Deloitte.

Together makes progress

Perspectivas de la banca y los mercados de capitales para 2026

El año que viene probablemente exigirá decisiones audaces a medida que los bancos equilibran los vientos macroeconómicos en contra, la ambición de la IA y la competencia aumentada por *fintechs.*

Cinco pasos que los bancos deberían considerar para superar proyectos aislados de IA

El 2026 podría ser decisivo para los bancos que aspiran a convertirse en organizaciones totalmente impulsadas por inteligencia artificial. Actualmente, la implementación de IA en el sector bancario suele verse limitada por bases de datos frágiles y fragmentadas, crecientes exigencias regulatorias, sistemas heredados obsoletos y resistencia interna al cambio. Muchas iniciativas de IA permanecen estancadas en pruebas piloto aisladas, caracterizadas por una gobernanza débil, duplicación de esfuerzos y un impacto desigual.

Además, numerosos ejecutivos bancarios parecen lidiar con expectativas poco realistas sobre productividad, mientras enfrentan una presión creciente para demostrar resultados tangibles. A pesar de los presupuestos cada vez mayores destinados a IA en los últimos dos años, la mayoría de los bancos estadounidenses solo ha logrado avances tácticos esporádicos, sin alcanzar una verdadera transformación estratégica. Nuestro análisis de los 40 principales bancos de Estados Unidos revela esfuerzos predominantemente "reactivos" y fragmentados, que generan un valor inconsistente.

1. Redefinir una visión y estrategia de IA más clara y unificada

Hasta ahora, la mayoría de los bancos ha adoptado un enfoque fragmentado y poco consistente hacia la inteligencia artificial, especialmente en lo que respecta a la IA generativa. Aunque muchas instituciones han realizado experimentos, la adopción carece de una visión integral. ¿El objetivo principal es impulsar la eficiencia, acelerar la innovación o fortalecer la gestión de riesgos y la resiliencia? Sin una visión unificada, los bancos pueden tener dificultades para identificar oportunidades escalables y medir avances frente a metas clave de desempeño.

Hasta la fecha, solo unas pocas instituciones han articulado una estrategia de IA coherente a nivel corporativo, en la que cada componente se integra y opera en armonía. Para lograrlo, la visión debe definir resultados concretos, reconocer riesgos, costos e implicaciones humanas, alinearse con la misión general del banco, comunicarse de manera consistente entre todos los grupos de interés y sustentarse en una asignación disciplinada de recursos. Bien ejecutada, esta estrategia puede evitar la proliferación de pilotos desconectados y canalizar los recursos hacia iniciativas con el mayor impacto estratégico.

2. Establecer una estructura clara de propiedad y gobernanza para la IA

Los bancos deben contar con una estructura clara de responsabilidades a lo largo del ciclo de vida de la IA, aunque en muchos casos la rendición de cuentas es fragmentada o inexistente. Además, los enfoques varían en cuanto al acceso y uso de herramientas de IA por parte de los empleados, lo que hace necesario definir qué funciones corresponden a un equipo central y cuáles a las unidades de negocio.

Para la mayoría de los bancos, un modelo radial podría ser la opción óptima. Este modelo puede ayudar a garantizar que las necesidades de las diferentes líneas de negocio se gestionen adecuadamente, con el respaldo de una unidad central como un centro de excelencia en IA.

Esta entidad central puede impulsar la calidad en toda la organización y garantizar el cumplimiento de los estándares de gobernanza, además de actuar como el núcleo operativo para la adopción de IA, manteniendo una hoja de ruta dinámica para su ejecución. Además de desarrollar la estrategia, también podría encargarse de la arquitectura de referencia, los estándares, los activos compartidos y los servicios de *MLOps* o *LLMOps* para asegurar la interoperabilidad. Más allá de la gobernanza, el centro de excelencia debería enfocarse en la capacitación, la creación de manuales y la difusión de conocimiento, así como en apoyar la implementación mediante la operación de plataformas centrales de IA.

3. Reevaluar el dilema "construir *vs.* comprar"

La decisión entre desarrollar internamente o adquirir soluciones externas es un dilema recurrente, pero adquiere una dimensión distinta en el contexto de la inteligencia artificial. Muchos bancos han adoptado un modelo híbrido para la IA tradicional, como el aprendizaje automático, construyendo modelos propios mientras compran soluciones puntuales y plataformas para necesidades menos diferenciadas. En el caso de la IA generativa, algunas instituciones han optado por un enfoque de ensamblaje, en el que adquieren la capa de modelo base y desarrollan capas propietarias personalizadas que incluyen conectores de datos, mecanismos de control y soluciones de terceros.

