

14 min de lectura

El Cliente que **No Vemos**

Panamá le exige al banco leer las señales de red de quien abre una cuenta a distancia. Europa le exige empezar por una credencial digital. Las dos reglas tienen fecha en 2027, con diez días de diferencia.

En una frase. Las dos reglas buscan lo mismo —reconocer a un cliente que no vemos—, pero preguntan cosas distintas. El Acuerdo 1-2026 de Panamá pregunta *dónde está* el solicitante y cuánto riesgo trae esa señal. El reglamento antiblanqueo europeo pregunta *con qué credencial prueba quién es*. No son reglas rivales: un banco con clientes en ambos mundos tendrá que responder las dos preguntas. Detrás de ambas hay una tercera, la que más importará pronto: quién actúa por el cliente. Un agente de inteligencia artificial (IA) no trae identidad propia ante el banco; hereda la de quien lo autorizó.

01 El problema es el mismo

Abrir una cuenta sin ver al cliente obliga al banco a resolver dos cosas: quién es esa persona y qué riesgo trae. El Grupo de Acción Financiera Internacional (GAFI; en inglés, FATF) fijó el marco global en su guía de identidad digital de 2020: la Recomendación 10 no exige una tecnología, pide entender los niveles de garantía del sistema y decidir si es «confiable e independiente». La identificación remota con un sistema de nivel adecuado puede considerarse de riesgo estándar, o incluso bajo.

El título es una metáfora: cuando el cliente no está, el banco trabaja con lo intangible —señales, credenciales, evidencia— en lugar de ver a una persona.

Panamá y la Unión Europea (UE) bajaron ese marco por caminos distintos.

02 Panamá: una señal obligatoria y una cédula que hay que validar

El Acuerdo 1-2026 de la Superintendencia de Bancos de Panamá (SBP) se emitió el 16 de enero de 2026, se publicó en la Gaceta Oficial el 23 de enero y rige desde julio de 2026, seis meses después de su promulgación. Deroga el Acuerdo 10-2015 y otros tres anteriores.

La señal. El artículo 14 obliga a los bancos que abran cuentas o presten servicios por medios digitales o remotos a incorporar la *geolocalización inferencial* del solicitante. Debe usarse como fuente primaria de evaluación de riesgo y construirse con señales técnicas: dirección IP (protocolo

de internet), tipo de red, proveedor de servicios de internet, uso de redes privadas virtuales (VPN), proxies y redes de anonimización, zona horaria y configuración regional del dispositivo, entre otras. En la apertura digital sirve para verificar el domicilio o la ubicación declarados y para mitigar el riesgo de aperturas desde jurisdicciones de alto riesgo, sancionadas o incoherentes con lo informado. El parágrafo 1 la define como estimar la ubicación de un usuario o dispositivo con el análisis combinado de señales de red, dispositivo y contexto digital, aun sin coordenadas físicas directas. Los bancos tienen hasta el 30 de junio de 2027 para adecuarse. Incumplir el Acuerdo se sanciona con multas de B/. 5,000 hasta B/. 5,000,000, según la gravedad y la reincidencia (artículo 44).

La identidad. Para panameños, el documento idóneo es la cédula. Los artículos 16, 18 y 20 permiten que el cliente la presente físicamente o que el banco la obtenga de la base de datos del Tribunal Electoral, *siempre que pueda validar que se trata de la persona que está requiriendo el servicio*. Para extranjeros, el documento idóneo es el pasaporte, y basta conservar copia de las páginas con fotografía, firma y generales y de la del sello de ingreso. Un extranjero también puede identificarse con el documento oficial de su país en tres casos: si el banco puede verificarlo con la entidad pública que lo emite, previa evaluación de la Superintendencia; si fue captado en el extranjero o por entidades del grupo; o si la vinculación la hace un banco de licencia internacional.

En las cuentas de apertura simplificada (artículo 15) la cédula puede verificarse al abrir o hasta 30 días después. El banco conserva el expediente al menos cinco años desde el fin de la relación (artículo 29).

Lo que el texto no dice. En ningún artículo del Acuerdo aparecen la biometría, la prueba de vida, el video, las billeteras digitales ni el Sistema de Identidad Digital (SID) del Tribunal Electoral. La norma es neutral en tecnología: *cómo* se valida que el solicitante es el titular de la cédula lo decide cada banco.

03 Europa: la credencial primero

El Reglamento Antiblancqueo de la UE (AMLR, por *Anti-Money Laundering Regulation*; Reglamento (UE) 2024/1624, del 31 de mayo de 2024) se aplica desde el 10 de julio de 2027. Su artículo 22(6) admite dos vías para verificar la identidad: un documento de identidad o pasaporte, con información de fuentes fiables e independientes, o un medio de identificación electrónica (eID) con nivel de garantía *sustancial* o *alto* según eIDAS y servicios de confianza cualificados.

