

19 min de lectura

Identidad Propia, Autoridad Delegada

El mundo converge en que un agente de inteligencia artificial necesita una identidad propia y verificable, y en que su autoridad es de otro. Lo que sigue abierto es lo que más le importa a un banco: cómo se prueba esa autoridad, quién certifica a los agentes de afuera y quién responde cuando se excede.

En una frase. El agente tiene nombre propio, pero su autoridad es de otro. Casi todos los que opinan ante el organismo de estándares de Estados Unidos piden que los agentes tengan una identidad distinta y verificable, y muchos subrayan que su autoridad la delega una persona o una entidad y debe poder rastrearse hasta ella. No hay acuerdo sobre cómo identificarlos, cómo expresar lo que se les autorizó, quién certifica a los que llegan de afuera ni quién responde si se exceden. Esas cuatro brechas son las que un banco tendrá que cerrar por su cuenta.

01 Dónde quedó la discusión

El DOC.20 cerró con una frase: un agente de inteligencia artificial (IA) «no trae autoridad propia ante el banco; la recibe de quien lo autorizó». Y dejó una pregunta pendiente: si el agente debería tener, además, un identificador técnico propio.

Esta pieza responde esa pregunta con lo que el mundo está construyendo hoy. La respuesta corta es que sí, y que la identidad del agente (quién es) y su autoridad (qué puede hacer y en nombre de quién) no se resuelven en el mismo lugar ni con las mismas herramientas.

02 Lo que ya está cerrado

La fuente principal es el resumen de comentarios del Instituto Nacional de Estándares y Tecnología de Estados Unidos (NIST, por *National Institute of Standards and Technology*), el organismo federal de estándares de ese país. En febrero de 2026, su Centro Nacional de Excelencia en Ciberseguridad (NCCoE, por *National Cybersecurity Center of Excellence*), el

laboratorio que prueba soluciones junto con la industria, publicó un borrador de concepto sobre identidad y autorización de agentes. Recibió 614 respuestas, 70 % de ellas del sector privado, y el 29 de septiembre de 2026 publicó un resumen.

El resumen no es un estándar. Recoge lo que dijeron los comentaristas y las conversaciones con el sector, y su propia página advierte que fue editado con asistencia de una herramienta de IA y revisado por sus autores. Aun así, muestra dónde hay acuerdo. «Cerrado» significa aquí acuerdo de principio, no norma terminada. Son cuatro.

Primero: el agente necesita una identidad distinta y verificable. Según el resumen, casi todos los comentaristas pidieron que los agentes tengan identidades no humanas distintas y verificables, y hubo casi unanimidad en que hay que identificarlos. La identidad, además, no es una etiqueta: combina la identidad de la carga de trabajo, la instancia en ejecución, la persona u organización que lo autorizó y la autoridad que tiene en ese momento.

Ya hay productos que lo aplican. En Microsoft Entra Agent ID, el servicio de identidad de Microsoft para agentes, cada agente recibe una identidad propia y la documentación exige al menos un patrocinador por cada una: la persona o el grupo humano responsable del agente, a quien se contacta, por ejemplo, ante un incidente de seguridad. Es una descripción de producto y no un estándar, pero ilustra el título de esta pieza: identidad propia para el agente y una persona detrás.

Segundo: la autoridad es delegada y debe poder rastrearse. Según el resumen del NIST, muchos comentaristas subrayaron que los agentes derivan su autoridad de personas u organizaciones, y que esa autoridad debe poder rastrearse criptográficamente hasta quien originó la instrucción. Lo que preocupa son las brechas de responsabilidad: acciones que no se pueden conectar de vuelta con el responsable humano o institucional.