Además de aprovechar la experiencia externa, este enfoque puede reducir el tiempo de salida al mercado y los costos de experimentación. La opción de "comprar" también permite trasladar el riesgo de posibles incrementos de costos a los proveedores. Los bancos más pequeños, en particular, suelen no tener alternativa más que adoptar un modelo híbrido debido a presupuestos limitados, escasez de talento y menor tolerancia al riesgo.

Sin embargo, el enfoque de ensamblaje no está exento de desafíos. Las capas propietarias deben integrarse adecuadamente con los modelos base. Asimismo, si todos los bancos utilizan los mismos modelos —o modelos similares de terceros—, la única diferenciación real se encuentra en las capas específicas desarrolladas por cada institución.

Para construir una ventaja competitiva con IA generativa, los bancos deberían apoyarse fuertemente en datos propios y ser creativos en la aplicación de los modelos: flujos de trabajo específicos y de alto impacto pueden superar proyectos ambiciosos pero dispersos. Finalmente, es clave invertir en talento especializado, como ingenieros en *prompting* o en *retrieval-augmented generation (RAG)*, evaluadores y diseñadores capaces de convertir los modelos en sistemas robustos. Allí podría residir la verdadera diferenciación.

4. Medir y monitorear el ROI con disciplina

A medida que la IA escala, medir su impacto se vuelve crítico, aunque algunos ejecutivos *senior* encuentran difícil evaluar el valor más allá de métricas anecdóticas o subjetivas, como horas ahorradas o llamadas acortadas. La productividad de los desarrolladores de software es quizá una de las áreas donde la medición del ROI está más avanzada.

Sin líneas base estandarizadas, escenarios contrafactuales o indicadores clave consistentes, los beneficios suelen depender de afirmaciones de los usuarios más que de resultados financieros medibles. Esto puede generar una brecha de credibilidad, dificultando vincular beneficios intangibles con ahorros concretos o incrementos en ingresos. Muchos beneficios también son indirectos: por ejemplo, llamadas más cortas en atención al cliente pueden mejorar la satisfacción y, a su vez, impulsar ventas cruzadas, aunque estos efectos son difíciles de cuantificar. La IA generativa complica aún más el panorama con afirmaciones de productividad que no se conectan con costos reales.

Obstáculos comunes que enfrentan los bancos al medir el retorno de la inversión

Obstáculo	Cómo se ve	Qué pueden hacer los bancos?
Declaraciones vagas con evaluación subjetiva	Beneficios descritos de manera vaga ("La IA ayuda a los empleados a trabajar más rápido") sin cuantificación; a menudo basados en la percepción del usuario más que en resultados comerciales.	Requerir resultados cuantificados vinculados a indicadores clave de desempeño (por ejemplo, tiempo ahorrado → casos procesados → impacto en ingresos). Vincularlos a métricas financieras o de riesgo.
Sin línea base o contrafactuales	Falta de comparaciones antes/después o grupos de control; dificulta probar si la IA generó la ganancia.	Establecer líneas de base cuando sea posible o utilizar indicadores aproximados. Utilizar pruebas de control o datos sintéticos o referencias históricas para crear contrafactuales.
Doble conteo	Varios equipos (por ejemplo, experiencia del cliente y operaciones) reclaman los mismos ahorros, inflando el impacto total.	Crear validación central del ROI. Requerir reglas de atribución (quién reclama qué) y consolidar resultados para evitar informes inflados.
"Productividad" ≠ ahorros realizados	Los equipos informan tiempo ahorrado, pero los costos permanecen sin cambios.	Rastrear la reasignación de capacidad. Vincular la productividad a resultados tangibles (por ejemplo, más préstamos procesados, más casos resueltos). Separar "eficiencia" de "ahorros financieros".
Sin métricas estandarizadas	Diferentes unidades de negocio miden el impacto de manera distinta (por ejemplo, minutos ahorrados vs. casos evitados); consistencia limitada entre métricas.	Definir categorías de ROI a nivel empresarial (costo, ingresos, riesgo, experiencia del cliente). Estandarizar plantillas y tableros de registro.
Comparación de proveedores	Las plataformas de IA y generación de IA de terceros pueden variar en costo, precisión y velocidad. La falta de referencias consistentes dificulta comparar proveedores.	Desarrollar una hoja de evaluación de proveedores (costo, precisión, explicabilidad, riesgo). Ejecutar pruebas piloto entre proveedores y documentar compensaciones.