El detalle operativo lo define la Autoridad de Lucha contra el Blanqueo de Capitales y la Financiación del Terrorismo (AMLA, por *Anti-Money Laundering Authority*). El 30 de septiembre de 2026 publicó el informe final de las normas técnicas de regulación (RTS, por *Regulatory Technical Standards*) sobre debida diligencia, que presentó a la Comisión Europea el 1 de octubre. Todavía falta que la Comisión las adopte; se aplicarían seis meses después de su entrada en vigor. Lo que dice el borrador:

- **La credencial va primero.** Los medios de identificación electrónica incluyen las billeteras europeas de identidad digital, estén o no notificados, si cumplen nivel sustancial o alto. Pueden usarse también en persona.
- **La vía remota por documento es el segundo recurso.** Las soluciones alternativas, como las herramientas de apertura remota con documento y video, solo proceden cuando el cliente no puede razonablemente presentarse en persona y no tiene acceso a un eID. El banco debe justificar por qué no usó las vías del artículo 22(6) y demostrar al supervisor que la solución cumple. Las herramientas existentes pueden seguir usándose si cumplen.
- **El segundo recurso trae garantías mínimas** (artículo 7): controles para asegurar que quien presenta el documento es su titular; integridad y confidencialidad de la comunicación; imagen, video y sonido de calidad suficiente para identificar sin ambigüedad a la persona; corte del proceso si hay fallas o dudas; y copias conservadas con sello de tiempo.
- **Los datos llegan estructurados.** El Anexo I lista los atributos mínimos que la credencial debe entregar en campos definidos (nombre, fecha y lugar de nacimiento, nacionalidad, residencia), basados en el reglamento europeo de datos de identificación de las billeteras. Si falta alguno, el banco lo obtiene por otro medio.
- **Un puente con la entrega anterior.** Los documentos «equivalentes» al pasaporte pueden basarse en la norma 9303 de la Organización de Aviación Civil Internacional (OACI).

La obligación de *aceptar* la billetera no está en el AMLR sino en eIDAS 2.0 (artículo 5f): a fines de 2027 para entidades obligadas a usar autenticación reforzada, entre ellas la banca (ver la entrega anterior de esta serie). Según análisis de terceros, el AMLR se limita a decir, en un considerando, que la identificación electrónica debe tenerse en cuenta y aceptarse.

Un matiz. Europa también habla de señales de red, pero en otro lugar: el borrador menciona *geofencing*, monitoreo y seguimiento de IP entre los factores de riesgo que un supervisor pesa al decidir cuánto exime a un instrumento de dinero electrónico de la debida diligencia. Es un factor de riesgo, no un control de identidad.

04 Lado a lado

	Panamá • Acuerdo 1-2026	Unión Europea • AMLR + borrador de RTS
Qué prueba quién es	Cédula, física o consultada en la base del Tribunal Electoral, si el banco valida que es la persona; pasaporte para extranjeros	Documento más fuentes fiables, o eID/billetera con nivel sustancial o alto
Qué es obligatorio en lo remoto	Geolocalización inferencial como fuente primaria de riesgo (art. 14)	Usar primero la credencial digital; la vía por documento solo con justificación (art. 7 del RTS)

	Panamá · Acuerdo 1-2026	Unión Europea · AMLR + borrador de RTS
Señales de red	Obligatorias: verifican domicilio y mitigan jurisdicciones de riesgo	Aparecen solo como factor de riesgo del dinero electrónico
Garantías mínimas del proceso remoto	El texto no las especifica	Cinco salvaguardas definidas (art. 7(2) del RTS)
Billeteras digitales	No se mencionan (el SID tampoco)	Incluidas como eID; aceptación obligatoria a fines de 2027 (eIDAS 2.0)
Quién actúa por el cliente	Apoderados y representantes de personas jurídicas (arts. 17, 19 y 21); no hallamos regla equivalente para personas naturales	Se verifica la identidad de quien actúa por el cliente y el alcance de su poder (art. 22 del AMLR; art. 14 del RTS)
Fecha clave	Art. 14: hasta el 30 de junio de 2027	AMLR: se aplica el 10 de julio de 2027
Estado del texto	Vigente desde julio de 2026	Reglamento vigente; RTS presentadas a la Comisión, pendientes de adopción

05 Lectura de IAB: preguntas distintas, no reglas rivales

Cada régimen responde a su riesgo dominante. El Acuerdo 1-2026 nace de un centro financiero internacional: sus bancos reciben solicitantes de muchos países, y el artículo 14 es explícito sobre jurisdicciones de alto riesgo y sancionadas. El AMLR nace de un bloque con 27 sistemas nacionales de identidad que quiere hacerlos interoperables, y por eso empieza por la credencial.

