ManagementSolutions
Making things happen

Delitos financieros: tendencias y retos en la era digital

I+D

www.managementsolutions.com

Diseño y Maquetación
Dpto. Marketing y Comunicación
Management Solutions - España

Fotografías
Archivo fotográfico de Management Solutions
iStock

© Management Solutions 2023
Todos los derechos reservados. Queda prohibida la reproducción, distribución, comunicación pública, transformación, total o parcial, gratuita u onerosa, por cualquier medio o procedimiento, sin la autorización previa y por escrito de Management Solutions.
La información contenida en esta publicación es únicamente a título informativo. Management Solutions no se hace responsable del uso que de esta información puedan hacer terceras personas. Nadie puede hacer uso de este material salvo autorización expresa por parte de Management Solutions.

Índice

Introducción

"Los delitos llevan a las espaldas el castigo"
Miguel de Cervantes[1]

El delito financiero es un concepto general que comprende un conjunto de actividades ilícitas. Aunque existen diferencias entre las jurisdicciones, en términos generales el delito financiero incluye actividades como el blanqueo de capitales (es decir, transformar en legal el dinero procedente de diferentes actividades ilegales), la financiación del terrorismo, el incumplimiento de sanciones económicas, el soborno y la corrupción, el fraude, y el abuso del mercado[2] .

El delito financiero y el blanqueo de capitales (ML/FT, *Money Laundering and Financing of Terrorism*) es una de las principales amenazas a las que se enfrenta el sector financiero en sus marcos de identificación, gestión y control de riesgos. Por ejemplo, en relación con el blanqueo de capitales, se calcula que la cantidad de dinero que se blanquea en el mundo en un año alcanza entre el 2% y el 5% del PIB mundial, es decir, entre 800.000 millones y 2 billones de dólares estadounidenses actuales[3]. Sin embargo, menos del 1% de este dinero es incautado o retenido por los organismos de seguridad[4].

En los últimos años, las entidades financieras de muchas zonas geográficas han invertido miles de millones de dólares en la mejora de sus sistemas, personal y procesos para poder hacer frente a la creciente amenaza que supone el delito financiero para su estabilidad y reputación. Según algunos informes del sector, la inversión anual de las entidades financieras de todo el mundo en el cumplimiento de la normativa sobre delito financiero se estima en más de 200.000 millones de dólares[5].

Son varios los factores que hacen que la lucha contra el delito financiero sea cada vez más compleja:

- Una economía cada vez más globalizada y el correspondiente sector financiero interconectado, lo que dificulta la trazabilidad completa del dinero.

- El enfoque local de la supervisión. Históricamente, el enfoque del delito financiero, y en particular las actividades de lucha contra el blanqueo de capitales, ha sido impulsado por los legisladores y supervisores locales, las autoridades policiales de cada país y los organismos de inteligencia financiera. A pesar de la existencia de organismos intergubernamentales, como el Grupo de Acción Financiera Internacional[6], no ha habido plataformas operativas, ni mecanismos de regulación y supervisión para la colaboración efectiva y el intercambio de información.

- La progresiva sofisticación de las estrategias de blanqueo de capitales, que implican otros tipos de delitos como el fraude o la ciberdelincuencia (por ejemplo, la usurpación de identidad)[7].

- La evolución del sector de los pagos hacia mecanismos de pago digitales más fáciles, rápidos y flexibles.

- La irrupción de las criptomonedas y su capacidad para evitar la trazabilidad de las fuentes de fondos[8].

- Los avances tecnológicos desplegados a raíz de la pandemia, que han obligado a las entidades financieras a reducir las interacciones cara a cara y a sustituirlas por procesos digitales (incluido el *onboarding* remoto de nuevos clientes), más susceptibles de ser objeto del delito digital que, a la larga, pueden dar lugar a delito financiero.

No obstante, las entidades financieras cuentan con condiciones favorables y pueden llegar a utilizar herramientas más potentes para poder luchar eficazmente contra el delito financiero, identificando, vigilando, midiendo y controlando este tipo de actividades ilícitas, entre otras:

