Inteligencia Artificial en Banca y Comercio Exterior: los Riesgos Legales que Nadie Está Evaluando

Marzo 2026

En sectores altamente regulados, el desafío de la inteligencia artificial no es tecnológico, sino jurídico: cómo justificar sus decisiones ante reguladores y tribunales.

Graciela Álvarez Agudo

Sebastián Chorén

Resumen Ejecutivo

La incorporación de inteligencia artificial (IA) en los procesos de comercio exterior y banca regulada en Argentina presenta una dicotomía fundamental. Si bien promete eficiencias operativas inéditas en clasificación documental, screening y detección de patrones, su implementación acrítica puede generar un riesgo jurídico y regulatorio significativo. Este artículo sostiene que el núcleo del problema no es tecnológico, sino probatorio: en un entorno donde cada decisión debe ser defendible ante el BCRA, la DGA, la UIF o un tribunal, la delegación de funciones en un algoritmo sin la correspondiente arquitectura de control, gobernanza y trazabilidad, transforma una ventaja competitiva en una exposición patrimonial y penal para la organización y sus decisores.

Más Allá de la Eficiencia Operativa, el Desafío de la Imputación

El sector financiero argentino se encuentra en un punto de inflexión. La presión por la eficiencia y la gestión de riesgos impulsa a bancos y plataformas de comercio exterior a explorar soluciones de IA para tareas como la validación documental de operaciones de importación/exportación, la detección de alertas tempranas en cumplimiento (AML/CFT) y la optimización de flujos operativos (Trade Operations).

Sin embargo, la pregunta que debería preceder a cualquier iniciativa de automatización no es ¿podemos hacerlo?, sino una de índole jurídico: ¿Podemos delegar una función de control o decisión en un sistema automatizado sin incrementar el riesgo de imputación por incumplimiento normativo o por daños?

Este documento analiza los puntos críticos donde la tecnología y la regulación se intersecan, proponiendo un marco de actuación que permita a las entidades financieras innovar sin comprometer su defensa jurídica. La tesis central es que la responsabilidad objetiva por el

incumplimiento no es delegable; lo que se automatiza es el proceso, no la rendición de cuentas.

El Nuevo Mapa de Riesgos: La Automatización como Redefinición de Roles y Evidencias

Tradicionalmente, las funciones de control en comercio exterior recaían en un operador humano, cuya defendibilidad se basaba en su pericia y en la trazabilidad manual de su actuación. La irrupción de la IA reconfigura este esquema en tres dimensiones fundamentales:

- **Agente Decisor ¿Quién decide?:** Se pasa de un criterio humano explícito a un modelo de inferencia algorítmica. La opacidad del proceso decisorio (el famoso caja negra) es el primer gran desafío.
- **Objeto de Documentación ¿Qué se documenta**?: Ya no basta con registrar la decisión final. Es imperativo documentar el proceso que llevó a ella: los datos de entrenamiento, los umbrales, las versiones del modelo y los logs de interacción.
- **Estándar Probatorio ¿Cómo se prueba?:** En una inspección o litigio, la carga de la prueba recae sobre la entidad. Demostrar que se actuó con la diligencia debida cuando un modelo de IA intervino requiere un estándar de evidencia mucho más robusto y complejo que el tradicional.

Los casos de uso más comunes que evidencian esta nueva realidad incluyen:

- Automatización del Compliance Documental:Sistemas que clasifican facturas comerciales, conocimientos de embarque (BL/AWB) y certificados de origen.
- Screening Predictivo:
- Herramientas que identifican operaciones con posible riesgo de fraude documental o Trade Based Money Laundering (TBML) basándose en patrones.
- Asistencia en la Decisión Operativa: Módulos de IA que recomiendan acciones como bloquear, escalar a un oficial de cumplimiento o aprobar con reservas.

