



EDICIÓN ESPECIAL - INNOVACIÓN

LAW JOURNAL

OCTUBRE 2026



TABLA DE CONTENIDO

www.asobanca.org.ec

Editorial

Dr. Marco Antonio Rodríguez.

La necesidad de una regulación dinámica en industrias críticas: desafíos entre innovación, continuidad operativa y supervisión en ecosistemas financieros y de seguridad **05**

Diego Andrés Merino Santacruz

Seguridad jurídica en tiempos de inteligencia artificial: retos regulatorios para el Estado y la producción normativa **10**

Libia Rivas Ordóñez

Pagarés con firma electrónica **15**

Bruno Pineda

La Inteligencia Artificial y el Derecho de los Contratos Tecnológicos: Entre la Innovación y el Vacío Regulatorio. Derecho Digital y Contratación Tecnológica **19**

Laura Ureta

Desafíos y oportunidades de la recuperación extrajudicial y judicial de la cartera vencida de las entidades financieras en la era de la inteligencia artificial **22**

Glenda Hipatia Lucero

Interoperabilidad y gobernanza digital en la ejecución de medidas precautelares **26**

Lisbeth Urquiza Aguiar

Corresponsalía no bancaria e innovación financiera en el Ecuador: lecciones del modelo japonés **30**

Tamara Alexandra Maldonado

Acceso al crédito y conocimiento del cliente financiero: reflexiones sobre el Registro de Datos Crediticios y el análisis con nuevas fuentes y tecnologías **34**

Maria Isabel Vergara

Innovación con Confianza: La nueva Ley de Ciberseguridad en Ecuador y sus desafíos regulatorios en la Transformación Digital del Sistema Financiero. **38**

Miguel Aguirre

PUBLICADO EN SEPTIEMBRE 2026

Elaborado por el Departamento Legal de Asobanca

Dr. Marco Antonio Rodríguez
Director Ejecutivo

Dra. María Gabriel López
Directora del
Departamento Legal

Henry Narváez
Asesor Legal

Víctor Obando
Asesor Legal

María Emilia Martínez
Asesor Legal Jr.

Juan Francisco Neira
Asesor Legal Jr.

La transformación de los servicios financieros ha cambiado la manera en que las personas realizan sus operaciones cotidianas, acercando soluciones que permiten administrar recursos con mayor facilidad. Hoy, un emprendedor puede recibir el pago de una venta en segundos, una familia transferir dinero y pagar servicios desde su teléfono, y una empresa gestionar sus pagos de manera inmediata. Esta transformación ha acercado la banca a las personas, facilitando el uso de los servicios financieros y abriendo oportunidades de inclusión para quienes antes encontraban barreras de distancia, tiempo o disponibilidad.

Detrás de cada una de estas operaciones existe una infraestructura que los bancos han construido y fortalecido a lo largo de los años, con inversiones sostenidas, desarrollo tecnológico y un trabajo continuo para ofrecer servicios más ágiles, seguros y accesibles. Este esfuerzo ha permitido ampliar el alcance de la banca y acompañar las necesidades de sus clientes, acompañado del fortalecimiento de la gestión de riesgos y la administración prudente de los recursos de los depositantes. En 2024, la banca privada registró 1.790 millones de transacciones, equivalentes a 57 por segundo, y los canales digitales concentraron cerca de siete de cada diez operaciones¹, dimensionando un cambio cuyo valor se aprecia en el tiempo que ahorra una persona, en la facilidad con la que un negocio cobra y en la posibilidad de participar en el sistema financiero de manera más sencilla y cotidiana.

La innovación sigue ampliando estas oportunidades y transformando la manera en que la banca se relaciona con sus clientes. La integración con proveedores tecnológicos y plataformas permite desarrollar servicios más ágiles y accesibles que, apoyados en herramientas como la inteligencia artificial y en el aprovechamiento de nuevas fuentes de información, pueden responder mejor a las necesidades de las personas y los negocios, evolución que abre posibilidades para simplificar procesos, mejorar la atención y ampliar el acceso al sistema financiero formal.

Este desarrollo exige que el Derecho evolucione junto con las nuevas formas de operar en las diferentes industrias. Cuando herramientas como la inteligencia artificial apoyan la evaluación de un cliente, el diseño de una estrategia de recuperación de cartera o la adopción de una decisión administrativa, es necesario comprender cómo sus resultados pueden contribuir al análisis y al

criterio de quienes deben decidir, bajo supervisión humana y con responsabilidades definidas. El desafío es que la legislación y quienes la aplican acompañen estas posibilidades y permitan aprovecharlas con seguridad jurídica, sin convertirse en una barrera para el desarrollo tecnológico.

Así, por ejemplo, aunque los documentos electrónicos y las certificaciones electrónicas están reconocidos por la legislación ecuatoriana, persisten dificultades para su uso y aceptación que limitan el aprovechamiento de sus beneficios. Superar estas y otras barreras contribuiría a simplificar las operaciones y dar mayor certeza a quienes las realizan, fortaleciendo la confianza necesaria para que más personas utilicen los servicios y productos digitales.

Una regulación moderna debe acompañar la evolución con criterios técnicos y proporcionales, preservando la estabilidad del sistema financiero y la protección del usuario, al tiempo que permita desarrollar soluciones que amplíen el acceso y mejoren la calidad del servicio. De igual manera, el diálogo entre autoridades, entidades financieras, empresas tecnológicas y academia resulta fundamental para que las respuestas regulatorias se apoyen en evidencia, se adapten a una realidad que continúa cambiando y acompañen la innovación, sin imponer restricciones o cargas que limiten su desarrollo.

La temática de esta edición de ASOBANCA Law Journal responde a esta reflexión: cómo acompañar la transformación financiera con un marco que permita aprovechar sus beneficios y sostener la confianza que la hace posible. En este sentido, los artículos reunidos en la presente edición desarrollan esa reflexión a través del análisis de la regulación dinámica en industrias críticas, los desafíos regulatorios de la ciberseguridad y el uso de la inteligencia artificial en la actuación administrativa, la contratación tecnológica y la recuperación de cartera. También se abordan las nuevas fuentes de información para ampliar el acceso al crédito, la circulación de pagarés con firma electrónica, la interoperabilidad y gobernanza en la ejecución de medidas precautelares, y la distribución de funciones y responsabilidades en la corresponsalia no bancaria. Estos temas permiten profundizar en las condiciones jurídicas necesarias para aprovechar el desarrollo tecnológico, preservar la confianza y ampliar las oportunidades de inclusión financiera.

¹ ASOBANCA, La resiliencia de la banca digital ante entornos desafiantes (2025).

La necesidad de una regulación dinámica en industrias críticas:

Desafíos entre innovación, continuidad operativa y supervisión en ecosistemas financieros y de seguridad.



**Diego Andrés
Merino Santacruz**

Head of Legal & Compliance
PROSEGUR CASH ECUADOR

Introducción:

Regular un sistema que ya está cambiando

En industrias altamente reguladas, la innovación rara vez llega de forma ordenada. Aparece primero en la operación: automatización de procesos, integración de plataformas, analítica avanzada, servicios digitales, nuevos esquemas de externalización de servicios, trazabilidad en tiempo real o modelos de atención que reducen fricciones para el usuario. Después llega la pregunta jurídica: ¿el marco vigente permite implementar esa solución, bajo qué condiciones y con qué nivel de supervisión?

Ese desfase no es necesariamente una falla del regulador. La norma, por definición, tiene un ciclo de formación más lento que el de la tecnología. El problema surge cuando esa diferencia temporal se convierte en una barrera estructural y la respuesta frente a cualquier innovación consiste en intentar encajarla, sin matices, en categorías diseñadas para realidades operativas distintas.

En el sistema financiero el estándar de cautela debe ser alto. La Constitución ecuatoriana califica las actividades financieras como servicio de orden público y somete su ejercicio a autorización estatal. Esa decisión constitucional responde a la protección de bienes jurídicos evidentes: estabilidad, confianza, protección del ahorro y correcto funcionamiento del sistema. Sin embargo, proteger esos objetivos no exige inmovilizar

“Una regulación dinámica no supone menos supervisión. Supone una supervisión más inteligente, proporcional y orientada a resultados.”

los modelos operativos. Exige regular mejor¹.

La experiencia práctica en industrias críticas muestra que el verdadero desafío no es escoger entre innovación y control. Es construir reglas capaces de distinguir qué cambia, qué riesgo introduce ese cambio y qué debe permanecer protegido.

1. Del cumplimiento formal a la regulación basada en funciones y riesgos

Los marcos prescriptivos tienen una virtud: ofrecen certeza. Definen actividades, requisitos, autorizaciones y límites. En sectores en los que existen recursos del público, infraestructura sensible o riesgos sistémicos, esa certeza es indispensable. Pero el mismo enfoque puede volverse rígido cuando la tecnología modifica la forma de prestar un servicio sin alterar necesariamente su función económica o el riesgo que la regulación pretendía controlar.

El Código Orgánico Monetario y Financiero contiene una señal relevante en esta materia. Al definir la actividad financiera, no solo enumera operaciones tradicionales, sino que reconoce la posibilidad de que la autoridad determine otras operaciones en función del desarrollo o innovación del mercado. Esa previsión es importante porque admite algo que en la práctica resulta evidente: el perímetro regulatorio no puede ser completamente estático².

¹ Artículo 308, Constitución de la República del Ecuador, R.O. 449, 20 de octubre de 2008.

² Artículo 143, Código Orgánico Monetario y Financiero, R.O. Segundo Suplemento 332, 12 de septiembre de 2014.

La pregunta correcta frente a una innovación no debería ser únicamente “¿esta tecnología aparece mencionada en la norma?”. Debería ser también: ¿qué función cumple?, ¿quién asume el riesgo?, ¿quién mantiene la relación con el usuario?, ¿quién custodia activos o información?, ¿se utilizan recursos de terceros?, ¿existe promesa de rendimiento?, ¿se modifica la cadena de responsabilidad?, ¿se incrementa o reduce el riesgo operativo?

Este enfoque funcional evita dos errores frecuentes. El primero es sobreregular por novedad tecnológica: tratar como una actividad completamente nueva algo que, en esencia, es una forma distinta de ejecutar una función ya conocida. El segundo es el opuesto: subestimar una innovación porque utiliza una etiqueta conocida, aunque materialmente haya trasladado riesgos hacia terceros, algoritmos, proveedores tecnológicos o infraestructuras que antes no formaban parte de la operación.

La Ley Fintech ecuatoriana constituye un reconocimiento expreso de que innovación y protección del usuario pueden y deben coexistir. Su finalidad incluye fomentar la adopción de nuevas tecnologías en productos y servicios financieros, al mismo tiempo que protege a usuarios y consumidores. Ese equilibrio debería proyectarse más allá del universo estrictamente fintech y convertirse en un criterio general de buena regulación³.

2. Continuidad operativa: el punto de encuentro entre innovación y prudencia

Durante años, la regulación financiera se concentró principalmente en solvencia, liquidez, gobierno corporativo y protección del usuario. Hoy esos pilares continúan siendo esenciales, pero la resiliencia operativa se ha convertido en una dimensión igualmente crítica. Un banco puede ser solvente y, sin embargo, sufrir una interrupción severa por una falla tecnológica, un ciberataque, un proveedor crítico, un desastre natural o una ruptura logística.

El Comité de Basilea ha desarrollado este concepto con claridad: la resiliencia operativa es la capacidad de mantener operaciones críticas durante una disrupción, responder, adaptarse, recuperarse y aprender de ella. Además, exige mapear interdependencias, gestionar terceros y fortalecer la continuidad del negocio y la infraestructura tecnológica⁴.

Esta visión tiene una consecuencia regulatoria profunda. La supervisión ya no puede observar únicamente a la entidad financiera como una organización cerrada. Debe mirar el ecosistema que hace posible su operación.

Los servicios financieros dependen de telecomunicaciones, centros de datos, sistemas de pago, proveedores de nube, ciberseguridad, redes de cajeros, transporte de especies monetarias y valores, procesamiento de efectivo, custodios, proveedores de software y múltiples terceros especializados. El Código Orgánico Monetario y Financiero reconoce dentro del sector financiero privado a las entidades de servicios auxiliares del sistema financiero, cuya participación resulta relevante para la operación y continuidad del ecosistema financiero⁵.

Ese reconocimiento debería tener una traducción regulatoria práctica: cuando una actividad soporta una operación crítica, su regulación debe evaluar no solamente el riesgo individual del proveedor, sino el riesgo que una interrupción generaría sobre la continuidad del sistema al que sirve.

El transporte de especies monetarias y valores es un ejemplo ilustrativo. La legislación de seguridad privada lo regula como una actividad especializada que comprende transporte, custodia, recepción y entrega de valores y actividades conexas. Su naturaleza combina seguridad física, logística, tecnología, gestión de riesgo, trazabilidad y coordinación con entidades financieras. Regular cualquiera de esos componentes de forma aislada puede producir exigencias formalmente correctas pero operacionalmente incompatibles⁶.

En este tipo de sectores, una buena regulación debe preguntarse no solo qué control agregar, sino cómo ese control afecta la continuidad, la seguridad y la capacidad de respuesta ante contingencias.



³ Artículo 2, Ley Orgánica para el Desarrollo, Regulación y Control de los Servicios Financieros Tecnológicos (Ley Fintech), R.O. Segundo Suplemento, 22 de diciembre de 2022.

⁴ Basel Committee on Banking Supervision, Principles for Operational Resilience (Basel: Bank for International Settlements, 2021), 1–6.

⁵ Artículo 162, numeral 3, Código Orgánico Monetario y Financiero, R.O. Segundo Suplemento 332, 12 de septiembre de 2014.

⁶ Artículo 17, Ley Orgánica de Vigilancia y Seguridad Privada, R.O. Suplemento 496, 9 de febrero de 2024.

3. El costo de regular con categorías demasiado rígidas

La rigidez regulatoria genera costos que no siempre aparecen en los análisis tradicionales de impacto normativo. Uno de ellos es la incertidumbre. Cuando una innovación no encaja con claridad en una categoría existente, los operadores pueden optar por no implementarla, aun cuando reduzca riesgos o mejore la experiencia del usuario, simplemente porque el costo de una interpretación adversa supera el beneficio esperado.

Otro costo es la fragmentación. Una misma solución puede involucrar simultáneamente regulación financiera, protección de datos, ciberseguridad, prevención de lavado de activos, seguridad privada, consumo y contratación electrónica. Si cada autoridad analiza únicamente su componente sin una visión funcional del modelo, el resultado puede ser un conjunto de exigencias individualmente razonables pero incompatibles entre sí.

Existe además un costo menos visible: la innovación defensiva. Las organizaciones terminan diseñando soluciones no necesariamente porque sean las mejores desde el punto de vista operativo, sino porque son las que mejor se parecen a las categorías que la regulación ya conoce. En el largo plazo, esto reduce competencia, limita eficiencia y puede incluso preservar riesgos que la tecnología permitiría mitigar.

La alternativa no es la desregulación. Es una regulación capaz de diferenciar niveles de intervención. No debería recibir el mismo tratamiento una herramienta que simplemente automatiza un proceso interno, una integración tecnológica con un tercero, una actividad que modifica la relación contractual con el usuario o un modelo que efectivamente introduce una nueva forma de hacer intermediación financiera.

El principio de proporcionalidad debe operar en ambos sentidos: las obligaciones deben aumentar cuando aumentan el riesgo y la intensidad de la función asumida; pero también deberían disminuir cuando el operador demuestra separación funcional, controles efectivos y ausencia de exposición material para el usuario o el sistema.

“Cuando una innovación no encaja con claridad en una categoría existente, los operadores pueden optar por no implementarla, aun cuando reduzca riesgos o mejore la experiencia del usuario, simplemente porque el costo de una interpretación adversa supera el beneficio esperado.”



4. Regulación dinámica: cinco criterios para un modelo más maduro

Un modelo regulatorio dinámico no requiere abandonar la legislación existente. Requiere utilizarla con una metodología capaz de acompañar el cambio. Cinco criterios pueden contribuir a ese objetivo.

Primero, neutralidad tecnológica. La norma debería concentrarse, siempre que sea posible, en la función, el resultado y el riesgo, no en una tecnología concreta. Regular una herramienta por su nombre puede volver obsoleta la regla antes de que termine su ciclo de implementación.

Segundo, proporcionalidad. El nivel de exigencia debe guardar relación con la materialidad del riesgo, el volumen, la complejidad, la criticidad de la función y el grado de exposición del usuario. Basilea utiliza precisamente naturaleza, tamaño, complejidad y perfil de riesgo como criterios para aplicar sus principios de resiliencia operativa⁷.

Tercero, trazabilidad de responsabilidades. La innovación suele distribuir funciones entre varios actores. Por ello, una regulación moderna debe permitir identificar con precisión quién contrata, quién ejecuta, quién custodia, quién decide, quién procesa datos y quién responde frente al usuario. La existencia de un tercero no es en sí misma el problema; el riesgo aparece cuando la responsabilidad se vuelve difusa.

Cuarto, diálogo temprano entre regulador e industria. Esperar a que un producto esté completamente desarrollado para recién discutir su encaje normativo genera costos innecesarios. Mesas técnicas, consultas previas, criterios interpretativos y mecanismos de acompañamiento permiten detectar riesgos antes de que se materialicen y evitan que la regulación opere únicamente de forma reactiva.

Quinto, experimentación controlada. Ecuador ya cuenta con una herramienta concreta: la regulación de sandboxes para desarrollos innovadores, cuyos objetivos incluyen fomentar innovación, proteger al usuario y preservar la integridad y estabilidad de los sistemas regulados. El valor del sandbox no está solamente en autorizar una prueba. Está en crear un entorno donde supervisor y operador pueden generar evidencia sobre riesgos reales antes de trasladar una solución a escala⁸.

La OCDE ha planteado una evolución desde el paradigma de “regular y olvidar” hacia uno de “adaptar y aprender”: marcos iterativos, evaluación continua, cooperación institucional y regulación preparada para ajustarse a nueva evidencia. Esa lógica resulta especialmente pertinente para mercados pequeños y altamente regulados, donde el costo de una regla equivocada puede ser proporcionalmente mayor⁹.

5. Supervisar para que la innovación sea sostenible

La madurez regulatoria no se mide por la cantidad de prohibiciones ni por la velocidad con la que se aprueba

una innovación. Se mide por la capacidad de identificar riesgos relevantes, exigir controles adecuados y permitir que los modelos evolucionen sin comprometer los objetivos que justifican la intervención estatal.