[1] Miguel de Cervantes Saavedra (1547-1616). Escritor español. Autor de la obra "El ingenioso hidalgo Don Quijote de la Mancha".
[2] Autoridad de Conducta Financiera (2021).
[3] Oficina de las Naciones Unidas contra la Droga y el Delito (2011).
[4] Foro Económico Mundial.
[5] Lexis Nexis Risk Solutions (2021).
[6] Un grupo de acción intergubernamental que reune a más de 200 países y que actúa como organismo normativo mundial en materia de blanqueo de capitales y financiación del terrorismo.
[7] Un ejemplo paradigmático de los ciberdelincuentes Carbanak y Cobalt puede discutirse: las bandas de delincuentes son capaces de (i) insertar un malware en las cuentas de trabajo de los empleados de los bancos (a través de técnicas estándar de phishing - ciberataque); (ii) utilizar las credenciales para aumentar los saldos de ciertas cuentas (fraude); (iii) permitir que el dinero sea transferido a través de las fronteras y/o extraído a través de los cajeros automáticos; y (iv) reinsertarlo en el sistema utilizando técnicas clásicas de blanqueo ecológico o greenwashing. Véase el comunicado de prensa de Europol https://www.europol.europa.eu/media-press/newsroom/news/mastermind-behind-eur-1-billion-cyber-bank-robbery-arrested-in-spain
[8] Paesano, F. (2021).

- Mayor capacidad computacional para ejecutar alertas y estrategias de identificación de riesgos en tiempo real, con un conjunto mucho más completo de *data points* para identificar estrategias sofisticadas.

- Modelización matemática más avanzada, incluyendo algoritmos de *machine learning* que pueden ejecutarse más rápidamente y son capaces de refinar las estrategias y mejorar la eficacia en la detección.

- Una mayor concienciación por parte de los directivos y del Consejo de Administración sobre las implicaciones de este tipo de delitos, lo que requiere un compromiso y una inversión plurianuales. Al mismo tiempo, una mayor visibilidad del coste total del delito financiero (incluyendo tanto las pérdidas directas como las derivadas de la reparación y las multas[9]), así como la conciencia de los riesgos que acarrean estas prácticas, cada vez más "conectadas".

- Aumento de la colaboración dentro de la entidad, con la eliminación de silos y la colaboración entre departamentos (tecnología, cumplimiento, legal, fraude, prevención del blanqueo de capitales, etc.) para garantizar que haya un pleno intercambio de información y transparencia entre los equipos encargados del delito financiero.

- A partir de los primeros trabajos del Grupo de Acción Financiera Internacional, y con la labor de otras organizaciones internacionales como la Oficina de las Naciones Unidas contra la Droga y el Delito, hay mucha más conciencia sobre la importancia de la cooperación internacional.

Prevención del blanqueo de capitales y la financiación del terrorismo (AML/CFT)

Tras una serie de casos muy notorios que afectaron a grandes bancos de importancia sistémica mundial, y el correspondiente y más intenso escrutinio normativo[10,11], una de las actividades de prevención del delito financiero que ha atraído inversiones especialmente importantes en los últimos años es la lucha contra el blanqueo de capitales y la financiación del terrorismo (AML/CFT). Sin embargo, a pesar de los importantes progresos realizados en el refuerzo de esas capacidades, la prevención de estas actividades ilícitas sigue siendo hoy en día uno de los principales ámbitos de preocupación para las entidades financieras.

Dada la naturaleza transfronteriza del blanqueo de capitales y la financiación del terrorismo, una de las acciones más decisivas es una mayor cooperación internacional entre países y regiones para llevar a cabo una acción sincronizada.

En este sentido, los reguladores y supervisores están desempeñando un papel fundamental a la hora de fomentar y posibilitar esta colaboración global y apoyar en general la prevención de estos delitos. Algunos de los ejemplos de acciones reguladoras son:

a. Reforzar los mecanismos de supervisión para que abarquen todas las jurisdicciones. Por ejemplo, la 5ª Directiva contra el blanqueo de capitales de la UE[12] exige que la CE realice una evaluación bianual de los riesgos de ML/FT que puedan

[9]Lexis Nexis Risk Solutions (2021).
[10]Sanction Scanner (2021).
[11]European Commission (2019). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52019DC0373
[12]Parlamento Europeo y Consejo (2015).

afectar al mercado interior de la región[13]. Los resultados de estas evaluaciones sirven para informar a los responsables políticos regionales y locales.

b. Fomentar una mayor cooperación entre los legisladores y supervisores locales, las autoridades policiales de cada país y los organismos de inteligencia financiera[14]. La Directiva de la UE sobre la lucha contra el blanqueo de capitales[15] exige una evaluación, por parte de la CE, del marco de cooperación entre las Unidades de Inteligencia Financiera de la Unión Europea con terceros. La Directiva incluye la posibilidad de establecer un mecanismo de coordinación y apoyo. En esa línea, recientemente la UE anunció la creación de una nueva autoridad a nivel de toda la Unión[16] para mejorar la supervisión y la cooperación en materia de lucha contra el blanqueo de capitales y la financiación del terrorismo entre las Unidades de Inteligencia Financiera locales. La nueva autoridad europea contra el blanqueo de capitales (AMLA[17]) actuará como autoridad central y coordinará a las autoridades nacionales para garantizar, entre otras cosas, que el sector privado de cada país aplique adecuadamente las normas de la UE. Como continuación de ese esfuerzo, la EBA ha publicado recientemente sus "Directrices sobre la cooperación y el intercambio de información entre los supervisores prudenciales, los supervisores de la lucha contra el blanqueo de capitales y la financiación del terrorismo y las unidades de inteligencia financiera con arreglo a la Directiva 2013/36/UE"[18].

