-reglamenta-el-uso-de-la-ia,-para-promover-el-desarrollo-econ%C3%B3mico-y-social-del-pa%C3%ADs/89984827>
89. Impacto de la Ley de Protección de Datos Personales en la ..., fecha de acceso: octubre 2, 2025, <https://ius360.com/impacto-de-la-ley-de-proteccion-de-datos-personales-en-la-inteligencia-artificial/>
90. El impacto de la Inteligencia Artificial en los derechos de protección de datos, fecha de acceso: octubre 2, 2025, <https://derechoytecnologiaperu.wordpress.com/2025/09/09/el-impacto-de-la-inteligencia-artificial-en-los-derechos-de-proteccion-de-datos/>
91. SAS: El 41% de entidades financieras del Perú utiliza Inteligencia Artificial para gestionar el riesgo crediticio - Microfinanzas, fecha de acceso: octubre 2, 2025, <https://microfinanzas.pe/sas-el-41-de-entidades-financieras-del-peru-utiliza-inteligencia-artificial-para-gestionar-el-riesgo-crediticio/>
92. SBS: utilizarán inteligencia artificial para reforzar la lucha contra el ..., fecha de acceso: octubre 2, 2025, <https://www.radionacional.gob.pe/noticias/economia/sbs-utilizaran-inteligencia-artificial-para-reforzar-la-lucha-contra-el-lavado-de-activos>
93. ¿Qué son los datos sintéticos? | IBM, fecha de acceso: octubre 2, 2025, <https://www.ibm.com/mx-es/think/topics/synthetic-data>
94. (PDF) Generative adversarial networks (GANs) for detecting adversarial crafted fraudulent claims - ResearchGate, fecha de acceso: octubre 2, 2025, <https://www.researchgate.net/publication/395136465_Generative_adversarial_networks_GANs_for_detecting_adversarial_crafted_fraudulent_claims>
95. Synthetic Data Generation Using GANs | Impetus Blog, fecha de acceso: octubre 2, 2025, <https://www.impetus.com/resources/blog/synthetic-data-generation-using-gans/>
96. A Hybrid Deep Learning Approach with Generative Adversarial Network for Credit Card Fraud Detection - MDPI, fecha de acceso: octubre 2, 2025, <https://www.mdpi.com/2227-7080/12/10/186>
97. AIS Electronic Library (AISeL) - AMCIS 2024 Proceedings: Generative Adversarial Networks in Fraud Detection: A Systematic Literature Review, fecha de acceso: octubre 2, 2025, <https://aisel.aisnet.org/amcis2024/security/security/35/>
98. Scotiabank México recomienda tomar medidas preventivas frente al fraude por deepfake, fecha de acceso: octubre 2, 2025, <https://redfinanciera.mx/scotiabank-mexico-recomienda-tomar-medidas-preventivas-frente-al-fraude-por-deepfake/>
99. Federated learning in fraud detection: From proof of concept to ..., fecha de acceso: octubre 2, 2025, <https://www.finextra.com/blogposting/29286/federated-learning-in-fraud-detection-from-proof-of-concept-to-practical-adoption>
100. Advancements of Credit Card Fraud Detection Based on Federated Learning - SciTePress, fecha de acceso: octubre 2, 2025, <https://www.scitepress.org/Papers/2024/135274/135274.pdf>
101. Federated Learning for secure data sharing in FinCrime ... - Lucinity, fecha de acceso: octubre 2, 2025, <https://lucinity.com/blog/federated-learning-in-fincrime-how-financial-institutions-can-fight-crime-without-sensitive-data-sharing>
102. Ataques adversariales en IA: 7 estrategias clave para protegerte - KeepCoding, fecha de acceso: octubre 2, 2025, <https://keepcoding.io/blog/ataques-adversariales-en-ia/>
103. Ataques Adversarios a la IA: Comprender y Prevenir la Manipulación de la IA - Focalx, fecha de acceso: octubre 2, 2025, <https://focalx.ai/es/inteligencia-artificial-es/ataques-adversarios-a-la-ia-comprender-y-prevenir-la-manipulacion-de-la-ia/>
