8 min de lectura

Resiliencia Operativa Bajo Fuego: la falsa seguridad de la IA y el vacío regulatorio en la banca de América Latina.

Categoría: Riesgo y Cumplimiento / Regulación y Gobernanza / Inteligencia Artificial · Agosto 2026

Existe una complacencia silenciosa en los Comités de Riesgo, Comités de Auditoría y Juntas Directivas de la banca latinoamericana: la firme convicción de que, mientras los congresos o las superintendencias locales no promulguen una "Ley de Inteligencia Artificial" explícita, la institución opera en una zona segura o bajo el amparo de los marcos de tecnología tradicionales.

Esta asunción constituye un peligroso espejismo de cumplimiento.

La velocidad con la que los motores de aprendizaje automático (*Machine Learning*), los Modelos de Lenguaje de Gran Escala (LLMs) y los sistemas agénticos se están integrando en el *core*, el *middle* y el *front-office* bancario ha sobrepasado la capacidad de respuesta de la regulación prudencial histórica. La banca de la región no está operando en un vacío legal; está operando bajo una red de leyes de protección de datos, ciberseguridad, prevención de blanqueo y responsabilidad fiduciaria que **ya penalizan severamente la opacidad algorítmica y la falta de control interno**, aunque no mencionen explícitamente las siglas "IA".

01 El Panorama Global: del cumplimiento voluntario a la exigencia prudencial

Para entender la magnitud del desafío en América Latina, es obligatorio examinar la arquitectura jurídica que los mercados de referencia han consolidado:

Unión Europea · EU AI Act & DORA

Bajo el Reglamento UE 2024/1689 (EU AI Act), la evaluación crediticia (*credit scoring*) de personas naturales está clasificada en el **Anexo III, Punto 5(b) como Sistema de Alto Riesgo**, exigiendo gestión continua de riesgos (Art. 9), auditorías de sesgos (Art. 10), registro de logs inalterables (Art. 12) y supervisión humana efectiva (Art. 14). Esta norma se entrelaza con **DORA (Reglamento UE 2022/2554)**, que somete a los *hyperscalers* (AWS, Google Cloud, Microsoft Azure) a supervisión regulatoria directa como Proveedores Críticos de TIC (CTPPs), obligando a las entidades bancarias a mantener y probar técnicamente planes de salida (*exit strategies*) que demuestren la capacidad real de migrar cargas de trabajo sin interrumpir la operación (Art. 28(8)).

Estados Unidos · CFPB y ECOA

La Consumer Financial Protection Bureau, mediante sus Circulares 2022-03 y 2023-03, dictaminó que la opacidad o el carácter de "caja negra" (*black box*) de un algoritmo de IA **no constituye una defensa legal válida** ante la obligación de entregar el aviso de acción adversa (*adverse action notice*) con las razones exactas de una denegación de crédito. Si la entidad no puede explicar la lógica del modelo, su uso para decisiones financieras es ilegal bajo la Equal Credit Opportunity Act (ECOA).

Singapur · MAS FEAT & MindForge

La Autoridad Monetaria de Singapur consolidó el estándar global mediante el marco FEAT (Fairness, Ethics, Accountability, Transparency), desarrollado a través del Veritas Toolkit y el AI Risk Management Toolkit, estableciendo que la responsabilidad final sobre cada inferencia algorítmica recae ineludiblemente en la Junta Directiva y la Alta Gerencia.

02 El Mapa Regulatorio en América Latina: una malla heterogénea

América Latina avanza a dos velocidades, donde los marcos avanzados coexisten con la regulación prudencial implícita:

01

Chile

La Ley N° 21.719 de Protección de Datos Personales crea la Agencia de Protección de Datos (APDP) y prohíbe el perfilamiento automatizado sin un consentimiento explícito e informado, mientras el Proyecto de Ley de IA (Boletines 16821-19 / 15869-19) ubica la evaluación crediticia en la categoría de Alto Riesgo.

02

Brasil

El Proyecto de Ley N° 2338/2023 establece un régimen de responsabilidad civil objetiva para agentes de IA de alto riesgo con inversión de la carga de la prueba a favor de la víctima, complementado por la Resolução Conjunta Nº 18 del Banco Central do Brasil en Open Finance.

