

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



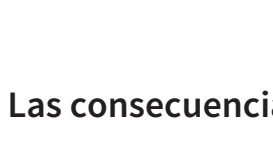
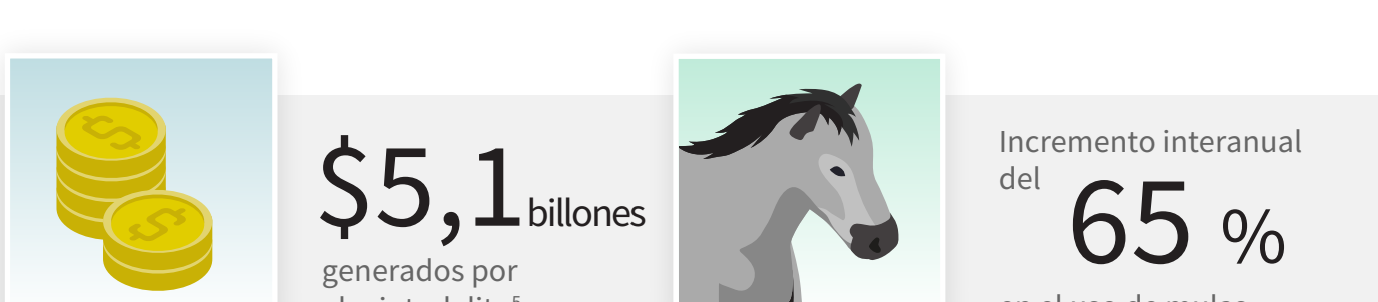
Acceso financiero para 1.300 millones de adultos sin cuenta bancaria³

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



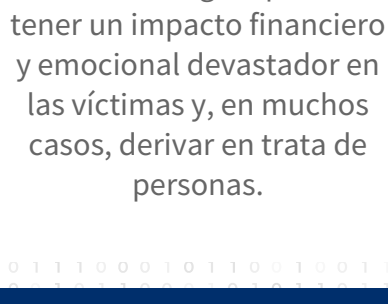
\$5,1 billones generados por el criptodelito⁵



Incremento interanual del 65 % en el uso de mulas financieras en el Reino Unido⁶

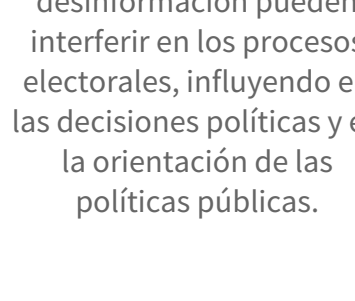
Las consecuencias de las actividades cibernéticas maliciosas

Personas



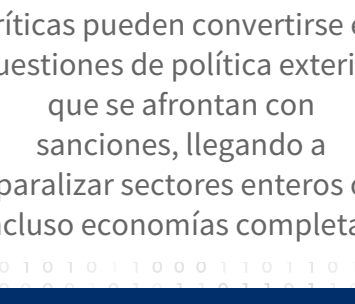
Las estafas que se inician en el entorno digital pueden tener un impacto financiero y emocional devastador en las víctimas y, en muchos casos, derivar en trata de personas.

Sistemas políticos



Los ciberataques y las campañas de desinformación pueden interferir en los procesos electorales, influyendo en las decisiones políticas y en la orientación de las políticas públicas.

Economías



Los ataques de ransomware contra infraestructuras críticas pueden convertirse en cuestiones de política exterior que se afrontan con sanciones, llegando a paralizar sectores enteros o incluso economías completas.

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.

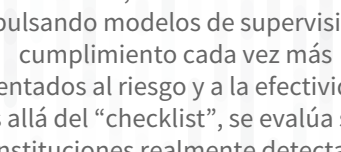
90 %

de las empresas de servicios financieros considera que los requisitos de cumplimiento se han vuelto más complejos⁷

74 %

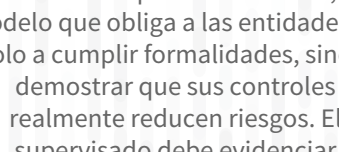
de las organizaciones afirma que la complejidad dificulta el lanzamiento de nuevos productos y servicios⁸

Priorizar los resultados frente a los procesos



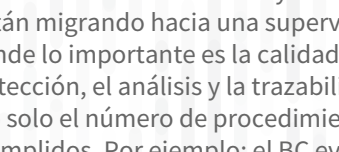
México: Enfoque de supervisión basada en riesgos y resultados medibles

En México, la CNBV ha venido impulsando modelos de supervisión y cumplimiento cada vez más orientados al riesgo y a la efectividad. Más allá del “checklist”, se evalúa si las instituciones realmente detectan operaciones inusuales, cómo gestionan alertas críticas y si sus sistemas generan reportes útiles para la UIF. Este enfoque ha empujado a los bancos y fintechs a priorizar mejoras reales en la gestión de riesgos, automatización y calidad de datos.