5. Prepararse para nuevos modelos específicos de la industria y para la IA agéntica

Los modelos generales de lenguaje son potentes, pero suelen ser limitados para abordar la complejidad de las operaciones bancarias. El verdadero cambio podría provenir de modelos entrenados con datos y flujos de trabajo específicos del sector. Por ejemplo, Claude for Financial Services se centra en investigación gobernada, modelado y procesos de cumplimiento con uso de datos auditables. Asimismo, modelos de código abierto como FinLlama Instruct han demostrado superar a ciertos *LLM* en operaciones de *trading* algorítmico. Paralelamente, los modelos de lenguaje pequeños están ganando terreno por ser más económicos, rápidos y fáciles de implementar en sistemas internos. Adaptados a datos del sector, estos modelos prometen un retorno más práctico, reduciendo gastos reactivos y permitiendo una adopción de IA más enfocada y confiable.

Posiblemente, la frontera más crítica hoy sea la IA agéntica: agentes autónomos capaces de tomar iniciativa y ejecutar acciones. Los bancos deberían comenzar a incorporar el cumplimiento normativo en los propios agentes, incluyendo permisos, trazabilidad y puntos de control humano. También deben preparar las bases para la escalabilidad: infraestructura en la nube, orquestación para sistemas multiagente y una gobernanza sólida de datos con protocolos de calidad, trazabilidad y accesibilidad. Además, será necesario evolucionar del modelo centrado en el humano hacia un enfoque centrado en el agente de IA, manteniendo la intervención humana en decisiones críticas y en la supervisión, respaldada por una gestión del cambio intencionada y, cuando sea necesario, rediseño organizacional.

A medida que la adopción crece, algunos bancos están replanteando su infraestructura. Muchos recurren a proveedores externos para ganar velocidad, pero los costos insostenibles de cómputo exigen una infraestructura híbrida de IA que combine sistemas locales con nubes públicas, privadas y especializadas, para escalar con flexibilidad, proteger datos sensibles y cumplir con las exigencias regulatorias.

La IA no funcionará sin las bases adecuadas

El éxito en la implementación de IA será limitado si los bancos no abordan otros desafíos, como la modernización de la infraestructura central, la migración a la nube y el fortalecimiento de la arquitectura y gobernanza de datos. Además, no deben evitar un cambio cultural que permita la colaboración fluida entre humanos e IA, impulsando la productividad sin sacrificar la responsabilidad, la confianza y el cumplimiento normativo en toda la organización. La clave está en definir la visión desde la alta dirección, respaldarla con inversión y generar alineación para que cada iniciativa de IA, por pequeña que sea, contribuya a una historia estratégica más amplia.

Redoblar el compromiso con una infraestructura moderna y preparada para IA

Muchos bancos han avanzado significativamente en la modernización de su infraestructura de datos. En particular, la migración de datos centrales a la nube ha contribuido a fortalecer las prácticas de gestión de información. Sin embargo, sin una infraestructura de datos diseñada para IA, los modelos pueden no alcanzar su rendimiento óptimo, los pilotos de IA generativa podrían estancarse o no cumplir con los estándares regulatorios y las expectativas de los clientes, y las futuras iniciativas de IA agéntica podrían no despegar. A medida que la IA evoluciona de proyectos piloto a implementaciones a escala empresarial, construir una arquitectura de datos más resiliente y preparada para el futuro se vuelve una prioridad crítica.

¿Qué han hecho los bancos para estar listos para la IA?

La preparación de datos para IA entre los bancos es altamente desigual, tanto entre instituciones como dentro de las mismas. Si bien la migración a la nube debería facilitar la organización y el acceso a los datos, en algunos casos se han trasladado datos de baja calidad o persisten silos incluso dentro del entorno en la nube.

Además, los bancos que prepararon sus datos para el cumplimiento normativo deberían haber contribuido a la preparación para la IA con datos más limpios, más trazables y mejor gobernados. Por ejemplo, las normas de capital y liquidez hacen un “deber ser” a consolidar los datos de riesgo y establecer un linaje; para tener conjuntos de datos más oportunos y auditables; y los informes sobre prevención de lavado de dinero y sanciones han exigido datos estandarizados de clientes y transacciones. Sin embargo, estas inversiones a menudo permanecen aisladas, cumpliendo únicamente su mandato original en lugar de escalarse hasta convertirse en una base que pueda impulsar la IA en toda la empresa.

Los bancos con experiencia previa en automatización robótica de procesos *(RPA)* e IA deberían contar con catálogos de datos establecidos, un linaje claro, metadatos de calidad, nuevos controles y una monitorización continua de la calidad para mejorar la precisión, la calibración y la estabilidad de los modelos de IA.

Lo que significa contar con datos preparados para IA

La IA está redefiniendo el significado de "datos de calidad" en la banca. La tabla presentada más adelante resume algunos de los pilares clave de una arquitectura de datos preparada para la IA.

