

TENDENCIAS QUE MARCARÁN EL CUMPLIMIENTO EN LA PREVENCIÓN DE DELITOS FINANCIEROS EN 2026

El cambio es inevitable. Ya sea impulsado por nuevas regulaciones, avances tecnológicos o factores políticos y económicos, las instituciones financieras deben adaptarse para seguir siendo competitivas.

El rápido aumento de amenazas emergentes y la creciente complejidad de los riesgos —que incluyen evasión de sanciones, flotas fantasma y cibercrimen sofisticado— obligarán a las organizaciones a replantear sus estrategias de cumplimiento y prevención del delito financiero durante 2026.

Estas son las cinco tendencias clave a seguir de cerca en 2026.

1 Los cambios geopolíticos crean nuevos riesgos y vulnerabilidades financieras

Los acontecimientos geopolíticos están acelerando la imposición de sanciones y controles a la exportación, además de modificar el acceso de ciertos países al sistema financiero internacional. Esto ha llevado a que naciones sancionadas y no sancionadas busquen reducir su dependencia de la infraestructura global de pagos, lo que genera brechas que pueden ser explotadas.

La fragmentación creciente del ecosistema de pagos¹ y el mayor escrutinio sobre los controles de exportación obligan a las instituciones financieras a ir más allá de “seguir el rastro del dinero”. En 2026, la capacidad de adaptación será un diferenciador clave.

Los perfiles de buques sancionados han aumentado de forma exponencial²



Principales factores detrás del crecimiento de los sistemas de pago alternativos



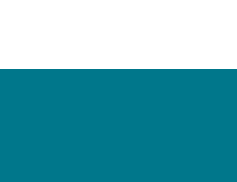
Instituciones financieras de países sancionados fuera de SWIFT



Demanda de pagos más rápidos y económicos



Países que buscan eludir restricciones comerciales y aranceles



Acceso financiero para 1.300 millones de adultos sin cuenta bancaria³

2 Las ciberamenazas siguen redefiniendo el riesgo

Las actividades maliciosas en el ciberespacio continúan erosionando la confianza digital, afectando procesos políticos, interrumpiendo servicios críticos y facilitando delitos como fraude, ransomware y lavado de dinero.

Reguladores como la Oficina de Control de Activos Extranjeros (OFAC), la Unión Europea y el Reino Unido ya están emitiendo sanciones contra actores vinculados a ciberataques y esquemas transnacionales de fraude. Este entorno exige que las instituciones fortalezcan su resiliencia y capacidades de detección.

