La era digital en la lucha contra la delincuencia económica para las entidades financieras: del control reactivo a la inteligencia predictiva

Observatorio de prevención de blanqueo de capitales y financiación del terrorismo.

Octubre 2025

La era digital en la lucha contra la delincuencia económica para las entidades financieras

Del control reactivo a la inteligencia predictiva

En la última década, los riesgos vinculados al blanqueo de capitales y la financiación del terrorismo al que están expuestas especialmente las entidades financieras han experimentado una transformación profunda.

La aparición de nuevos canales de pago, el auge de los criptoactivos, la globalización de los servicios financieros y el uso malicioso de tecnologías emergentes —como la inteligencia artificial o los deepfakes— han diversificado las tipologías delictivas y ampliado las superficies de riesgo. Ante este nuevo escenario, los modelos tradicionales y ya conocidos de prevención se ven desbordados, y las entidades financieras tienen que adaptar sus estrategias y mecanismos de control a este entorno más dinámico, descentralizado y difícil de trazar.

El blanqueo de capitales y la financiación del terrorismo se ha visto exponencialmente beneficiado con la llegada de las nuevas tecnologías y la digitalización de los sistemas financieros.

La última opinión publicada por la EBA en relación con los riesgos en materia de PBC/FT en el sector financiero (julio 2025) confirma esta tendencia: un ecosistema financiero moldeado por la innovación tecnológica, las reformas regulatorias y unas tipologías delictivas cada vez más sofisticadas.

“Las criptomonedas, las plataformas financieras descentralizadas (DeFi) y la automatización basada en IA facilitan un mayor anonimato, lo que permite a los delincuentes ocultar transacciones ilícitas con mayor eficacia y ofuscar a los beneficiarios finales de los flujos financieros ilícitos. Además, la proliferación de tokens no fungibles (NFT) y los mercados de la dark web dificultan aún más la detección y regulación de las actividades financieras ilícitas”.

EUROPOL. 2025. “The Changing DNA of serious and organized crime”. European Union. Serious and organized crime threat assessment.
Obtenido de https://www.europol.europa.eu/publication-events/main-reports/changing-dna-of-serious-and-organised-crime

En las últimas décadas, el ecosistema financiero ha vivido una transformación radical impulsada por la digitalización. La expansión de las FinTech ha traído consigo servicios y productos innovadores como la banca móvil, los pagos sin contacto, el uso de IBANs virtuales, el dinero electrónico, los "*bot-advisors*" o los procesos remotos de incorporación y verificación de identidad basados en biometría y tratamiento de datos personales. Estos avances han permitido mejorar la eficiencia operativa, ampliar el acceso a servicios financieros y reducir barreras de entrada.

Pero la tecnología no ha sido el único catalizador del cambio. La pandemia de la COVID-19 aceleró la digitalización de las relaciones económicas, normalizando la contratación remota y el intercambio de valor en entornos virtuales. A ello se suman un contexto geopolítico y económico inestable, el auge de nuevos activos digitales —como las criptomonedas o los NFT—, y el desarrollo de tecnologías emergentes como la inteligencia artificial generativa o los *deepfakes*.

Desde 2020, también se ha impulsado la digitalización del consumo, del trabajo y del propio sistema financiero. A ello se han sumado crisis económicas, conflictos armados y tensiones regulatorias.