03

Colombia

El Proyecto de Ley N° 043/2025 (Senado) / 324/2025 (Cámara) impone sandboxes regulatorios obligatorios para IA de alto riesgo, mientras la Superintendencia Financiera aplica la Circular Externa 029 (SARO/SARC) exigiendo trazabilidad y validación conceptual de modelos.

04

México

El Artículo 328 de la Circular Única de Bancos (CUB) de la CNBV establece que la subcontratación de infraestructura en la nube requiere autorización previa, resguardo de datos en territorio nacional e informes traducidos al español.

03 Los 4 Frentes de Colisión Técnico-Jurídica

El uso de modelos complejos genera cuatro frentes donde la práctica bancaria común choca con el ordenamiento jurídico:

DIMENSIÓN DE ANÁLISIS	SUPUESTO BANCARIO INTERNO	REALIDAD REGULATORIA Y JURISPRUDENCIAL
1. Credit Scoring y Sesgo Algorítmico	“El modelo no discrimina porque eliminamos género, raza o religión del dataset.”	Discriminación por Proxy: los algoritmos explotan proxies (código postal, hábitos de compra, dispositivo) que reproducen el sesgo histórico (Disparate Impact). Además, el TJUE (Casos SCHUFA C-634/21 y Dun & Bradstreet C-203/22) estableció que el derecho del consumidor a la explicación prevalece sobre el secreto comercial del algoritmo.
2. Fuga Transfronteriza de Datos (PII)	“Hacer llamadas a la API de un proveedor externo no es transferencia porque no almacenamos datos allá.”	Infracción de Soberanía: enviar datos de clientes mediante APIs transfronterizas es una transferencia consumada. Bajo la US CLOUD Act y la FISA 702, los datos en nubes estadounidenses quedan sujetos a acceso gubernamental extranjero, invalidando las cláusulas privadas de confidencialidad.

DIMENSIÓN DE ANÁLISIS	SUPUESTO BANCARIO INTERNO	REALIDAD REGULATORIA Y JURISPRUDENCIAL
3. Concentración de Hyperscalers	"Tenemos un contrato de nivel de servicio (SLA) del 99.9% y un BCP en papel."	Exigencia de Exit Strategy Real: DORA y los supervisores exigen probar técnicamente la migración (failover) de cargas de trabajo hacia un proveedor alternativo o nube privada, sin depender de la buena voluntad contractual del vendor.
4. Responsabilidad Directiva	"Si el modelo falla o alucina, la responsabilidad es del proveedor del software."	Responsabilidad Indelegable: los contratos de proveedores limitan su responsabilidad al monto de las licencias abonadas. Bajo la doctrina fiduciaria (Caremark / Marchand / McDonald's), los directores y ejecutivos responden personalmente por falta de supervisión en riesgos de misión crítica.

04 Caso de Estudio: el espejismo de cumplimiento en Panamá y mercados similares

El Centro Bancario Internacional (CBI) de Panamá ofrece una radiografía perfecta de esta paradoja. El mercado opera bajo el principio de **neutralidad tecnológica**, donde los supervisores no regulan la herramienta con nombre propio, sino el riesgo inherente.

La Alta Gerencia suele asumir que el **Acuerdo SBP N° 008-2010** (Riesgo Operativo) y el **Acuerdo SBP N° 011-2018** (Riesgo de TI, Ciberseguridad y Nube) cubren la IA. Sin embargo, la irrupción de modelos agénticos y generativos expone cuatro vacíos regulatorios inmediatos:

> **Validación Estática vs. Deriva Dinámica**
>
> El Acuerdo 011-2018 exige validaciones de modelos previas al lanzamiento. Un modelo con aprendizaje continuo modifica sus umbrales de decisión dinámicamente sin generar un release de código tradicional, eludiendo la gobernanza estática aprobada.

> **Auditabilidad vs. Ininteligibilidad**
>
> El Acuerdo 008-2010 exige la trazabilidad completa del procesamiento. Un modelo analítico basado en representaciones vectoriales profundas no puede ser auditado mediante esquemas lógicos lineales tradicionales frente a una inspección in situ de la SBP.

