

El agente se queda en la puerta

Schwab y JPMorgan cerraron sus sistemas a los agentes de IA de terceros que intentaban mover el dinero de sus clientes, y la pregunta de fondo es quién responde cuando un agente se equivoca con dinero ajeno.

Por [Oscar Obando Chaves](#) · Chief AI Officer · Legal AI Engineer · Octubre 2026 · Documento de distribución libre ·
[Publicado originalmente en LinkedIn](#)

Lo que pasó en Schwab y en JPMorgan

El 13 de octubre de 2026, en la presentación de resultados del tercer trimestre, Jamie Dimon dijo que JPMorgan no dejará que agentes de IA de afuera actúen dentro de sus sistemas, y advirtió sobre los agentes que se salen de control. Dos días después, Rick Wurster, presidente de Charles Schwab, explicó que su firma bloquea a los agentes de IA que intentan entrar por su cuenta al sitio para mover el dinero de los clientes, nombró entre ellos a Muse, el asistente de Meta, y dijo que esa es la única vía que su firma no considera segura.

Al día siguiente, en Bloomberg Television, Wurster lo resumió en una frase, puesto que dijo que ni la firma ni el cliente pueden controlar a ese agente, que algo puede salir mal y que entonces nadie sabe quién responde. Según la misma entrevista, los agentes grandes que Schwab detiene se cuentan por decenas cada semana, y él lo lee como una señal de que los clientes todavía no están listos para entregarle su cuenta a una IA.

Ninguno de los dos cerró la puerta a la IA. Schwab ofrece a sus clientes su propio asistente, Charley, anunciado el 30 de septiembre, y una conexión controlada por MCP para que el modelo que el cliente elija consulte saldos y haga análisis bajo las reglas de la firma, sin poder mover dinero, mientras JPMorgan permite que algunas herramientas de terceros vean datos de la cuenta y les impide transferir fondos o pagar facturas.

Fuentes: American Banker (15 de octubre de 2026), The Next Web (16 de octubre de 2026, con la entrevista de Rick Wurster en Bloomberg Television) y Cybernews, sobre la política de JPMorgan con agentes externos.

La pregunta que nadie ha contestado

Lo que los dos bancos describen es, en el fondo, un problema de responsabilidad. Cuando un cliente le entrega sus credenciales a un agente de IA y ese agente entra al banco como si fuera él, mueve dinero y se equivoca, la cuenta tiene al menos tres partes, que son el cliente que le

dio acceso, la empresa que hizo el agente y el banco que recibió la orden, y en Estados Unidos el Congreso todavía discute de quién es la responsabilidad por lo que hace un agente.

Mientras ese reparto no esté escrito, el banco hace lo único que tiene a mano, que es cerrar la puerta, puesto que es el que tiene la relación regulada con el cliente y el que tendría que explicarle por qué salió de su cuenta un dinero que él no ordenó en persona.

Es la misma escena con la que abrí mi ponencia en Arequipa, la de la aseguradora cuyo asistente rechaza reembolsos un lunes porque su proveedor cambió el modelo el fin de semana, con la diferencia de que aquí el agente lo trae el cliente. En los dos casos la respuesta tiene un lugar natural, que es el contrato, siempre que alguien lo haya escrito antes de que el agente toque la puerta.

Fuentes: The Next Web (16 de octubre de 2026) y la ponencia «Del sistema de gestión a la cláusula exigible», III Jornadas Latinoamericanas de Derecho y Tecnología, Universidad Católica San Pablo, Arequipa, 15 de octubre de 2026.

Qué tiene que ver con Ecuador

No encontré un pronunciamiento de bancos ecuatorianos sobre los agentes de IA de terceros, sin embargo las reglas que ya rigen en el país alcanzan a esta situación. El artículo 20 de la Ley Orgánica de Protección de Datos Personales le da a toda persona el derecho a no ser objeto de una decisión basada única o parcialmente en valoraciones automatizadas que produzca efectos jurídicos o afecte sus derechos fundamentales, y a pedir una explicación motivada, mientras la Norma General de IA de la Superintendencia de Protección de Datos Personales (Resolución SPDP-SPD-2026-0009-R) obliga a quien trate datos personales con IA a informarlo, gestionar el riesgo y evaluar el impacto antes de desarrollar el sistema.