La misma idea aparece en el Grupo de Trabajo de Ingeniería de Internet (IETF, por *Internet Engineering Task Force*), el foro donde se escriben los estándares técnicos de la red. El 15 de septiembre de 2026 publicó, como trabajo en curso, el borrador «AI Identity Management System», del grupo WIMSE (*Workload Identity in Multi-System Environments*, identidad de cargas de trabajo en entornos de varios sistemas). Propone aplicar estándares existentes a los agentes en lugar de definir protocolos nuevos. Su antecesor, un borrador individual de marzo de 2026, afirma que si el agente actúa en nombre de un usuario o sistema, este debe delegarle autoridad, y que ese contexto se conserva, se usa en las decisiones de autorización y se registra en las pistas de auditoría.

Tercero: la autorización debe ser determinista, acotada y revocable. Hubo muy fuerte oposición a que un modelo de lenguaje sea el árbitro principal de una autorización: el consenso es que la política determinista es esencial y que lo probabilístico, como mucho, aporta contexto.

Los comentaristas piden un ancla de confianza estable y credenciales efímeras, acotadas y revocables que se estrechan a lo largo de la cadena de delegación, de modo que un subagente nunca reciba más acceso del necesario.

El Fondo Monetario Internacional (FMI; en inglés, IMF) llega a la misma idea desde los pagos. Una nota de abril de 2026, firmada por Sonja Davidovic y Hervé Tourpe, propone un modelo de tres capas: la intención y la orquestación, que son probabilísticas; el control y la autorización, deterministas; y la liquidación, también determinista. La nota aclara que expresa las opiniones de sus autores, no las del FMI, y que no busca conclusiones definitivas ni propone medidas prescriptivas.

Cuarto: el registro debe explicar, no solo anotar. Los comentaristas señalan que los registros tradicionales dicen qué ocurrió, pero no por qué, bajo qué autoridad ni qué información influyó. Piden cadenas de delegación, decisiones de política, registros de intención y evidencia a prueba de manipulación.

03 Lo que sigue abierto

Cuatro desacuerdos, y son los que tocan al banco.

Cómo identificar al agente. Hay casi unanimidad en que hay que hacerlo, pero no hay consenso sobre cómo: se dividen en enfoques técnicos, estándares, modelos de confianza y en centralizado frente a descentralizado. Las credenciales verificables y los identificadores descentralizados del Consorcio de la Web (W3C, por *World Wide Web Consortium*) son estándares ya maduros y algunos comentaristas los proponen para los agentes, pero no hay acuerdo. El propio NIST concluye que la identidad de agentes emerge como una pila de estándares compuesta, no como un estándar único.

Cómo expresar lo que se le autorizó al agente. La «intención firmada», una declaración de lo que el usuario espera, firmada con una clave de confianza, se considera una necesidad, sobre todo para el consumo, pero el resumen dice que no existe consenso sobre cómo implementarla y que la intención aún no es una categoría madura de estándares.

El trabajo más avanzado está en pagos. El Protocolo de Pagos de Agentes (AP2, por *Agent Payments Protocol*), que Google presentó en septiembre de 2025, usa mandatos firmados: uno de intención, otro de carrito y otro de pago. Verifiable Intent, que Mastercard y Google presentaron el 5 de marzo de 2026, apunta a dejar un registro a prueba de manipulación de lo que el usuario autorizó. Google donó AP2 a la alianza FIDO (*Fast IDentity Online*, «identidad rápida en línea»), la organización detrás de las llaves de acceso (*passkeys*), y Mastercard aportó Verifiable Intent a su trabajo. El 28 de abril de 2026 la FIDO anunció un grupo de trabajo de autenticación agéntica, presidido por miembros de CVS Health, Google y OpenAI, y otro de pagos, presidido por Mastercard y Visa. Son especificaciones en desarrollo, no estándares terminados.