La preparación de los bancos para IA suele verse limitada por las bases de datos sobre las que dependen los modelos. Una infraestructura deficiente puede generar dispersión de datos, vulnerabilidades y escasa innovación basada en información, reduciendo la eficacia de los modelos. Además, los silos de datos suelen dejar conjuntos de entrenamiento incompletos y sesgados. El impacto es evidente: en la Encuesta de Mercado de Datos y Analítica en Banca y Mercados de Capitales 2024 de Deloitte, más del 90% de los usuarios de datos en bancos reportaron que la información que necesitan suele no estar disponible o tarda demasiado en obtenerse. La calidad de los datos también se ubicó como un desafío crítico, con el 81% de los encuestados señalándola como uno de los principales problemas.

Los bancos deben enfocarse en los siguientes cuatro pilares de una arquitectura de datos lista para IA

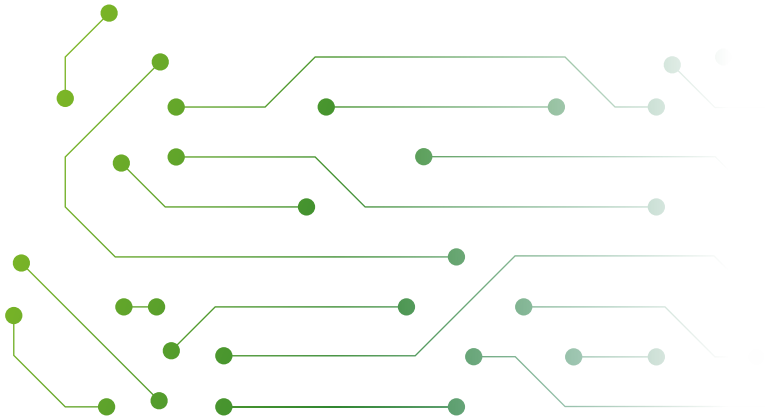
Pilar	Descripción	Por qué esto es importante para la IA
Integridad y confianza	Datos precisos, completos, consistentes y confiables; verificados continuamente y corregidos automáticamente; con trazabilidad y linaje de extremo a extremo, reproducibilidad; monitoreados para estabilidad, desviación y equidad, de modo que el rendimiento se mantenga en el tiempo.	Puede ayudar a reducir errores y sesgos en los modelos, habilitar resultados reproducibles y hacer que las decisiones sean auditables—esencial para revisiones regulatorias y para mantener el rendimiento del modelo a medida que cambian las condiciones.
Velocidad y acceso	Datos que llegan a tiempo y son fáciles de usar: latencia óptima (en tiempo real donde se necesite, por lotes donde sea suficiente); acceso unificado y definido entre silos; autoservicio basado en roles y políticas para humanos y agentes.	Puede ayudar a impulsar decisiones en el momento (por ejemplo, en fraude, servicio, precios), acelerar la experimentación y el despliegue, y reducir el ciclo desde los datos hasta el modelo y la acción empresarial.
Amplitud y semántica	Datos completos y bien descritos: gran amplitud y profundidad en modalidades (estructura, texto, voz, imágenes); semántica clara, etiquetado y metadatos; interoperables entre plataformas y funciones.	Puede ayudar a mejorar la recuperación y la base de modelos de lenguaje grandes/generación de recuperación aumentada, impulsa la reutilización de características y aumenta la precisión al brindar a los modelos una señal completa y bien etiquetada, en lugar de fragmentos limitados.
Propiedad y seguridad	Datos que cumplen por diseño: propiedad y gobernanza definidas; seguridad y privacidad sólidas; cumplimiento local y transfronterizo; puertas de política como código en el uso y en la promoción a producción.	Puede ayudar a mantener la confianza del cliente y la certeza legal, habilitar escalamiento seguro entre jurisdicciones y prevenir incidentes costosos aplicando reglas automáticamente, no después del hecho.

Los datos listos para IA deben ser lo suficientemente confiables para evitar que errores o desviaciones deterioren el rendimiento de los modelos; oportunos para alinearse con el ritmo de las decisiones; amplios para capturar señales en distintos formatos; y gobernados con rigor para cumplir con las exigencias de seguridad y normativas.

Estos atributos son interdependientes. Por ejemplo, la velocidad sin confianza solo entrega datos erróneos más rápido; la amplitud sin contexto añade ruido en lugar de generar conocimiento; y la gobernanza sin usabilidad puede frenar la innovación. Fortalecer una dimensión suele exponer debilidades en las demás. El desafío para los bancos no consiste en elegir cuál optimizar, sino en avanzar en las cuatro de manera simultánea, para que la base de datos esté a la altura de la escala, velocidad y sofisticación que exige la IA moderna.