c. Proseguir con la colaboración entre la supervisión prudencial y la no prudencial[19].

d. Para los riesgos emergentes o las áreas de debilidad identificadas como parte de su proceso de supervisión, los reguladores de todo el mundo están siendo muy activos en cuanto a la emisión de una nueva regulación. Una de las áreas que ha evolucionado más rápidamente es la de las criptomonedas[20].

e. Fomentar la inversión en datos, modelización avanzada e IA, incluyendo el análisis avanzado de valores atípicos y el análisis de gráficos para la modelización de redes y las relaciones de orden múltiple[21].

En este contexto, el objetivo de este *white paper* es doble:

- Definir el ámbito del delito financiero y analizar el contexto normativo.
- Desarrollar un enfoque específico sobre las tendencias y retos en materia de AML/CFT, incluyendo la respuesta de las entidades financieras para mejorar los marcos de gestión y control de riesgos, y establecer algunas relaciones entre AML/CFT y otros riesgos que conforman el concepto de delito financiero.

El documento está estructurado de la siguiente manera: tras un resumen ejecutivo, la sección 2 contiene una visión general del concepto y del panorama normativo sobre el delito financiero. La sección 3 abarca las principales tendencias y retos en materia de AML/CFT, incluidos el marco y la gobernanza, el diseño organizativo, las necesidades de datos, los procesos empresariales y la infraestructura tecnológica. Y, por último, la sección 4 se centra específicamente en las capacidades y tendencias de la modelización matemática avanzada utilizada con el fin de mejorar la eficiencia y la eficacia en la detección.

[13] Véase, e.g. , el Informe de Evaluación de Riesgos Supranacionales de la Comisión de la UE y el Informe de la Comisión al Parlamento Europeo y al Consejo sobre la evaluación del riesgo de blanqueo de capitales y de financiación del terrorismo que afecta al mercado interior y se refiere a las actividades transfronterizas. COM (2019) 370. Véase también la evaluación nacional del riesgo de blanqueo de capitales y financiación del terrorismo del Reino Unido en 2020. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/945411/NRA_2020_v1.2_FOR_PUBLICATION.pdf
[14] Autoridad Bancaria Europea (2021).
[15] Parlamento Europeo y Consejo (2015).
[16] Parlamento Europeo (2021).
[17] No debe confundirse con la Ley contra el Blanqueo de Capitales de Estados Unidos (2020).
[18] Autoridad Bancaria Europea (2021).
[19] Mersch, Y. (2019). La lucha contra el blanqueo de capitales y la financiación del terrorismo: iniciativas recientes y el papel del ECB.
[20] Autoridad Bancaria Europea (2021).
[21] Autoridad de Conducta Financiera (2022). Sandbox regulatorio.

Resumen ejecutivo

"El capital no es un mal en sí mismo, el mal radica en su mal uso"
Mahatma Gandhi[22]

1. ***Definición.*** El delito financiero es un término amplio que hace referencia a un conjunto de riesgos no prudenciales a los que se enfrentan las organizaciones del sector financiero como parte de sus actividades de generación de negocio. Entre otros, el delito financiero incluye el blanqueo de dinero procedente de diferentes actividades ilegales (incluyendo el tráfico de drogas, de armas o de personas, la esclavitud, etc.), la financiación del terrorismo, el incumplimiento de sanciones económicas, el soborno y la corrupción, el fraude, y el abuso de mercado. Recientemente también se ha incluido en esta categoría el ciber riesgo y la delincuencia digital.

2. ***Enfoque.*** Aunque todos esos subtipos de riesgo han recibido mucha atención e inversión en los últimos años, este análisis se centra en tres subtipos de riesgo que suelen ser tratados bajo marcos similares por las organizaciones: el blanqueo de capitales, la financiación del terrorismo y las sanciones económicas. Siguiendo la convención estándar del sector y de la normativa, este documento se refiere a ellos de forma genérica como AML/CFT (*Anti-Money Laundering and Combating the Financing of Terrorism*). La justificación de centrarse en estos subtipos de riesgo, además de permitir una mayor profundidad de análisis, responde también al creciente escrutinio normativo y de supervisión, y a la naturaleza evolutiva de los riesgos (por ejemplo, dos directivas en materia de lucha contra el blanqueo de capitales en la UE en menos de cinco años), así como a la correspondiente inversión creciente y a la importancia que las entidades financieras están dando a sus marcos de AML/CFT (relacionado con el gran daño reputacional y las multas económicas que suponen las deficiencias en su modelo de control).