La diferencia práctica es dónde queda la prueba. En Panamá, la señal de red es obligatoria y *la prueba de que el solicitante es el titular la define cada banco*. En Europa, la prueba es el eID o, en su defecto, una solución con garantías mínimas escritas.

El AMLR obliga a las entidades de la UE, no a los bancos panameños. Su efecto sobre Panamá es indirecto: clientes que llegan con credenciales europeas, grupos con presencia en la UE y contrapartes que adopten el estándar como referencia. Es una lectura de IAB, no una obligación.

06 Quién actúa por el cliente

Hasta aquí, el solicitante es una persona que se presenta por sí misma. Pero también abre y mueve cuentas quien actúa por otro: un apoderado, un representante legal, un tutor. Para ese caso ya existe un marco, escrito para personas y no para software.

- **Europa.** El artículo 22 del AMLR extiende la verificación de identidad a cualquier persona que pretenda actuar en nombre del cliente, con las mismas vías del artículo 22(6). El borrador de RTS añade que el banco debe obtener información que le permita verificar *la existencia y el alcance del poder de representación* (artículo 14). Su considerando 13 da como ejemplos el poder notarial y la prueba de representación legal o parental, incluida una tutela dictada por un tribunal.

- **Panamá.** El Acuerdo exige identificar a apoderados, representantes legales y firmantes de las personas jurídicas (artículos 17, 19 y 21) y, cuando el cliente actúa como intermediario del beneficiario final, hacer la debida diligencia sobre ese beneficiario (artículo 10). Para personas naturales, el Acuerdo solo menciona a un tercero que actúa en representación del cliente en un caso: el reporte de pagos y cobros en efectivo de B/. 10,000 o más (artículo 28, numeral 6). No hay una regla equivalente para identificar al apoderado de una persona natural.

Por qué importa para los agentes de IA. Es una lectura de IAB: un agente que opera una cuenta no trae identidad propia ante el banco; hereda la de quien lo autorizó. Los comentarios que recibió el Centro Nacional de Excelencia en Ciberseguridad (NCCoE, por *National Cybersecurity Center of Excellence*) del Instituto Nacional de Estándares y Tecnología (NIST) de EE. UU. en su consulta sobre identidad de agentes lo plantean igual: el agente deriva su autoridad de una persona u organización, y esa autoridad debe poder rastrearse hasta ella. Para el banco, el agente cae en la misma categoría que el apoderado: alguien que actúa por el cliente, con un poder cuya existencia y alcance hay que verificar.

Una hipótesis, no un hallazgo. La lógica de señales del artículo 14 está pensada para una persona con un dispositivo. Un agente suele correr en servidores en la nube, a menudo detrás de proxies, justo el tipo de señal que el artículo trata como riesgo. Si es así, la geolocalización inferencial se descalibraría con agentes, mientras que la lógica de credenciales sí se extiende: el poder puede expresarse como una credencial firmada. Hay dos reservas: el artículo 14 se refiere a la vinculación de clientes nuevos, y este Acuerdo no regula la autenticación del canal en una cuenta ya abierta. Sus artículos 24 y 25 tratan el seguimiento y el monitoreo, y el 25 permite al banco diseñar controles complementarios según el canal o las nuevas tecnologías.

07 Qué cambia para el diseño de la apertura a distancia

Cinco decisiones que un comité puede tomar sin esperar a que cambie la norma:

1. **Escribir qué significa «validar que se trata de la persona».** El Acuerdo lo deja al banco. Las cinco salvaguardas del artículo 7(2) europeo son una referencia útil para definirlo; no son norma panameña.
2. **Registrar por separado la señal de ubicación y la prueba de identidad.** La señal responde al riesgo de domicilio y jurisdicción; no prueba que el solicitante sea el titular, y la cédula no prueba dónde está.
3. **Diseñar la ruta de excepción.** Un cliente legítimo con una VPN corporativa, de viaje o expatriado puede contradecir lo que declaró. El banco debe definir qué pasa, quién decide y qué queda registrado.
4. **Dejar un espacio para la credencial.** Si el SID o una billetera extranjera se vuelven verificables, el flujo debería poder recibir un atributo firmado en lugar de una imagen. Para credenciales extranjeras, el artículo 16 exige evaluación previa de la Superintendencia.

5. Registrar por separado al titular y a quien actúa por él. El expediente debe distinguir quién es el titular, quién actúa y con qué poder: hoy un apoderado, mañana quizá un agente de IA. Si se mezclan, la auditoría no podrá responder quién autorizó qué.