104. Adversarial Machine Learning: ataques a modelos de ML, fecha de acceso: octubre 2, 2025, <https://www.welivesecurity.com/la-es/2022/05/30/adversarial-machine-learning-introduccion-ataques-modelos-ml/>
105. ¿Qué es el aprendizaje automático adversarial? Tipos de ataques y defensas - DataCamp, fecha de acceso: octubre 2, 2025, <https://www.datacamp.com/es/blog/adversarial-machine-learning>
106. Prototipo de detección de fraudes con tarjetas de crédito basado en ..., fecha de acceso: octubre 2, 2025, <https://repositorio.ulima.edu.pe/handle/20.500.12724/15294>
107. The Amazing Ways How Mastercard Uses Artificial Intelligence To ..., fecha de acceso: octubre 2, 2025, <https://bernardmarr.com/the-amazing-ways-how-mastercard-uses-artificial-intelligence-to-stop-fraud-and-reduce-false-declines/>
108. 5 Ways MasterCard is Using AI [Case Study][2025] - DigitalDefynd, fecha de acceso: octubre 2, 2025, <https://digitaldefynd.com/IQ/ways-mastercard-use-ai/>
109. Inside the algorithm: How gen AI and graph technology are cracking down on card sharks, fecha de acceso: octubre 2, 2025, <https://www.mastercard.com/news/perspectives/2024/inside-the-algorithm-how-gen-ai-and-graph-technology-are-cracking-down-on-card-sharks/>
110. AI is changing fraud — and how to fight back | Visa, fecha de acceso: octubre 2, 2025, <https://corporate.visa.com/en/sites/visa-perspectives/security-trust/ai-and-the-future-of-fraud.html>
111. Visa Advanced Authorisation, fecha de acceso: octubre 2, 2025, <https://corporate.visa.com/content/dam/VCOM/corporate/solutions/documents/visa-eu-advanced-authorization-case-study.pdf>
112. Visa ayuda a prevenir fraudes de los pagos en tiempo real en ..., fecha de acceso: octubre 2, 2025, <https://www.visa.cl/acerca-de-visa/sala-de-noticias/notas-de-prensa/visa-ayuda-a-prevenir-fraudes-en-tiempo-real-con-inteligencia-artificial.html>
113. BBVA México usará IA para reducir la espera en ... - La Jornada, fecha de acceso: octubre 2, 2025, <https://www.jornada.com.mx/noticia/2025/08/12/economia/bbva-mexico-usara-ia-para-reducir-la-espera-en-llamadas-a-solo-30-segundos>
114. IA generativa: atención al cliente, pymes y detección de fraude ganaron la primera competición BBVA Bot Talent, fecha de acceso: octubre 2, 2025, <https://www.bbva.com/es/innovacion/ia-generativa-atencion-al-cliente-pymes-y-deteccion-de-fraude-ganaron-la-primera-competicion-bbva-bot-talent/>
115. Banco Santander ahorra 200 millones con IA y acelera su alianza con OpenAI - The Officer, fecha de acceso: octubre 2, 2025, <https://theofficer.es/banco-santander-ahorra-200-millones-ia-acelera-alianza-openai/>
116. El Banco Santander acelera la implementación de la IA con la que ..., fecha de acceso: octubre 2, 2025, <https://www.infobae.com/espana/2025/08/12/el-banco-santander-acelera-la-implementacion-de-la-ia-con-la-que-ha-ahorrado-en-2024-mas-de-200-millones-de-euros/>
117. Santander firma un acuerdo con OpenAI para ser un banco "nativo en IA" - Forbes España, fecha de acceso: octubre 2, 2025, <https://forbes.es/economia/781628/santander-firma-un-acuerdo-con-openai-para-ser-un-banco-nativo-en-ia/>
118. 5 casos de éxito de empresas que usan IA en Latinoamérica | Aicad, fecha de acceso: octubre 2, 2025, <https://www.aicad.es/5-casos-de-exito-de-empresas-que-usan-ia-en-latinoamerica>