Quién certifica al agente que no es del banco. Aquí las redes de pago van adelante, y ya no solo con anuncios. El 10 de septiembre de 2026, Ant International, Mastercard y Visa anunciaron que empiezan a colaborar en un marco de interoperabilidad de KYA (*Know Your Agent*, «conozca a su agente»), en paralelo al KYC (*Know Your Customer*, «conozca a su cliente»). Tiene tres pilares: rastrear cada agente hasta un operador, tarjetahabiente o empresa validados; certificarlo contra requisitos compartidos de seguridad y comportamiento; y monitorearlo de forma continua con señales de identidad y de transacción. El comunicado habla de principios compartidos que respetan los procesos de verificación de cada red, dice que las tres explorarán cómo llegar a principios comunes y que lo harán a través de BuildFin.ai, una plataforma convocada por la Autoridad Monetaria de Singapur (MAS, por *Monetary Authority of Singapore*). No incluyó criterios de certificación ni una especificación técnica.

Mientras tanto, cada red ya opera su propio KYA. El Trusted Agent Protocol de Visa, presentado en octubre de 2025, hace que el agente firme cada solicitud con un estándar del IETF para firmar mensajes web, y el comercio verifica esa firma contra un directorio de agentes que mantiene Visa. El marco de aceptación de Mastercard Agent Pay exige registrar y verificar a cada agente antes de que opere en su red, y lo hace transaccionar con credenciales tokenizadas propias. El 30 de septiembre de 2026 Mastercard sumó servicios de confianza e inteligencia y una alianza con Skyfire, un proveedor de KYA.

América Latina no es espectadora. El 24 de marzo de 2026 Mastercard anunció transacciones reales iniciadas por agentes en la región, hechas en entornos controlados, con 17 emisores y procesadores, entre ellos BAC, Bancolombia, Davivienda, Itaú y Santander; dijo además que casi el 100 % de los emisores de la región ya tiene habilitada su tecnología de tokens para agentes. Visa completó con Santander un piloto controlado con credenciales de cinco países y, desde abril de 2026, su programa Agentic Ready reúne a decenas de emisores de la región que prueban estos pagos. Son pilotos y despliegues controlados, no operación masiva.

Desde el lado de los supervisores, los autores de la nota del FMI proponen que los reguladores consideren pasar de KYC a KYA, con identidades verificables obligatorias para los agentes financieros, vinculadas a entidades legales, y recomiendan que las redes de pago construyan registros globales de agentes. Es una propuesta de los autores, no una política.

Quién responde. La nota del FMI observa que la mayoría de los regímenes de pago exigen que una orden de pago sea rastreable hasta una instrucción autorizada del titular o de su agente legalmente reconocido. Los pagos iniciados por agentes desafían ese modelo, porque cada operación puede no corresponder a una instrucción explícita: la autorización pasa a ser estructural y basada en un mandato. Los autores hablan de falta de claridad regulatoria sobre la responsabilidad. Singapur, que lanzó en enero de 2026 un marco modelo de gobernanza para IA agéntica, orienta a limitar los poderes del agente y a definir puntos de control donde se exija aprobación humana. Su regulador financiero fue más lejos: en julio de 2026 la MAS publicó con la industria el documento SAFR (*Safeguards for Agentic Finance at Runtime*, salvaguardas para las

finanzas agénticas en tiempo de ejecución), que propone puntos de control que verifican y registran cada acción que propone un agente antes de ejecutarla, para mantenerlo dentro de los mandatos y límites de riesgo que fija la institución.

04 Europa: lo que ya regula y lo que no

La respuesta corta es que la Unión Europea regula a quien representa a otro y regula los sistemas de IA, pero todavía no regula al agente de IA como representante.

La ley de IA cubre a los agentes, pero no como figura propia. Según las preguntas frecuentes de la Comisión Europea sobre su ley de IA, los agentes no son una categoría separada: les aplican las reglas de los sistemas de IA y de los modelos de uso general. La propia Comisión advierte que sus consideraciones sobre agentes son, por ahora, solo preliminares.

La identidad digital europea es de personas. La billetera de identidad de eIDAS 2.0 es para personas naturales y, según un análisis de la Cloud Security Alliance, sus actos de ejecución todavía no tratan a los agentes de IA como sujetos de identidad. La futura billetera para empresas (*European Business Wallets*), que la Comisión propuso el 19 de noviembre de 2025 y que sigue en negociación, gestionará mandatos para representantes autorizados; en el texto, esos representantes son empleados u otras personas naturales o jurídicas.