En industrias críticas, la innovación que importa no siempre es disruptiva ni visible para el usuario. Puede consistir en optimizar una ruta, automatizar una conciliación, digitalizar una evidencia, integrar un proveedor, anticipar una falla, sustituir una actividad manual o mejorar la trazabilidad de una operación. Cada uno de esos cambios puede producir eficiencia, pero también modificar el mapa de riesgos.

Por eso, la regulación dinámica debe estar estrechamente vinculada a la resiliencia operativa. La pregunta no es si un proceso es “tradicional” o “digital”. La pregunta es si el sistema puede seguir prestando sus funciones críticas de manera segura cuando ese proceso falla.

Esa perspectiva también exige mayor coordinación entre autoridades. El ecosistema financiero contemporáneo supera las fronteras institucionales tradicionales. Una innovación puede ser financieramente prudente y, al mismo tiempo, introducir riesgos de datos; puede mejorar la eficiencia tecnológica, pero generar dependencia excesiva de un proveedor; puede fortalecer la seguridad física y requerir una actualización de requisitos operativos concebidos para otra realidad tecnológica.

La respuesta no puede ser un debilitamiento del control. Debe ser un control más conectado, capaz de compartir información, evitar duplicidades y distinguir entre riesgos prudenciales, operativos, tecnológicos y de conducta.



⁷ Basel Committee on Banking Supervision, Principles for Operational Resilience, 2–3.

⁸ Artículo 4, Resolución Nro. JPRF-T-2025-0156, Norma de requisitos y parámetros para el funcionamiento de espacios controlados de pruebas regulatorias (Sandboxes Regulatorios) para Desarrollos Innovadores, R.O. 58, 12 de junio de 2025.

⁹ OECD, G20 Survey on Agile Approaches to the Regulatory Governance of Innovation (Paris: OECD Publishing, 2021), 7–9.



Conclusión:

Regular sin congelar.

La regulación cumple una función esencial en los ecosistemas financieros y de seguridad: preservar confianza, estabilidad, transparencia y continuidad. Precisamente por esa importancia, no puede permitirse quedar desconectada de la realidad que pretende gobernar.

Un marco regulatorio excesivamente estático puede producir una paradoja: intentando reducir riesgos, puede impedir tecnologías o modelos que permiten gestionarlos mejor. Del mismo modo, una regulación demasiado permisiva puede trasladar al usuario o al sistema riesgos que todavía no han sido comprendidos. La solución está en el equilibrio.

Ecuador ha comenzado a incorporar elementos valiosos: reconocimiento legal de la innovación financiera, regulación diferenciada de servicios tecnológicos, mecanismos de sandbox y un creciente énfasis en riesgo operativo y continuidad. El siguiente paso debería ser consolidar una cultura regulatoria más funcional, proporcional, tecnológicamente neutral y basada en evidencia.

Para las industrias críticas, esa evolución no es un lujo. Es una condición de resiliencia. Innovar responsablemente implica aceptar que el riesgo cambia; regular responsablemente implica que la supervisión también pueda hacerlo.

La mejor regulación no es la que intenta predecir cada innovación futura. Es la que establece objetivos claros, responsabilidades identificables y controles proporcionales, y conserva suficiente capacidad de

adaptación para seguir siendo efectiva cuando la realidad cambia.



Seguridad jurídica en tiempos de inteligencia artificial: retos regulatorios para el Estado y la producción normativa



**Libia Rivas
Ordóñez**

Presidenta Instituto Ecuatoriano
de Estudios Legislativos

“A mayor incidencia de la tecnología en la decisión final, mayor debe ser la supervisión humana, la trazabilidad, la explicabilidad y los mecanismos de revisión.”

Introducción:

Los avances tecnológicos de las últimas décadas han convertido en realidad escenarios, que parecían reservados a la ciencia ficción. Ya en 1950, Alan Turing planteó una pregunta que marcaría el desarrollo de la inteligencia artificial, ¿pueden pensar las máquinas?¹. Siete décadas más tarde, esta interrogante adquiere nuevas dimensiones, a medida que se intensifica el debate sobre la aproximación de la inteligencia artificial a la singularidad tecnológica. En este contexto, actividades que requerían conocimientos especializados o dedicar varias horas de trabajo, pueden realizarse con relativa facilidad mediante el apoyo de sistemas de inteligencia artificial generativa.

El acelerado desarrollo de la inteligencia artificial, ha llevado a varios países y regiones como la Unión Europea, a adoptar respuestas regulatorias, a través de marcos normativos de diferente naturaleza: integrales, sectoriales o fragmentados, orientados a generar y fortalecer las oportunidades y beneficios que se derivan de su utilización; pero también, a prevenir, reducir o mitigar los riesgos que puede generar, estableciendo condiciones para un uso responsable de estas tecnologías. A esto se suman, los principios, estándares y recomendaciones formuladas por organismos internacionales como la OCDE y la UNESCO que promueven el uso ético de la inteligencia artificial y la no vulneración de los derechos humanos.

Ecuador ha iniciado este proceso con la Estrategia para el Fomento del Desarrollo y Uso Ético y Responsable de la Inteligencia Artificial, expedida por el Ministerio de Telecomunicaciones y de la Sociedad de la Información en enero de 2026, y con la oficialización voluntaria de la NTE-INEN-ISO/IEC 22989 en junio del mismo año. Sin embargo, estas iniciativas no resuelven una cuestión central del Derecho Administrativo: hasta dónde puede intervenir la IA en la formación y adopción de actuaciones administrativas².

De la lectura sistemática de la Constitución y del Código Orgánico Administrativo se desprende, que el ordenamiento jurídico ecuatoriano admite el uso de la IA como una herramienta de apoyo a la actuación administrativa, inclusive, permite ciertos grados de automatización en actuaciones regladas y de bajo riesgo. Sin embargo, no existe una habilitación normativa que autorice a sustituir íntegramente a la autoridad cuando la decisión requiera motivación, ponderación de derechos o intereses, comporte el ejercicio de potestades discrecionales o sea susceptible de afectar derechos de las personas. A mayor incidencia de la tecnología en la decisión final, mayor debe ser la supervisión humana, la trazabilidad, la explicabilidad y los mecanismos de revisión.

¹ Alan Turing, Computing Machinery and Intelligence, Mind 59, n.º 236 (1950): 433-460.

² Acuerdo MINTEL-MINTEL-2025-0030, Registro Oficial, Suplemento n.º 206, 19 enero 2026; Resolución MPCEI-SC-2026-0090-R, R.O., Quinto Suplemento 306, 16 junio 2026.

2.- La inteligencia artificial en la Administración Pública ecuatoriana: fundamento jurídico y límites:

La Constitución del Ecuador, en su artículo 227, contempla los principios de la administración pública: eficacia, eficiencia, calidad, transparencia y evaluación; que a su vez son desarrollados en los artículos 3, 4 y 5 del Código Orgánico Administrativo, COA. De ahí que, la simplificación de trámites, reducción de tiempos y la mejora en la gestión pública, a través del uso de la tecnología, tenga asidero en estos principios.

El artículo 90 del Código Orgánico Administrativo señala:

“Gobierno electrónico. Las actividades a cargo de las administraciones pueden ser ejecutadas mediante el uso de nuevas tecnologías y medios electrónicos, en la medida en que se respeten los principios señalados en este Código, se precautelen la inalterabilidad e integridad de las actuaciones y se garanticen los derechos de las personas.”³

La norma invocada autoriza el uso de la tecnología, pero simultáneamente fija límites materiales. Su alcance debe interpretarse junto con los principios de juridicidad, de interdicción de la arbitrariedad, de control, de seguridad jurídica y confianza legítima, de racionalidad⁴, y el principio constitucional de legalidad⁵. El artículo 76 de la Constitución exige además, se garantice el derecho al debido proceso en toda actuación en la que se determinen derechos y obligaciones.

De ahí que, son jurídicamente viables, los usos instrumentales que apoyan pero no sustituyen, el ejercicio de las competencias de la autoridad pública, tales como: automatización del registro y trámite de documentos, gestión documental y archivo, mapeo y localización de documentos, generación de reportes de evaluación y seguimiento; entre otros.

A manera ejemplificativa, la Guía de Uso de Herramientas de Inteligencia Artificial de la Superintendencia de Competencia Económica constituye una referencia institucional útil para usos instrumentales como: gestión documental, búsqueda de información, generación de reportes, transcripciones o asistentes internos⁶.

La factibilidad jurídica de la implementación de herramientas similares a nivel de todo el sector

público, dependerá de los datos tratados, el nivel de riesgo y la intensidad con la que el resultado tecnológico influya en la decisión final. Cuando mayor sea la incidencia, más exigente debe ser la supervisión humana, la trazabilidad y la explicación ofrecida al administrado.

3.- La Inteligencia artificial frente a las actuaciones administrativas

A continuación analizaré la viabilidad de implementar la IA, en las actuaciones de la administración pública descritas en el artículo 89 del COA.

En los actos administrativos, la IA puede emplearse como herramienta de apoyo para la búsqueda de antecedentes normativos y jurisprudenciales, la identificación de resoluciones similares, la detección de inconsistencias y la sistematización de información relevante para la decisión. Incluso podría intervenir en su emisión, en el caso actuaciones regladas, sustentadas en datos objetivos y verificables y en las que no exista margen de valoración. En cambio, cuando el ejercicio de la potestad administrativa implique discrecionalidad, ponderación de derechos o intereses, valoración de pruebas o apreciaciones jurídicas complejas, la decisión final debe permanecer bajo control humano.

En los hechos administrativos, la IA puede apoyar en la automatización de actividades materiales y técnicas. Si hay el riesgo de afectación de derechos, bienes o la seguridad de las personas, la supervisión y la revisión humana deben reforzarse.

En los actos de simple administración, para clasificar y distribuir automáticamente trámites según urgencia, materia o unidad competente, para priorizar expedientes, resumir informes, generar reportes, matrices, etc.

En los actos normativos de carácter administrativo, la IA puede asistir en evaluación ex ante y ex post, técnica legislativa, detección de contradicciones, entre otros, pero no puede sustituir la competencia de la autoridad, ni la deliberación, participación y motivación.

En los contratos administrativos, la IA puede utilizarse para seguimiento de ejecución contractual, control de plazos e hitos, entre otros.

³ Artículo 90, Código Orgánico Administrativo [COA]. R.O. Segundo Suplemento 31 de viernes 07 de julio de 2017.

⁴ Artículos 14, 18, 20, 22, 23, COA.

⁵ Artículo 226, Constitución de la República del Ecuador, R.O. 449, 20 de octubre de 2008.

⁶ Superintendencia de Competencia Económica, Guía de Uso de Herramientas de Inteligencia Artificial “IA” (2025).

4. Automatización y protección de datos

Automatización e inteligencia artificial no son conceptos equivalentes. Una actuación puede ejecutarse automáticamente al verificar reglas predeterminadas o al interoperar bases de datos, sin aprendizaje, inferencia ni ponderación autónoma.

En el Derecho español, el artículo 41 de la Ley 40/2015⁷, define a la actuación administrativa automatizada, como cualquier acto o actuación realizada íntegramente a través de medios electrónicos dentro de un procedimiento, sin intervención directa de un empleado público, y exige determinar previamente los órganos responsables de las especificaciones, programación, mantenimiento, supervisión, control de calidad y, de ser el caso, auditoría, así como el órgano responsable a efectos de impugnación.

El artículo 13 del Real Decreto 203/2021⁸, complementa este régimen. En el ámbito estatal se requiere una resolución previa que autorice la automatización, su publicación en sede electrónica, la indicación de recursos y medidas para salvaguardar derechos e intereses legítimos.

“Automatización e inteligencia artificial no son conceptos equivalentes. Una actuación puede ejecutarse automáticamente al verificar reglas predeterminadas o al interoperar bases de datos, sin aprendizaje, inferencia ni ponderación autónoma.”

Ecuador carece de una regulación equivalente. Aunque en la práctica existen certificaciones y verificaciones generadas electrónicamente por entidades públicas, el COA no contiene disposiciones específicas sobre actuaciones administrativas automatizadas, en la que se detalle: la forma de configuración y supervisión del sistema, a quién se imputa el acto, cómo se acredita la autenticidad, qué información debe recibir el administrado y

cuál es el alcance de la revisión humana.

Lo que si contempla nuestra legislación, es una protección específica a los titulares de datos personales⁹. Los artículos 12 y 20 de la Ley Orgánica de Protección de Datos Personales, reconocen derechos frente a decisiones basadas única o parcialmente en valoraciones automatizadas cuando producen efectos jurídicos o afecten derechos y libertades. La Resolución No. SPDP-SPD-2026-0009-R¹⁰ desarrolla obligaciones de información y oposición en sistemas de IA. Sin embargo, este régimen protege principalmente al titular de datos; no resuelve por sí solo cuestiones administrativas sobre competencia, motivación, validez, control, imputación y responsabilidad.



⁷ Arts. 41-42. Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público. BOE No. 236 de 2 de octubre de 2015.

⁸ Art. 13. Real Decreto 203/2021, de 30 de marzo, BOE No. 77, 31 de marzo de 2021.

⁹ Arts. 12 y 20. Ley Orgánica de Protección de Datos Personales. R. O. V Suplemento. No 459. 26 de mayo de 2021.

¹⁰ Norma General para la Garantía del Derecho de Protección de Datos Personales en el Uso de Sistemas de Inteligencia Artificial, Resolución SPDP-SPD-2026-0009-R, R.O. n.º 240, 10 de marzo de 2026.

5.- Transparencia algorítmica, trazabilidad y revisión

La Corte Constitucional Colombiana ha desarrollado valiosos criterios sobre los sistemas de decisiones automatizados. En la Sentencia T-067/25¹¹ señaló, que la adopción de sistemas de decisiones automatizadas pueden generar grandes beneficios para las entidades y para la población. Sin embargo, también puede ocasionar riesgos y vulneraciones de derechos fundamentales como la no discriminación, el debido proceso y la protección de datos personales. Por lo que, la transparencia en el uso de esta herramienta es una garantía fundamental para asegurar un empleo adecuado de los datos personales y evitar que el uso de sistemas algorítmicos para la toma de decisiones por parte del Estado derive en decisiones arbitrarias o discriminatorias.

Desde esta perspectiva, la Corte destaca varias experiencias comparadas en las que se exige a las autoridades públicas, mantener un registro público de todos los sistemas de decisiones automatizadas o de inteligencia artificial que se utiliza para la toma de decisiones. En ciudades como Nueva York, las entidades públicas tienen la obligación de reportar todas las herramientas algorítmicas que: (i) utilicen u operen sobre sistemas complejos de análisis de datos, (ii) apoyen el proceso de toma de decisiones de las entidades, y (iii) tengan un efecto público material. En el registro se debe precisar el nombre de la herramienta algorítmica y el propósito, y explicar su funcionamiento general. En algunos casos, se incluye también un repositorio con el código fuente de los sistemas.

La existencia de estos registros constituye, por tanto, un mecanismo concreto de transparencia administrativa aplicado al uso de sistemas automatizados e inteligencia artificial, especialmente cuando su utilización puede incidir en los derechos e intereses de las personas.

En la sentencia T-008/26¹² la Corte Constitucional Colombiana, analiza la eventual incorporación de sistemas de inteligencia artificial en la adopción de decisiones administrativas y advierte que su utilización exige una valoración especialmente rigurosa, dada su incidencia en elementos esenciales del acto administrativo.

En particular, la Corte identifica los siguientes ámbitos de afectación:

- i. la configuración de la voluntad administrativa, entendida como la expresión racional, deliberada y responsable del ente público a través de sus servidores;
- ii. la motivación del acto administrativo, que debe garantizar transparencia y explicabilidad respecto de la forma en que se expidió;
- iii. el principio de legalidad, que exige la existencia de una base jurídica expresa que sustente toda potestad ejercida por la Administración, incluso cuando intervienen sistemas algorítmicos;
- iv. la discrecionalidad administrativa, en la medida en que la tecnología puede incidir en la ponderación de los fines que la ley asigna a cada decisión;
- v. la presunción de legalidad del acto administrativo, que se ve tensionada cuando existe incertidumbre sobre la voluntad o la motivación de un acto adoptado con apoyo de inteligencia artificial; y
- vi. la responsabilidad administrativa y estatal, particularmente en lo relativo a la delegación algorítmica y al deber de supervisión humana”

La relevancia de este pronunciamiento radica en que la Corte no limita el análisis al uso instrumental de la inteligencia artificial, sino que examina su incidencia sobre categorías estructurales del Derecho Administrativo.

De este modo, la sentencia destaca que la incorporación de la inteligencia artificial en la actividad administrativa no constituye únicamente una cuestión tecnológica o de eficiencia institucional, sino un problema estrictamente jurídico. Su utilización puede incidir en la formación de la voluntad administrativa, la motivación, la legalidad, el ejercicio de potestades discrecionales, la presunción de legitimidad de los actos y el régimen de responsabilidad estatal. En consecuencia, su implementación exige reglas que aseguren transparencia, trazabilidad, explicabilidad, supervisión humana y mecanismos adecuados de control e impugnación.

En el caso del Ecuador, garantías como: la trazabilidad, la explicabilidad, la identificación de la autoridad responsable, la revisión humana, el conocimiento del uso de IA por parte del administrado, no están configuradas en el COA, como requisitos de validez de las decisiones adoptadas por IA; por lo que se requiere un desarrollo legislativo expreso.

¹¹ Sentencia T-067/25, Corte Constitucional de Colombia, Sala Novena de Revisión, 26 febrero de 2025, párrs. 64–66, 77–81.

¹² Sentencia T-008/26, Corte Constitucional de Colombia, Sala Segunda de Revisión, 30 enero de 2026, párr. 132.