Prioridades para las estrategias de datos en 2026: el camino hacia el éxito en la era de la IA

La preparación de datos para IA será probablemente un proceso de varios años. Los bancos que logren alinear el patrocinio ejecutivo, los presupuestos y cronogramas realistas para construir una base de datos lista para IA estarán mejor posicionados para aprovechar todo su potencial.



Evaluar la preparación de los datos para la IA en función de los cuatro pilares

Los bancos deben realizar una revisión de la preparación de los datos en toda la empresa para ayudar a identificar, en todos los dominios y casos de uso, las soluciones específicas necesarias para liberar el valor de la IA.

Algunas preguntas que los bancos deberían hacerse para evaluar su preparación de datos para IA

Integridad y confianza
Más allá de "¿los conjuntos de datos son precisos?", los líderes deberían explorar:
- ¿Qué **puntos ciegos** podrían existir en nuestros datos y cómo los descubrimos antes de que afecten los modelos de IA?
- ¿Estamos invirtiendo lo suficiente en **enriquecimiento de datos**—conjuntos de datos externos, datos alternativos o datos sintéticos—para mantenernos competitivos?
- ¿Qué tan seguros estamos de que nuestros datos más críticos pueden **resistir el escrutinio regulatorio** o una auditoría externa?
- ¿Qué salvaguardas tenemos para **garantizar equidad, estabilidad y consistencia** en los resultados a lo largo del tiempo?

Amplitud y semántica
Ir más allá del linaje y los glosarios:
- ¿Capturamos el **espectro completo de modalidades** (estructura, texto, voz, imágenes) relevantes para nuestro negocio?
- ¿Tenemos una **comprensión empresarial** de las entidades principales o seguimos conciliando definiciones contradictorias?
- ¿Qué tan **detectables y reutilizables** son nuestras características y conjuntos de datos entre equipos?
- ¿Qué tan bien estamos **etiquetando, enriqueciendo y documentando** los datos para su uso futuro en IA?

Velocidad y acceso
Además de las métricas de latencia, preguntar:
- ¿Entendemos realmente dónde los **datos en tiempo real agregan valor al negocio** frente a dónde "el momento adecuado" es suficiente?
- ¿Cuánto valor empresarial se pierde hoy debido a la latencia, acceso aislado o toma de decisiones retrasada?
- ¿Qué tan fácilmente pueden los equipos de IA y analítica **descubrir y acceder a los datos** que necesitan sin fricción?
- ¿Nuestra arquitectura de datos es **lo suficientemente ágil para soportar nuevos casos de uso imprevistos** sin meses de reingeniería?

Propiedad y seguridad
Ir más allá de "¿quién posee qué?":
- ¿Los líderes empresariales **se sienten responsables de los datos** en su dominio o todavía se percibe como un "problema de TI"?
- ¿Cómo equilibramos **velocidad, innovación y gobernanza** sin frenar ni ejercer un control excesivo?
- ¿La **privacidad, el consentimiento y la residencia se aplican automáticamente** en tiempo de ejecución en lugar de adaptarse después?
- ¿Qué tan resilientes somos frente a **riesgos intencionales** (envenenamiento de datos, inyección de instrucciones) y uso **indebido no intencional?**

Los bancos pueden desarrollar una matriz de evaluación con umbrales mínimos para analizar los casos de uso de IA. Por ejemplo, ningún proyecto debería avanzar sin identificar los conjuntos de datos y características relevantes, evidenciar las puntuaciones actuales y comprometerse a mejorar aquellas áreas que estén por debajo del umbral. Este enfoque puede contribuir a lograr un mejor rendimiento y estabilidad de los modelos, acelerar los despliegues, facilitar auditorías y garantizar mayor repetibilidad entre equipos.

Resolver el desafío persistente de la propiedad de los datos

Para algunos bancos, el mayor obstáculo es la ausencia de un responsable único para los datos críticos y la falta de claridad sobre quién asume la responsabilidad cuando surgen errores. Las funciones del director de información *(CIO),* el director de datos *(CDO)* y los centros de excelencia en IA suelen superponerse, lo que complica la gobernanza. Si bien no existe un modelo único, un enfoque híbrido puede resultar eficaz en muchos casos. En este esquema, las unidades centralizadas supervisan los estándares de datos y plataformas, además de gestionar el cumplimiento normativo, posiblemente bajo el liderazgo del *CDO*. Por ejemplo, los principios de HSBC para el uso ético de datos e IA proporcionan una política a nivel corporativo que establece lineamientos para la responsabilidad, el acceso y el uso responsable. Al mismo tiempo, las líneas de negocio pueden asumir la responsabilidad de los datos tratándolos como un producto y manteniendo su calidad.