La prevención de lavado verifica a quien actúa por el cliente, pensando en personas. Como vimos en el DOC.20, el reglamento antilavado extiende la verificación de identidad a quien actúa en nombre del cliente, y el borrador de sus normas técnicas pide verificar la existencia y el alcance de su poder de representación, con ejemplos como el poder notarial.

Los pagos siguen atados a la persona. El nuevo Reglamento de Servicios de Pago, cuyo texto final se respaldó en abril de 2026 y se espera publicar en el segundo semestre, mantiene la autenticación reforzada con dos de tres elementos del usuario: algo que sabe, algo que tiene o algo que es. En los análisis jurídicos que leímos no encontramos una regla específica para agentes.

Hay propuestas para cerrar la brecha: en marzo de 2026, un consorcio europeo de billeteras pidió una estrategia para agentes seguros apoyada en la billetera europea y en la de empresas. A la fecha, son propuestas.

05 Quién se mueve

Frente	Quiénes	Qué proponen	En qué estado está
Estándares abiertos	NIST, IETF, W3C, FIDO	Una pila compuesta: identidad de cargas de trabajo, autorización delegada, credenciales verificables, mandatos firmados	Borradores y grupos de trabajo; el NCCoE aún no publicó el borrador de descripción de su proyecto

Frete	Quiénes	Qué proponen	En qué estado está
Redes de pago	Visa, Mastercard, Ant International	KYA conjunto: operador validado, certificación y monitoreo; cada red ya exige firmar o registrar al agente en su propio programa	Principios en exploración, sin especificación; programas propios en pilotos y despliegues controlados, también en América Latina
Organismos y supervisores	FMI, Singapur (IMDA y MAS)	Tres capas; paso de KYC a KYA; puntos de control antes de ejecutar	Una nota de autores, un marco de orientación y un documento con la industria; ninguna norma vinculante
Unión Europea	Comisión, Consejo y Parlamento	Regula los sistemas de IA y a los representantes humanos; billetera para empresas con mandatos	No regula aún al agente como representante; la billetera para empresas sigue en negociación
Proveedores de identidad	Microsoft	Identidad por agente, con patrocinador humano obligatorio	Producto documentado; no es un estándar

06 El caso del banco: el agente que llega de afuera

El resumen del NIST distingue tres modelos. En los dos primeros, la empresa es dueña del agente y controla su identidad. En el tercero, el agente es de propiedad externa y entra a los servicios de la empresa: el ejemplo del propio resumen es un agente del consumidor con acceso a sus cuentas financieras. Ese es el caso del banco.

Ahí la influencia de la institución sobre cómo se identifica y autoriza al agente es limitada. El agente puede tener identidad propia, o puede recibir la identidad o una credencial estática de una persona. Puede usar las interfaces del banco o «raspar» pantallas y parecer un cliente con navegador. Los servicios al consumidor ya tienen dificultad para distinguir a una persona de un agente, y esto empeora cuando el cliente le da sus credenciales al agente para que lo suplante. Un comentarista planteó el problema completo: cómo diferenciar a una persona, a un agente que ella autorizó y a un programa que dice tener esa autorización sin tenerla. El resumen advierte que mientras el camino seguro no sea también el fácil, seguirán proliferando la suplantación y el uso compartido de credenciales.

Hay un dato práctico sobre los plazos. El NCCoE planea dos casos de uso: primero uno empresarial, con una «fábrica de software», y más adelante uno de consumo con agentes de propiedad del consumidor. Como el caso de consumo viene después, es razonable no esperar pronto una guía del NCCoE para el caso que le importa al banco.

