

2 min de lectura

El Fin del SMS OTP:

Fricción Adaptativa vs. Fraude Generativo.

Por qué el segundo factor más extendido es estructuralmente inseguro y qué arquitecturas lo sustituyen.

Defender el SMS OTP en la banca moderna ya no es conservadurismo; es negligencia técnica. Asumir que una identidad es legítima solo porque el sistema valida un dispositivo conocido y una contraseña es la vulnerabilidad arquitectónica más explotada hoy.

Frente a la IA generativa, que fabrica identidades sintéticas y clona voces en tiempo real, los sistemas legacy colapsan porque fueron diseñados para autenticar la validez del dato, no la "autenticidad de la intención". La transición hacia una plataforma CIAM de élite exige reestructurar la defensa bajo tres vectores innegociables:

01 Autenticación Basada en Riesgo (RBA) y Fricción Adaptativa

La identidad no debe ser un interrogatorio constante. El sistema debe evaluar pasivamente la telemetría del dispositivo y la dinámica de interacción para generar un Risk Score en milisegundos. El 95% de las transacciones fluyen invisibles. Solo ante anomalías, el motor inyecta fricción adaptativa exigiendo un token criptográfico resistente al phishing (FIDO2/Passkeys).

02 Biometría Conductual como Señal, no como Absoluto

Confiar ciegamente en un solo algoritmo genera sesgos operativos. Una arquitectura de vanguardia asume la falibilidad de la telemetría e integra múltiples capas (inteligencia de red, giroscopios, presión táctil) para aislar comportamientos robóticos sin imponer bloqueos discriminatorios al cliente legítimo que cambia de hábitos.

03 Correlación Transaccional y el Dolor del Legacy

En un fraude de Pagos Push Autorizados (APP), la víctima aprueba el envío bajo manipulación. La seguridad no puede morir en el login. Sabemos que intervenir un core heredado para correlacionar telemetría en tiempo real es una hemorragia financiera, pero

es ineludible. En lugar de intentar leer "dudas", el motor debe auditar latencias atípicas y patrones de indecisión inducida, bloqueando el capital solo cuando el comportamiento anómalo coincide con un destinatario de riesgo.

El Desafío para la Alta Dirección

La seguridad de la próxima década se basa en orquestar el riesgo en silencio, no en apilar factores estáticos.

Directores de TI y Operaciones: ¿Sus infraestructuras están diseñadas para orquestar estratégicamente la fricción, o sus sistemas legacy siguen imponiendo controles ciegos que castigan al cliente legítimo mientras facilitan el fraude a escala?

Siga a [Inteligencia Bancaria](https://InteligenciaBancaria.net) para liderar el estándar técnico y la gobernanza de infraestructura en el sector financiero.

CÓMO CITAR ESTE DOCUMENTO

InteligenciABancaria.net · DOC.03 · Junio 2026