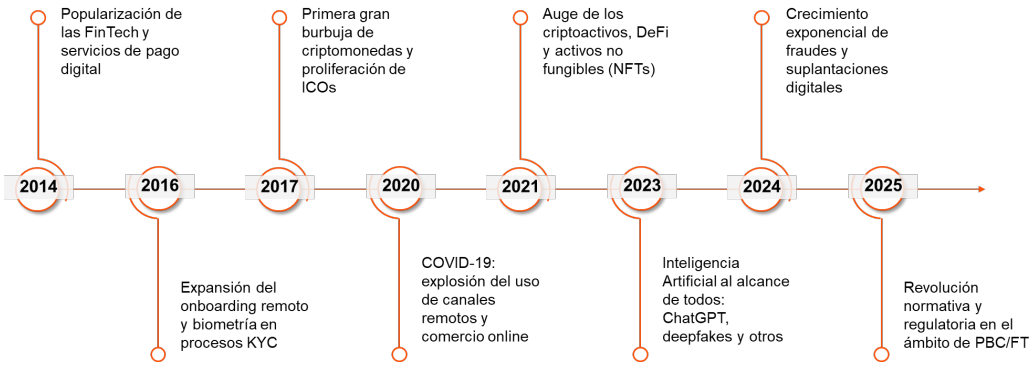


Gráfico 1 – Evolución de los factores de riesgo en materia de PBC/FT

Todos estos factores han cambiado la forma a las que las entidades tienen que afrontar el riesgo de ser abusadas para el blanqueo o la financiación del terrorismo. La delincuencia económica no utiliza sólo grandes transferencias opacas o el efectivo de un modo intensivo: hoy puede apoyarse en microtransacciones, activos digitales, identidades ficticias o estructuras algorítmicas difíciles de auditar.

Por tanto, el proceso tradicional del blanqueo de capitales es ahora mucho más complejo ya que: una parte significativa de los fondos ilícitos se generan directamente en activos digitales, haciendo que los esfuerzos del proceso de blanqueo se centren en la estratificación, el ocultamiento de los flujos de capital y su distanciamiento de la red de delincuentes.

Frente a este escenario, los sujetos obligados ya no pueden limitarse a revisar alertas o aplicar reglas estáticas: necesitan evolucionar. La innovación en el ámbito de la prevención del blanqueo de capitales y la financiación del terrorismo (PBC/FT) no es una cuestión de vanguardia tecnológica, sino de supervivencia operativa.

Anatomía del riesgo digital: así operan las nuevas amenazas

Canales digitales: más ágiles, más vulnerables

La digitalización del sistema financiero ha transformado la forma de operar y de delinquir. Plataformas de pago, fragmentación de las cadenas de prestación de servicios, esquemas de pagos instantáneos, tarjetas digitales y servicios financieros permiten movilizar fondos con rapidez y desde cualquier lugar, pero también facilitan el anonimato, la suplantación de identidad y el uso de terceros, como mulas, para dar apariencia de licitud a fondos generados al margen de la legalidad del sistema financiero.

IBANs virtuales: trazabilidad en entredicho

Los IBANs virtuales permiten a un mismo cliente gestionar múltiples cuentas o subcuentas desde un único punto de acceso. Se trata de una solución útil para mejorar la eficiencia operativa y el control de pagos, pero también pueden fragmentar la trazabilidad y dificultar la identificación del titular real o del beneficiario final, especialmente cuando se combinan con estructuras transfronterizas o entidades no supervisadas por los reguladores financieros, como bien han alertado varios organismos reguladores (EBA en su informe sobre los IBANs virtuales, EBA/Rep/2024/08 , mayo 2024).

Mulas del siglo XXI: la pieza clave del blanqueo digital

Las redes criminales se apoyan cada vez más en mulas —conscientes o no— que reciben y transfieren dinero, ya sea digitalmente (con criptos, tarjetas o plataformas online) o en efectivo. El fraude, la suplantación de identidad y la presión económica aumentan el riesgo de captación, especialmente entre colectivos vulnerables o poco concienciados.

Ciberdelincuencia: robar, suplantar y mover dinero

Phishing, malware o ingeniería social bruta permiten a los delincuentes obtener credenciales, operar en nombre de terceros y esquivar los controles de prevención. El robo de identidad ya no es solo una amenaza para las personas: también lo es para la integridad del sistema financiero.

Deepfakes e IA generativa: nuevas armas, viejos delitos

La inteligencia artificial ha democratizado el delito, en ocasiones, de modo sofisticado. Hoy es posible crear vídeos, audios o documentos falsos con apariencia real, capaces de engañar incluso a sistemas biométricos. Además, permite diseñar campañas de ingeniería social altamente sofisticadas para captar mulas o extraer información confidencial sin levantar sospechas.