07 Lectura de Inteligencia Bancaria (IAB)

Esta sección es una lectura de IAB, no un hallazgo. Las fuentes convergen, con distintas palabras, en cuatro preguntas que un banco tendrá que poder responder cuando le llegue el agente de un cliente:

Pregunta	Qué la responde	Estado
¿Quién es el agente?	Un identificador propio y verificable, anclado a quien lo produjo	Principio cerrado; método abierto
¿Quién lo autorizó?	Una delegación rastreable hasta una persona o entidad	Principio cerrado
¿Qué puede hacer en esta tarea?	Un mandato acotado, revocable y, si es posible, firmado	Abierto
¿Quién responde y con qué evidencia?	Un expediente que muestre decisión y autoridad, no solo la acción	Abierto

De las cuatro, la pieza que menos controla el banco y más necesita es el mandato. En el DOC.20 vimos que el borrador europeo pide verificar la existencia y el alcance del poder de representación de quien actúa por el cliente. Para un agente, ese poder sería el mandato. Y como en el caso del apoderado, la pregunta del banco no es solo quién es, sino qué le dio el cliente permiso de hacer y si esa autorización sigue vigente.

La segunda lectura es sobre el papel del banco. Cuando el agente es de afuera, el banco no lo emite: lo verifica. Esa es la diferencia con las empresas que dan identidad a sus propios agentes y les asignan un patrocinador. Con el agente de afuera, el banco necesita que alguien certifique al agente (en pagos con tarjeta, ese lugar ya lo ocupan de hecho las redes: Visa y Mastercard exigen firmar o registrar al agente antes de operar y lo están probando con bancos de la región) y necesita el mandato del cliente. Fuera de las tarjetas (transferencias, cuentas, crédito), quién ocupará ese lugar es todavía una pregunta abierta.

08 Tres preguntas para el comité

1. Cuando alguien opera hoy una cuenta con credenciales prestadas a un agente, ¿puede el banco distinguirlo de la persona?
2. ¿Qué evidencia guardaría el banco de que el cliente delegó en un agente, con qué límites y hasta cuándo?
3. Si un agente excede su mandato, ¿quién responde y cómo lo demuestra el expediente?

09 Lo que no encontramos

No encontramos una norma panameña específica sobre agentes de IA. El Acuerdo 1-2026 de la Superintendencia de Bancos, que leímos completo para el DOC.20, no menciona al agente como figura propia. Tampoco lo hacen la Ley 81 de 2019, de protección de datos personales, ni su reglamento, el Decreto Ejecutivo 285 de 2021, que leímos completos para esta pieza.

Esas dos normas sí tocan dos piezas de esta discusión, pero pensadas para personas. La primera es la representación: el titular puede ejercer sus derechos por medio de quien lo represente, y el reglamento exige acompañar la documentación que acredite esa representación. La segunda son las decisiones automatizadas: el titular tiene derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado de sus datos que le produzca efectos jurídicos negativos, como una evaluación de crédito, salvo que la haya consentido, sea necesaria para un contrato o la autorice una ley especial, y tiene derecho a recibir información significativa sobre la lógica aplicada. Ese derecho mira las decisiones que toma la institución con sus propios sistemas, no al agente que actúa por el cliente. En la Unión Europea no encontramos una norma vigente que regule al agente de IA como representante; revisamos la ley de IA, la identidad digital, la propuesta de billetera para empresas, el reglamento ant blanqueo y el nuevo reglamento de pagos, este último a través de análisis jurídicos.

No encontramos publicado, al 17 de octubre de 2026, el borrador de descripción de proyecto que el NCCoE dijo que lanzaría. El comunicado del marco KYA de Ant International, Mastercard y Visa no trae criterios de certificación ni una especificación técnica, y no los encontramos publicados después. No decimos que no existan; decimos que no son públicos o que no los hallamos. Quedan como preguntas pendientes.