Impacto económico global del cibercrimen



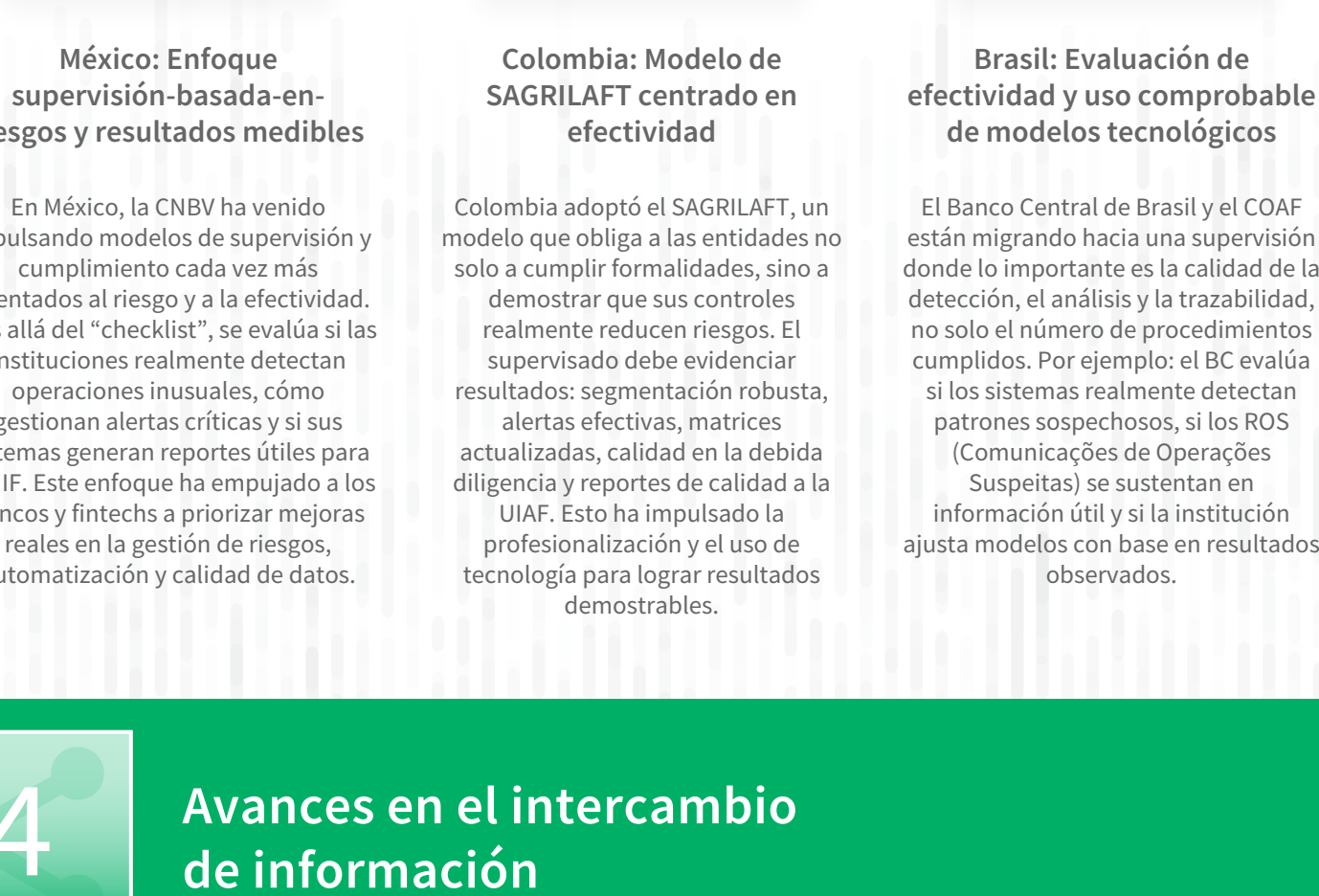
Las consecuencias de las actividades cibernéticas maliciosas



3 La regulación basada en resultados toma protagonismo

Durante años, el cumplimiento técnico fue el principal indicador de eficacia. Sin embargo, pese al incremento de requisitos, el delito financiero persiste. Por ello, los reguladores están migrando hacia un enfoque centrado en resultados reales y medibles.

Este cambio reduce costos y complejidad al enfocarse en efectividad y no en requisitos rígidos, permitiendo reasignar recursos, explorar innovaciones y fortalecer la inclusión financiera sin sacrificar eficiencia.



4 Avances en el intercambio de información

El intercambio de datos ya sea mediante convenios público privados o consorcios es cada vez más crucial para combatir un delito financiero sofisticado y global.

Sin embargo, las diferencias regulatorias en privacidad, competencia y obligaciones legales pueden dificultar la colaboración. Esto abre espacio para que actores criminales utilicen vacíos normativos para ocultar la titularidad real o evadir divulgaciones.

Las regulaciones emergentes buscan impulsar un intercambio de datos relevante y responsable que permita mitigar riesgos, tendencia que se consolidará en 2026.