Finanzas descentralizadas (DeFi): sin entidades financieras, sin controles

70%

Autoridades competentes advierten de riesgos elevados en el sector FinTech.

Las plataformas DeFi ofrecen préstamos, inversiones o intercambios sin necesidad de intermediarios ni procedimientos KYC tradicionales. Aunque las transacciones son transparentes en la blockchain, su descentralización y accesibilidad global pueden facilitar la elusión de controles y diversificar los riesgos. Además, se observa una creciente interoperabilidad entre entidades financieras y no financieras —por ejemplo, en la intersección con el juego online—, donde determinados sujetos obligados no financieros, más vulnerables por su menor madurez en materia de control, llegan a desempeñar funciones similares a las de entidades financieras. Según la última opinión de la EBA sobre riesgos en materia de PBC/FT (EBA/Op/2025/10, 28 de julio 2025), el 70 % de las autoridades competentes advierte riesgos elevados en el sector FinTech por priorizar el crecimiento frente al cumplimiento de PBC/FT. Esta advertencia es especialmente relevante en el contexto de las DeFi, donde la falta de controles tradicionales amplifica la exposición.

Criptomonedas: anonimato y opacidad

Aunque las operaciones con criptomonedas quedan registradas, la compraventa cruzada, el uso de monedas centradas en la privacidad, como Monero o los servicios de intercambio descentralizados dificultan la trazabilidad del capital. Los puentes entre cadenas aumentan aún más la complejidad y reducen la eficacia del control regulatorio.

NFTs, stablecoins y activos digitales

Los criptoactivos permiten representar y mover valor de forma no convencional: desde obras digitales hasta activos físicos o derechos económicos. Su volatilidad, su creciente uso en operaciones y los vacíos legales en vías de control los convierten en vehículos idóneos para disimular el origen del capital.

Darknet: el mercado oculto

La *darknet* actúa como un entorno paralelo donde es posible contratar servicios de blanqueo, comprar credenciales falsas o intercambiar activos sin dejar rastro. Su combinación con criptomonedas refuerza el anonimato, dificulta la trazabilidad y permite esquivar los controles financieros tradicionales.

Fraude: la sofisticación e innovación puesta en práctica

La sofisticación de las estrategias de fraude ha evolucionado significativamente en los últimos tiempos beneficiándose de los avances tecnológicos. El uso de los canales digitales, IA, *deepfakes*, ciberdelincuencia, criptomonedas y/o mulas ha fomentado la creatividad de las redes de criminales tanto en las estrategias y operaciones de blanqueo de dinero como en la captación de víctimas y cómplices (conscientes o no).

Los grandes retos del cumplimiento en la era digital

La transformación del ecosistema financiero ha situado a las entidades ante un nuevo desequilibrio. A medida que los riesgos se diversifican y los canales se digitalizan, las funciones de cumplimiento en materia de PBC/FT afrontan una creciente presión operativa, tecnológica y regulatoria. Estos son algunos de los principales desafíos que las entidades financieras deben considerar:

Saturación operativa y falsas alertas

El aumento del volumen transaccional digital ha disparado el número de alertas generadas por los sistemas tradicionales. Sin una capacidad de filtrado inteligente, los equipos de análisis se ven obligados a invertir recursos en revisar señales irrelevantes, lo que diluye la eficacia del sistema y retrasa las respuestas frente a amenazas reales.

Tecnología sin gobernanza efectiva

Muchas entidades han iniciado procesos de digitalización o automatización sin un modelo claro de gobierno del dato, trazabilidad de decisiones o explicabilidad de los algoritmos. El uso de soluciones opacas puede aumentar el riesgo de incumplimiento, o ineficiencias en la detección.