Cómo verificamos

Cada cifra y cada fecha de esta pieza está registrada con su fuente en el registro de verificación de IAB. Leímos completos el resumen de comentarios del NIST y la nota del FMI; del borrador del IETF y de la nota del W3C leímos los extractos citados. El anuncio de KYA y los programas de Visa y Mastercard se verificaron en sus comunicados originales. Lo que proviene de fuentes secundarias, como las fechas de AP2 y Verifiable Intent y algunos análisis sobre la Unión Europea, está atribuido en el texto. El resumen del NIST recoge opiniones de comentaristas, no una posición oficial; la nota del FMI es de sus autores. Las lecturas de IAB están marcadas como tales.

Anexo. La pila de estándares que citan los comentaristas

Según el resumen del NIST, la identidad de agentes es una pila compuesta, con madurez muy desigual. Su inclusión aquí no implica respaldo.

Capa	Estándares que se mencionan
Modelo conceptual	Borrador del IETF «AI Identity Management System» (AIMS, sistema de gestión de identidad de IA)
Identidad de cargas de trabajo	WIMSE; SPIFFE y SPIRE (identificadores de carga de trabajo y su implementación de referencia)

Capa	Estándares que se mencionan
Autorización y delegación	OAuth 2.0 y sus extensiones: intercambio de tokens, cadenas de identidad y tokens de transacción
Credenciales portables	W3C Verifiable Credentials 2.0; Identificadores Descentralizados (DID) 1.0
Integración de agentes	MCP (<i>Model Context Protocol</i> , protocolo de contexto de modelos) y A2A (<i>Agent-to-Agent Protocol</i> , protocolo agente a agente); según el NIST, no son estándares completos de identidad ni de autorización
Intención y pagos	Trabajo de la FIDO sobre autenticación agéntica; AP2; Verifiable Intent
Decisión y señales	OpenID AuthZEN (interfaz para preguntar si un sujeto puede hacer una acción) y las señales compartidas CAEP y RISC (evaluación continua de acceso y coordinación de incidentes de riesgo)
Evidencia	SCITT (<i>Supply Chain Integrity, Transparency and Trust</i> , integridad, transparencia y confianza en la cadena de suministro)

Fuentes

- NIST, NCCoE, resumen de comentarios sobre identidad y autorización de agentes de IA (29 sep. 2026): <https://page.s.nist.gov/nccoe-ai-identity/summary-of-comments.html>
- NIST, comunicado sobre el resumen de comentarios (29 sep. 2026): <https://www.nist.gov/news-events/news/2026/09/comments-software-and-agentic-ai-identity-concept-paper>
- FMI, Nota 2026/004, «How Agentic AI Will Reshape Payments» (abril de 2026): <https://www.imf.org/en/publications/imf-notes/issues/2026/04/22/how-agentic-ai-will-reshape-payments-575560> ; PDF: <https://www.imf.org/en/-/media/files/publications/imf-notes/2026/english/insea2026004.pdf>
- IETF, borrador «AI Identity Management System» (15 sep. 2026): <https://datatracker.ietf.org/doc/draft-ietf-wimse-a-ims/00/> ; antecesor: <https://datatracker.ietf.org/doc/html/draft-klrc-aiagent-auth>
- W3C, «Verifiable Credentials Overview» (17 jun. 2026): <https://www.w3.org/TR/2026/NOTE-vc-overview-20260617/>
- FIDO Alliance, comunicado (28 abr. 2026): <https://www.fidoalliance.org/fido-alliance-to-develop-standards-for-trusted-ai-agent-interactions/>
- Google dona AP2 a la FIDO Alliance; Mastercard aporta Verifiable Intent: <https://www.pymnts.com/artificial-intelligence-2/2026/google-and-mastercard-contribute-agentic-commerce-standards-to-fido-alliance/> ; <https://ppc.land/fido-alliance-forms-working-groups-to-lock-down-ai-agent-payments/>
- Ant International, Mastercard y Visa, comunicado sobre el marco de KYA (10 sep. 2026): <https://www.ant-intl.com/en/news/detail/?id=ant-international-mastercard-and-visa-initiate-collaboration-on-know-your-agent-interoperability-to-scale-agentic-commerce> ; ausencia de especificación: <https://technode.global/2026/09/10/ant-international-mastercard-visa-develop-kya-framework/>
- Visa, especificación del Trusted Agent Protocol: <https://developer.visa.com/capabilities/trusted-agent-protocol/trusted-agent-protocol-specifications/>
- Visa, Agentic Ready en América Latina y el Caribe (29 abr. 2026): <https://www.visa.com.mx/acerca-de-visa/sala-de-noticias/notas-de-prensa/visa-agentic-ready-comercio-inteligencia-artificial-lac.html> ; Santander y Visa (12 mar. 2026): <https://www.santander.com/es/sala-de-comunicacion/notas-de-prensa/2026/03/santander-y-visa-completan-en-latinoamerica-los-primeros-pagos-gestionados-integramente-por-agentes-de-ia>
- Mastercard, transacciones con agentes en América Latina y el Caribe (24 mar. 2026): <https://www.mastercard.com/news/latin-america/en/newsroom/press-releases/pr-en/2026/march/mastercard-advances-agentic-payments-in-lat-in-america-and-the-caribbean-with-live-transactions-completed-across-the-region/>