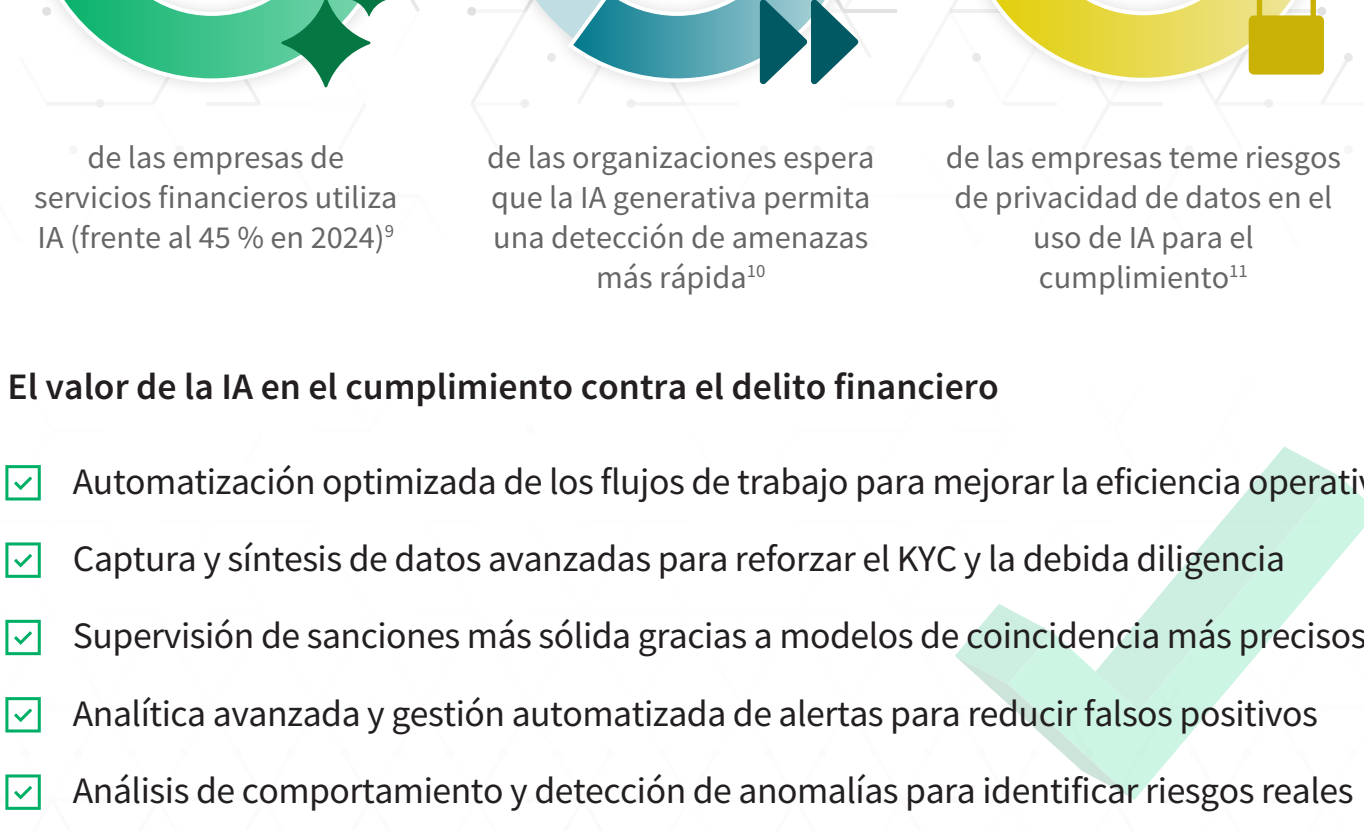
Avances en el intercambio de datos



5 La IA impulsa tanto el delito como el cumplimiento

La inteligencia artificial (IA) es un arma de doble filo. Los actores maliciosos están utilizando la IA generativa para estafas, contenidos falsos, fraude de identidad y lavado de activos. Al mismo tiempo, las instituciones están respondiendo incorporando herramientas basadas en IA en sus procesos de cumplimiento para mejorar la detección.

El reto para el sector en 2026 será encontrar el equilibrio adecuado: aprovechar el potencial de la IA en la lucha contra el delito financiero mediante una sólida calidad de datos y marcos de gobernanza, sin imponer controles excesivos que frenen la innovación, y garantizando al mismo tiempo la transparencia y la explicabilidad.



El valor de la IA en el cumplimiento contra el delito financiero

- ✓ Automatización optimizada de los flujos de trabajo para mejorar la eficiencia operativa
- ✓ Captura y síntesis de datos avanzadas para reforzar el KYC y la debida diligencia
- ✓ Supervisión de sanciones más sólida gracias a modelos de coincidencia más precisos
- ✓ Analítica avanzada y gestión automatizada de alertas para reducir falsos positivos
- ✓ Análisis de comportamiento y detección de anomalías para identificar riesgos reales

Descubra cómo la inteligencia global de riesgos y la tecnología avanzada de LexisNexis® Risk Solutions pueden ayudar a su organización a adaptarse al cambio, reforzar el cumplimiento normativo y fortalecer la lucha contra el delito financiero. Visite risk.lexisnexis.com/cumplimiento para obtener más información.