Integración de criptoactivos y nuevos productos

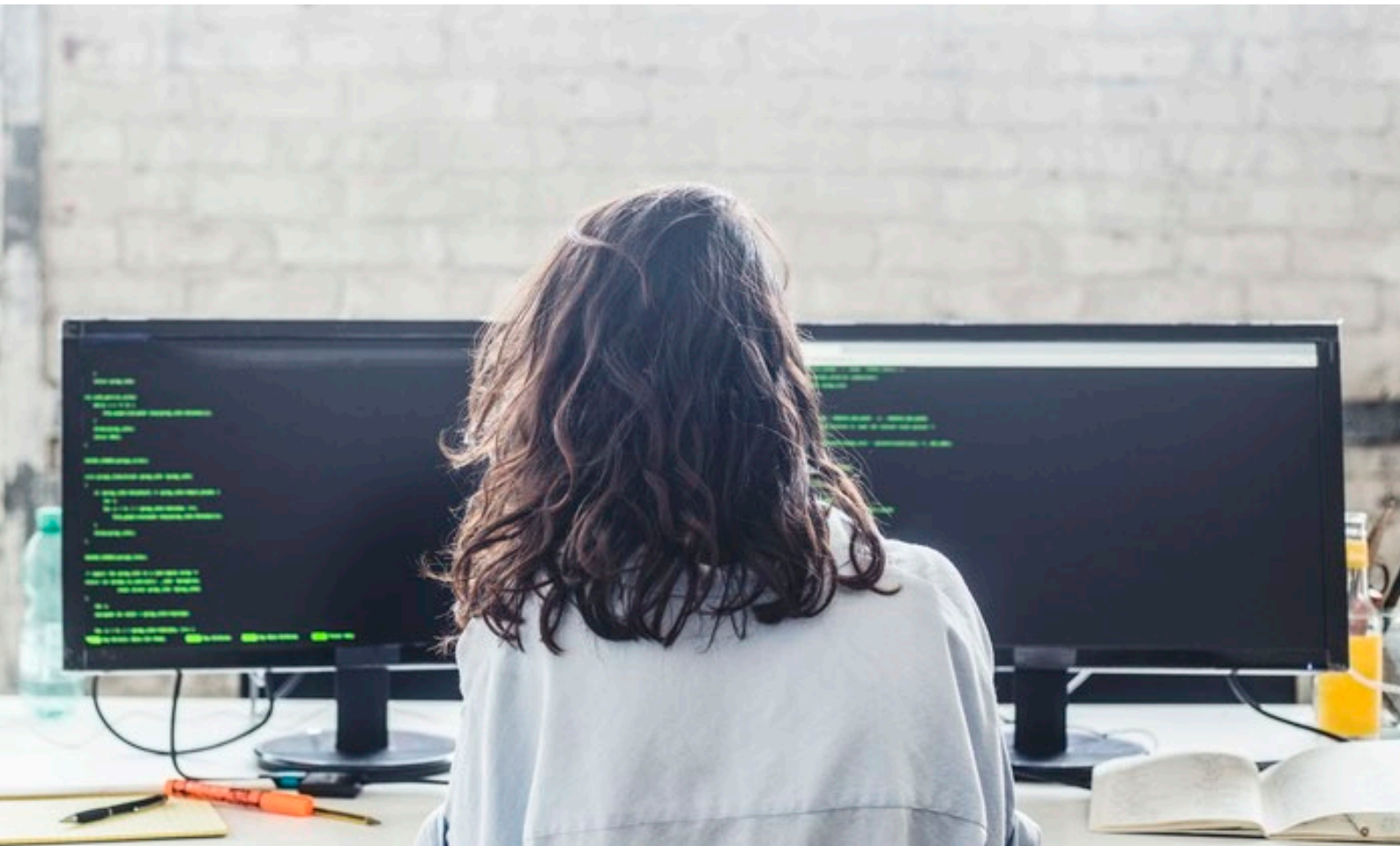
El uso creciente de criptomonedas, IBANes virtuales, *stablecoins* o plataformas DeFi genera fricciones entre la oferta comercial y los mecanismos de control interno. Muchas entidades aún carecen de criterios estandarizados para evaluar el riesgo de estos productos o sus clientes asociados, incluso antes de lanzar el producto o servicio.

KYC desalineado con la operativa real de sus clientes

Los modelos de conocimiento del cliente siguen siendo en muchos casos estáticos y desactualizados e incoherentes con respecto la operativa real canalizada por sus clientes. Esto genera una percepción de cumplimiento formal, pero impide detectar comportamientos anómalos o cambios en el perfil socioeconómico de los clientes.