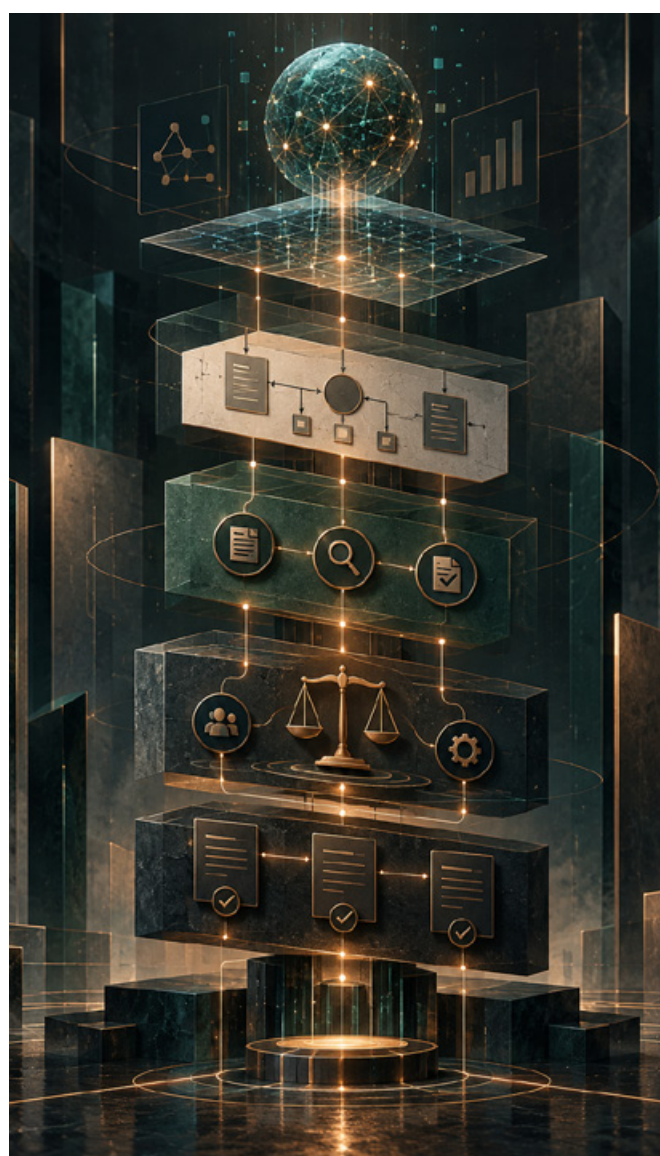


6. Conclusión:

El artículo 90 del COA constituye una habilitación suficiente para utilizar nuevas tecnologías e IA como apoyo de la actividad administrativa, siempre que se respeten los principios del Código, la integridad de las actuaciones y los derechos de las personas. También permite sostener la admisibilidad de automatizaciones regladas y de bajo riesgo, siempre que la competencia permanezca atribuible a un órgano público y existan mecanismos de control.

Sin embargo, la legislación actual es insuficiente para legitimar decisiones íntegramente automatizadas que requieran el ejercicio de potestad discrecional, ponderar derechos o intereses, observar la garantía de la motivación, o sean susceptibles de afectar derechos de las personas. En estos casos, la IA debe operar exclusivamente, como una herramienta de apoyo y no como sustituto de la autoridad competente.

Por ello, resulta conveniente reformar el COA para definir las actuaciones automatizadas y las decisiones asistidas por IA; establecer niveles de riesgo; identificar los órganos responsables de diseño, supervisión, control y auditoría; regular la trazabilidad, explicabilidad e información al administrado; determinar los supuestos de revisión humana obligatoria; y asegurar recursos administrativos y judiciales efectivos. La modernización administrativa es compatible con la seguridad jurídica solo cuando la eficiencia tecnológica se integra con legalidad, motivación, transparencia, control y responsabilidad.



Pagarés con firma electrónica



Bruno Pineda

Socio en Pérez
Bustamante & Ponce

Introducción:

Este artículo no pretende ser un tratado sobre pagarés, firmas electrónicas o repositorios públicos de información o un documento final que selle una discusión (que no ha existido hasta el momento en Ecuador). Por el contrario, solo busca iniciar la revisión de un tema que puede activar un mecanismo para acelerar la utilización de pagarés con firma electrónica, con todos los beneficios que esto puede acarrear.

Para ello iniciaré este análisis con la revisión de algunos temas básicos, como el rol de la firma, la firma electrónica versus la firma autógrafa, la validez de los pagarés, para luego analizar la circulación de éstos y lo que se requeriría para dicha circulación si el pagaré es suscrito no con una firma autógrafa sino con una firma electrónica.

1. El rol de la firma:

Si bien no existe norma legal alguna que defina lo que es una firma, que establezca su función o que desarrolle su uso, la firma tiene múltiples roles, entre los cuales podemos destacar:

La identificación del firmante, esto es, el establecimiento de quien firma un documento y la confirmación de su identidad.

La expresión de su voluntad, esto es, establecer que el documento firmado es un reflejo de la intención del firmante, por lo que se asume que éste está al tanto de lo indicado en el documento firmado.

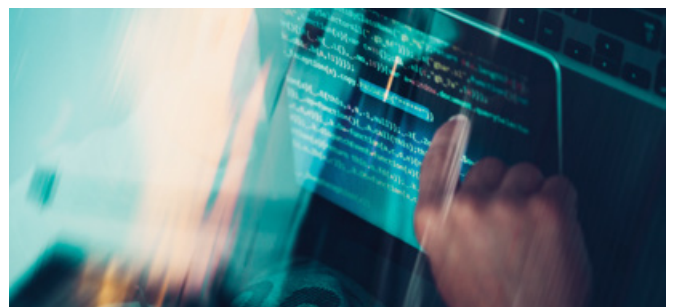
Derivado de lo anterior, como un efecto de la expresión de voluntad del firmante, su validación del

“Un pagaré suscrito con firma electrónica tiene el mismo valor que un pagaré suscrito con firma autógrafa, al no disponer norma alguna un requerimiento especial de firma y al haberse consagrado la equivalencia funcional entre firma autógrafa y firma electrónica en la Ley de Comercio Electrónico.”

documento suscrito y su aceptación del contenido específico de este. Esta aceptación, adicionalmente, permite utilizar el documento firmado como un medio de prueba de lo incorporado en él, tanto para el establecimiento de derechos como para el cumplimiento de obligaciones.

La comprobación de la firma se realiza en la práctica con su correspondencia con la constante en la documentación emitida por un registro público (en Ecuador el documento de identidad emitido por el Registro Civil).

Luego de la expedición de la Ley de Comercio Electrónico, Firmas y Mensajes de Datos (en adelante la “Ley de Comercio Electrónico”), las funciones indicadas pueden ser cumplidas tanto por una firma autógrafa como por una firma electrónica.



2. La firma electrónica

Hasta la aprobación y publicación de la Ley de Comercio Electrónico, Firmas y Mensajes de Datos en 2002 (la “Ley de Comercio Electrónico”), únicamente la firma autógrafa podía cumplir las funciones previamente indicadas de identificación, expresión de voluntad y de aceptación y validación de un documento escrito. Por tanto, las normas emitidas previamente a la aprobación y publicación de dicha ley no podían sino hacer referencia a dicha firma autógrafa.

Con la Ley de Comercio Electrónico, se incorporó la firma electrónica como una firma válida y totalmente equiparable a la firma autógrafa¹ y se indicó que los documentos firmados con firma electrónica tendrán la misma validez que aquellos suscritos con firma autógrafa². Esto no es más que un reconocimiento de la doctrina y práctica a nivel mundial, reconocida en la legislación común europea, entre otra normativa importante³.

Esto implica que, si una ley emitida antes de la publicación de la Ley de Comercio Electrónico requería que un documento, instrumento o contrato fuera firmado, este requerimiento será válida y legamente cumplido con la firma electrónica de quien debe suscribirlo.

Pero la norma no se refiere a que cualquier firma electrónica pueda tener el mismo valor que una firma autógrafa, sino solamente a aquella que cumpla los siguientes requerimientos:

- a) Ser individual y estar vinculada exclusivamente a su titular;
- b) Que permita verificar inequívocamente la autoría e identidad del signatario, mediante dispositivos técnicos de comprobación establecidos por esta ley y sus reglamentos;
- c) Que su método de creación y verificación sea confiable, seguro e inalterable para el propósito para el cual el mensaje

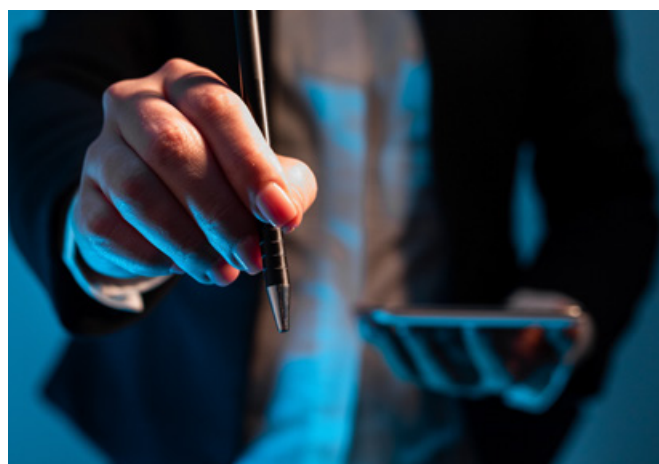
fue generado o comunicado;

d) Que al momento de creación de la firma electrónica, los datos con los que se crease se hallen bajo control exclusivo del signatario, y,

e) Que la firma sea controlada por la persona a quien pertenece.

Adicionalmente, en la Ley de Comercio Electrónico se establece dos tipos de firmas electrónicas equiparables a una firma autógrafa: la firma electrónica en general y la firma electrónica certificada. La firma electrónica en general es cualquier firma electrónica que cumple con los requerimientos indicados en el artículo 15 de la Ley de Comercio Electrónico. La firma electrónica certificada es aquella emitida por una entidad de certificación acreditada⁴.

En la práctica la diferencia sustancial entre ambos tipos de firma es que la firma electrónica certificada goza de presunción legal de validez⁵ mientras que la firma electrónica “no certificada”, en caso de ser impugnada podría requerir de un paso adicional para ser considerada como equivalente a una firma autógrafa, la designación por parte de un juez de un perito⁶ (que determine que dicha firma cumpla con los requerimientos establecidos en referido artículo 15 de la Ley de Comercio Electrónico, lo que en la práctica no genera mayores complicaciones).



¹ Artículo 14, Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, R.O. Suplemento 557 de 17 de abril de 2002.- Efectos de la firma electrónica. - La firma electrónica tendrá igual validez y se le reconocerán los mismos efectos jurídicos que a una firma manuscrita en relación con los datos consignados en documentos escritos, y será admitida como prueba en juicio.

² Artículo 44, Ley de Comercio Electrónico.- Cumplimiento, de formalidades. - Cualquier actividad, transacción mercantil, financiera o de servicios, que se realice con mensajes de datos, a través de redes electrónicas, se someterá a los requisitos y solemnidades establecidos en la ley que las rija, en todo lo que fuere aplicable, y tendrá el mismo valor y los mismos efectos jurídicos que los señalados en dicha ley.

³ Ver, Juan Francisco Rodríguez Ayuso, *Ámbito Contractual de la Firma Electrónica* (Barcelona: Librería Bosch, 2018), 169.

⁴ Artículo 29, Ley de Comercio Electrónico.- Entidades de certificación de información.- Son las empresas unipersonales o personas jurídicas que emiten certificados de firma electrónica y pueden prestar otros servicios relacionados con la firma electrónica, autorizadas por el Consejo Nacional de Telecomunicaciones, según lo dispuesto en esta ley y el reglamento que deberá expedir el Presidente de la República.

⁵ Artículo 53, Ley de Comercio Electrónico.- Presunción.- Cuando se presentare como prueba una firma electrónica certificada por una entidad de certificación de información acreditada, se presumirá que ésta reúne los requisitos determinados en la ley, y que por consiguiente, los datos de la firma electrónica no han sido alterados desde su emisión y que la firma electrónica pertenece al signatario.

⁶ Artículo 63, Ley de Comercio Electrónico.- Veracidad de la firma electrónica dentro de distintos tipos de procedimiento. La autoridad a cargo de la resolución de un proceso, cualquiera que sea su índole, en el caso de que tenga dudas fundamentadas al respecto de la veracidad de la firma electrónica contenida en un documento sometido a su consideración, deberá proceder a la verificación de la veracidad de la firma electrónica estampada en un documento electrónico. Para el efecto, el ente rector en materia de telecomunicaciones dispondrá el software adecuado que utilizarán las autoridades con capacidad resolutoria para dar cumplimiento a lo previsto en este artículo. El ente regulador en materia de telecomunicaciones deberá fundamentar la determinación de cuál será el software adecuado a través de la aplicación del principio de neutralidad funcional de la tecnología y estándares y buenas prácticas internacionales.

3. Firma en los Pagarés

En el artículo 187 de la codificación del Código de Comercio, publicada en el Suplemento del Registro Oficial 497, de 29 de mayo de 2019, constan los requisitos de validez de un pagaré, entre ellos expresamente la firma del suscriptor⁷.

Es interesante constatar que estos requisitos, y la normativa del pagaré, no han cambiado desde la Codificación del Código de Comercio del año 1925, y que ésta, a su vez, simplemente transcribe los requerimientos para los pagarés discutidos en el Congreso de Bruselas, de 1888, el primer foro internacional sobre documentos cambiarios.

Si bien la Codificación es posterior a la emisión de la Ley de Comercio Electrónico, no fue incorporada en dicha codificación enmienda o actualización alguna a las normas aplicables a letra de cambio o al pagaré, por lo que no consta expresamente en el artículo 197 el tipo de firma requerida (esto es si es autógrafa o si es electrónica). Por tanto, al haber sido consagrada en la Ley de Comercio Electrónico la equivalencia funcional de la firma electrónica, ésta cumple perfectamente lo prescrito en la letra h) del artículo 187 del Código de Comercio.

Por otro lado, si bien en otro título incorporado en la codificación, relativo a los títulos valores, sí se hace una referencia expresa al uso de firma electrónica, en el Título I, Libro III, de los Títulos Valores⁸, esta referencia no es expresamente aplicable al pagaré.

4. Validez de un pagaré con firma electrónica.

Por lo indicado anteriormente, un pagaré suscrito con firma electrónica tiene el mismo valor que un pagaré suscrito con firma autógrafa, al no disponer norma alguna un requerimiento especial de firma y al haberse consagrado la equivalencia funcional entre firma autógrafa y firma electrónica en la Ley de Comercio Electrónico.

Adicionalmente, es necesario recalcar que la obligación contenida en un pagaré (tenga firma autógrafa o electrónica) es válida entre el suscriptor y el beneficiario

mencionado como tal en el pagaré desde que el suscriptor lo suscribe (y lo “entrega” a dicho beneficiario). Esta obligación no está condicionada ni vinculada a que el pagaré circule posteriormente.

Por lo anterior, incluso si el pagaré no circula éste es válido como pagaré desde su creación⁹. De hecho, Santiago Andrade Ubidia indica, en su definición de pagaré, que éste “es un documento por el cual un firmante se compromete incondicionalmente a pagar una suma cierta de dinero a determinada persona o a su orden en el plazo especificado en el mismo”. La validez del pagaré desde su creación es también reconocida por tratadistas del exterior, tales como José Gómez Gordoa¹⁰, quien, citando a Lorenzo Mossa, indica que “el derecho cambiario es un derecho formal perfecto, que atribuye el efecto de la obligación solamente a la creación del título”.

Por ende, una vez el pagaré es suscrito y entregado al beneficiario constante en su texto, éste es exigible contra el suscriptor y genera derechos al beneficiario inicial (incluyendo el beneficio que ofrece un título de ejecución, de acuerdo con lo establecido en el Código Orgánico General de Procesos).

En el caso de un pagaré con firma autógrafa existe un documento físico, que es entregado por el suscriptor al beneficiario constante en el pagaré. Por el contrario, en el caso de un pagaré con firma electrónica, ésta es incorporada a un documento electrónico, y enviada por el suscriptor al beneficiario inicial del pagaré mediante un mensaje de datos.



⁷ Artículo 187, Código de Comercio, R.O. Suplemento 497 de 29 de mayo de 2019. “Art. 187.- El pagaré contendrá: ... h) La firma del que emite el documento (suscriptor).”

⁸ Artículo 80, Código de Comercio. “Art. 80.- Además de lo dispuesto para cada título valor en particular, los títulos valores deberán tener los siguientes requisitos: ... b) La firma de quién lo crea. La firma podrá sustituirse, bajo la responsabilidad del creador del título, por un signo o contraseña inserto mecánicamente. Este signo o contraseña debe ser protocolizado en una notaría previo su utilización. La firma podrá ser física o electrónica siempre y cuando esta última se encuentre debidamente registrada ante las entidades de certificación de información previstas en la Ley de Comercio Electrónico y Mensajes de Datos.”

⁹ Santiago Andrade Ubidia, Los Títulos Valor en el Derecho Ecuatoriano (Quito: Ediciones Legales, 2002), 301.

¹⁰ José Gómez Gordoa, Títulos de Crédito (México: Editorial Porrúa, 1988), 91.

5. Endoso y circulación

Sin perjuicio de que la validez de un pagaré, como se mencionó anteriormente, no está condicionada a la circulación posterior, una vez el pagaré es entregado por el suscriptor al beneficiario inicial constante en él, el pagaré, igual de la letra de cambio, tiene como función la circulación posterior.

En esencia, nada impide que un pagaré con firma electrónica pueda ser endosado, para lo cual el beneficiario solo tendría que incorporar una cláusula de endoso y suscribir el documento electrónico contentivo del pagaré con firma electrónica y entregarlo en un mensaje de datos al endosatario. Este endoso igual que el pagaré endosado tendría los mismos efectos que el realizado con una firma autógrafa en un pagaré suscrito con firma autógrafa.

Sin embargo el hecho de que el pagaré conste en un documento electrónico implica que eventualmente el tenedor podría endosarlo a diferentes personas en diferentes “ejemplares” del pagaré, en una evidente acción fraudulenta. Si bien es técnicamente posible determinar la fecha y hora del primer endoso y establecer su precedencia, esta posibilidad de endosos fraudulentos complica en la práctica la circulación posterior del pagaré con firma electrónica.

6. Posibles soluciones:

La circulación posterior segura y verificable de un pagaré con firma electrónica pasa por la existencia de un repositorio para el registro de endosos o cesiones de pagarés con firma electrónica.

Se podría utilizar estructuras existentes, como los depósitos centralizados de valores. Esto implicaría, sin embargo, inscribir los pagarés con firma electrónica como valores genéricos y negociarlos a través de las bolsas de valores, con la participación de una casa de valores, lo que permite el acceso solamente a pagarés avalados o endosados por instituciones financieras, dejando de lado a otros posibles beneficiarios iniciales de

pagarés con firma electrónica que no pueden inscribir y negociar valores como valores genéricos en el mercado de valores.

Otra opción sería crear un mecanismo por parte de alguna asociación u organización privada, que pueda ser un repositorio de registro de pagarés con firma electrónica a ser endosados a terceros. Este repositorio puede utilizar métodos de verificación ágiles (con la utilización de blockchain, por ejemplo) que permitan dar seguridad a los potenciales suscriptores y endosatarios de los pagarés electrónicos de la propiedad actual del pagaré, fechas de endoso así como otros detalles necesarios operativamente, como correos electrónicos, direcciones de pago, teléfonos, requeridos para el pago al acreedor o contacto del deudor. Este repositorio permitiría hacer un seguimiento de los pagarés electrónicos creados y endosados y de esta forma impedir endosos separados de documentos electrónicos contentivos de pagarés con firma electrónica a diferentes personas.