Ninguna de las dos reglas se cumple con una prueba solo de mayoría de edad: el Acuerdo pide datos de identificación completos y el Anexo I europeo, una lista de atributos definida.

08 Tres preguntas para el comité

1. ¿Qué evidencia guarda el banco de que quien abrió la cuenta es el titular de la cédula, y no solo de que la cédula existe?
2. Cuando la señal de red contradice el domicilio declarado, ¿quién decide y qué queda registrado?
3. ¿Distingue hoy la política del banco entre el cliente y alguien, o algo, que actúa por el cliente, y qué evidencia exige del poder que lo respalda?

09 Lo que no encontramos

No encontramos guía pública de la SBP, posterior al Acuerdo, sobre cómo medir la geolocalización inferencial: umbrales, fuentes de señales o tratamiento de excepciones. Tampoco encontramos un mecanismo público para que un banco verifique una cédula digital, tema de la entrega anterior. En los textos revisados (el Acuerdo completo, el borrador de RTS y el artículo 22 del AMLR) tampoco aparece el agente de IA como figura propia. No decimos que no exista; decimos que no lo encontramos. Son preguntas abiertas, no reproches.

Próxima entrega

Hacia dónde va el mundo con la identidad del agente de IA. Persona, mandato y agente: qué piezas ya existen, qué sigue abierto y quién emite, quién verifica y quién responde por la autoridad que se delega. La serie cierra con las alternativas de un banco ante el agente de IA de un cliente.

Cómo verificamos

Cada cifra y cada fecha de esta pieza está registrada con su fuente en el registro de verificación de IAB. Lo que proviene de fuentes secundarias está atribuido o se declara aquí.

Sobre la norma europea. El reglamento antiblanqueo (Reglamento (UE) 2024/1624) está adoptado, y su fecha de aplicación, el 10 de julio de 2027, la confirmamos en el texto oficial (artículo 90). Lo que sigue siendo borrador son las normas técnicas de la AMLA: el artículo describe lo que dice su

informe final del 30 de septiembre de 2026, que cambiaría si la Comisión Europea lo modifica al adoptarlo. La fecha en que la banca europea debe aceptar la billetera (fines de 2027) es un cálculo a partir de los plazos de eIDAS 2.0 y se apoya en fuentes secundarias.

Sobre el Acuerdo 1-2026. Revisamos el texto completo del Acuerdo, de 38 páginas y 54 artículos, tal como lo publica la Superintendencia de Bancos. La fecha desde la que rige se calcula a partir de su publicación en la Gaceta Oficial.

La lectura sobre los agentes de IA es de IAB y está marcada como tal.

Fuentes

- Superintendencia de Bancos de Panamá, Acuerdo 1-2026: https://www.superbancos.gob.pa/documentos/regulacion/acuerdos_otros_sujetos/2026/Acuerdo_01-2026.pdf
- Superintendencia de Bancos de Panamá, acuerdos bancarios y plazos de adecuación: <https://www.superbancos.gob.pa/acuerdos/bancarios> ; <https://www.superbancos.gob.pa/node/1652>
- Reglamento (UE) 2024/1624 (AMLR), EUR-Lex: <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX%3A32024R1624>
- AMLR, artículo 22: <https://amlr.eu/article-22-identification-and-verification-of-the-identity-of-customers-and-beneficial-owners/>
- AMLA, informe final del borrador de RTS (30 sep. 2026): https://www.aml.europa.eu/document/download/e15ab2e5-4074-4de8-bb9d-613dd8b7fdd1_en?filename=Final+Report+-+draft+RTS+28%281%29+AMLR.pdf
- AMLA, comunicado (1 oct. 2026): https://www.aml.europa.eu/press-release-aml-finalises-key-standards-private-sector_en
- Fecha de aplicación del AMLR: <https://rapidlei.com/eu-aml-package-readiness/> ; <https://www.namirial.com/en/blog/ecosystem/customer-due-diligence-aml-final-rt/>
- Aceptación de la billetera (eIDAS 2.0, art. 5f): <https://didit.me/blog/amlr-eudi-wallet-acceptance/>
- NCCoE/NIST, resumen de comentarios sobre identidad de agentes (29 sep. 2026): <https://pages.nist.gov/nccoe-ai-identity/summary-of-comments.html>
- GAFI, guía de identidad digital (2020): <https://www.fatf-gafi.org/en/publications/Financialinclusionandnpoissues/Digital-identity-guidance.html>

Criterio Humano. Inteligencia Escalable.

CÓMO CITAR ESTE DOCUMENTO

InteligenciABancaria.net · DOC.20 · Octubre 2026