3. ***Desafíos.*** Las entidades financieras se enfrentan a un entorno difícil en lo que se refiere a AML/CFT. La economía global hace que el seguimiento de los movimientos de dinero sea cada vez más difícil. Esto se ve agravado por la irrupción de las criptomonedas y la proliferación de multitud de tecnologías de pago. Además, los enfoques locales de la regulación y la legislación, con una capacidad limitada para compartir información e inteligencia a través de las fronteras, han permitido a las organizaciones criminales internacionales encontrar puntos débiles en el sistema. Estas organizaciones criminales evolucionan continuamente sus estrategias y construyen esquemas donde se combinan los ciberataques con las estrategias de fraude y blanqueo de dinero, que las entidades financieras que todavía operan en silos encuentran difícil de abordar. Además, la pandemia del COVID-19 y la necesidad de utilizar canales *on-line* y reducir el contacto personal ha hecho que los procesos de *Know Your Customer* sean más exigentes. Las entidades financieras tienen que hacer frente a estos retos tras un entorno sostenido de bajos tipos de interés y fuerte presión de costes.

4. ***Condiciones favorables.*** A pesar de lo anterior, hay condiciones favorables que las entidades financieras están utilizando para hacer frente a estos desafíos, incluyendo el uso de la tecnología y los datos. La automatización avanzada, el BPM (Business Process Management) y la robótica son algunos de los más destacados y ayudan a agilizar los procesos de negocio. Por otro lado, también es relevante el uso de mecanismos de aprendizaje automático e IA, que ayudan a perfilar a los clientes y su transaccionalidad de una manera más eficaz, con un menor número de alertas improductivas o falsos positivos. Pero las compañías también están evolucionando significativamente su marco de gobernanza, con una mayor formación y concienciación (desde el Consejo de Administración y el Comité Ejecutivo hasta los equipos operativos) y una mayor colaboración entre los diferentes subtipos de riesgos (especialmente el fraude).

5. ***Entorno normativo.*** Los reguladores también están evolucionando significativamente sus marcos y recursos, mediante la creación de organismos de colaboración o supervisión supranacionales, la creación de bases de datos comunes, la realización de evaluaciones de riesgo en toda la jurisdicción y el fortalecimiento del diálogo y la colaboración entre la supervisión prudencial y la no prudencial. Los reguladores también están siendo muy activos en cuanto a la publicación de nuevas políticas y orientaciones sobre los riesgos emergentes que se identifican como puntos débiles

[22] Mohandas Karamchand Gandhi (1869-1948) fue el dirigente más destacado del Movimiento de independencia de la India contra el Raj británico, para lo que practicó la desobediencia civil no violenta, además de pacifista, político, pensador y abogado hinduista indio.

en su capacidad de supervisión, así como alentando a las entidades a utilizar la innovación para hacer frente a los riesgos de ML/FT.

6. ***Reacción de las entidades financieras.*** Las entidades financieras están reforzando sus marcos de AML/CFT, mediante un rediseño total o intervenciones específicas en su marco y gobernanza (incluyendo mejoras en su evaluación de riesgos, políticas y normas, su reparto de responsabilidades entre 1ª, 2ª y 3ª líneas de defensa, así como su colaboración entre subtipos de riesgo). También están evolucionando su organización, dando más importancia jerárquica al responsable de delito financiero, realizando un análisis estratégico de las necesidades futuras, creando funciones especializadas o centralizando capacidades. Otras áreas de gran interés son sus programas de cultura y comportamiento, la infraestructura de datos y la información de gestión, así como la racionalización y la automatización de los procesos empresariales básicos de AML/CFT (KYC, supervisión continua, gestión de alertas e investigaciones hasta el compromiso con los cuerpos de seguridad y los informes de actividades sospechosas). Por último, la infraestructura tecnológica que sustenta el marco está mejorando considerablemente, al igual que las capacidades matemáticas y la taxonomía de los modelos.