Esta solución consta ya esbozada, de alguna manera, en el Código de Comercio, en el último párrafo¹¹ del artículo innumerado añadido en la reforma realizada en febrero de 2023.

Otro tipo de opción para la negociación de pagarés no cartulares, a través de su tokenización, es el Project Promissa del Bank for International Settlements¹².

Es necesario buscar alternativas viables para posibilitar la circulación segura de pagarés con firma electrónica, para posibilitar su uso y su difusión en Ecuador. Este artículo solo busca iniciar una discusión sobre este tema.



¹¹ Art. (...) La posesión en los títulos valor electrónicos.- Cuando por ley se requiera o permita la posesión de un título valor, tal requisito se dará por cumplido respecto de los títulos valor electrónicos si se utiliza un método fiable: 1. Para determinar que ese título valor electrónico está bajo el control exclusivo de una persona; y, 2. Para identificar a dicha persona como la persona que tiene el control sobre el título valor electrónico. Cuando por ley se requiera o permita que se transfiera la posesión de un título valor, tal requisito se cumplirá con respecto de los títulos valor electrónicos mediante la transferencia del control del mismo. En el caso de que se empleen sistemas para la gestión de los títulos valor electrónicos, como los basados en registros descentralizados, que identifiquen a la persona que ejerce el control empleando seudónimos o cualquier mecanismo que no sea directamente el nombre verdadero, esta forma de identificación, y la posibilidad de vincular el seudónimo al nombre verdadero, de ser necesario, permitirá cumplir el requisito de identificar a la persona que tiene el control conforme el numeral 2 del presente artículo. En el caso de que se utilice un seudónimo la persona que se encuentra en poder del título valor debe ser plenamente identificable.

¹² Bank for International Settlements, “Project Promissa”, <https://www.bis.org/about/bisih/topics/fmis/promissa.htm> (último acceso: 14 de septiembre de 2026).

La Inteligencia Artificial y el Derecho de los Contratos Tecnológicos: Entre la Innovación y el Vacío Regulatorio

Derecho Digital y Contratación Tecnológica



Laura Ureta Arreaga

Gerente de Seguridad de la Información BANCO BOLIVARIANO

Antecedentes:

La incorporación de la inteligencia artificial (IA) a los productos y servicios tecnológicos ha dejado de ser una promesa de futuro para convertirse en infraestructura cotidiana. En apenas un lustro, la IA generativa pasó de ser un experimento de laboratorio a un componente central de software empresarial, plataformas de atención al cliente, sistemas de contratación pública, herramientas de diagnóstico médico y motores de decisión crediticia. Este ritmo de adopción, sin embargo, ha corrido a una velocidad muy superior a la de los marcos jurídicos llamados a ordenarlo.

Durante años, los contratos tecnológicos se construyeron sobre categorías relativamente estables: licencias de software, acuerdos de nivel de servicio (SLA), cláusulas de confidencialidad y de protección de datos personales. La IA ha introducido una variable que estas categorías no anticipaban: un sistema que aprende, que puede modificar su comportamiento con el tiempo, que produce resultados no siempre predecibles ni explicables, y cuyo funcionamiento depende con frecuencia de un tercero, el proveedor del modelo base, sobre el que ni el desarrollador ni el usuario final tienen control directo.

El punto de inflexión regulatorio más visible ha sido el Reglamento de Inteligencia Artificial de la Unión

“Un contrato redactado hoy puede volverse inadecuado en meses, no años, porque el proveedor actualiza el modelo, cambia sus políticas de uso de datos, o porque una nueva norma, como ha ocurrido repetidamente con el reglamento europeo, modifica plazos y obligaciones.”

Europea, cuyas obligaciones de transparencia entraron en aplicación en agosto de 2026¹. En paralelo, Estados Unidos ha optado por un mosaico de leyes estatales, como las de Colorado o California, en ausencia de una ley federal integral, y América Latina transita apenas sus primeros pasos: Ecuador, por ejemplo, aprobó en enero de 2026 una Estrategia Nacional de Uso Ético de la IA² y, recientemente, por parte de la Superintendencia de Protección de Datos se emitió una resolución relacionada con la Norma General para la Garantía del Derecho de Protección de Datos Personales en el uso de Sistemas de Inteligencia Artificial³, sin que exista todavía una ley específica que la desarrolle, dejando que los contratos privados se rijan por normas generales de contratación y protección de datos.

Este escenario, de regulación fragmentada, en constante movimiento y con vigencias escalonadas, configura el contexto en el que hoy deben redactarse los contratos tecnológicos que incorporan IA. No se trata de un vacío legal absoluto, pero sí de un terreno donde la ley disponible cubre solo una fracción de los riesgos reales, y donde la responsabilidad de anticipar esos riesgos recae, en la práctica, sobre quienes redactan el contrato.

¹ Reglamento (UE) 2024/1689, Parlamento Europeo y del Consejo de la Unión, Diario Oficial Serie L de 12 de julio de 2026.

² Acuerdo MINTEL-MINTEL-2025-0030, Registro Oficial, Suplemento 206, 19 de enero de 2026.

³ Norma General para la Garantía del Derecho de Protección de Datos Personales en el Uso de Sistemas de Inteligencia Artificial, Resolución No. SPDP-SPD-2026-0009-R, Superintendencia de Protección de Datos Personales, Registro Oficial 371 de 10 de marzo de 2026.

Desafíos en el ámbito legal de la inteligencia artificial

El primer desafío es la fragmentación normativa. Un mismo producto de IA puede estar sujeto simultáneamente al Reglamento europeo si tiene usuarios en la Unión Europea, a normas estatales estadounidenses si opera en ciertos mercados de ese país, y a un vacío casi total si su despliegue ocurre en jurisdicciones latinoamericanas que aún no han legislado la materia. Esto obliga a redactar contratos que sean simultáneamente conformes con estándares altos, generalmente los europeos y flexibles para adaptarse a marcos más laxos, sin que ello se traduzca en una reducción de garantías para el usuario final.

El segundo desafío es la atribución de responsabilidad. Cuando un sistema de IA produce un resultado erróneo, discriminatorio o dañino, la cadena de causalidad suele involucrar a varios actores: quien desarrolló el modelo base, quien lo ajustó o integró en un producto, quien lo desplegó operativamente y, en ocasiones, quien decidió actuar sobre la base de su output. Las categorías tradicionales de responsabilidad contractual y extracontractual no siempre distinguen con claridad estos roles, lo que ha llevado a marcos como el europeo a introducir definiciones específicas: proveedor, integrador, distribuidor que buscan, precisamente, evitar que la responsabilidad se diluya entre varios intervinientes sin que ninguno la asuma.

El tercer desafío es la opacidad técnica, comúnmente descrita como el problema de la 'caja negra'. Muchos modelos de IA, en particular los de aprendizaje profundo, no permiten una explicación completa y determinista de por qué produjeron un resultado específico. Esto tensiona principios jurídicos consolidados, como el derecho a una explicación en decisiones automatizadas que afectan a una persona, o el estándar probatorio necesario para demostrar negligencia en un litigio.

El cuarto desafío es el uso de datos para entrenamiento. Los sistemas de IA, especialmente los generativos, dependen de grandes volúmenes de datos, y la línea entre datos de entrenamiento legítimamente obtenidos y datos protegidos por propiedad intelectual o por normas de protección de datos personales es frecuentemente difusa. Esto genera un riesgo doble: el de infringir derechos de terceros al entrenar un modelo, y el de que los propios datos del cliente sean reutilizados sin su consentimiento explícito para mejorar el sistema del proveedor.

El quinto desafío es la velocidad de obsolescencia contractual. Un contrato redactado hoy puede volverse inadecuado en meses, no años, porque el proveedor actualiza el modelo, cambia sus políticas de uso de datos, o porque una nueva norma, como ha ocurrido repetidamente con el reglamento europeo, modifica plazos y obligaciones. Los contratos estáticos, pensados para relaciones comerciales estables de varios años, resultan mal equipados para este ritmo de cambio.

Finalmente, existe un desafío de continuidad operativa. La dependencia de un proveedor externo de IA, muchas veces un único actor con posición dominante en el mercado de modelos fundacionales, introduce un riesgo sistémico: si ese proveedor discontinúa el modelo, cambia sustancialmente sus condiciones, o queda inaccesible por razones comerciales, técnicas o incluso geopolíticas (como ha ocurrido puntualmente con restricciones de exportación de ciertos modelos), el producto o servicio que depende de él puede quedar inoperante de la noche a la mañana, sin que el contrato original haya anticipado un plan de contingencia.

Estrategias de protección legal en productos y servicios tecnológicos con IA

Frente a este panorama, la práctica contractual más sólida no intenta esperar a que la regulación se estabilice, sino que construye protección a través de mecanismos contractuales propios, complementados por marcos de buenas prácticas internacionales aun cuando estos no sean vinculantes en la jurisdicción del contrato. Una primera estrategia es la clasificación temprana del riesgo del sistema. Antes de redactar cláusula alguna, conviene determinar si el sistema de IA involucrado se ubica en una categoría de riesgo mínimo, limitado o alto, tomando como referencia, incluso fuera de la Unión Europea, la metodología del Reglamento europeo por ser hoy el estándar más desarrollado. Esta clasificación determina el nivel de exigencia contractual razonable: no es lo mismo un chatbot de atención al cliente que un sistema que participa en decisiones de contratación laboral o de otorgamiento de crédito.

Una segunda estrategia es la transferencia contractual estructurada de obligaciones regulatorias. Cuando un producto integra un modelo de un tercero, el contrato debe precisar con exactitud qué obligaciones de transparencia, gestión de riesgo y documentación técnica corresponden al proveedor del modelo base, y

cuáles recaen sobre quien lo integra y lo despliega ante el usuario final. La experiencia reciente demuestra que dejar esto implícito genera disputas justamente en el momento en que una autoridad regulatoria o un usuario afectado exige respuestas.

Una tercera estrategia es la incorporación de cláusulas de transparencia y supervisión humana como estándar contractual, incluso cuando la ley local no las exija todavía. Esto incluye comprometerse a informar al usuario final cuando interactúa con un sistema de IA, a mantener un punto de intervención humana para decisiones de alto impacto, y a documentar el razonamiento del sistema en la medida técnicamente posible. Estas cláusulas no solo anticipan obligaciones regulatorias que llegarán tarde o temprano a la mayoría de las jurisdicciones, sino que reducen el riesgo reputacional y probatorio en caso de litigio.

Una cuarta estrategia, frecuentemente subestimada, es la protección contractual de la continuidad del negocio. Esto se traduce en cláusulas de sustitución de modelo que permitan migrar a un proveedor alternativo sin degradar el servicio, en compromisos de portabilidad de datos y configuraciones, en acuerdos de nivel de servicio con métricas concretas de disponibilidad y tiempos de recuperación, y, cuando sea comercialmente viable, en mecanismos de depósito en garantía (escrow) de los componentes técnicos críticos. La dependencia de un proveedor único de IA debe tratarse contractualmente con el mismo rigor que la dependencia de cualquier proveedor crítico de infraestructura.

Una quinta estrategia es el diseño de contratos adaptativos. Dado el ritmo de cambio regulatorio, conviene incorporar cláusulas de revisión periódica obligatoria, mecanismos de actualización automática de obligaciones cuando entre en vigor nueva normativa aplicable, y ventanas de renegociación que no requieran rescindir el contrato completo. Esto evita que un contrato quede jurídicamente desactualizados meses después de su firma.

Finalmente, una sexta estrategia consiste en la combinación de protección contractual y aseguramiento de riesgos, mediante pólizas de responsabilidad civil tecnológica que cubran específicamente daños derivados del uso de sistemas de IA, complementando, nunca sustituyendo, las cláusulas contractuales de responsabilidad e indemnización.



Conclusión

La inteligencia artificial no ha creado una nueva rama del derecho, pero sí ha expuesto con particular crudeza las limitaciones de instrumentos contractuales pensados para una tecnología más predecible. La fragmentación regulatoria, la dificultad para atribuir responsabilidad, la opacidad técnica de los modelos, el uso de datos para entrenamiento, la rápida obsolescencia de los acuerdos y la dependencia de proveedores externos configuran un mapa de riesgos que ninguna ley, por sí sola, cubre todavía de manera integral.

En ausencia de un marco jurídico uniforme y estable, la protección legal efectiva en productos y servicios que incorporan IA depende, en gran medida, de la calidad de la redacción contractual: de la capacidad de anticipar escenarios que la ley aún no regula, de distribuir con claridad responsabilidades entre los distintos actores de la cadena de valor de la IA, y de construir mecanismos de continuidad operativa que no dependan exclusivamente de la buena voluntad de un proveedor tecnológico. Las organizaciones que adopten estas estrategias de manera proactiva, adelantándose a una regulación que sin duda seguirá evolucionando estarán mejor posicionadas no solo para cumplir con las normas que eventualmente se consoliden, sino para generar la confianza que el mercado y los usuarios finales exigen de cualquier sistema que, en última instancia, toma decisiones o produce resultados que afectan a personas reales.

Desafíos y oportunidades de la recuperación extrajudicial y judicial de la cartera vencida de las entidades financieras en la era de la inteligencia artificial



Glenda Hipatia Lucero

Gerente de Recuperación Comercial PRODUBANCO

Antecedentes:

Para toda entidad financiera la morosidad es uno de los indicadores más importantes y sensibles. La morosidad nos obliga a constituir provisiones afectando directamente al gasto y por tal, afecta la liquidez de la Institución, así como también incrementa el costo operativo al requerir más personal dedicado a la gestión de cobranza, en lugar de enfocar mayores esfuerzos a generar más negocios. Un tema importante es que este indicador revela la calidad de la originación de las operaciones. Por ello, la recuperación de cartera extrajudicial y judicial no se debe entender únicamente como la exigencia de pago de una obligación vencida, sino como un todo que busca establecer la capacidad de cumplimiento de un cliente, preservar el valor económico del activo y reducir pérdidas para la institución.

1. La recuperación de cartera vencida y su transformación

La gestión de cobranza extrajudicial conlleva los trabajos de contacto con el cliente, entendimiento, negociación, aplicación de soluciones especiales como reestructuración, refinanciamiento, acuerdos de pago e inclusive realización voluntaria de garantías. Los resultados positivos de esta gestión dependen de una adecuada segmentación, la oportunidad de la gestión y la capacidad de ofrecer soluciones compatibles con la situación real del deudor. La recuperación judicial, en cambio, busca obtener una sentencia y ejecutar bienes o garantías.

“La automatización debe respetar el debido proceso y evitar que una inferencia algorítmica sea presentada como hecho probado.”

Tradicionalmente, la gestión extrajudicial y judicial han operado de manera independiente y con una elevada carga operativa. La inteligencia artificial (IA) modifica esta situación al permitir el análisis masivo de datos, la predicción de probabilidades de pago, la priorización de casos e, incluso, la recomendación de estrategias. Sin embargo, su utilización también conlleva riesgos relevantes, pues podría optimizar la recuperación sobre la base de patrones que amplifiquen errores históricos, incorporar variables incongruentes que deriven en decisiones equivocadas o intensificar indebidamente el contacto con los clientes. Por ello, la innovación en la gestión de cobranza debe estar subordinada a la legalidad y a una supervisión humana efectiva. El criterio de quien lidera la gestión de recuperación continuará siendo determinante para asegurar que las estrategias aplicadas produzcan el efecto esperado.

2. Marco jurídico ecuatoriano

Nuestra Constitución establece que las actividades financieras son un servicio de orden público y deben preservar seguridad, transparencia y solidez. Al mismo tiempo, la Constitución reconoce el derecho a la protección de datos personales, al honor, a la intimidad, a recibir información precisa y a acceder a tutela judicial efectiva. En tal virtud, la recuperación del crédito no autoriza prácticas abusivas ni el tratamiento ilimitado de la información. La entidad debe equilibrar su derecho de cobro con los derechos del titular¹.

¹ Artículos 52, 66 numeral 19, 75 y 308, Constitución de la República del Ecuador, R.O. 449, 20 de octubre de 2008.

El Código Orgánico Monetario y Financiero (COMYF) regula el sistema y la relación de las entidades con sus usuarios; entre sus objetivos figuran la sostenibilidad financiera y la protección de los usuarios. Esto obliga a que las políticas de cobranza estén integradas a una correcta gestión de riesgos, a una debida seguridad de la información y gestión de reclamos². El Código de Derechos del Usuario del Sistema Financiero refuerza los conceptos de trato digno, información, libertad de elección y protección de datos, que deben reflejarse en las gestiones de contacto como en la aplicación de la negociación y escalamiento³.

La Ley Orgánica de Protección de Datos Personales (LOPD) es fundamental para cualquier aplicación de IA en cobranzas. Exige base de legitimación, transparencia, finalidad determinada, exactitud, seguridad y responsabilidad. La existencia de una relación contractual o de un interés legítimo no convierte en lícito todo tratamiento: los datos deben ser pertinentes para la cobranza. Cuando el procesamiento automatizado produzca afectación al titular, la entidad debe proporcionar información, habilitar mecanismos de impugnación y asegurar una intervención humana significativa⁴.

También resulta relevante que antes de desplegar un modelo, la entidad debe inventariar las fuentes de datos, explicar el porqué es necesaria cada variable, verificar calidad y sesgos, documentar umbrales de decisión y establecer controles de acceso, trazabilidad, continuidad y respuesta ante incidentes⁵. La tercerización no traslada la responsabilidad jurídica del banco a un proveedor.

En la fase judicial, el Código Orgánico General de Procesos (COGEP) regula los procedimientos judiciales como el ejecutivo y el proceso de ejecución. La IA puede apoyar para el control de términos, detección de inconsistencias y la estimación de recuperabilidad; pero, nunca puede sustituir la valoración jurídica del profesional, ni la decisión del juez⁶. La automatización debe respetar el debido proceso y evitar que una inferencia algorítmica sea presentada como hecho probado.

3. Oportunidades del uso de la inteligencia artificial en la recuperación de la cartera vencida



La primera oportunidad es una segmentación de la cartera más precisa. En lugar de aplicar campañas uniformes, los modelos pueden combinar historial de pagos, antigüedad de mora, comportamiento transaccional, características de la obligación y resultados de gestiones previas para estimar probabilidad de recupero y seleccionar el canal y momento adecuados. Utilizada correctamente, la IA permite dar a los gestores los casos complejos y reservar la automatización para recordatorios o alternativas sencillas.