Usar IA para mejorar los datos

Las capacidades actuales de IA pueden ayudar significativamente a monitorear, reparar y enriquecer datos a gran escala. Por ejemplo, los bancos pueden emplear modelos supervisados de detección de anomalías entrenados con patrones históricos de errores y ubicados en puntos de ingestión para identificar anomalías en segundos. Los responsables de datos también pueden usar modelos de IA para trazabilidad y documentación. Los *LLM* pueden interpretar herramientas como *SQL* y generar automáticamente gráficos de trazabilidad y diccionarios de datos, lo que permite mantener los metadatos actualizados incluso cuando el código evoluciona.

El resultado es un ciclo de retroalimentación en el que la IA mejora los datos para la propia IA: la calidad aumenta, la trazabilidad se mantiene, la privacidad se refuerza y se generan nuevos materiales de entrenamiento de forma segura y bajo demanda. Los bancos que implementen estos agentes de "IA para datos" podrían reportar ciclos de modelos más rápidos, menores costos operativos y una interacción regulatoria más fluida, acercándose a un estado verdaderamente preparado para IA.

Otras consideraciones

Además de las prioridades mencionadas, existen varias consideraciones adicionales que los bancos deben tener en cuenta.

- Cumplir con los requisitos de cumplimiento interno. Es posible que los bancos deban documentar el origen de cada registro de entrenamiento, cómo se procesó, si contiene atributos sensibles y cómo influye en el comportamiento del modelo.

- Designar al director de datos *(CDO)* y al director de riesgos *(CRO)* como administradores conjuntos de datos. Los *CDO* implementan el linaje, los metadatos y la aplicación de la normativa, mientras que los *CRO* alinean los umbrales con el apetito de riesgo y las expectativas regulatorias, además de escalar las brechas con planes de remediación financiados.

- Reconocer que la IA agéntica requiere datos organizados. Los agentes autónomos no pueden prosperar con datos aislados o desorganizados. De lo contrario, podrían volverse poco fiables, agravar las brechas de propiedad y correr el riesgo de tomar decisiones erróneas o incluso incompatibles.

- Modernizar la arquitectura de datos con conceptos como la malla de datos y el tejido de datos. El objetivo debe ser reconocer los beneficios de estos enfoques y reconstruir las bases para un banco preparado para la IA: escalable, flexible y con mayor capacidad de adaptación.

Liberar todo el potencial de la IA

Algunos bancos ya han demostrado que pueden invertir estratégicamente, migrar y modernizar sus prácticas de datos. El siguiente paso consiste en escalar estas inversiones hacia un ritmo constante de mejora en múltiples dimensiones, tal como se destaca en este informe. Adoptar una cultura organizacional que favorezca la colaboración entre humanos e IA y redoblar el compromiso con una infraestructura de datos moderna y preparada para IA permitirá materializar la promesa completa de una banca impulsada por inteligencia artificial.

Los bancos deben adoptar un enfoque más dinámico y tecnológico para combatir el crimen financiero

El crimen financiero está aumentando en escala, velocidad y sofisticación, lo que incrementa los costos de cumplimiento y la presión operativa sobre los bancos. Así como mayor escrutinio no solo por los reguladores locales sino por el foco que ha puesto US en la materia. De cara al futuro, los bancos enfrentarán mayores complejidades derivadas de nuevas fuentes de riesgo. Si bien las instituciones deben cumplir con los requisitos legales y normativos, la Red de Control de Delitos Financieros del Departamento del Tesoro (FinCEN) está coordinando esfuerzos con diversas agencias para enfocar la supervisión en nuevas prioridades gubernamentales, como la lucha contra el lavado de dinero basado en el comercio, el tráfico de sustancias controladas y las actividades transaccionales vinculadas a cárteles. Estas expectativas regulatorias más estrictas ejercerán mayor presión sobre los bancos para monitorear los flujos de transacciones en busca de indicadores de financiamiento de opioides y otras actividades ilícitas realizadas por organizaciones criminales transnacionales.

Los reguladores también podrían aplicar sanciones con mayor rigor, especialmente si las tensiones geopolíticas y comerciales generan nuevas designaciones contra actores clave.

Por otro lado, los bancos también podrían enfrentar un aumento de actores maliciosos que explotan la IA, especialmente la IA generativa. Agentes autónomos malintencionados pueden simular comportamientos humanos fraudulentos, aprender a evadir sistemas de detección y anonimizar identidades.