Colombia: Modelo de SAGRILAF centrado en efectividad

Colombia adoptó el SAGRILAF, un modelo que obliga a las entidades no solo a cumplir formalidades, sino a demostrar que sus controles realmente reducen riesgos. El supervisor debe evidenciar resultados: segmentación robusta, alertas efectivas, matrices actualizadas, calidad en la debida diligencia y reportes de calidad a la UIF. Esto ha impulsado la profesionalización y el uso de tecnología para lograr resultados demostrables.



Brasil: Evaluación de efectividad y uso comprobable de modelos tecnológicos

El Banco Central de Brasil y el COAF están migrando hacia una supervisión donde lo importante es la calidad de la detección, el análisis y la trazabilidad, no solo el número de procedimientos cumplidos. Por ejemplo: el BC evalúa si los sistemas realmente detectan patrones sospechosos, si los ROS (Comunicações de Operações Suspeitas) se sustentan en información útil y si la institución ajusta modelos con base en resultados observados.

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.

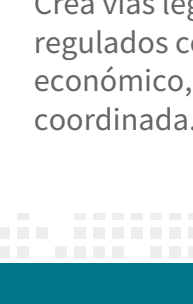
Las regulaciones emergentes buscan impulsar un intercambio de datos relevante y responsable que permita mitigar riesgos, tendencia que se consolidará en 2026.

Avances en el intercambio de datos



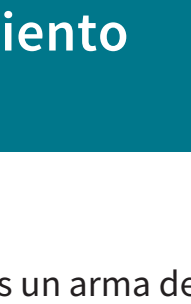
Reglamento AMLR de la UE – Artículo 75

Establece el marco jurídico para asociaciones de intercambio de información, fomentando la colaboración intersectorial y transfronteriza.



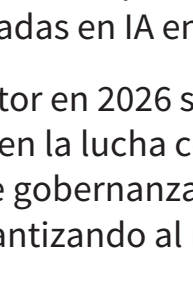
Exención de la Regla CIP de FinCEN

Fomenta el intercambio de información y la colaboración al permitir que los bancos se asocien con proveedores externos para la verificación de clientes.



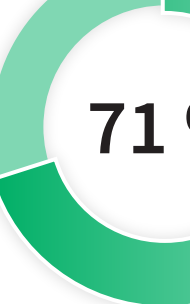
Marco de Banca Impulsada por el Consumidor de Canadá

Permite a empresas y particulares canadienses compartir de forma segura sus datos financieros con proveedores externos autorizados.



Recomendación 16 de GAFI

Exige que los participantes en la cadena de pagos recopilen y compartan información ampliada sobre el ordenante y el beneficiario.



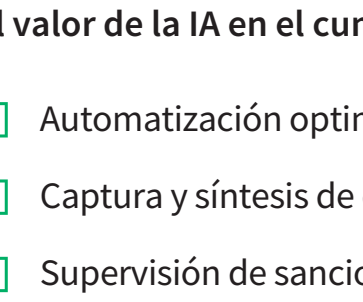
Intercambio de información EDDTA del Reino Unido

Crea vías legales que permiten a los sectores regulados compartir sospechas de delito económico, facilitando una detección coordinada.

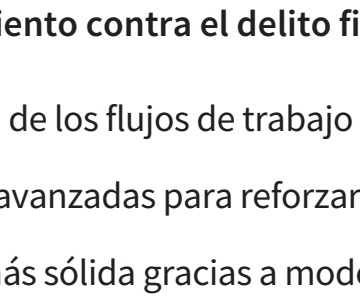
5 La IA impulsa tanto el delito como el cumplimiento

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.

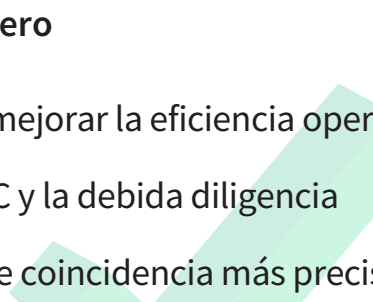
El reto para el sector en 2026 será encontrar el equilibrio adecuado: aprovechar el potencial de la IA en la lucha contra el delito financiero mediante una sólida calidad de datos y marcos de gobernanza, sin imponer controles excesivos que frenen la innovación, y garantizando al mismo tiempo la transparencia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



71 % de las empresas de servicios financieros utiliza IA (frente al 45 % en 2024)⁹



Más de 60 % de las organizaciones espera que la IA generativa permita una detección de amenazas más rápida¹⁰



89 % de las empresas teme riesgos de privacidad de datos en el uso de IA para el cumplimiento¹¹

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.