El Eslabón Perdido: La Diligencia Debida en la Era Algorítmica

La implementación de IA no ocurre en un vacío legal. Se inserta en un entramado normativo denso y exigente, cuya infracción acarrea sanciones económicas, administrativas y penales. Un análisis de riesgo integral debe considerar, como mínimo, el siguiente plexo normativo:

- **Riesgo Cambiario y de Exterior:** Las Comunicaciones del BCRA (Texto Ordenado Exterior y Cambios) exigen trazabilidad y documentación fehaciente para cada operación de acceso al mercado de cambios. Un error algorítmico en la clasificación de una operación puede derivar en una infracción al Régimen Penal Cambiario (Ley 19.359).
- **Riesgo Aduanero:** El Código Aduanero (Ley 22.415)tipifica como infracción la inexactitud en las declaraciones. Si un sistema de IA procesa erróneamente una declaración, la responsabilidad recae sobre el declarante, no sobre el software.
- **Riesgo de Compliance (AML/CFT):** La Ley 25.246 y las resoluciones de la UIF imponen a los sujetos obligados la responsabilidad de implementar políticas de prevención de

lavado de activos y financiación del terrorismo. Un sistema de IA que no sea auditable o que presente sesgos podría ser considerado un incumplimiento de estas obligaciones.

- **Riesgo Civil y de Responsabilidad Profesional:** El Código Civil y Comercial de la Nación (arts. 1724 y ss.) establece el estándar de la diligencia debida. Un daño causado por una decisión automatizada defectuosa puede generar responsabilidad directa de la entidad financiera.
- **Riesgo de Protección de Datos (Privacidad**): El procesamiento masivo de documentos comerciales puede involucrar datos personales, activando las obligaciones de la Ley 25.326, incluyendo los principios de finalidad, minimización y seguridad.
- **Riesgo Tecnológico y de Seguridad de la Información:** Las normas del BCRA sobre gestión de riesgos en servicios financieros digitales exigen controles específicos para proveedores tecnológicos (tercerización), continuidad operativa y seguridad de la información.

Corolario: El algoritmo puede ser una herramienta de asistencia, pero ante un incumplimiento, la autoridad de control o el juez preguntarán a la organización: ¿Qué controles implementó? ¿Cómo supervisó? ¿Puede acreditar la cadena de decisiones?

Hacia una Arquitectura de Defensa: El Control Humano Significativo y la Gobernanza del Modelo

Para que una decisión automatizada sea defendible, la organización debe construir un marco de control ex ante y ex post. Esto implica trascender la mera supervisión formal y adoptar un control humano significativo (meaningful human control). Los pilares de esta arquitectura son:

- **Delimitación Jurídica del Caso de Uso (Análisis de Materialidad):** Definir con precisión el alcance de la automatización, distinguiendo entre funciones de apoyo (recomendación), funciones de control con supervisión humana (human-in-the-loop) y funciones estrictamente prohibidas de automatizar.
- **Diseño Basado en Riesgos (Risk-based Design):** Establecer una matriz de decisión y escalamiento con umbrales cuantitativos y cualitativos que activen alertas y puntos de control obligatorios.
- **Gobernanza del Modelo (Model Governance):** Implementar un ciclo de vida para el modelo de IA que incluya:
    1) documentación de diseño y propósito;
    2) pruebas de sesgo y precisión previas a la implementación;
    3) control de versiones y procedimientos de actualización/rollback;
    4) monitoreo continuo de desvíos (model drift).
- **Trazabilidad Forense (Forensic Readiness**): Generar y conservar registros (logs) inmutables y con sellos de tiempo que permitan reconstruir la cadena de custodia digital de cada decisión: qué datos de entrada se usaron, qué versión del modelo intervino, qué umbral se aplicó, quién y cuándo supervisó (si corresponde), y cuál fue la acción final.

- **Gestión de Terceros (Vendor Management):** Realizar una due diligence exhaustiva de los proveedores tecnológicos, estableciendo Acuerdos de Nivel de Servicio (ANS/SLA) que contemplen no solo la disponibilidad, sino también la auditabilidad, la seguridad y la continuidad del servicio.