La segunda oportunidad es la personalización para cada caso. La IA puede simular flujos de pago y proponer acuerdos sostenibles según capacidad verificable, reduciendo reincidencias y refinanciamientos inviables. Un asistente puede explicar saldos, fechas y requisitos con lenguaje claro, y derivar inmediatamente a una persona cuando exista una necesidad de asesoría especializada. La finalidad no debe ser maximizar la presión, sino mejorar la solución.

La tercera oportunidad se encuentra en la etapa judicial. La IA puede extraer datos de pagarés, contratos, y garantías; identificar documentos faltantes; generar liquidaciones, ordenar precedentes; y generar alertas sobre términos y medidas cautelares. Asimismo, modelos analíticos pueden comparar costos, duración esperada, valor de garantías y probabilidad de cobro para decidir, con revisión profesional, si conviene negociar, demandar o ejecutar. Esto mejora la asignación de recursos. Además, con la creación de un agente de IA, con los permisos y controles correspondientes, puede apoyarnos en la búsqueda de información en los archivos y sistemas del banco de pruebas a favor de la institución financiera a fin de demostrar la existencia de la obligación. Sabemos que los correos electrónicos y mensajes de WhatsApp pueden constituir prueba en juicio de la aceptación de la deuda.

² Artículos 1, 2 y 3 numerales 4 y 6, Código Orgánico Monetario y Financiero [COMYF], R.O. Segundo Suplemento 332, de 12 de septiembre de 2014.

³ Código de Derechos del Usuario del Sistema Financiero, Resolución JB-2010-1782, Junta Bancaria, R.O. 283, 21 de septiembre de 2010.

⁴ Artículos 10, 12, 20 y 30, Ley Orgánica de Protección de Datos Personales [LOPD], R.O. Quinto Suplemento 459, de 26 de mayo de 2021.

⁵ Artículos 38, 40 y 47, LOPDP1.

⁶ Artículos 347, 348, 349 y 362, Código Orgánico General de Procesos [COGEP], R.O. Suplemento 506, de 22 de mayo de 2015.

4. Riesgos y desafíos de implementación

El principal desafío es la explicabilidad. Un puntaje que determina la intensidad de la gestión, rechaza un acuerdo, o recomienda demandar, debe traducirse en razones comprensibles y auditables. La opacidad dificulta corregir datos inexactos, detectar discriminación y atribuir responsabilidades. Por ello, la institución financiera debe preferir modelos interpretables para decisiones de alto impacto, sin confundir una explicación estadística con una justificación jurídica.

El segundo riesgo es el sesgo. Variables aparentemente neutrales —zona geográfica, tipo de producto, o vías de contacto— pueden actuar como sustitutos de condiciones socioeconómicas. El control exige pruebas periódicas de desempeño, muestras representativas, revisión de falsos positivos y negativos, monitoreo para corregir resultados. Ningún objetivo de recuperación justifica diferenciar el trato por factores ajenos a la capacidad o conducta de pago.

El tercer desafío es la seguridad. Tanto los expedientes físicos como electrónicos de cobranza reúnen información financiera, patrimonial, contractual y de contacto sensible. La integración de modelos generativos abre riesgos de filtración, instrucciones maliciosas, y uso secundario por proveedores, por tal se requieren ambientes controlados, cifrado, segregación, autenticación robusta, registros de actividad auditables, y prohibiciones expresas de entrenar modelos externos con datos de clientes.

5. Comparación con normativa internacional

El Reglamento General de Protección de Datos (RGPD) reconoce el derecho a no quedar sujeto a decisiones basadas únicamente en tratamiento automatizado que produzcan efectos jurídicos o lo afecten significativamente, salvo excepciones acompañadas de salvaguardas, entre ellas intervención humana, expresión del punto de vista e impugnación⁷. La LOPDP ecuatoriana va en esta misma línea, pero la normativa europea cuenta con mayor desarrollo y experiencia supervisora, necesaria para hacer valer una revisión humana real sobre la IA.

El Reglamento Europeo de Inteligencia Artificial clasifica como de alto riesgo determinados sistemas utilizados para evaluar la solvencia o establecer la puntuación crediticia de los clientes y por tal exige que se realice una adecuada gestión de riesgos, exista un gobierno de datos, transparencia, supervisión humana, precisión y ciberseguridad⁸. Aunque la gestión de cobranza no aparece íntegramente como categoría, un sistema que permita acceso a refinanciamientos, acuerdos de pago o servicios esenciales puede producir efectos comparables. Así, considero que Ecuador podría incorporar criterios semejantes para clasificar casos y elevar controles según la necesidad.

En Estados Unidos, la Fair Debt Collection Practices Act y la Regulation F buscan evitar prácticas abusivas, engañosas o desleales, controlar comunicaciones y proporcionar validación de la deuda⁹. Además, la autoridad de protección financiera ha sostenido que el uso de modelos complejos no exime de comunicar razones específicas y exactas cuando se adopta una decisión crediticia no favorable para el cliente¹⁰.



⁷ Artículo 22, Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, Diario Oficial de la Unión Europea L 119, 4 de mayo de 2016.

⁸ Artículos 6, 9-15 y anexo III, numeral 5(b), Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, Diario Oficial de la Unión Europea L, 2024/1689, 12 de julio de 2024.

⁹ Fair Debt Collection Practices Act, 15 U.S.C. §§ 1692-1692p; Debt Collection Practices, Regulation F, 12 C.F.R. parte 1006.

¹⁰ Consumer Financial Protection Bureau, "CFPB Issues Guidance on Credit Denials by Lenders Using Artificial Intelligence", 19 de septiembre de 2023, Recuperado de: <https://www.consumerfinance.gov/about-us/newsroom/cfpb-issues-guidance-on-credit-denials-by-lenders-using-artificial-intelligence/>

6. Propuesta para las Entidades Financieras

La implementación de IA requiere indefectiblemente un inventario de casos y una clasificación por impacto.

La administración debe asignar responsabilidades desde el comité delegado y a todos sus partícipes como el negocio, riesgos, asesoría jurídica, cumplimiento, seguridad, protección de datos, auditoría y por supuesto a quien es responsable de manejar la gestión de cobranza de la Entidad. Cada sistema necesita un dueño del proceso, límites de uso, métricas, umbrales de escalamiento y un plan de cierre.

Debe establecerse una supervisión humana efectiva, con autoridad suficiente para apartarse de las recomendaciones generadas por la inteligencia artificial cuando ello resulte conveniente para los intereses institucionales. En este sentido, es indispensable precisar que una validación meramente mecánica no constituye un verdadero mecanismo de control ni puede sustituir la decisión final de la entidad.

Finalmente, los resultados que se reflejan en los indicadores deben combinar recuperación con calidad y derechos para lo cual es importante analizar detalladamente el resultado de las promesas cumplidas, los acuerdos realizados, reclamos, contactos fallidos, derivaciones por producto, diferencias de resultado entre segmentos, incidentes y anulaciones por revisión humana. Si solo se mide el monto cobrado, el algoritmo aprenderá a intensificar la presión; pero si se mide la gestión, exactitud y reincidencia, la optimización podrá estar alineada con el objetivo de una gestión óptima.

7. Conclusión

La IA puede transformar y potenciar la recuperación extrajudicial y judicial mediante una mejor segmentación, ayudándonos a tomar decisiones oportunas, contando con expedientes bien documentados y manejando un abanico de soluciones de pago más realistas. Su valor en innovación no reside en automatizar la presión ni reemplazar el juicio humano, sino en ampliar la capacidad de análisis y ofrecer intervenciones acordes a la necesidad del cliente y apoyar en la reducción de la carga operativa.

En Ecuador, la Constitución, el COMYF, la LOPDP, la

normativa de protección al usuario y el COGEP proporcionan un marco jurídico suficiente para exigir legalidad, transparencia, seguridad, trato digno y respeto al debido proceso. Bajo estas condiciones, la aplicación de inteligencia artificial en la recuperación de cartera resulta jurídicamente viable, siempre que su implementación se encuentre respaldada por criterios de gobernanza, proporcionalidad, trazabilidad y supervisión humana efectiva.

El desafío pendiente es desarrollar correctamente los algoritmos para las estrategias de cobranza extrajudicial y judicial. La experiencia internacional aporta una clasificación por riesgos y obligaciones de gobernanza, demostrando que la innovación no elimina el deber de evitar prácticas abusivas. La estrategia ecuatoriana debe habilitar innovación, pero conservar trazabilidad, revisión humana efectiva. Así, la recuperación de cartera podrá contribuir a la estabilidad financiera sin vulnerar los derechos del usuario.

Finalmente, y no siendo menos importante, la experiencia del cliente debe ocupar un lugar central en la transformación digital de la cobranza. La inteligencia artificial debe apalancar a las entidades financieras para ofrecer una gestión más clara, oportuna, empática y personalizada. En consecuencia, el verdadero éxito de la inteligencia artificial en cobranzas deberá medirse no solo por los montos recuperados, sino también por la calidad del trato, la efectividad de los acuerdos y la conservación de una relación comercial responsable con el cliente.



Interoperabilidad y gobernanza digital en la ejecución de medidas precautelares



Lisseth Urquiza Aguiar

Abogada Especialista en procesos coactivos

“La automatización no garantiza un resultado jurídicamente correcto si las reglas que gobiernan la actuación no forman parte del diseño tecnológico.”

Digitalizar una actuación no significa digitalizar el proceso

La ejecución de medidas precautelares y cautelares sobre fondos y créditos coloca a las instituciones financieras en el punto de encuentro de autoridades, procedimientos y regímenes jurídicos distintos. En el ámbito de la ejecución coactiva, el ordenamiento jurídico permite ordenar la retención de fondos y créditos y contempla la retención como medida cautelar. A ello se suman disposiciones provenientes de órganos jurisdiccionales que pueden afectar recursos mantenidos en el sistema financiero¹.

La tecnología ha mejorado una parte de este proceso. El Sistema Automatizado de Providencias Judiciales y Coactivas permite canalizar electrónicamente las disposiciones hacia las entidades financieras, superando esquemas basados en la remisión individual de oficios. Sin embargo, digitalizar la notificación no equivale a digitalizar el proceso completo².

Para la autoridad ordenante, el canal electrónico reduce tiempos de comunicación. Para la institución financiera, la recepción apenas inicia otra operación: identificar, procesar y ejecutar disposiciones provenientes de múltiples autoridades y comunicar posteriormente su resultado. Además, las capacidades de automatización no son homogéneas: dependen del volumen de requerimientos y de los recursos económicos y tecnológicos de cada entidad.

Así, frente a una necesidad común pueden coexistir soluciones distintas, desarrolladas individualmente y sin una arquitectura jurídica y operativa previamente acordada. Esta asimetría es relevante porque las

entidades financieras reciben requerimientos de múltiples autoridades, mientras que cada autoridad ordenante opera desde su propio procedimiento y sus propios mecanismos institucionales. El problema, por tanto, no es solo la cantidad de información, sino la ausencia de un diseño común que conecte recepción, ejecución, respuesta y control.

Automatizar también exige aplicar el Derecho

La automatización no garantiza un resultado jurídicamente correcto si las reglas que gobiernan la actuación no forman parte del diseño tecnológico. La concurrencia de medidas sobre los mismos recursos es un ejemplo claro. Una lógica basada exclusivamente en el orden de recepción puede ser sencilla de automatizar, pero la cronología no constituye por sí misma una regla de prelación.

El ordenamiento ecuatoriano establece preferencias entre créditos. El Código Civil reconoce causas legales de preferencia y regula su orden; el Código Tributario reconoce privilegio general al crédito tributario, con las excepciones previstas por la ley, y establece reglas para la concurrencia entre sujetos activos tributarios. Por ello, “¿qué orden ingresó primero?” y “¿qué crédito debe satisfacerse con preferencia?” son preguntas distintas³.

La diferencia importa cuando concurren medidas sobre recursos que continúan retenidos y aún no han sido transferidos. No se sostiene que una medida posterior pueda alterar una ejecución consumada. Mientras los fondos permanezcan en poder de la institución

¹ Artículo 164, Código Tributario, R.O. Suplemento 38 de 14 de junio de 2005; artículo 281, Código Orgánico Administrativo, R.O. Segundo Suplemento 31 de 7 de julio de 2017.

² Superintendencia de Bancos, Circular Nro. SB-IG-2026-0004-C, 25 de marzo de 2026; Circular Nro. SB-IG-2026-0006-C, 2 de abril de 2026.

³ Artículos 2372-2391, Código Civil, R.O. Suplemento 46 de 24 de junio de 2005; artículos 57-58, Código Tributario, R.O. Suplemento 38 de 14 de junio de 2005.

financiera, esta no debe crear ni decidir una prelación: debe aplicar la establecida por el ordenamiento jurídico.

El artículo 169 del Código Tributario regula la retención o embargo de créditos y contempla supuestos de responsabilidad solidaria del tercero notificado. No establece expresamente qué ocurre si una institución financiera entrega recursos a un acreedor de menor preferencia mientras concurre un crédito legalmente preferente. Sin embargo, su lectura conjunta con las normas de prelación permite identificar un riesgo jurídico interpretativo que conviene considerar en el diseño de los procedimientos⁴. El riesgo no se plantea como una consecuencia automática que la norma describa literalmente, sino como una posibilidad interpretativa: una autoridad recaudadora podría sostener que la actuación del tercero debe examinarse junto con las reglas legales de preferencia. Precisamente por esa incertidumbre, incorporar la prelación desde el diseño reduce la exposición de la entidad financiera y evita que una regla puramente operativa sustituya una regla jurídica.

La tecnología podría incorporar estas reglas mediante un árbol de decisiones: identificar la naturaleza de los créditos concurrentes y aplicar la preferencia legal mientras los recursos sigan retenidos. La temporalidad operaría cuando no exista una regla de prelación aplicable; si la clasificación no puede resolverse mediante reglas parametrizadas, el caso requeriría validación jurídica.

También importa la naturaleza de los fondos. La Corte Constitucional, en la sentencia 105-10-JP/21, desarrolló límites a la retención y embargo de prestaciones jubilares. Identificar el origen de los recursos puede, por tanto, modificar la actuación jurídicamente procedente⁵.

El tiempo es otra variable jurídica. Las órdenes dirigidas al sistema financiero no están necesariamente sujetas a un término uniforme: algunos regímenes fijan términos legales específicos —como ocurre en materia tributaria— y, en otros casos, el término puede constar en la providencia. La regulación de la Superintendencia de Bancos también ha evolucionado desde términos uniformes hacia el cumplimiento dentro del término señalado en la providencia⁶.

Orden de recepción, término de cumplimiento y prelación son variables distintas. Una automatización que las reduzca a una sola lógica cronológica puede ser eficiente y, al mismo tiempo, jurídicamente insuficiente.

Un flujo digital de ida y un retorno fragmentado

La fragmentación se evidencia después de ejecutada la disposición. Existe un canal centralizado para que las autoridades remitan providencias al sistema financiero, pero el procedimiento exige un retorno: la entidad financiera debe comunicar a la autoridad el resultado de su actuación⁷.

Conviene distinguir la obligación de informar, la forma documental y el canal de retorno. Como se expuso en la sección anterior, los términos de cumplimiento no son necesariamente uniformes. Sin embargo, definir qué comunicar, en qué término o mediante qué documento no resuelve necesariamente por qué canal debe ingresar la respuesta⁸.

En la normativa revisada se identifica un canal centralizado para recibir providencias en el sistema financiero, pero no con igual claridad un canal digital uniforme para devolver información a las autoridades. El oficio puede ingresar físicamente, mediante sistemas institucionales de gestión documental u otros mecanismos electrónicos. En la práctica también pueden utilizarse correos electrónicos o plataformas particulares.

Cada alternativa puede resolver la necesidad de quien la implementa sin satisfacer la trazabilidad de quien recibe. Un correo puede llegar a un funcionario sin garantizar su incorporación al sistema institucional, su vinculación al expediente, su supervisión o su permanencia ante cambios de personal. Cumplir una comunicación y asegurar su trazabilidad no son equivalentes. La dificultad se vuelve especialmente visible cuando la ejecución financiera ya ocurrió, pero la información no ha ingresado por un mecanismo que permita a la institución ordenante identificarla, asignarla y controlarla. En ese escenario, el dato existe, pero no necesariamente se transforma oportunamente en información útil para el expediente ni para la gestión recaudatoria.

⁴ Artículo 169, Código Tributario, R.O. Suplemento 38 de 14 de junio de 2005.

⁵ Corte Constitucional del Ecuador, Sentencia No. 105-10-JP/21, 10 de marzo de 2021, párrs. 64-69.

⁶ Artículo 169, Código Tributario, R.O. Suplemento 38 de 14 de junio de 2005; Superintendencia de Bancos, Circular Nro. SB-DS-2020-0001-C, 20 de enero de 2020; Circular Nro. SB-IG-2023-0046-C, 21 de agosto de 2023; Circular Nro. SB-IG-2026-0006-C, 2 de abril de 2026.

⁷ Superintendencia de Bancos, Circular Nro. SB-IG-2026-0006-C, 2 de abril de 2026, que remite a la disposición general primera del capítulo III, título XXIII, Libro I de las Normas de Control para las Entidades de los Sectores Financieros Público y Privado.

⁸ Superintendencia de Bancos, Circular Nro. SB-DS-2020-0001-C, 20 de enero de 2020; Circular Nro. SB-IG-2023-0046-C, 21 de agosto de 2023; Circular Nro. SB-IG-2026-0006-C, 2 de abril de 2026.

Tampoco una plataforma desarrollada por una institución financiera resuelve por sí sola el problema. La entidad puede invertir en una herramienta para consultar retenciones, embargos, transferencias o levantamientos y encontrar que ciertas administraciones no la utilizan por no formar parte de sus canales habilitados. Una solución puede ser tecnológicamente eficiente e institucionalmente insuficiente.

Soluciones individuales y fragmentación regulatoria

La fragmentación no se limita al canal de retorno. También puede surgir cuando distintas autoridades establecen, de manera independiente, requisitos y mecanismos para recibir y procesar información. A ello se suma la diferencia entre las velocidades de desarrollo tecnológico público y privado. Una institución financiera puede identificar una necesidad e invertir en una herramienta. En el sector público, un desarrollo puede requerir definición funcional, estimación, aprobación, priorización y disponibilidad presupuestaria antes de implementarse.

Esta diferencia incentiva soluciones individuales, pero también genera riesgos. Las administraciones públicas, en ejercicio de sus competencias, pueden establecer mecanismos y requisitos para recibir y procesar información. Una institución financiera que ya invirtió en una solución puede verse obligada a adaptarla o a mantener mecanismos distintos para responder a varias autoridades.

