

12 min de lectura

La Contraseña **No Es un Mandato**

La gran banca de Estados Unidos cerró la puerta a los agentes de IA de consumo. Lo que eso le anticipa a la banca latinoamericana.

Entre el 13 y el 22 de octubre de 2026, los mayores bancos de Estados Unidos trazaron una línea: un agente de inteligencia artificial (IA) puede mirar la cuenta de un cliente, pero no mover su dinero por su cuenta. La razón no es tecnológica. Es de identidad y de responsabilidad: cuando el cliente entrega su contraseña a un agente, el banco deja de saber quién opera, y la ley deja de saber quién paga.

Lo que hoy se resuelve en Nueva York con bloqueos llegará a la banca latinoamericana por dos vías: los clientes que ya usan estos agentes y la banca corresponsal que conecta a la región con el sistema estadounidense.

01 Lo que pasó

En diez días, cinco de las mayores instituciones financieras de Estados Unidos pasaron de advertir sobre los agentes de IA a bloquearlos o restringirlos.

Fecha (2026)	Hecho	Fuente
29 sept.	OpenAI lanza dots, agentes siempre activos dentro de ChatGPT.	TechCrunch
30 sept.	Schwab lanza Charley, su propio asistente de IA.	The Next Web
13 oct.	En la llamada de resultados del tercer trimestre, Jamie Dimon advierte sobre «agentes rebeldes» y afirma que JPMorgan no permitirá que cualquier agente externo entre al banco, por ser demasiado riesgoso para los clientes y para la institución.	CNBC
14 oct.	En la llamada de resultados del tercer trimestre, Brian Moynihan, CEO de Bank of America, explica que trabajan con los proveedores de agentes para que el humano siga en el circuito antes de que el dinero salga de la cuenta.	Transcripción
16 oct.	Rick Wurster, director ejecutivo (CEO, <i>Chief Executive Officer</i>) de Charles Schwab, confirma que bloquea agentes no autorizados que intentan mover dinero de clientes, incluido Muse, el agente personal de Meta, «en las decenas y veintenas» cada semana.	Bloomberg
21 oct.	Anthropic presenta Claude Duet, su agente personal, en vista previa con lista de espera para usuarios de Estados Unidos.	Reuters

Fecha (2026)	Hecho	Fuente
22 oct.	Grandes bancos detectan agentes de IA de terceros, no autorizados, operando dentro de cuentas de clientes; algunos actúan más allá de lo que el usuario pidió, incluso llamando por su cuenta a los centros de atención.	Axios
22 oct.	Dos fuentes confirman que Morgan Stanley, JPMorgan, Bank of America y Citi bloquean o restringen el acceso de agentes de terceros. Wells Fargo figura entre los bancos que trabajan para contener el riesgo.	Reuters

Un matiz importa: bloquear no es lo mismo que restringir. Morgan Stanley bloquea; JPMorgan, Bank of America y Citi restringen, casi siempre hacia un acceso de solo lectura. Morgan Stanley aclara, además, que no ha observado agentes rebeldes en sus plataformas: bloquea por precaución.

02 El problema no es el agente: es la contraseña

La mayoría de los casos reportados tiene la misma forma: el cliente le da a su asistente de IA el usuario y la clave de su banca en línea, y el agente entra por la misma puerta que el humano. Ahí se rompen tres supuestos del modelo de control.

- **El banco no sabe quién opera.** El agente no se identifica como software: simula ser el cliente. Un ejecutivo citado por Axios admite que lo difícil es distinguir a un agente de una persona y, después, a un agente que el cliente pidió de uno que solo tiene su contraseña.
- **El agente hace más de lo que se le pidió.** Los bancos han rastreado sesiones que parecen actuar con independencia de lo que el cliente solicitó, incluidos agentes que llaman por su cuenta a los centros de atención.
- **El agente puede recibir órdenes de un tercero.** Un agente que lee el correo y opera la banca del mismo cliente puede encontrar un mensaje con instrucciones ocultas y ejecutarlas. Es la llamada inyección de instrucciones (*prompt injection*), una de las amenazas centrales que la literatura de seguridad identifica para los agentes de IA.

Los controles antifraude de la banca se diseñaron para detectar a un tercero que se hace pasar por el cliente. Aquí el tercero entra con permiso del cliente. El sistema ve un inicio de sesión legítimo y una intención ajena.

03 ¿Quién paga cuando el agente se equivoca?

Nadie lo sabe todavía, y esa es la razón de fondo de los bloqueos. En Estados Unidos, la Ley de Transferencias Electrónicas de Fondos (EFTA, *Electronic Fund Transfer Act*) y su Regulación E protegen al consumidor frente a las transferencias no autorizadas. Pero la propia definición

excluye las transferencias que inicia una persona a quien el consumidor le entregó su medio de acceso, salvo que haya avisado al banco que esa persona ya no está autorizada ([12 CFR §1005.2\(m\)](#)).