Del 24 de septiembre al 22 de octubre de 2026 esa misma Superintendencia tuvo en consulta pública un borrador sobre datos crediticios que prohíbe el perfilamiento que dé lugar a decisiones automatizadas sin una intervención humana efectiva, y que exige a quien use IA, modelos predictivos o algoritmos de puntuación para evaluar la solvencia garantizar la calidad, la exactitud y la trazabilidad de los datos y de los resultados. Todavía no rige, aunque muestra hacia dónde va el regulador.

La Superintendencia de Bancos, en su norma de canales de atención al consumidor financiero (Resolución SB-2026-1691, del 27 de mayo de 2026), define el chatbot como un canal que usa inteligencia artificial o procesamiento de lenguaje natural, sin deberes propios de la IA, de modo que el caso del agente externo que actúa en nombre del cliente queda en las reglas generales. La Ley Orgánica para el Fortalecimiento de la Ciberseguridad, cuyo régimen de sanciones ya se puede exigir en el sector financiero, obliga a los operadores de infraestructura crítica digital a notificar los incidentes de seguridad relevantes a más tardar en 72 horas.

Fuentes: Ley Orgánica de Protección de Datos Personales, artículo 20; Resolución SPDP-SPD-2026-0009-R (Registro Oficial N° 240, 10 de marzo de 2026); borrador de Norma General para el Tratamiento de Datos Crediticios de la Superintendencia de Protección de Datos Personales; Resolución SB-2026-1691; Ley Orgánica para el Fortalecimiento de la Ciberseguridad (Quinto Suplemento del Registro Oficial N° 290, 22 de mayo de 2026). El estado de cada norma, al día, está en oscarobando.ai/es/regulacion-ia-ecuador.

Lo que puede hacer tu empresa desde hoy

Si tu empresa presta servicios financieros, o cualquier servicio en el que un cliente pueda delegar en un agente, conviene dejar ordenados tres puntos antes de que el primer agente toque la puerta.

1. Qué puede hacer un agente externo y qué no, escrito en los términos del servicio, con la consulta separada de las operaciones que mueven dinero, que es justamente lo que hizo Schwab con su conexión de solo lectura.
2. Cómo se identifica el agente y cómo confirma el cliente cada operación que importa, con una confirmación humana para pagos y transferencias y una bitácora que permita reconstruir después quién ordenó qué.
3. Qué dicen los contratos con los proveedores de IA de la propia empresa, porque ahí se reparte la responsabilidad cuando algo sale mal, con plazos para avisar los cambios de modelo, acceso a los registros y remedios concretos. La ISO/IEC 42001, que en Ecuador es norma técnica voluntaria desde julio de 2026, sirve como lenguaje común para escribirlos, con certificado o sin él.

Ninguna de las tres espera a una ley, puesto que están al alcance de cualquier empresa desde hoy y se vuelven exigibles apenas entran al contrato.

Fuentes: The Next Web (16 de octubre de 2026), para el modelo de acceso de Schwab; NTE INEN-ISO/IEC 42001, oficializada con carácter voluntario (Suplemento del Registro Oficial N° 329, 20 de julio de 2026).

Algo puede salir mal, ¿y quién es responsable?

Rick Wurster, presidente de Charles Schwab, en Bloomberg Television (octubre de 2026)

Oscar Obando Chaves es Chief AI Officer y Legal AI Engineer ecuatoriano, con formación en derecho. Ayuda a las empresas a decidir cómo usan la IA y construye con ella sistemas para el negocio y para lo legal. Chief AI Officer y Senior AI Counsel en HEKA Law, ISO 42001 AI Management Leader e ISO 38507 AI Governance Leader. Publica análisis semanal sobre el impacto real de la IA.