- Mastercard, servicios de confianza e inteligencia de Agent Pay (30 sep. 2026): <https://www.mastercard.com/global/en/news-and-trends/press/2026/september/new-trust-and-intelligence-services.html>
- MAS, SAFR (julio de 2026): <https://www.mas.gov.sg/publications/monographs-or-information-paper/2026/safeguards-for-agentic-finance-at-runtime>
- Singapur, IMDA, Model AI Governance Framework for Agentic AI (22 ene. 2026): <https://www.mddi.gov.sg/newsroom/singapore-launches-new-model-ai-governance-framework-for-agentic-ai--/>
- Comisión Europea, servicio de atención de la Ley de IA, «How are AI agents addressed within the AI Act?»: <https://ai-act-service-desk.ec.europa.eu/en/ai-act/faq/how-are-ai-agents-addressed-within-ai-act-0>
- Comisión Europea, propuesta de European Business Wallets, COM(2025) 838: https://www.eerstekamer.nl/bijlage/20251121/com_2025_838_proposal_for_a/document3/f=/vmsoctgrbbbeb.pdf ; orientación general del Consejo (9 jun. 2026): <https://data.consilium.europa.eu/doc/document/ST-10346-2026-INIT/en/pdf>
- Cloud Security Alliance, billetera europea e identidad de agentes (abr. 2026): <https://labs.cloudsecurityalliance.org/research/csa-research-note-enisa-eu-digital-wallet-ai-agent-identity/>
- Reglamento de Servicios de Pago, texto final de compromiso (abr. 2026): <https://legal.pwc.de/content/services/reg-core-client-alert/pwc-client-alert-eus-new-payments-framework-april-2026.pdf>
- Panamá, Ley 81 de 2019 sobre protección de datos personales (Gaceta Oficial 28743-A): https://s3-legispan.asamblea.gob.pa/legispan/NORMAS/2010/2019/LEY/Administrador%20Legispan_28743-A_2019_3_29_ASAMBLEA%20NACIONAL_81.pdf
- Panamá, Decreto Ejecutivo 285 de 2021 que reglamenta la Ley 81 (Gaceta Oficial 29296-A, 28 de mayo de 2021): http://gacetas.procuraduria-admon.gob.pa/29296-A_56425.pdf
- Microsoft, Entra Agent ID, identidades de agente y patrocinadores: <https://learn.microsoft.com/entra/agent-id/agent-identities> ; <https://learn.microsoft.com/en-us/entra/agent-id/agent-owners-sponsors-managers>

Criterio Humano. Inteligencia Escalable.

CÓMO CITAR ESTE DOCUMENTO

InteligenciABancaria.net · DOC.21 · Octubre 2026