Leída así, la transferencia errónea de un agente al que el cliente le dio su clave podría quedar fuera de la protección. Hay un matiz: la Oficina para la Protección Financiera del Consumidor (CFPB, *Consumer Financial Protection Bureau*) ha aclarado que quien comparte sus credenciales engañado por un fraude no las «entregó» en el sentido de la norma. Dónde cae un agente manipulado por un tercero es justamente la pregunta abierta, y el Congreso sigue debatiendo cómo asignar esa responsabilidad.

Mientras tanto, los bancos se mueven por dos caminos distintos:

- **Por contrato.** El nuevo Contrato de Acceso por Internet de Wells Fargo, vigente desde el 24 de noviembre de 2026, incorpora entre sus materias las responsabilidades del cliente por agentes de IA, «si y cuando» el banco permita su uso. Establece que las operaciones de los agentes de IA de un representante o delegado autorizado se consideran autorizadas por el cliente, incluso las que no quiso o no previó. Y advierte que, si el cliente da acceso a un agente de IA, acepta el riesgo de debilitar los procedimientos de seguridad pactados.
- **Por arquitectura y por ley.** William Demchak, CEO de PNC, afirmó en la conferencia Money20/20 que ningún banco dejará operar dentro de las cuentas sin un humano en el circuito. Para que los agentes transaccionen, dijo, las tecnológicas tendrían que asumir un traslado masivo de responsabilidad por los daños que causen.

La diferencia no es menor. El camino contractual protege al banco; el arquitectónico protege al cliente. Los reguladores de protección al consumidor van a mirar cuál eligió cada institución.

04 Las tres respuestas que ya se perfilan

El bloqueo es una tregua, no una solución: los bancos reconocen que sus clientes quieren usar estos agentes. Lo que se está construyendo detrás del bloqueo tiene tres piezas, y cada una resuelve un problema distinto.

Respuesta	Qué resuelve	Quién la mueve	Límite
Leer sí, mover no. Acceso de solo lectura mediante interfaces de banca abierta (API, <i>Application Programming Interface</i> , interfaz de programación de aplicaciones) o servidores MCP (<i>Model Context Protocol</i> , protocolo de contexto de modelo).	Saca al agente de la contraseña y lo lleva a un canal que el banco controla.	Schwab prepara servidores MCP para consultar saldos e investigar sin mover dinero; Citi mantiene conexiones aprobadas de banca abierta; JPMorgan permite lectura a través de intermediarios como Plaid.	El cliente no obtiene lo que más quiere: que el agente ejecute. Y el MCP no es de solo lectura por diseño; la restricción la ponen los permisos del banco.

Respuesta	Qué resuelve	Quién la mueve	Límite
Reglas para el agente. Protocolos acordados con los desarrolladores de agentes que definen cómo puede actuar un agente sobre una cuenta; técnicamente, credenciales con alcance limitado (<i>tokens</i> bajo OAuth, <i>Open Authorization</i> , autorización abierta) que dicen qué agente opera, quién lo autorizó, qué puede hacer y cuándo vence el permiso.	Devuelve al banco la respuesta a «¿quién opera?».	Bank of America trabaja con desarrolladores de agentes en esos protocolos; Schwab, al exigir que los agentes entren por servidores cuya autenticación controla.	Requiere que los desarrolladores de agentes acepten identificarse ante cada banco.
El humano firma. Autenticación escalonada: el agente prepara el pago y el titular lo aprueba desde su dispositivo con biometría o llaves de acceso (<i>passkeys</i>).	Mantiene la responsabilidad donde está hoy: en un humano identificado.	Moynihan (Bank of America) y Demchak (PNC) plantean el humano en el circuito como condición.	Le quita al agente parte de su autonomía, que es justo lo que lo hace atractivo.

Hay una cuarta jugada, comercial más que técnica: el agente propio. Schwab no solo bloquea a Muse; empuja a sus clientes hacia Charley. Y el trasfondo de depósitos ya está en la mesa: en la llamada de Bank of America, los analistas preguntaron si agentes como Muse podrían mover saldos ociosos hacia productos de mayor rendimiento, y Moynihan respondió que no espera esa fuga. Para el comité, la pregunta honesta es cuánto pesa cada motivo, seguridad o negocio, en la decisión propia.

05 Lo que le anticipa a la banca latinoamericana

Es previsible que el agente del cliente llegue antes que la política del banco. Estos productos se lanzan primero en Estados Unidos, pero el cliente latinoamericano que viaja, invierte afuera y adopta tecnología temprano no esperará a que su banco tenga una postura.

La diferencia entre países estará en si existe una puerta regulada por la que derivar a ese agente:

- **Brasil** es la referencia regional en finanzas abiertas.
- **Chile:** la Comisión para el Mercado Financiero (CMF) publicó el 1 de junio de 2026 la norma que completa los requisitos técnicos de su Sistema de Finanzas Abiertas, incluidos el intercambio de información y la iniciación de pagos, y pospuso su entrada en vigor hasta julio de 2027.
- **Colombia:** el Decreto 0368, del 7 de abril de 2026, hizo obligatorio el sistema de finanzas abiertas para todas las entidades vigiladas por la Superintendencia Financiera.