Este nivel elevado de amenaza representa un llamado crítico a la acción para que los bancos adopten un modelo más dinámico y basado en inteligencia para gestionar riesgos asociados. La industria no puede seguir dependiendo de datos fragmentados y sistemas heredados para ofrecer resultados significativos frente a ataques externos, eventos geopolíticos y escrutinio regulatorio. Las instituciones que no construyan un marco tecnológico sólido para combatir el crimen financiero serán cada vez más vulnerables a pérdidas económicas y ataques criminales.

Gestión de riesgos emergentes en activos digitales e innovación financiera

Los bancos deben anticipar los riesgos que pueden surgir al ofrecer nuevos servicios y avanzar en la innovación digital. En el caso de las monedas estables, las instituciones deben evaluar los riesgos de *AML* (prevención de lavado de dinero) y *KYC* (conocimiento del cliente) que son únicos en las transacciones basadas en *blockchain*. Dado que las monedas estables pueden transferirse a billeteras digitales que no están asociadas con información personal, los bancos deberán desarrollar procesos para verificar el origen de los fondos, validar la identidad de los propietarios de las billeteras, aprobar previamente remitentes y destinatarios y rastrear las transferencias a través de la red *blockchain*.

Para la *tokenización* de activos, deberían construir sistemas de monitoreo que conecten la actividad dentro y fuera de la cadena, desarrollar plataformas que puedan ingerir metadatos que rijan la emisión de tokens y las reglas de contratos inteligentes, y entrenar modelos de IA para detectar riesgos como la acuñación ilícita y las transferencias rápidas de propiedad.

La importancia estratégica de la IA y la innovación tecnológica para mitigar riesgos

Integrar IA e innovación tecnológica para ayudar a mitigar riesgos

Aunque muchas instituciones ya utilizan automatización robótica de procesos *(RPA)* y modelos básicos de aprendizaje automático en el cumplimiento contra el crimen financiero, la adopción de IA avanzada para análisis profundo y detección de patrones sigue siendo limitada.

Los bancos deberían enfocar sus pilotos de IA en resultados prácticos, como resumir perfiles de riesgo de clientes, calificar alertas y redactar informes de casos. Con el tiempo, podrán habilitar decisiones con un solo clic para casos simples y utilizar IA para eliminar automáticamente alertas de bajo riesgo, mientras que las más complejas se envían a analistas con resúmenes listos para revisión.

Los equipos de cumplimiento contra el crimen financiero también deben considerar una visión a largo plazo, desplegando IA en cada etapa del ciclo de vida del cumplimiento. Estas integraciones pueden mejorar la debida diligencia al inicio de nuevas relaciones, fortalecer procesos de *KYC* continuo, optimizar el monitoreo conductual de clientes y sus conexiones, y reducir el volumen de alertas de baja calidad.

Oportunidades para que la IA mejore los resultados en todo el ciclo de vida del cumplimiento contra delitos financieros

	Controles iniciales	Detección	Escalamiento	Retroalimentación y mejora
Funciones clave	• Perfilado de riesgo del cliente • Debida diligencia • Incorporación de clientes	• Selección de transacciones • Monitoreo de perfiles *KYC* • Debida diligencia continua	• Enrutamiento de casos • Investigación y toma de decisiones • Informes regulatorios posteriores	• Revisiones posteriores al incidente • Refinamiento del modelo • Ajustes del flujo de trabajo
Puntos de integración de IA	• Analizar medios en diferentes idiomas para identificar noticias adversas • Realizar segmentación dinámica basada en riesgos prioritarios • Incorporar inteligencia de dispositivos y comportamiento en la identificación de clientes	• Recalcular y rastrear continuamente las puntuaciones de riesgo a lo largo del tiempo • Evaluaciones periódicas de clientes usando datos *KYC* actualizados • Inicio automático de revisiones basadas en eventos • Mapeo de relaciones para descubrir vínculos en redes criminales	• Clasificar casos según urgencia y nivel de riesgo • Recomendar próximos pasos basados en resultados anteriores • Optimizar salidas de clientes e informes de cumplimiento • Realizar resolución de entidades para identificar cuentas asociadas	• Procesar rutinariamente nuevos datos para detectar patrones que indiquen actividad de alto riesgo • Filtrar datos de alertas, casos e informes para identificar causas raíz de ineficiencias • Detectar tendencias emergentes de delitos a partir de archivos y notas de casos
Indicadores clave de desempeño	• Aperturas fraudulentas de cuentas bloqueadas • Incumplimientos por fallas en incorporación	• Reducción en volúmenes de alertas • Alerta sobre la tasa de conversión de casos	• Tasa de precisión en escalamiento • Tiempo de resolución del caso	• Tasa de detección de anomalías a lo largo del tiempo • Eficiencia en la investigación del analista

Si bien las formas tradicionales y novedosas de IA pueden ayudar a mitigar los delitos financieros, los bancos deben asegurarse de que expertos humanos manejen escenarios ambiguos o de alto riesgo e integren la explicabilidad en la toma de decisiones impulsada por IA para promover la transparencia en el razonamiento del modelo y mantener la confianza de los reguladores.