7. ***Evaluación de riesgos.*** Una sólida evaluación del riesgo es el núcleo del marco de AML/CFT de una organización. Las buenas prácticas en el sector implican la realización de una evaluación de riesgos a diferentes niveles, comenzando con una evaluación de riesgos supranacional y nacional realizada por entidades internacionales y autoridades reguladoras, que establecen el escenario de los riesgos específicos regionales/jurisdiccionales asociados a AML/CFT. Estas aportaciones informan de una evaluación de riesgos específica de las entidades financieras. Esto incluirá la identificación y evaluación de los riesgos asociados al perfil de su base de clientes, productos y canales, su escala, geografía, etc. Por último, la evaluación del riesgo individual para cada relación con el cliente utiliza esos datos como base y los complementa con el conocimiento específico del cliente, la estructura de la organización, los propietarios efectivos, las fuentes de fondos y la riqueza.

8. ***Apetito al riesgo.*** Esta evaluación exhaustiva del riesgo informa sobre el apetito al riesgo y los umbrales que se utilizarán cuando se lancen nuevos productos o servicios, nuevas iniciativas empresariales (fusiones, adquisiciones, nuevas líneas de negocio, etc.). Además, también determina una puntuación de *"new to bank"* que establece una expectativa preliminar en relación con el comportamiento del cliente (tipo de transacciones, canales a utilizar, etc.), y el riesgo de ML/FT asociado a la relación. Esto se asocia a un conjunto de normas en torno a la frecuencia de revisión periódica de la relación, y a unos umbrales de seguimiento de los pagos y la transaccionalidad que activan las alertas cuando se producen desviaciones del comportamiento esperado. Además, las organizaciones más avanzadas disponen de un bucle de retroalimentación regular entre los incidentes identificados en su supervisión del comportamiento y la evaluación del riesgo del cliente, de modo que el perfil de riesgo y las acciones de mitigación asociadas pueden actualizarse inmediatamente.

9. ***Alcance de la cobertura de riesgos.*** La evaluación de riesgos debe abarcar no solo a los clientes, sino también a los terceros proveedores. Las entidades financieras dependen de una serie de terceros para ejecutar sus actividades diarias. Dependiendo de la naturaleza del negocio, estos terceros también pueden exponer a la organización al delito financiero, incluido ML/FT o la corrupción.

10. ***Políticas y normas.*** En un entorno tan regulado, es esencial que las entidades financieras redacten y formalicen políticas, normas y mejores prácticas que permitan a la organización actuar bajo formas de trabajo y procesos empresariales comunes. Este conjunto de conocimientos es también una acción mitigadora instrumental, ya que permite la formación, la concienciación y la comunicación en toda la organización. Algunas de las organizaciones más avanzadas cuentan con una arquitectura de políticas, con jerarquías formalizadas de documentos interconectados y con referencias cruzadas

(trazabilidad vertical), publicados en un formato digital que permite una fácil navegación, y con principales ideas, resúmenes, etc. También cuentan con un modelo operativo que garantiza la supervisión continua de la nueva normativa y los riesgos emergentes, las lecciones aprendidas de los incidentes en materia de AML/CFT (internos o de sus homólogos), etc., y la actualización oportuna del conjunto de documentos.

11. ***Marco de gobernanza.*** Uno de los aspectos que requieren más inversión y un fuerte liderazgo es el marco de gobernanza y el modelo de tres líneas de defensa (LOD) para la identificación, gestión, control y supervisión del riesgo de ML/FT. Es una de las áreas a las que los reguladores y supervisores han dedicado más tiempo y escrutinio. La tendencia en el sector incluye una clara definición y formalización del papel de cada una de las líneas de defensa, firmada por el Comité Ejecutivo / Consejo de Administración como parte del marco de prevención del riesgo de ML/FT.

12. ***Líneas de defensa.*** En uno de los arquetipos más extendidos, la primera LOD que origina el negocio y es dueña de la relación con el cliente, es también responsable de la identificación, gestión y control del riesgo. Esto incluye el despliegue de un marco de control del riesgo para garantizar que el perfil de riesgo se mantiene dentro del apetito al riesgo, y que las operaciones diarias cumplen tanto las políticas internas como la normativa externa. Las organizaciones también han reforzado su segunda línea de defensa, con el nombramiento formal de un responsable de cumplimiento AML/CFT o equivalente. En algunas jurisdicciones, esta función obligatoria debe ser aprobada formalmente por el regulador y se espera que tenga la suficiente antigüedad como para realizar un cuestionamiento independiente y efectivo del negocio. Alrededor de esta función, hay fuertes equipos de cumplimiento y supervisión que asesoran al negocio en temas básicos de AML/CFT, emiten orientación, políticas y normas para la adecuada identificación, seguimiento y control de los riesgos, y supervisan la adopción y la incorporación de estos en la actividad recurrente. La segunda línea de defensa en las organizaciones más maduras cuenta con un plan formal de supervisión de AML/CFT que implica el seguimiento de los Indicadores clave de riesgo (KRI, *Key Risk Indicator*) y de control (KCI, *Key Control Indicator*), la realización de pruebas de control independientes, las revisiones temáticas y las investigaciones prácticas más intrusivas de las áreas que están en el radar regulatorio o sobre las que existen preocupaciones. Una herramienta fundamental de esta segunda línea de defensa es la información sobre la gestión, tanto en términos de la propia información producida por el negocio y utilizada como base en el plan de supervisión como de su información independiente y propia, que tiende a ser la utilizada para reportar al Comité Ejecutivo y al Consejo / Comités delegados del Consejo. La tercera LOD, que suele recaer en la función de Auditoría Interna, evalúa el marco y el desafío efectivo adoptado por la segunda línea, así como el nivel de adopción de dicho marco por parte de la primera LOD.