Propuesta de Actuación: El Informe de Impacto Jurídico y Probatorio (IIJP) como Requisito Previo (GO/NO GO)

Para mitigar el riesgo de que la innovación tecnológica se convierta en una contingencia legal, se propone la elaboración de un Informe de Impacto Jurídico y Probatorio (IIJP)como paso previo y mandatorio a cualquier implementación de IA en procesos de alto riesgo. Este informe, de carácter interdisciplinario (legal, compliance y tecnología), debe contener:

- **Mapeo Normativo Aplicable:** Identificación detallada de las obligaciones de cumplimiento, reporting y conservación de evidencia para el caso de uso concreto.
- **Análisis de Riesgos y Escenarios de Responsabilidad:** valuación de los supuestos de incumplimiento (error del modelo, sesgo, fallo de seguridad) y determinación de los potenciales responsables (entidad, directorio, oficial de cumplimiento, proveedor).
- **Diseño del Marco de Control Humano y Trazabilidad:** Especificación de los puntos de control obligatorios, los roles y responsabilidades, y los requisitos técnicos para la generación de evidencia auditable.
- **Evaluación de Proveedores y Cadena de Suministro Tecnológica:** Análisis de la solvencia técnica, la seguridad y la capacidad de respuesta del vendor.
- **Conclusión y Dictamen:** Determinación fundada de si el proyecto es viable (GO) y, en su caso, establecimiento de condiciones y requisitos previos (checklist) para su implementación.
- **Diagnóstico Rápido:** Diez Preguntas para Evaluar su Exposición Actual

Antes de avanzar en cualquier proyecto de automatización, sugerimos responder a este cuestionario:

- **Impacto Regulatorio**: ¿Cuál es el impacto normativo específico (cambiario, aduanero, AML) de la decisión que el sistema tomará o asistirá?
- **Nivel de Autonomía:** ¿El sistema aprueba/bloquea operaciones o solo emite recomendaciones? ¿Está claramente definido y documentado quién ejerce la última palabra?
- **Origen y Calidad del Dato**: ¿Se han identificado y minimizado los datos personales en las fuentes de información? ¿Existe un proceso de validación de la calidad de los datos de entrada?
- . **Explicabilidad (XAI**): ¿Puede el sistema explicar, en términos comprensibles para un auditor o un juez, las razones que motivaron una alerta o decisión?
- **Registros (Logs) y Cadena de Custodia:** ¿Se generan logs detallados, inmutables y con sellos de tiempo que permitan reconstruir end-to-end el proceso de decisión? ¿Quién tiene acceso y cómo se preserva su integridad?

- **Gestión del Ciclo de Vida del Modelo:** ¿Existe un procedimiento formal para el versionado, las pruebas de regresión, la actualización y, en su caso, el rollback del modelo de IA?
- **Tolerancia al Error y Plan de Contingencia**: ¿Se han definido escenarios de error aceptables? ¿Existe un umbral de confianza por debajo del cual el sistema deriva automáticamente la decisión a un humano? ¿Cuál es el procedimiento manual de respaldo (fallback)?
- **Dependencia de Terceros:** ¿Qué proveedores participan en la cadena de valor? ¿Se han auditado sus controles y se ha definido un plan de salida (exit strategy) en caso de contingencia?
- **Capacitación del Equipo**: ¿Se ha entrenado al personal de Trade Operations, Cumplimiento y Legal no solo en el uso de la herramienta, ¿sino en la interpretación de sus resultados y en la gestión de los nuevos riesgos?
- **Gobernanza Interna:** ¿Existe un comité o procedimiento interdisciplinario (Legal, Cumplimiento, IT, ¿Negocio que evalúe y autorice estos proyectos antes de su puesta en producción?)

Conclusión: La Viabilidad Jurídica como Requisito de la Viabilidad Técnica

La inteligencia artificial ofrece un potencial transformador para el comercio exterior y la banca regulada en Argentina. Sin embargo, su adopción en un entorno de alta exigencia normativa no puede ser impulsada únicamente por consideraciones de eficiencia operativa.

La verdadera viabilidad de un proyecto de IA en este sector es jurídica y probatoria. Una implementación exitosa no es la que técnicamente funciona mejor, sino aquella cuyas decisiones pueden ser justificadas, auditadas y defendidas ante los reguladores y los tribunales. La construcción de esa defensa no es un paso posterior, sino el punto de partida del diseño. De lo contrario, la promesa de la automatización se convertirá en una nueva fuente de exposición legal para las organizaciones y sus decisores.