Fortalecer las plataformas de datos para un motor *AML* más confiable

La gestión de grandes volúmenes de datos para generar inteligencia basada en IA requerirá, probablemente, la consolidación de canales de datos que actúen como una única fuente de verdad para los indicadores de riesgo y los flujos de trabajo de investigación. Esta base de datos no solo puede ofrecer una visión más amplia del cliente, sino también arrojar luz sobre sus estructuras corporativas, contrapartes y perfiles de riesgo en evolución. Además, al complementar fuentes externas como listas de sanciones, registros de comercio y aduanas, e interfaces de motores de búsqueda, los bancos podrán rastrear de manera más efectiva las puntuaciones de riesgo a lo largo del tiempo.

Las acciones recientes de los reguladores han subrayado la necesidad de contar con datos oportunos, precisos y completos, así como con sistemas tecnológicos más sólidos que respalden los programas para combatir el crimen financiero. Los reguladores esperan que los datos y sistemas de los bancos sean el núcleo de los programas *AML* y no una función secundaria. También han solicitado una supervisión más rigurosa, incluyendo la creación de comités a nivel de junta directiva para monitorear y corregir defectos en los datos. De cara al futuro, se prevé que los bancos mantengan un inventario actualizado de los sistemas de cumplimiento contra el crimen financiero, diccionarios que definan los elementos críticos de datos, documentación sobre trazabilidad y bibliotecas centrales que expliquen cómo se catalogan y gestionan los riesgos.

Reguladores impulsan nuevos enfoques para combatir el crimen financiero

Los reguladores federales, conscientes del desafío de equilibrar el cumplimiento con las iniciativas estratégicas, podrían aliviar algunas cargas de supervisión para promover enfoques más ágiles en la gestión de riesgos. El Departamento del Tesoro, por ejemplo, busca reducir los requisitos de reporte y alentar a los bancos a enfocarse en actividades de mayor riesgo. Recientemente, se unió a otras cuatro agencias regulatorias para aclarar que los bancos no necesitan presentar un *SAR* si una transacción o serie de transacciones supera los USD10,000, a menos que exista conocimiento, sospecha o indicios de que el cliente intenta evadir los requisitos de reporte.

Este enfoque más centrado en las amenazas más graves podría estar tomando forma, ya que algunos examinadores han comenzado a reducir investigaciones en áreas como riesgo reputacional, sostenibilidad e inclusión. Además, nuevas normativas y guías bajo la Ley contra el Lavado de Dinero de 2020 podrían otorgar a los bancos mayor flexibilidad para reasignar recursos desde controles de bajo impacto hacia sistemas más avanzados basados en IA y analítica, respaldados por gobernanza de modelos y trazabilidad de datos.

Estas reformas también permitirían a los bancos diseñar programas más estratégicos y eficaces contra el crimen financiero para enfrentar los desafíos futuros. Por ejemplo, podrían adoptar un modelo de riesgo integrado que permita a los analistas de ciberseguridad, *AML* y fraude monitorear un conjunto amplio de indicadores, priorizar alertas críticas y coordinar investigaciones con mayor rapidez. Este marco ayudaría a identificar actores maliciosos que intentan evadir controles mediante métodos diversos. Además, al retroalimentar los hallazgos exitosos en las evaluaciones tempranas y los controles de primera línea, las unidades de cumplimiento podrán redirigir continuamente sus esfuerzos hacia las amenazas más urgentes.

Convertir la reforma regulatoria y la tecnología en una ventaja estratégica contra el crimen financiero

En conjunto, estos cambios podrían marcar el inicio de una nueva era en inteligencia financiera. Con el respaldo regulatorio y la mejora continua de la tecnología, los bancos tienen la oportunidad de fortalecer sus capacidades para combatir el crimen financiero. Aquellos líderes que integren analítica avanzada e inteligencia artificial, al tiempo que aseguren una infraestructura de datos robusta, estarán mejor posicionados para anticipar y contrarrestar un panorama de amenazas cada vez más complejo. Sin embargo, deben actuar con rapidez, porque la adaptación ágil probablemente se convertirá en el estándar para garantizar resiliencia y confianza.

Contactos

Gustavo Méndez
Socio Líder de Servicios Financieros
Deloitte Spanish Latin America

Rafael Sánchez
Socio Líder de Crecimiento
Deloitte Centroamérica, Panamá y República Dominicana

Centro de contacto
centrodecontacto@deloittemx.com

Deloitte.