13. ***Integración entre riesgos.*** Las organizaciones criminales son cada vez más sofisticadas en sus esquemas de blanqueo de capitales, combinando con frecuencia ciberataques (robo de credenciales y suplantación de identidad), uso ilícito de esos accesos privilegiados para cometer un fraude, y múltiples mecanismos para blanquear los beneficios de este. Como reacción, las entidades financieras están evolucionando sus modelos hacia un marco de prevención del delito financiero cada vez más integrado, con un modelo de gobernanza unificado que incorpora todos los subtipos de riesgo en un único modelo operativo (ML/FT, evasión fiscal y fraude, junto con el ciber riesgo). Aunque hay diferentes niveles de madurez, esto suele implicar grados de taxonomía de riesgos comunes, infraestructura de datos y conjuntos de datos unificados, estrategias conjuntas que tratan de detectar eventos sincronizados de los diferentes tipos de riesgo o marcos comunes para el análisis de alertas y las investigaciones. Algunas entidades incluso han centralizado la responsabilidad bajo una única figura y han creado centros de excelencia que proporcionan capacidades operativas en todos los subtipos de riesgo.

14. ***Diseño organizativo.*** Aunque no exista una norma del sector en torno a la estructura organizativa que implemente de forma más eficaz el modelo de las tres líneas de defensa de AML/CFT, tanto los reguladores como las entidades financieras esperan que los responsables de esos equipos cuenten con líneas jerárquicas que permitan cuestionar de forma independiente el negocio y escalar directamente al nivel ejecutivo y al Consejo de Administración si es necesario. Asimismo, se espera que cuenten con la antigüedad y las competencias adecuadas, y que los equipos dispongan de personal y recursos tecnológicos suficientes para ser eficaces en su actividad. En la segunda línea de defensa, el responsable de la supervisión de AML/CFT tiende a depender de un nivel ejecutivo, es decir, del Director de Riesgos, del Director de Cumplimiento o del Director de Legal/Consejo General.

15. ***Planificación de la plantilla.*** Una de las tendencias y mejores prácticas del sector consiste en ligar la ambición de los objetivos en torno a AML/CFT, el apetito al riesgo y la estrategia con un ejercicio de planificación estratégica para evaluar las necesidades de personal en términos de volumen, conjunto de aptitudes y experiencia, ubicaciones, etc. Una vez realizado el análisis, se lleva a cabo una ejecución estricta para garantizar que dicha capacidad esté disponible cuando se necesite. Esto incluye la formación/reciclaje del personal existente y la contratación de nuevo talento (parcialmente formados desde la base, a través de programas de graduados, para garantizar una disponibilidad continua de expertos en la materia, independientemente de las condiciones del mercado).

16. ***Capacidades analíticas.*** Como parte de este ejercicio de planificación estratégica, la mayoría de las entidades financieras están experimentando una fuerte demanda de capacidades analíticas, ya que muchos de los procesos subyacentes en AML/CFT se basan cada vez más en los datos (y en la ciencia de los datos): análisis de riesgos, escaneo de nombres, monitorización de transacciones, detección de falsos positivos, etc. La mayoría de las organizaciones maduras están creando sólidos y avanzados equipos de análisis (en algunos casos, contratándolos en el mercado y, en otros, reubicando perfiles cuantitativos de otras áreas -por ejemplo, la modelización del riesgo prudencial- para aplicar sus conocimientos a nuevos problemas empresariales). También hay una fuerte demanda de perfiles especializados en pagos, incluyendo personas con conocimientos técnicos detallados sobre criptomonedas o, más ampliamente, sobre nuevas tecnologías de pagos. Por último, otro perfil que suele señalarse en estos ejercicios son las personas con múltiples habilidades capaces de abarcar diferentes disciplinas dentro del ámbito del delito financiero, que también escasean en el mercado. Suelen ser perfiles que provienen de la lucha contra el fraude y se convierten también en expertos en materia de AML/CFT. Estos perfiles están resultando muy útiles tanto para perfeccionar la detección de estrategias conjuntas de delito financiero, como para apoyar a los centros de excelencia polivalentes que abarcan todos los tipos de riesgo.