Regulación en la UE en movimiento, expectativas de cumplimiento en alza

La inminente entrada en vigor del Reglamento Europeo de Prevención del Blanqueo, y su paquete de normas de segundo nivel, acompañado con el despliegue de AMLA, y así lo ha recalcado en su reciente programa de trabajo- supondrán un cambio de paradigma. Las entidades deberán demostrar no solo cumplimiento técnico, sino la eficiencia y eficacia real de sus sistemas. La transparencia, la trazabilidad y la capacidad de adaptación pasarán a ser criterios centrales.



Innovación contra innovación: tecnología al servicio de la PBC/FT

La sofisticación de las redes criminales y el uso creciente de tecnologías para eludir los controles han hecho que la innovación deje de ser una ventaja competitiva para convertirse en una necesidad funcional. Hoy, la PBC/FT requiere integrar soluciones tecnológicas avanzadas capaces de detectar, adaptarse y anticiparse a nuevos patrones de riesgo.

Concienciación, automatización e inteligencia artificial: el nuevo triángulo de defensa

Las entidades deben impulsar tres líneas de acción prioritarias:

- **Mayor concienciación** sobre el impacto real del blanqueo de capitales y la financiación del terrorismo.
- **Automatización de procesos repetitivos**, para liberar capacidad analítica y reducir tiempos de respuesta.
- **Desarrollo e implementación de sistemas de inteligencia artificial (IA)** que complementen y superen los límites de los modelos tradicionales

El triángulo de defensa se beneficia y enriquece del posible intercambio de información sobre clientes, operativa sospechosa, y factores y análisis de riesgo entre entidades y asociaciones de intercambio de información. Las entidades han de fomentar que la recopilación, uso e intercambio de datos tengan como objetivo el cumplimiento regulatorio. Este flujo de datos debe estar orientado al cumplimiento regulatorio, pero también alineado con los principios de protección de datos y proporcionalidad en su uso.

De las reglas a la inteligencia

Durante años, los sistemas basados en reglas lógicas han sido el núcleo de los modelos de monitorización em materia PBC/FT: reglas predefinidas, umbrales fijos y perfiles de riesgo parametrizados. Aunque siguen siendo útiles ya no son suficientes porque su capacidad de adaptación es limitada y generan altos niveles de falsos positivos por falta de definición y contextualización.

Frente a ello, los modelos de Inteligencia Artificial (IA) permiten un enfoque más flexible y dinámico:

Característica	**Reglas tradicionales**	**Inteligencia Artificial**
Tecnología	Lógica condicional y umbrales fijos	Modelos de aprendizaje automatizado
Datos	Históricos y limitados	Masivos, actualizados en tiempo real
Adaptabilidad	Estática, reconfiguración manual	Dinámica, aprendizaje continuo
Precisión	Alta tasa de falsos positivos	Reducción significativa de los falsos positivos por contextualización
Tipo de respuesta	Reactiva y manual	Proactiva, automatizada y explicativa

La combinación de ambos enfoques permite construir sistemas más sólidos, eficaces y resilientes. La IA no sustituye las reglas: las complementa, las refuerza y amplía su alcance.

¿Estamos preparados para un riesgo que ya no se comporta como antes?

Las redes criminales ya han dado el salto a la automatización, a la inteligencia artificial y a las finanzas descentralizadas. La pregunta no es si debemos innovar, sino cuánto están dispuestas las entidades a arriesgar por no hacerlo.

En PwC ayudamos a las organizaciones a transformar su enfoque en materia de PBC/FT con soluciones que combinan tecnología, profundo conocimiento experto y visión estratégica. En un entorno donde el riesgo evoluciona a diario, solo las entidades que se anticipan pueden seguir cumpliendo y liderando

Contacta con

África Pinillos Lorenzana
Directora de Auditoría en PwC España
africa.pinillos.lorenzana@pwc.com

Francisco Javier Caro del Moral
Socio de Auditoría en PwC España
francisco.javier.caro@pwc.com

pwc.es