Si distintas administraciones establecen individualmente anexos, plataformas, sistemas documentales u otros estándares, soluciones razonables desde cada perspectiva pueden producir, en conjunto, fragmentación regulatoria. Para la banca esto implica tiempo, costos de adaptación, nuevos desarrollos y mantenimiento simultáneo de canales. La eventual discusión jurídica sobre el alcance de un requerimiento no elimina las cargas operativas que produce mientras esté vigente. El riesgo se proyecta también sobre inversiones ya realizadas: un desarrollo creado para solucionar el flujo de una entidad financiera puede requerir modificaciones posteriores si una administración define unilateralmente una forma distinta de recepción. Cuanto mayor sea el número de autoridades con requerimientos propios, mayor será la posibilidad de duplicar esfuerzos tecnológicos para resolver una misma necesidad de intercambio de información.

“La eficiencia tecnológica no debe medirse solo por la velocidad de imposición de una medida, sino también por la oportunidad con que puede ejecutarse, comunicarse, aplicarse y levantarse.”

En medio del intercambio existe una persona

El problema no se agota en autoridades e instituciones financieras. Existe una persona sobre cuyos recursos recae la medida.

Una transferencia puede haber sido ejecutada sin que la entidad acreedora haya incorporado aún la información necesaria para identificarla y aplicarla a la obligación. El afectado puede terminar obteniendo certificados o respaldos bancarios para lograr que una actuación ya ocurrida financieramente sea reconocida dentro del procedimiento. Durante ese intervalo, el dinero puede haber salido de la esfera de disponibilidad del deudor sin que la obligación refleje todavía el efecto económico de la transferencia. La fragmentación deja entonces de ser un problema interno de las instituciones y produce consecuencias directas para quien soporta la medida.

Algo semejante ocurre con los levantamientos: la rapidez alcanzada para imponer una retención no siempre tiene equivalente en la liberación de los fondos. Pueden existir recursos indisponibles para su titular que aún no han sido aplicados al cobro, o recursos cuyo levantamiento ya fue ordenado pero permanecen bloqueados mientras la información completa su recorrido institucional.

La eficiencia tecnológica no debe medirse solo por la velocidad de imposición de una medida, sino también por la oportunidad con que puede ejecutarse, comunicarse, aplicarse y levantarse.



Antes de desarrollar tecnología, construir gobernanza

Continuar desarrollando soluciones unilaterales puede profundizar la fragmentación. El desafío no es decidir quién construye primero una nueva plataforma, sino acordar las reglas comunes bajo las cuales debe operar cualquier solución.

La Superintendencia de Bancos es un actor relevante para articular esta discusión. El Libro I del Código Orgánico Monetario y Financiero le atribuye funciones de vigilancia, control y supervisión y contempla la canalización y verificación de información requerida a entidades financieras públicas y privadas para uso de otras instituciones del Estado. La infraestructura existente demuestra, además, experiencia institucional en centralizar parte de este intercambio⁹.

Esto no significa que la solución deba diseñarse unilateralmente por el organismo de control. Precisamente porque intervienen autoridades con competencias propias, entidades financieras con capacidades distintas y personas cuyos recursos son afectados, la siguiente solución debería empezar por una mesa común y no por una línea de código.

Esa discusión debe definir, entre otros aspectos, los datos mínimos de cada actuación, el régimen jurídico aplicable, la administración de términos diferentes y las reglas ante medidas concurrentes. También debe abordar la identificación de fondos protegidos, la acreditación de las respuestas, la trazabilidad y qué actuaciones pueden automatizarse o requieren validación jurídica.

Asimismo, debería contemplar reglas de escalamiento para los casos que no puedan resolverse automáticamente y criterios comunes que permitan distinguir entre retención, embargo, transferencia y levantamiento. La finalidad no es uniformar las competencias de autoridades distintas, sino construir un lenguaje operativo común para que la tecnología pueda ejecutar correctamente decisiones jurídicas que ya provienen de esas autoridades.

Solo después debería definirse la arquitectura tecnológica. Una alternativa es evolucionar hacia un flujo bidireccional en el que la infraestructura utilizada para canalizar disposiciones al sistema

financiero permita también estructurar el retorno de información a las autoridades, sin perjuicio de sus mecanismos internos de trazabilidad.

La solución no consiste necesariamente en crear más plataformas, sino en evitar que cada actor digitalice aisladamente su parte del problema. La transformación digital de la ejecución de medidas precautelares requiere primero gobernanza del proceso. Solo entonces la automatización podrá aportar velocidad, seguridad jurídica, trazabilidad, eficiencia y protección para todos los involucrados.



⁹ Artículos 59, 60 y 62, numeral 13, Código Orgánico Monetario y Financiero, Libro I, R.O. Segundo Suplemento 332 de 12 de septiembre de 2014; Superintendencia de Bancos, Resolución No. SB-2017-893, R.O. Edición Especial 230 de 17 de enero de 2018.

Corresponsalía no bancaria e innovación financiera en el Ecuador: lecciones del modelo japonés



Tamara Alexandra Maldonado

Asesor Legal Experto
BANCO PICHINCHA

1. Introducción

La innovación financiera no depende únicamente de nuevas tecnologías o modelos fintech, sino también del marco jurídico que define quién puede participar en el sistema financiero, qué funciones puede cumplir y bajo qué responsabilidades actúa.

En Ecuador, la corresponsalía no bancaria se ha consolidado como un mecanismo relevante para ampliar la cobertura de servicios financieros. Sin embargo, su desarrollo mantiene una lógica institucional: los corresponsales actúan como canales de entidades autorizadas y no como prestadores independientes.

A partir del caso japonés se aprecia un contraste relevante: el modelo ecuatoriano concentra la titularidad de la actividad financiera y la responsabilidad frente al usuario en la entidad autorizada, mientras que la regulación japonesa separa con mayor precisión la prestación del servicio, su distribución y la infraestructura operativa que la sostiene.

2. El modelo ecuatoriano: expansión de canales bajo una lógica institucional

El régimen ecuatoriano parte de una concepción de la actividad financiera como un servicio de orden público sujeto a regulación, autorización y control estatal. El Código Orgánico Monetario y Financiero estructura el sistema financiero nacional sobre la base de entidades previamente autorizadas para realizar actividades y operaciones financieras determinadas¹. Desde esta lógica, la participación en el sistema no depende únicamente del tipo de actividad realizada, sino también de la condición jurídica del sujeto autorizado para ejecutarla.

“A partir del caso japonés se aprecia un contraste relevante: el modelo ecuatoriano concentra la titularidad de la actividad financiera y la responsabilidad frente al usuario en la entidad autorizada, mientras que la regulación japonesa separa con mayor precisión la prestación del servicio, su distribución y la infraestructura operativa que la sostiene.”

Dentro de este esquema, la corresponsalía no bancaria se ha consolidado como uno de los principales mecanismos de expansión de los servicios financieros. A través de estos canales, las entidades financieras han logrado ampliar su cobertura territorial y acercar servicios a sectores donde la presencia física de oficinas resulta limitada. La evolución de los medios de pago y de los servicios financieros digitales ha reforzado además la importancia de estos canales dentro de las estrategias de inclusión financiera.

La normativa aplicable a los corresponsales no bancarios refleja con claridad esta lógica institucional, ya que la regulación los incorpora dentro del régimen de canales de atención de las entidades financieras y establece que las operaciones deben ejecutarse mediante infraestructura tecnológica conectada a la entidad financiera correspondiente. Además, exige que la responsabilidad frente al usuario permanezca en la entidad financiera y dispone que se informe expresamente que el corresponsal no se encuentra autorizado para prestar servicios financieros por cuenta propia².

Esta regulación contempla requisitos de seguridad, gestión de riesgos, capacitación, límites operativos, obligaciones contractuales y facultades de supervisión por parte de la Superintendencia de Bancos. En consecuencia, el modelo ecuatoriano es un sistema que

¹ Asamblea Nacional del Ecuador. Código Orgánico Monetario y Financiero. Registro Oficial Suplemento No. 332, 12 de septiembre de 2014, y reformas posteriores.

² Superintendencia de Bancos del Ecuador. Codificación de las Normas de la Superintendencia de Bancos. Libro I, normativa aplicable a canales de atención y corresponsales no bancarios.

³ Superintendencia de Bancos del Ecuador. Resolución SB-2016-940. Norma de control para la apertura y cierre de oficinas y canales de las entidades bajo control de la Superintendencia de Bancos.

busca ampliar la prestación de servicios financieros a través de terceros sin desvincular la actividad financiera de la entidad autorizada³.

Por ello, el elemento central del modelo ecuatoriano no es la existencia de canales no bancarios, sino la forma en que se distribuyen las funciones y responsabilidades dentro del sistema. Aunque el corresponsal no bancario participa materialmente en la atención al usuario y en la ejecución de determinadas operaciones, la titularidad de la actividad financiera y la responsabilidad principal continúan vinculadas a la entidad financiera autorizada. Esta característica constituye uno de los principales rasgos distintivos del régimen ecuatoriano y sirve como punto de partida para contrastarlo con otros modelos regulatorios.

3. El modelo japonés: disociación funcional y redes comerciales financieras

El modelo japonés se caracteriza por una distribución más diferenciada de funciones dentro del sistema financiero. A diferencia del enfoque ecuatoriano, que vincula la prestación de servicios financieros a entidades autorizadas y a los canales que operan bajo su responsabilidad, la regulación japonesa ha desarrollado mecanismos que permiten distinguir entre la titularidad del servicio financiero, su distribución y determinadas actividades de pago.

Uno de los pilares de este modelo es la figura del agente bancario (銀行代理業, ginkō dairi gyōsha) incorporada al Banking Act (Ley N.º 59 de 1981, reformada por Ley N.º 109 de 2006). Esta figura habilita a una persona jurídica no bancaria para prestar servicios bancarios en nombre de un banco principal, mediante un permiso (kyoka) otorgado por el Primer Ministro a través de la Financial Services Agency (FSA). El elemento relevante no es la participación de terceros en sí misma, sino el reconocimiento normativo de funciones diferenciadas dentro de la prestación del servicio financiero⁴.

A ello se suma el Payment Services Act (Ley N.º 59 de 2009, en vigor desde 2010), que introdujo un régimen específico para determinados servicios de pago

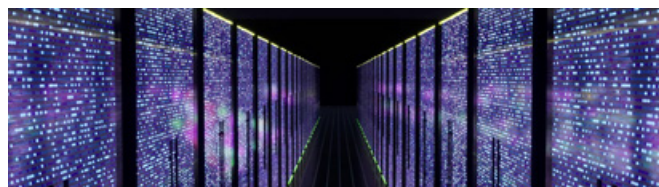
prestados por operadores no bancarios. Esta regulación parte de una lógica funcional, según la cual determinadas actividades pueden desarrollarse bajo requisitos distintos a los aplicables a una licencia bancaria plena, siempre que el operador cumpla las condiciones de registro, control y protección establecidas por la autoridad competente⁵.

Este modelo ha favorecido una mayor integración entre actividades comerciales y servicios financieros. Las redes de konbini⁶ constituyen uno de los ejemplos más visibles de esta interacción, al combinar infraestructura comercial, servicios de pago, redes de cajeros automáticos y acceso a distintas operaciones financieras dentro de un mismo punto de atención. Sin embargo, el aspecto relevante no es la existencia de tiendas de conveniencia ni la magnitud de sus redes, sino la forma en que la regulación permite distribuir funciones entre distintos participantes sin exigir que todos asuman la condición de entidad bancaria^{7,8}.

Por ello, el modelo japonés muestra una forma distinta de organizar jurídicamente la participación de actores bancarios y no bancarios dentro del sistema financiero, mediante una separación más clara entre titularidad del servicio, distribución, infraestructura y responsabilidades regulatorias.

4. Brechas estructurales del modelo ecuatoriano

La comparación entre ambos modelos no revela una diferencia en términos de infraestructura, alcance territorial o capacidad operativa. Ecuador ha desarrollado una regulación específica para los corresponsales no bancarios y ha incorporado nuevas categorías de participantes en materia de pagos y servicios financieros tecnológicos⁹. Sin embargo, la estructura jurídica sobre la que se organiza esa participación difiere de la observada en Japón¹⁰.



⁴ Financial Services Agency of Japan. Banking Act (Act No. 59 of 1981, reformada por Act No. 109 of 2006).

⁵ Financial Services Agency of Japan. Payment Services Act (Act No. 59 of 2009).

⁶ Por ejemplo, 7-Eleven, la cadena de konbini más grande de Japón, constituyó en 2001 su propio banco, el Seven Bank como una persona jurídica independiente con licencia bancaria y red de 27.000 ATM. Lawson Bank, la segunda cadena más grande de konbini, por su parte informa una red de más de 13.000 cajeros automáticos y alianzas con instituciones financieras, además de servicios de carga a aplicaciones de pago y operaciones mediante smartphone.

⁷ Seven Bank. Integrated Report 2025.

⁸ Lawson Bank. Disclosure Report 2024.

⁹ Asamblea Nacional del Ecuador. Ley Orgánica para el Desarrollo, Regulación y Control de los Servicios Financieros Tecnológicos. Registro Oficial Suplemento No. 215, 22 de diciembre de 2022.

¹⁰ Banco Central del Ecuador y Junta de Política y Regulación Monetaria. Resolución JPRM-2024-018-M. Norma que regula los medios y sistemas de pago y actividades fintech.

4.1. Concentración de la titularidad de la actividad financiera

La primera brecha se relaciona con la forma en que el ordenamiento ecuatoriano organiza la prestación de servicios financieros. Tanto el Código Orgánico Monetario y Financiero como la normativa específica de corresponsales no bancarios parten de una lógica en la que la actividad financiera permanece vinculada a entidades previamente autorizadas. En consecuencia, aunque los corresponsales participan en la ejecución material de determinadas operaciones, la titularidad jurídica del servicio continúa asociada a la entidad financiera que los habilita.

Esta configuración ha permitido ampliar la cobertura de servicios financieros sin alterar el esquema institucional del sistema. No obstante, también limita la posibilidad de reconocer a determinados operadores no bancarios como participantes con funciones propias dentro de la prestación del servicio financiero. Frente a ello, el caso japonés ofrece un enfoque distinto sobre la manera de asignar jurídicamente esas funciones.

4.2. Diferenciación funcional limitada entre participantes del sistema

La segunda brecha se refiere al nivel de diferenciación existente entre los distintos actores que intervienen en la prestación de servicios financieros. Durante los últimos años, el ordenamiento ecuatoriano ha incorporado entidades fintech, proveedores especializados y nuevas figuras vinculadas a los sistemas de pago. Sin embargo, la evolución normativa todavía se desarrolla sobre una estructura en la que varias funciones continúan estrechamente vinculadas a la entidad financiera autorizada.

Desde una perspectiva funcional, resulta posible distinguir entre actividades como la distribución de servicios, el procesamiento de pagos, la provisión de infraestructura tecnológica, la atención al usuario o la administración de fondos. Mientras el modelo japonés ha construido regímenes diferenciados para varias de estas funciones, el sistema ecuatoriano todavía mantiene una separación menos marcada entre ellas. La diferencia no consiste en la

ausencia de nuevos participantes, sino en el grado de especialización jurídica reconocido a cada uno de ellos.

4.3. Concentración de responsabilidades en la entidad autorizada

La tercera brecha se relaciona con la distribución de responsabilidades dentro del sistema financiero. La normativa ecuatoriana permite la intervención de terceros en la ejecución de determinados servicios, pero conserva la responsabilidad principal frente al usuario en la entidad financiera autorizada. La regulación de corresponsales no bancarios refleja con claridad esta lógica al exigir que la entidad financiera asuma la responsabilidad por los servicios prestados a través del canal.

Este modelo ofrece ventajas desde la perspectiva de protección al usuario y certeza jurídica, pues identifica con claridad al sujeto responsable de la operación. Sin embargo, también evidencia una diferencia con aquellos sistemas que distribuyen determinadas obligaciones entre los distintos participantes que intervienen en la prestación del servicio. Bajo el modelo ecuatoriano, la expansión de canales y operadores no altera sustancialmente el esquema de responsabilidad construido alrededor de la entidad autorizada.

5. La distribución de funciones como eje de comparación

Tanto el modelo ecuatoriano como el japonés recurren a terceros para acercar servicios financieros a los usuarios, pero no les asignan el mismo tratamiento jurídico. Ecuador y Japón admiten la intervención de actores distintos de la entidad financiera en ciertas fases del servicio; sin embargo, cada sistema define de manera diferente el alcance de esa participación.

En el caso ecuatoriano, la corresponsalía no bancaria se desarrolla bajo un esquema en el que la actividad financiera, la responsabilidad frente al usuario y la prestación del servicio permanecen vinculadas a la entidad autorizada. En Japón, en cambio, la regulación distingue con mayor claridad entre la entidad financiera y quienes intervienen en la distribución de servicios bancarios o en la ejecución de determinadas actividades de pago.

“En el caso ecuatoriano, la corresponsalía no bancaria se desarrolla bajo un esquema en el que la actividad financiera, la responsabilidad frente al usuario y la prestación del servicio permanecen vinculadas a la entidad autorizada. En Japón, en cambio, la regulación distingue con mayor claridad entre la entidad financiera y quienes intervienen en la distribución de servicios bancarios o en la ejecución de determinadas actividades de pago.”

- El contraste con Japón aparece en el reconocimiento jurídico de determinadas funciones. Mientras el régimen ecuatoriano mantiene la prestación del servicio financiero armada alrededor de la entidad autorizada, el modelo japonés distingue con mayor claridad entre la entidad financiera, la distribución de servicios bancarios y ciertas actividades de pago.
- Se trata de dos formas distintas de organizar una misma realidad económica. Ambos sistemas admiten la intervención de terceros, pero difieren en la forma de distribuir habilitaciones, funciones y responsabilidades.

Más que una propuesta de reforma, la experiencia japonesa ofrece un punto de contraste. Su interés radica en mostrar que la participación de terceros en la prestación de servicios financieros puede organizarse de maneras distintas, permitiendo apreciar con mayor claridad los rasgos que caracterizan al modelo ecuatoriano de corresponsalía no bancaria.

El objetivo de esta comparación no es establecer la superioridad de un modelo sobre otro, sino evidenciar cómo distintas respuestas normativas atienden una misma necesidad: ampliar el acceso a servicios financieros sin debilitar la supervisión ni la protección del usuario. Desde esa mirada, el contraste principal aparece en la distribución de funciones, habilitaciones y responsabilidades dentro de la prestación de servicios financieros.

6. Conclusión

La comparación entre la corresponsalía no bancaria ecuatoriana y el agente bancario japonés evidencia que la diferencia entre ambos modelos no radica en la participación de terceros dentro de la prestación de servicios financieros, sino en la posición jurídica que esos terceros ocupan dentro del sistema financiero.