17. ***Quality Assurance.*** A medida que las organizaciones se vuelven más maduras, tienden a crear equipos especializados para aumentar la eficacia, atravesar los diferentes negocios y garantizar la profesionalización de las actividades de control de AML/CFT. Algunas de esas funciones son los equipos de control y *quality assurance*, encargados de garantizar que los procesos empresariales clave en los que pueden surgir riesgos se ejecuten adecuadamente de acuerdo con la política y los procedimientos. También equipos especializados de aseguramiento de la segunda línea de defensa, para apoyar la ejecución efectiva del plan de supervisión.

18. ***Centros de excelencia.*** Como parte de esta especialización, un paso natural dado por las instituciones más avanzadas ha sido la creación de centros de excelencia. La intención suele ser mejorar la eficacia y captar sinergias en la ejecución de procesos operativos como diligencia debida del cliente (CDD, *Customer Due Diligence*), diligencia debida reforzada (EDD, *Enhanced Due Diligence*), escaneo de nombres, monitorización de transacciones, escaneo de pagos, pero también la producción de información de gestión, o la prestación de servicios de mejora continua y remediación. Algunas de estas entidades financieras han encontrado más sinergias al incorporar a estos centros de excelencia aspectos operativos relacionados con el fraude, tanto interno (investigación de empleados) como externo. Aspectos como el proceso de KYC y *onboarding* (por ejemplo, un único equipo de *onboarding*, con la correspondiente visión holística del delito financiero, y la simplificación de la experiencia del cliente), o el desarrollo y parametrización de escenarios para la detección de blanqueo de capitales, fraude, etc., son áreas comunes de sinergia.

19. ***Regionalización.*** Para los grandes grupos financieros internacionales, una evolución natural en su camino de centralización ha sido la regionalización de las actividades. En concreto, la creación de centros de excelencia a nivel regional, con los correspondientes beneficios en términos de una mejor gestión del conjunto de recursos, la eliminación de duplicidades, la racionalización de la estructura organizativa y la mejora de las trayectorias profesionales y las oportunidades de formación cruzada para los trabajadores, con las correspondientes tasas de retención. En la misma línea de evolución, algunas grandes entidades financieras que ya operaban en países *off-shore* o *near-shore* con menor coste de los recursos humanos han podido construir con éxito centros de excelencia en esos lugares para prestar servicios en la región.

20. ***Externalización.*** Aunque la subcontratación de algunas actividades operativas sigue siendo una opción elegida por diferentes instituciones financieras, hay una serie de factores que empujan a algunas de esas instituciones a internalizar esas capacidades subcontratadas y desarrollar esos conjuntos de habilidades dentro de la organización. Uno de ellos es el aumento de las exigencias normativas en torno a las actividades externalizadas que son fundamentales para la organización y la consiguiente necesidad de crear sólidas estructuras de supervisión y control en torno a los servicios externalizados, el nivel de excelencia operativa que esperan las diferentes partes interesadas (inversores, supervisores, sociedad) y el impacto en la reputación de los fallos operativos.

21. ***Cultura y comportamientos.*** Un área clave de inversión en los programas estratégicos de AML/CFT es el diseño y la incorporación de la cultura, los métodos de trabajo y los comportamientos del personal adecuados para combatir los riesgos subyacentes del delito financiero. El control de la supervisión está aumentando en todas las jurisdicciones, y la importante reducción de los perfiles especializados en AML/CFT requiere una articulación e integración efectivas de la cultura y los comportamientos adecuados para los empleados existentes y, especialmente, para los nuevos.

22. ***Formación.*** Como parte de los programas culturales de AML/CFT, las entidades financieras están invirtiendo en el fortalecimiento de los procesos de contratación y selección del personal con responsabilidades en materia de AML/CFT. También, en el desarrollo de programas de formación y certificación ambiciosos (con modelos operativos ajustados para mantener los materiales actualizados, medir la eficacia y mejorar continuamente), y que estén conectados con la progresión de la carrera y la remuneración. Esto también requiere una capacidad de seguimiento y medición de las competencias para reaccionar ante el deterioro de los conocimientos y la experiencia. Estos programas también invierten en el desarrollo de mensajes claros y transparentes desde la cúpula directiva (hasta el Consejo de Administración y el nivel ejecutivo), y en fuertes campañas de comunicación dirigidas a los diferentes segmentos de la estructura de empleados, con contenidos específicos para cada uno de ellos. Por último, las entidades financieras también dedican tiempo a diseñar los incentivos y la medición del rendimiento adecuados para su personal, en consonancia con el apetito al riesgo y las políticas asociadas.