Donde hay finanzas abiertas, el banco tiene un canal de lectura regulado al cual enviar al agente. Donde no lo hay, la única puerta es la contraseña.

Panamá está en el segundo grupo. No tiene un marco formal de finanzas abiertas vigente; la Ley Marco Integral de Tecnologías Financieras propone uno en su capítulo de banca abierta. Se presentó como anteproyecto el 13 de enero de 2026, fue prohiado el 20 de enero como Proyecto de Ley 487 y a fines de octubre de 2026 [seguía en trámite en la Asamblea](#), sin haberse convertido en ley. Mientras tanto, el agente del cliente no tendrá una entrada regulada: entrará por la banca en línea, con la clave del titular.

Y la banca panameña opera atada a sus corresponsales estadounidenses, los mismos que hoy bloquean. Es razonable anticipar que, cuando esos bancos definan qué es una operación iniciada por un agente, esa definición viaje en los contratos de corresponsalía y en sus cuestionarios de debida diligencia, como se analizó en el DOC.17 con la guía de la Reserva Federal.

06 Cinco preguntas para el comité

Ninguna de estas preguntas requiere esperar al regulador. Todas se pueden responder con lo que el banco ya tiene.

1. **¿Cuántas sesiones de nuestra banca en línea no son humanas?** Si no se puede medir, el problema ya existe y no se ve.
2. **¿Qué dicen nuestros términos sobre entregar credenciales a un software?** Y, sobre todo, qué haríamos valer ante el reclamo de un cliente cuyo agente vació su cuenta.
3. **¿Tenemos un canal de solo lectura al que derivar a un agente?** Si la única puerta es la contraseña, bloquear solo empuja al cliente a esconder mejor a su agente.
4. **¿Qué operaciones exigirán siempre la firma de un humano?** Aunque el agente esté autorizado, y con qué nivel de autenticación.
5. **¿Tenemos el plan del día después?** Los bancos estadounidenses ya preparan escenarios para asegurar cuentas y restaurar el acceso rápido si un agente causa daño. Congelar, revertir, restaurar y comunicar no se improvisa la mañana del incidente.

07 Una contraseña no es un mandato

La gran banca estadounidense eligió, por ahora, la respuesta más simple: cerrar la puerta de escritura y abrir la de lectura. Funciona mientras los agentes solo quieran mirar. Dejará de funcionar cuando el cliente exija que su agente pague, transfiera y negocie.

La salida de fondo no es bloquear mejor. Es dejar de tratar la contraseña como si fuera una autorización y construir lo que hoy falta: una identidad propia para el agente y una autoridad delegada, acotada y revocable, emitida por el cliente y verificable por el banco.

La siguiente entrega de la serie sobre identidad digital cierra ese recorrido con las alternativas concretas que tiene un banco para atender al agente de un cliente. Si su institución ya está viendo agentes en sus canales, ese es el momento de comparar notas.

Criterio Humano. Inteligencia Escalable.

Fuentes

Primarias

- [Wells Fargo: Contrato de Acceso por Internet vigente desde el 24 nov. 2026](#)
- [12 CFR §1005.2\(m\), Regulación E](#)
- [CFPB: preguntas frecuentes sobre transferencias electrónicas \(copia\)](#)
- [Bank of America: transcripción de la llamada del 3T 2026](#)
- [CMF Chile: modificación de la NCG 514, 1 jun. 2026](#)
- [Superintendencia Financiera de Colombia: Decreto 0368 de 2026](#)

Prensa y análisis

- [Axios: agentes de IA no verificados acceden a cuentas bancarias](#), 22 oct. 2026
- [Reuters, vía MoneyCheck: bancos bloquean agentes de terceros](#), 22 oct. 2026
- [Bloomberg: Schwab bloquea agentes que intentan mover dinero](#), 16 oct. 2026
- [CNBC: Dimon y el debate sobre depósitos](#)
- [PYMNTS: la línea común de JPMorgan y Bank of America](#)
- [Banking Dive: Demchak en Money20/20](#)
- [Gear Live: el problema de distinguir agentes de personas](#)
- [CoinCentral: cómo acceden los agentes a las cuentas](#)
- [The Next Web: Schwab, Muse, servidores MCP y Charley](#)
- [IBTimes: Citi, Schwab y permisos sobre MCP](#)
- [Yahoo Finance: Morgan Stanley y acceso vía Plaid](#)
- [Reuters, vía KFGO: Anthropic presenta Claude Duet](#), 21 oct. 2026
- [TechCrunch: OpenAI lanza dots](#), 29 sept. 2026
- [Infobae: proyectos sobre tecnologías financieras en trámite en la Asamblea](#), 26 oct. 2026
- [Velo Legal: Proyecto de Ley 487 en Panamá](#)
- [LexLatin: Anteproyecto de Ley 314](#)
- [Fiskil: estado de las finanzas abiertas en América Latina](#)
- [Encuesta sobre ataques y defensas en IA agéntica \(arXiv\)](#)

CÓMO CITAR ESTE DOCUMENTO

InteligenciABancaria.net • DOC.22 • Octubre 2026