- El CNB ecuatoriano constituye una extensión operativa de la entidad financiera. Su actuación se desarrolla bajo la autorización, infraestructura y responsabilidad de la entidad que lo habilita.
- La corresponsalía no bancaria se encuentra plenamente regulada. La normativa prevé mecanismos específicos de supervisión, gestión de riesgos, control operativo y protección al usuario.



Acceso al crédito y conocimiento del cliente financiero: reflexiones sobre el Registro de Datos Crediticios y el análisis con nuevas fuentes y tecnologías



María Isabel Vergara Caicedo

Experta en Asesoría Jurídica del Banco Central del Ecuador y Docente de la Universidad Andina Simón Bolívar

“La exclusión no solo genera pérdidas microeconómicas y estrés en las personas, sino que reduce el bienestar y el crecimiento económico.”

Resulta casi inverosímil que hoy en día, en pleno 2026, en la era de la información digital, en un mundo y sociedad supuestamente hiperconectados, no logremos superar la gran brecha de información asimétrica en el mercado de crédito, que afecta principalmente a las pymes y a las personas en la titánica tarea de incluirse financieramente. Si bien ya no cabe hablar de falta de información, sino de su calidad, la cual se ve afectada por la licitud de sus fuentes, anacronismo normativo y falta de acuerdos; estos son los temas que se abordan a continuación, con el propósito de proponer alternativas que mejoren el acceso al crédito y el conocimiento del cliente financiero, a partir del Registro de Datos Crediticios y del análisis con nuevas fuentes y tecnologías.

Corresponde partir de un concepto básico: el mercado de crédito no es perfecto, en parte por fallos de mercado, entre los cuales, a efectos de este texto, se destaca la información asimétrica¹. Los fallos de mercado pueden justificar una medida estatal como la regulatoria o la de control para su corrección, que en el caso ecuatoriano es la regla². En 1981, Stiglitz y Weiss analizaron los efectos de la opacidad de la información sobre los posibles deudores y advirtieron que esta puede generar selección adversa y riesgo moral, pues el contenido del análisis de riesgo se vicia hacia una dinámica más cercana al azar y apuestas, en lugar de una estimación de la pérdida esperada en función de la información disponible³.

Ahora bien, la falta de información oportuna y la ausencia de metodologías de evaluación de capacidad de pago provocan la “re-exclusión financiera”. En el Ecuador, este fenómeno afecta a más de 1,2 millones de ciudadanos que, habiendo ingresado al sistema formal, vuelven a quedar fuera de él debido al deterioro de sus perfiles crediticios o caídas en su score. La exclusión no solo genera pérdidas microeconómicas y estrés en las personas, sino que reduce el bienestar y el crecimiento económico⁴.

Situación que guarda alarmante parecido con lo descrito hace más de 40 años, lo cual indica que el problema probablemente no es tecnológico, no se trata necesariamente de recursos, sino de diseño institucional⁵.

Por tanto, conviene detenerse en el diseño institucional, que radica en normas, entidades y actores, y las formas en las que estas se relacionan; partiendo de ello, la operatividad del sistema de información crediticia previsto en el Libro I del Código Orgánico Monetario y Financiero⁶, en particular en sus artículos 357 y 358, ampliamente discutidos y reformados en los últimos años. Para su análisis corresponde dividirlo en dos secciones, la primera se refiere a las fuentes y a la conceptualización; y la segunda, a las nuevas tendencias legislativas sobre los periodos sujetos a análisis y la disponibilidad de la información.

¹ Joseph E. Stiglitz y Jay K. Rosengard, La economía del sector público (4a. ed.) (Antoni Bosch editor, 2015), 55–90.

² Artículo 308, Constitución de la República del Ecuador, R.O. 449 de 20 de octubre de 2008.

³ Joseph E. Stiglitz y Andrew Weiss, “Credit rationing in markets with imperfect information”, American Economic Review 71, n.º 3 (1981): 393–410.

⁴ Rossana Bonilla et al., Boletín Especializado de Re exclusión Financiera, Boletín Especializado n.º 41 (Quito: Instituto de Estudios Empresariales, Universidad San Francisco de Quito (USFQ) y Red de Instituciones Financieras de Desarrollo (RFD), 2025).

⁵ Sebastián Bozzo Hauri, “Sobreendeudamiento, sistemas de información crediticia y la protección de los datos personales del consumidor en Chile”, Revista de Derecho (Valparaíso), n.º 55 (diciembre de 2020): 99–124, <https://doi.org/10.4067/S0718-68512020000200099>.

⁶ Artículo 357, Código Orgánico Monetario y Financiero, R.O. Segundo Suplemento 332 de 12 de septiembre de 2014.

El precitado artículo enfrentó reformas significativas en los años 2017 y 2018 en lo que refiere a las fuentes y el tipo de información que debe revelarse, aclarando que dicho registro refiere a información positiva y negativa del deudor e incorporando otro tipo de información asociada a la capacidad de pago por medio del consumo. Estos cambios permitirían aportar información significativa más allá de la obtenida desde el mismo sistema financiero, al acoger buenas prácticas que promueven la personalización y la generación de productos adaptados a las necesidades y riesgos inherentes de cada segmento⁷. Además, estas reformas permitieron incorporar a entidades que, sin ser financieras, otorgan créditos, aportando información en doble vía con miras a mitigar riesgos asociados a un posible arbitraje regulatorio⁸.

El incremento de estas fuentes, por medio de su reconocimiento legal y la consecuente licitud, genera un reto operativo relacionado con el mecanismo de análisis dentro de sistemas diseñados para entidades financieras cuyas metodologías tardan en actualizarse. Este desafío se profundiza cuando su implementación demanda una necesaria articulación política e interinstitucional; en ese sentido, el regulador financiero ecuatoriano impone de forma explícita que la Superintendencia de Bancos debe coordinar con el SRI, las empresas de servicios básicos

y el Ministerio de Infraestructura y Tecnología (o quien haga sus veces) las acciones normativas, operativas y tecnológicas para canalizar y depurar los datos complementarios de tributos y servicios básicos en un plazo máximo de 18 meses, contados desde el 20 de agosto de 2026⁹. Resulta fundamental concretar estos convenios de intercambio de datos para superar la resistencia de las instituciones a transferir información¹⁰.

Sin perjuicio de ello, las reformas sobre las fuentes de información constituyen un terreno fértil para la implementación de nuevas tecnologías. La Inteligencia Artificial y la analítica avanzada (Big Data) permiten procesar masivamente variables cualitativas e información no tradicional como redes sociales, huella digital, comportamiento tributario y transaccional¹¹.

Los expertos señalan que la IA democratiza el acceso al crédito para personas históricamente excluidas de la banca tradicional al generar perfiles predictivos y ajustar de manera dinámica las ofertas de crédito sin sacrificar la prudencia ni la liquidez del sistema¹²¹³. Estas herramientas permitirían aplicar de forma eficiente criterios basados en la economía del comportamiento¹⁴, como notificaciones personalizadas basadas en sesgos de autoeficacia, sesgo del presente e impulsividad; con el objeto de mejorar la salud financiera y mitigar la



⁷ Matilde Cuenca Casas, "Intercambio de información positiva de solvencia y funcionamiento del mercado de crédito", *InDret: Revista para el Análisis del Derecho*, n.º 3 (2017), <http://www.indret.com>.

⁸ Estas reformas además establecieron normativa sobre los derechos sobre los datos y protección al consumidor, elementos que por sí solos superan el enfoque de este texto pero son indispensables para su efectiva implementación de forma concordante con el ordenamiento jurídico; procurando mitigar riesgos como la extrema opacidad de los algoritmos de inteligencia artificial ("cajas negras") y el arbitraje regulatorio de las empresas tecnológicas, con el objeto de asegurar que la innovación no devenga en discriminación algorítmica ni exclusión oculta de grupos vulnerables.

⁹ Resolución No. JPRFM-2026-033-F, Junta de Política y Regulación Financiera, 20 de agosto de 2026.

¹⁰ Patricia González, "Estos son los cambios que tendrá el registro de datos crediticios con el que se calcula el 'score'", *Primicias*, 23 de agosto de 2026, <https://www.primicias.ec/economia/cambios-registro-datos-crediticios-score-credito-buro-bancos-deudas-130881/>.

¹¹ International Bank for Reconstruction and Development y World Bank, *Global Financial Development Report 2019/2020: Bank Regulation and Supervision a Decade after the Global Financial Crisis* (Washington, DC: World Bank, 2020), <https://doi.org/10.1596/978-1-4648-1447-1>.

¹² Wilson Araque Jaramillo, *La inclusión financiera frente a los desafíos actuales*, Serie Inclusión y Desarrollo (Quito: Universidad Andina Simón Bolívar, 2025).

¹³ Pese a no ser un elemento central de esta discusión, como parte de la operatividad y adecuada implementación del Registro de Datos Crediticios corresponde tener muy en cuenta ciertas limitaciones impuestas por el legislador sobre decisiones automatizadas, que si bien buscan proteger al titular del derecho, constituyen una barrera de entrada importante al análisis de información por medios tecnológicos y las sinergias que pueden surgir de su implementación. Artículo 20, Ley Orgánica de Protección de Datos Personales, R.O. Quinto Suplemento 459 de 26 de mayo de 2021.

¹⁴ Richard H. Thaler y Cass R. Sunstein, *Nudge: Improving Decisions about Health, Wealth, and Happiness*, ed. rev. y ampliada (Nueva York: Penguin, 2009).

morosidad antes de que ocurra el impago¹⁵.

Estos elementos tienen la capacidad de generar sinergias tanto para la oferta como para la demanda. Por ejemplo, uno de los mecanismos para obtener información de calidad consiste en contrastar la que se genera por el consumo con la que se reporta a entes públicos; así ocurre con la facturación frente a la declaración del impuesto a la renta, pues, si ambas fuentes están adecuadamente relacionadas, el resultado puede ser altamente confiable y útil para la toma de decisiones. Por otro lado, si esta información más confiable está disponible a los oferentes de crédito, el costo de transacción asumido por el demandante asociado a su obtención y prueba fehaciente se reduciría de forma significativa, con la consecuente disminución de las barreras de entrada al producto.

También, en un análisis crítico de la realidad nacional es evidente, público y notorio que existe la errada creencia generalizada de que las personas se ven impedidas de obtener un crédito por la mera existencia del registro de datos crediticios, creencia que tampoco distingue la información positiva de la negativa, desconociendo su función en la generación de confianza en el sistema financiero. Esta creencia ha impactado las más recientes reformas legislativas, que en aras de la “inclusión financiera” han segmentado y reducido el volumen de información disponible. A modo de ejemplo, la Ley Orgánica para Impulsar la Economía de las Mujeres Emprendedoras, en su Disposición Reformatoria Sexta, modificó la antigüedad de la información de riesgo crediticio (positiva o negativa) de 6 a 4 años y de 3 a 2 años en la disponibilidad dentro de los reportes¹⁶; ello sin contar la disposición expresa de eliminar información del registro de datos crediticios de personas a las que se busca incluir financieramente.

Corresponde puntualizar que, si bien puede existir información reciente altamente relevante que dé cuenta de la situación presente del sujeto de crédito, la reducción de la antigüedad disponible impide un análisis

histórico capaz de reflejar un comportamiento de largo plazo que podría resultar relevante y positivo para analizar obligaciones sostenidas en el tiempo como es el caso de un crédito hipotecario. En ese mismo sentido, no faltan los proyectos que buscan promover la actualización de la información demostrando el comportamiento reciente de un deudor, pese a que la normativa vigente no lo limita, sino que ya lo reconoce¹⁷. Estos ejemplos permiten observar que no toda normativa, pese a sus fines loables, tiene la capacidad de alcanzar los objetivos propuestos; de ahí la importancia de sustituir la referida creencia por una premisa más precisa: nadie presta a quien no conoce.

Fuera de ello, de forma transversal, existen elementos adicionales que promueven la implementación de un sistema de scoring basado en nuevas tecnologías que merecen ser mencionados. Uno de ellos es el incremento de información contrastable mediante la obligatoriedad de la facturación electrónica¹⁸ inmediata y la imposibilidad de anulación de comprobantes emitidos al “Consumidor Final”¹⁹. El Servicio de Rentas Internas (SRI) ha promovido importantes acciones hacia la formalización y mejora recaudatoria que de forma paralela generan información que podría ser de alta calidad sobre los medios de pago empleados, si la operación fue a crédito y el comportamiento de consumo del solicitante de un crédito; con las sinergias y riesgos que conlleva.

También la implementación de tecnología financiera y la transición del uso de medios de pago como el efectivo y los cheques hacia medios digitales o electrónicos²⁰ permiten obtener información relacionada con la trazabilidad de la información en sí misma y el perfilamiento del deudor, así como la obtención de metadatos para la construcción de productos personalizados; reduciendo la brecha hacia una información menos asimétrica.

De todo lo expuesto se desprende una propuesta concreta de diseño institucional. Lo que falta no es,

¹⁵ José Luis Negrin, “Mecanismos para compartir información crediticia: Evidencia internacional y la experiencia mexicana”, *El Trimestre Económico* 68, no 271(3) (2001): 405–66.

¹⁶ Disposición Reformatoria Sexta, Ley Orgánica para Impulsar la Economía de las Mujeres Emprendedoras del Ecuador, R.O. Tercer Suplemento 758 de 10 de marzo de 2025.

¹⁷ Asamblea Nacional de la República del Ecuador. Sala de prensa, “John Polanco propone actualizar el historial crediticio de quienes cancelen sus deudas”, 9 de junio de 2026, <https://www.asambleanacional.gob.ec/es/noticia/117091-john-polanco-propone-actualizar-el-historial-crediticio>.

¹⁸ Servicio de Rentas Internas (SRI). Dirección General, “Resolución Nro. NAC-DGERCGC25-00000014: Normas para la anulación de comprobantes de venta, retención y documentos complementarios, emitidos en modalidad electrónica”, 27 de junio de 2025.

¹⁹ Servicio de Rentas Internas (SRI). Dirección General, “Resolución Nro. NAC-DGERCGC25-00000017: Reformar la Resolución NAC-DGERCGC25-00000014 ‘Establecer las normas para la anulación de comprobantes de venta, retención y documentos complementarios, emitidos en modalidad electrónica’”, 29 de julio de 2025.

²⁰ Redacción Primicias, En 2025, en Ecuador, se redujeron los retiros de efectivo y aumentó el monto de transacciones por canales digitales., 31 de agosto de 2026, <https://www.primicias.ec/economia/reduccion-retiros-dinero-efectivo-pagos-digitales-billeteras-ecuador-108556/>.

nueva normativa en estricto rigor, sino la implementación efectiva de lo ya normado. El diseño institucional no se agota en la norma, requiere de acuerdos y de coordinación interinstitucional para su adecuada ejecución. En consecuencia, el marco legal vigente debe complementarse con instrumentos de gobernanza que traduzcan el mandato normativo en operación real, tales como: convenios vinculantes de intercambio de datos entre la Superintendencia de Bancos, el Servicio de Rentas Internas, los prestadores de servicios básicos y el Ministerio rector de las tecnologías, sobre estándares comunes de interoperabilidad, calidad y trazabilidad; protocolos técnicos y plazos exigibles; y mecanismos de rendición de cuentas que superen la resistencia institucional a transferir información.

Nada de ello es viable sin un alineamiento integral que articule al Legislativo, Ejecutivo, a los organismos de control y a las entidades públicas titulares de la información en torno a un objetivo compartido; de lo contrario, aun la mejor norma quedará en el plano del enunciado y el Registro de Datos Crediticios no alcanzará su potencial como infraestructura de inclusión.

El acceso al crédito y el conocimiento del cliente financiero no se agotan en la mera apertura de un producto ni en la bancarización básica. El camino hacia una inclusión real y sostenible, orientada al bienestar financiero, requiere de un ecosistema cimentado en información crediticia y de consumo confiable, simétrica y de alta calidad. Como sostiene la doctrina económica y jurídica, la opacidad informativa y la limitación regulatoria de los historiales solo propagan la selección adversa; de tal forma, encarecería el crédito para más del 90% de deudores que cumplen adecuadamente con sus obligaciones en Ecuador²¹, propendiendo al pernicioso fenómeno de la re-exclusión financiera²², o peor, la usura²³. En este escenario, el rol de las nuevas tecnologías, como la Inteligencia Artificial, la analítica de Big Data, las billeteras digitales y los modelos de score alternativos, constituye un avance decisivo hacia dicho objetivo. Estas herramientas permiten que miles de ciudadanos informales o sin historial bancario tradicional construyan su “capital reputacional” para acceder a financiamiento justo y oportuno.

“El marco legal vigente debe complementarse con instrumentos de gobernanza que traduzcan el mandato normativo en operación real, tales como: convenios vinculantes de intercambio de datos entre la Superintendencia de Bancos, el Servicio de Rentas Internas, los prestadores de servicios básicos y el Ministerio rector de las tecnologías, sobre estándares comunes de interoperabilidad, calidad y trazabilidad; protocolos técnicos y plazos exigibles; y mecanismos de rendición de cuentas que superen la resistencia institucional a transferir información.”

El corolario es claro: sin conocimiento no hay crédito, y sin información de calidad no hay conocimiento. Cada norma que recorta el historial crediticio, que fragmenta las fuentes o que posterga la articulación interinstitucional no elimina el riesgo, sino que lo traslada: lo encarece para quien cumple, lo vuelve invisible para quien evalúa y lo empuja hacia mercados informales donde la única garantía es la usura. La inclusión financiera, entendida con rigor, no consiste en borrar el pasado del deudor, sino en permitirle construir y demostrar su reputación de pago con todas las fuentes lícitas disponibles: las del sistema financiero, las tributarias, las de servicios básicos y las que emergen de la huella digital y transaccional. De ahí que el desafío ecuatoriano sea menos tecnológico que institucional: concretar los convenios de intercambio de datos dentro del plazo previsto, dotar de gobernanza y trazabilidad a los modelos de scoring, y explicar al ciudadano que el Registro de Datos Crediticios no es una lista de castigo, sino la infraestructura que le permite ser conocido y, por lo tanto, ser sujeto de crédito en condiciones razonables, oportunas y transparentes.

²¹ Ver. La información publicada por los entes de supervisión y control del sistema financiero nacional ubican a la morosidad en cifras inferiores a 10%, lo que significa que la diferencia corresponde a usuarios financieros que han cumplido en tiempo y forma con sus obligaciones. Es recomendable analizar estas cifras en conjunto con otras métricas. “Morosidad, crédito, activos y utilidades; así están los indicadores de las cooperativas de cara al Fenómeno de El Niño”, Economía, Primicias, 14 de septiembre de 2026, <https://www.primicias.ec/economia/morosidad-credito-utilidades-indicadores-cooperativas-fenomeno-nino-132369/>.