> **Segregación de Funciones (Maker-Checker)**
>
> Los principios de gobierno corporativo (Acuerdo SBP 005-2011) exigen doble autorización humana. La ejecución agéntica autónoma donde la máquina aprueba aumentos de límites o ejecuta transferencias rompe la separación de responsabilidades.

> **Tensión de Datos con la Ley 81 de 2019**
>
> Aunque el Acuerdo SBP N° 001-2022 exime del consentimiento previo el tratamiento de datos para obligaciones legales o evaluación crediticia, el envío masivo de prompts con información del cliente a APIs de hyperscalers externos excede la excepción bancaria legítima, constituyendo un procesamiento ilícito si no existe autorización explícita.

05 Recomendaciones de Mitigación: de la reacción a la resiliencia operativa

Para transitar del cumplimiento ilusorio hacia la resiliencia real, los Comités de Riesgo y Juntas Directivas deben exigir la implementación de tres pilares de gobernanza:

PILAR 01

Adopción de SLMs Locales y Soberanos (Small Language Models)

Evolucionar del consumo de APIs públicas hacia el despliegue de **Modelos Pequeños Especializados (SLMs)** alojados en infraestructura bajo control directo del banco dentro del territorio nacional o en nubes privadas locales. Los ensayos de supervisores financieros demuestran que SLMs ajustados (*fine-tuned* de 7B a 14B parámetros) superan en tareas específicas la precisión de modelos comerciales masivos, garantizando inmunidad frente a la *US CLOUD Act* y cumplimiento absoluto con la residencia de datos.

PILAR 02

Gobernanza Perimetral y Pasarelas de Control (AI Firewall)

Ningún modelo debe conectarse al *core* ni a los usuarios sin pasar por una Pasarela de Gobernanza Perimetral que incorpore:

- **Sanitización Dinámica de PII:** anonimización automática de datos personales antes de alimentar los motores analíticos.
- **Disyuntores Automáticos (Circuit Breakers):** monitoreo en MLOps que suspenda automáticamente el modelo y desvíe las solicitudes hacia evaluación humana si se detecta una deriva de equidad o un cambio inusual en las tasas de aprobación demográficas.
- **Registro Inalterable de Logs:** trazabilidad criptográfica de cada entrada, parámetro y respuesta emitida.

PILAR 03

Mallas de Auditoría Algorítmica y Supervisión Humana (HITL)

- **Debiasing Adversarial:** aplicación de técnicas estadísticas (como el re-pesaje de datos de entrenamiento o redes adversariales) para corregir el impacto dispar sin comprometer la rentabilidad del portafolio de crédito.
- **Regla de No-Delegación Exclusiva (Human-in-the-Loop):** prohibición absoluta de que decisiones adversas (rechazos de crédito, cierre de cuentas, alertas AML) sean ejecutadas al 100% por un algoritmo sin una revisión por parte de un analista humano capacitado que posea la facultad de anular (*override*) la recomendación de la máquina.

---

06 Conclusión

El cumplimiento regulatorio prudencial no es la meta final; es apenas el piso mínimo de la operación bancaria.

Esperar a que el regulador local publique una normativa específica de Inteligencia Artificial para empezar a construir estos controles es una imprudencia estratégica. Las leyes de protección de datos, los marcos de riesgo operativo y los deberes de responsabilidad fiduciaria de la alta gerencia ya están vigentes.

Las instituciones financieras de América Latina que adopten hoy una postura de **soberanía tecnológica**, **gobernanza perimetral** y **resiliencia en la inferencia** no solo estarán blindadas ante la inevitable ola fiscalizadora de las Superintendencias: convertirán la confianza y la auditabilidad en su mayor ventaja competitiva en el mercado.

Criterio humano. Inteligencia escalable. En ese estricto orden.

Únete a la conversación sobre resiliencia operativa y gobernanza de IA y síguenos en @InteligenciABancaria.

CÓMO CITAR ESTE DOCUMENTO

```
InteligenciABancaria.net · DOC.10 · Agosto 2026
```


© 2026 INTELIGENCIABANCARIA · TODOS LOS DERECHOS RESERVADOS