²² Bonilla et al., Boletín Especializado de Re exclusión Financiera.

²³ Marco Rodríguez: “Salir del chulco es salir de la violencia y la extorsión”, s. f., accedido 16 de septiembre de 2026, <https://www.lahora.com.ec/economia/marco-rodriguez-salir-del-chulco-es-salir-de-la-violencia-y-la-extorsion-20260429-0009.html>.

Innovación con Confianza: La nueva Ley de Ciberseguridad en Ecuador y sus desafíos regulatorios en la Transformación Digital del Sistema Financiero.



Miguel Matías Aguirre Peña

Investigador Independiente

I. Introducción:

La Paradoja de la Innovación Financiera y el Nuevo Hito Normativo.

Es importante iniciar indicando que el ecosistema Fintech en América Latina y el Caribe ha registrado un crecimiento superior al 340% entre los años 2017-2023, alcanzando un récord de más de tres mil plataformas en 26 países¹. Este ecosistema dinámico promete una mayor inclusión financiera y una eficiencia operativa sin precedentes. Sin embargo, trae consigo una paradoja inherente: a mayor digitalización y apertura de datos, mayor es la superficie de exposición ante amenazas cibernéticas. La prueba de esta vulnerabilidad estructural es que más de la mitad de las empresas del sector financiero en la región reconocen este riesgo y cuentan con un marco de ciberseguridad o planean implementarlo a corto plazo.

Para situarse en el contexto ecuatoriano y, teniendo en cuenta la parte histórica, nuestro marco jurídico carecía de normativa transversal y de aplicación general, pese a que sectores como el financiero y cooperativo ya contaban con regulación técnica especializada en riesgo tecnológico y seguridad de la información. No obstante, este panorama experimentó un giro radical con la publicación de la Ley Orgánica para el Fortalecimiento de la Ciberseguridad, mediante Registro Oficial Nro. 290, el pasado 22 de mayo de 2026. Un faro normativo que transforma el debate nacional; la ciberseguridad

“Este ecosistema dinámico promete una mayor inclusión financiera y una eficiencia operativa sin precedentes. Sin embargo, trae consigo una paradoja inherente: a mayor digitalización y apertura de datos, mayor es la superficie de exposición ante amenazas cibernéticas.”

pasa a aportar coordinación interinstitucional, alcance a infraestructura crítica digital en distintas industrias y determina sanciones unificadas, así empieza a concebirse como un habilitador estratégico indispensable para la construcción de un entorno digital de “innovación protegida”.

La transformación digital del sistema financiero ecuatoriano ha dejado de ser una estrategia de diferenciación competitiva para convertirse en un imperativo de supervivencia institucional. En la última década, la adopción acelerada de tecnologías disruptivas como las Interfaces de Programación de Aplicaciones (APIs) y la integración de soluciones Fintech ha reconfigurado profundamente la relación entre los usuarios y las instituciones financieras. A ese proceso se suma el horizonte, todavía no implementado de forma obligatoria en el Ecuador, de modelos de Banca Abierta (Open Banking), que permitirían a los usuarios compartir de forma segura sus datos bancarios con aplicaciones financieras externas, dando paso a la necesidad de leyes y normativas de ciberseguridad robustas que velen por los derechos y exijan obligaciones mínimas a las partes correspondientes, especialmente a las instituciones financieras.

El propósito de este artículo es analizar críticamente cómo la nueva legislación mitiga los riesgos sistémicos de la infraestructura digital financiera privada, y evaluar

¹ Banco Interamericano de Desarrollo y Finnovista, Fintech en América Latina y el Caribe: Un ecosistema consolidado para aportar a la inclusión (Washington, D.C.: Banco Interamericano de Desarrollo, 2024), 22-25.

² Comité de Basilea de Supervisión Bancaria, Principios para la resiliencia operativa (Basilea: Banco de Pagos Internacionales, 2021), 1.

los desafíos inmediatos que enfrentan las entidades de control sectorial para diseñar una regulación secundaria ágil. En un mercado globalizado donde la confianza del consumidor es el activo intangible más valioso, el Comité de Basilea de Supervisión Bancaria ha enfatizado que la salvaguarda del sistema financiero exige que las entidades desarrollen la capacidad de absorber ciber incidentes y fallas tecnológicas para evitar perturbaciones sistémicas a gran escala². Bajo esta premisa, el éxito de la transformación digital bancaria en el Ecuador dependerá de la robustez y resiliencia de su marco de seguridad jurídica y operativa.

II. La Infraestructura Crítica Digital y la Gestión del Riesgo de Terceros.

El cambio de paradigma que introduce la Ley Orgánica para el Fortalecimiento de la Ciberseguridad encuentra su anclaje operativo en la delimitación de su ámbito de aplicación. El artículo 20-A de la norma introduce formalmente en el ordenamiento jurídico ecuatoriano la categoría de “Infraestructura Crítica Digital”, vinculando de forma obligatoria a aquellas entidades privadas que presten servicios esenciales o cuya actividad tenga un impacto sistémico en la economía nacional³. En este nuevo mapa de responsabilidades, el sector bancario no solo se posiciona como el núcleo de esta infraestructura, sino también como el principal dinamizador de la innovación a través de la preparación del terreno para una eventual arquitectura de Banca Abierta.

La implementación de modelos de innovación abierta exige que los bancos tradicionales compartan datos financieros e interactúen con terceros mediante Interfaces de Programación de Aplicaciones (APIs). Si bien esta interconexión democratiza el acceso al crédito y diversifica los servicios, también descentraliza el perímetro de seguridad de las instituciones financieras. En términos de ciberseguridad, esto se traduce en el denominado “Riesgo de Terceros”, de esta manera la vulnerabilidad de un banco ya no depende exclusivamente de sus robustas defensas internas, sino del nivel de seguridad de la Fintech, la empresa emergente o el proveedor tecnológico transaccional más pequeño que se conecte a su red⁴. Un incidente digital en

una pasarela de pagos externa puede generar un efecto dominó capaz de comprometer toda la infraestructura financiera.

Lejos de convertirse en un obstáculo que asfixie la colaboración con el ecosistema Fintech, el artículo 20-A debe ser interpretado como el “pilar de certidumbre” que la industria requería. Al catalogar legalmente al sector financiero como infraestructura crítica, la ley dota a los bancos de una base jurídica legítima para exigir estándares mínimos y homogéneos de ciberseguridad a cualquier actor tecnológico que pretenda integrarse a sus sistemas. Esto mitiga la asimetría regulatoria donde los bancos soportaban una carga de cumplimiento extrema mientras que otros participantes del ecosistema operaban en la laxitud normativa.

Por lo tanto, la Ley del 22 de mayo de 2026 institucionaliza una red de confianza técnica. El verdadero desafío ya no consiste en restringir el acceso a los datos por temor al fraude, sino en utilizar este respaldo legal para co-diseñar, junto al regulador, un marco de “seguridad por diseño” que permita al Ecuador transitar hacia las finanzas digitales interoperables dentro de un entorno sistémicamente resiliente, con la necesidad de seguirlo aplicado por entidades internacionales como la Unión Europea⁵, que cuenta con un desarrollo llamativo en este campo y en la actualidad ha servido como modelo para lo desarrollado en el Ecuador y la región.



³ Artículo 20-A, Ley Orgánica para el Fortalecimiento de la Ciberseguridad, R.O. Quinto Suplemento 290 de 22 de mayo de 2026.

⁴ Erick Rincón Cárdenas, El desarrollo jurídico de Fintech: Las bases regulatorias de la Tecnología Financiera, 2.ª ed. (Valencia: Editorial Tirant lo Blanch, 2023), 115; Comité de Basilea de Supervisión Bancaria, Cyber-resilience: Range of Practices (Basilea: Banco de Pagos Internacionales, 2018), 7.

⁵ Unión Europea, Directiva (UE) 2022/2555 (Directiva NIS2) relativa a medidas para un alto nivel común de ciberseguridad en toda la Unión, Diario Oficial de la Unión Europea, 27 de diciembre de 2022, Art. 21.

III. Descentralización de la Supervisión y el Reto de la Regulación Secundaria Sectorial.

El acierto más significativo de la Ley Orgánica para el Fortalecimiento de la Ciberseguridad radica en el diseño de su arquitectura institucional. Al contrario de lo que ha ocurrido en otras jurisdicciones de la región, donde la centralización de las competencias en una sola agencia estatal de carácter administrativo suele generar cuellos de botella técnicos y jurídicos, el legislador ecuatoriano optó por consagrar el principio de especialidad. A través de los artículos 20-Y y 20-Z, la norma delega de forma explícita la potestad sancionadora, de supervisión y de control en los órganos de regulación especializados de cada sector, determinando que la autoridad rectora general tendrá únicamente una actuación subsidiaria⁶.

Para el sistema financiero, esta descentralización representa una garantía fundamental de seguridad jurídica y estabilidad operativa. La Superintendencia de Bancos y la Junta de Regulación Financiera son los entes que verdaderamente comprenden la complejidad inherente al negocio bancario, la gestión del riesgo de liquidez, el funcionamiento de las pasarelas de pago y la naturaleza transaccional de la banca digital. Además, el reconocimiento expreso del principio de “non bis in ídem” dentro del texto legal asegura y evita el doble juzgamiento o sanciones contradictorias por parte de una autoridad administrativa común y su supervisor natural ante la ocurrencia de un incidente tecnológico⁷.

El supervisor financiero se encuentra ante una oportunidad histórica, convertirse en un arquitecto de la resiliencia nacional, para lograrlo, la regulación secundaria debe instrumentalizar herramientas innovadoras, previstas en la ley, como los mecanismos de hacking ético y pruebas de penetración autorizadas⁸, integrándolos en esquemas de supervisión continuos. Asimismo, si bien la Superintendencia de Bancos ya exige, en su Norma de Control para Sandboxes Regulatorios, que toda solicitud incorpore aspectos de seguridad de la información, ciberseguridad y continuidad del negocio⁹, la regulación secundaria debería profundizar ese requisito con parámetros técnicos específicos de resiliencia, permitiendo que las entidades financieras y las empresas tecnológicas aliadas experimenten con nuevas arquitecturas digitales dentro de perímetros controlados de seguridad.

El éxito de la descentralización no se medirá por el número de sumarios administrativos iniciados bajo el amparo del artículo 20-Z¹⁰, sino por la capacidad del supervisor financiero para co-diseñar estándares de resiliencia operativa que transformen la mitigación del riesgo tecnológico en una verdadera ventaja competitiva para el país.

IV. Derecho Comparado Aplicado: Lecciones de Chile y la Unión Europea para una Regulación Pro-Innovación

Para que la descentralización prevista en la legislación ecuatoriana se traduzca en un ecosistema financiero competitivo y seguro, la Superintendencia de Bancos debe mirar hacia las mejores prácticas internacionales. Ciertos marcos normativos resultan fundamentales para guiar la redacción de la regulación secundaria en el país: la Ley Marco de Ciberseguridad de Chile (Ley N° 21.663) y el modelo regulatorio de la Unión Europea, específicamente a través del Reglamento de Resiliencia Operativa Digital y la Directiva NIS2.



⁶ Artículo 20-Z, Ley Orgánica para el Fortalecimiento de la Ciberseguridad, R.O. Quinto Suplemento 290 de 22 de mayo de 2026.

⁷ Artículo 20-Y, Ley Orgánica para el Fortalecimiento de la Ciberseguridad, R.O. Quinto Suplemento 290 de 22 de mayo de 2026.

⁸ Artículo 20-L, Ley Orgánica para el Fortalecimiento de la Ciberseguridad, R.O. Quinto Suplemento 290 de 22 de mayo de 2026.

⁹ Superintendencia de Bancos, Resolución Nro. SB-2025-2852, Norma de Control para el Funcionamiento de Espacios Controlados de Pruebas Regulatorias (Sandboxes Regulatorios) para Desarrollos Innovadores, art. 7.4, noviembre de 2025.

¹⁰ Artículo 20-Z, Ley Orgánica para el Fortalecimiento de la Ciberseguridad.

En el contexto regional, Chile promulgó en 2024 su Ley Marco de Ciberseguridad, un instrumento que comparte una filosofía institucional muy similar a la ecuatoriana. La legislación chilena crea la Agencia Nacional de Ciberseguridad (ANCI), pero respeta rigurosamente las competencias de las demás autoridades, para el cumplimiento de la función administrativa relacionada a la ciberseguridad¹¹. La Comisión para el Mercado Financiero ha emitido normativas técnicas diferenciadas que permiten a las entidades de menor escala transaccional adoptar medidas proporcionales a su nivel de riesgo. De este modo, se evita que las exigencias de ciberseguridad se conviertan en una barrera de entrada para la innovación financiera y el emprendimiento tecnológico y se trabaja en el objetivo de mitigar riesgos y posibles incidentes cibernéticos¹².

Por otro lado, la Unión Europea ofrece el estándar más avanzado del mundo en la materia, con la Directiva NIS2 establece el marco general para las infraestructuras críticas europeas¹³, el Parlamento Europeo identificó que el sector financiero requería una norma de especialidad absoluta debido a su alto nivel de digitalización. Así nació el Reglamento DORA, el cual unifica bajo un solo cuerpo legal las reglas sobre gestión de riesgos de las Tecnologías de la Información y la Comunicación (TIC), notificación de incidentes, pruebas de resiliencia operativa y, de manera crucial, la supervisión de los proveedores terceros de servicios tecnológicos¹⁴.

DORA introduce el concepto de “supervisión directa” sobre las grandes empresas tecnológicas de la nube que prestan servicios a la banca, liberando a las entidades financieras individuales de la carga de auditar por sí solas a gigantes globales¹⁵.

Para el Ecuador, la asimilación de este enfoque en la normativa secundaria permitiría diseñar esquemas de certificación conjunta. Esto facilitaría que las Fintech locales que cumplan con un estándar técnico preestablecido puedan integrarse de forma ágil y segura a la infraestructura de cualquier banco privado, acelerando los procesos de onboarding y potenciando el desarrollo de la Banca Abierta bajo un entorno de riesgo controlado.



¹¹ Artículo 1, Ley N° 21.663, Ley Marco de Ciberseguridad e Infraestructura Crítica de la Información, Diario Oficial de la República de Chile, 8 de abril de 2024.

¹² Comisión para el Mercado Financiero, Recopilación Actualizada de Normas: Capítulo 20-10 sobre Gestión de Seguridad de la Información y Ciberseguridad (Santiago: CMF, 2020).

¹³ Unión Europea, Directiva (UE) 2022/2555 (Directiva NIS2), arts. 1-2.

¹⁴ Reglamento (UE) 2022/2554 del Parlamento Europeo y del Consejo (Reglamento DORA), Diario Oficial de la Unión Europea L 333, 27 de diciembre de 2022, considerando 10.

¹⁵ Reglamento (UE) 2022/2554 del Parlamento Europeo y del Consejo (Reglamento DORA), cap. V, sec. II, art. 31.



V. Conclusiones y Propuesta:

Hacia una “Innovación Protegida” en el Ecuador.

La Ley Orgánica para el Fortalecimiento de la Ciberseguridad redefine las reglas del juego para la transformación digital en el Ecuador, pero es solo un marco habilitador: su éxito dependerá de la visión con la que la Superintendencia de Bancos y la Junta de Política y Regulación Financiera redacten la regulación secundaria. Ciberseguridad e innovación no son fuerzas opuestas, sino dos caras de la misma moneda; sin un entorno jurídicamente seguro y técnicamente resiliente, propuestas como la banca abierta, las finanzas embebidas o las billeteras digitales fracasarán ante la primera brecha sistémica.

Para materializar el espíritu pro-innovación de la ley, se plantean tres propuestas estratégicas para la regulación secundaria.

En primer lugar, aunque la Superintendencia de Bancos ya exige aspectos de ciberseguridad y continuidad del negocio en las solicitudes de Sandbox Regulatorio¹⁶ y delimita su rol de supervisión sobre la materia, la normativa técnica debería profundizar ese requisito incorporando un carril específico de pruebas de resiliencia cibernética, donde las entidades financieras y sus aliados Fintech evalúen soluciones disruptivas bajo esquemas adaptativos antes de su lanzamiento al mercado.

En segundo lugar, es necesario adoptar el principio de proporcionalidad mediante normativas técnicas diferenciadas según el tamaño, volumen transaccional y nivel de riesgo sistémico de cada actor, de modo que las exigencias del artículo 20-A no asfixien a los nuevos competidores del ecosistema financiero¹⁷.

Finalmente, debe institucionalizarse el co-diseño técnico público-privado, aprovechando la Red Nacional de

Confianza (RNC) prevista en la ley¹⁸ para conformar mesas de trabajo permanentes entre entidades financieras, el supervisor financiero y la academia, que permitan emitir circulares y guías técnicas alineadas con la velocidad de la innovación del mercado.

Solo con una regulación secundaria inteligente, ágil y colaborativa el Ecuador transformará el cumplimiento normativo en una ventaja competitiva regional, consolidando un sistema financiero resiliente y blindando su activo más valioso: la confianza del ciudadano.



¹⁶ Superintendencia de Bancos, Resolución Nro. SB-2025-2852.

¹⁷ Artículo 20-A, Ley Orgánica para el Fortalecimiento de la Ciberseguridad.

¹⁸ Disposición Transitoria Sexta, literal c), Ley Orgánica para el Fortalecimiento de la Ciberseguridad, R.O. Quinto Suplemento 290 de 22 de mayo de 2026.



El conocimiento converge aquí

+20

speakers

nacionales e
internacionales

1 día

de conferencias,

aprendizaje
y networking

1 objetivo

compartido:

Fortalecer la prevención del lavado de activos,
cooperación y la integridad del sistema financiero

IV ENPLA 2026

Aplica 7 créditos de educación continua FIBA

Visión estratégica y regulatoria, nuevas amenazas y tecnología

18 noviembre
2026

Quito
Ecuador

Conoce más detalles en:

www.enpla-asobanca.com





La información contenida en el presente documento es de exclusiva propiedad de la Asociación de Bancos Privados del Ecuador. Toda reproducción, total o parcial, deberá realizarse incluyendo la referencia correspondiente; y se deberá procurar contar con la autorización de su autor. El presente documento es un espacio de opinión, el cual recoge la visión de sus autores sin que, la información en él contenida deba, ni pueda, entenderse de manera alguna como la posición oficial de la Asociación de Bancos Privados

www.asobanca.org.ec