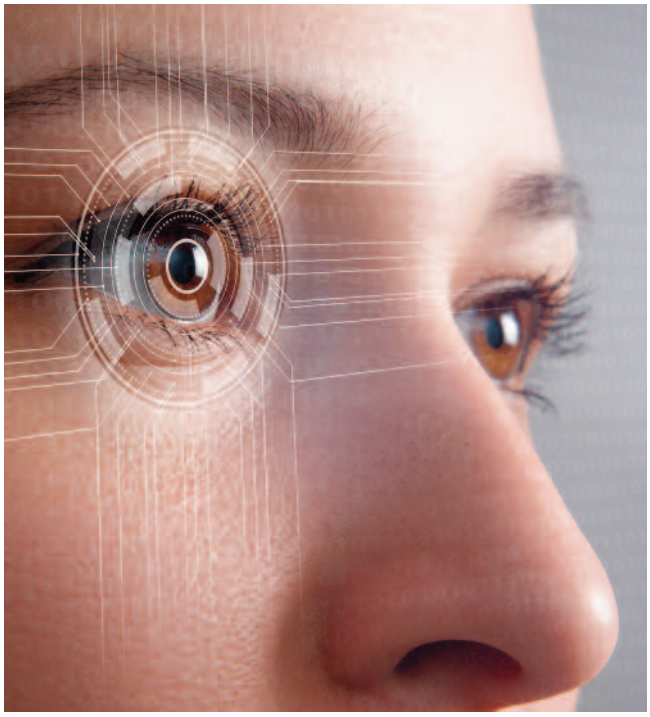
23. ***Infraestructura de datos e información de gestión.*** En una economía cada vez más impulsada por los datos, una de las áreas clave de desarrollo dentro del espacio de AML/CFT es la infraestructura de datos subyacente y la información de gestión utilizada para la toma de decisiones. Desde el punto de vista de la información de gestión, una tendencia del mercado es incorporar, en los informes del Consejo de Administración y a nivel ejecutivo, un conjunto completo de métricas e información cualitativa para garantizar que se tengan en cuenta todos los riesgos subyacentes (actuales y emergentes) asociados a la entidad. La información de gestión detalla los cambios en la Evaluación de Riesgos a nivel de toda la organización, así como una representación de los riesgos asociados a las nuevas relaciones comerciales (incluyendo el número de nuevas relaciones comerciales por categoría de riesgo, cualquier nueva relación de alto riesgo, cualquier PEP, etc.). En el caso de las relaciones existentes, la alta dirección de la organización recibe información sobre los resultados de las actividades de supervisión en curso (por ejemplo, la monitorización de las transacciones, el escaneo de pagos o las revisiones periódicas de los clientes), así como el resumen de los informes de actividades sospechosas que ha tenido lugar, y las estadísticas sobre los resultados positivos por encima y por debajo del umbral determinado. La estructura de los informes también debería contener la salida de las relaciones existentes, y la justificación de estas. Por último, es una práctica avanzada incorporar en la información de gestión tanto las cuestiones abiertas procedentes del trabajo de *Quality Assurance*, la Auditoría Interna o la acción de investigación de la Supervisión, como una sección sobre el enlace regulador o el compromiso de la industria (que suele incluir un elemento de exploración del horizonte para la nueva regulación o los requisitos legales).

24. ***Información externa.*** Además de la información de gestión, el panorama de los datos y la taxonomía en que se basa el marco de AML/CFT es muy amplio y puede suponer un reto. Además de los datos sobre clientes y transacciones generados por la organización, las organizaciones se basan más que nunca en información externa (oficinas de reputación, organismos nacionales de lucha contra la delincuencia, sentencias

judiciales, registros públicos de beneficiarios finales, etc.) para complementar sus modelos analíticos. Esta información externa, en muchos casos, requiere la ingesta, el mantenimiento y la comparación con listas para encontrar posibles coincidencias de los clientes y transacciones actuales o potenciales. Estas listas se están enriqueciendo con nuevas incorporaciones, como los activos digitales prohibidos (por ejemplo, direcciones de monedas virtuales o carteras digitales asociadas a empresas o personas sancionadas). Además, la adopción de las nuevas normas de mensajería en el marco de la norma ISO20022 ayudará al escaneo y comparación de las transacciones.

25. ***Gestión de listas y sancionados.*** Especialmente en el ámbito de las sanciones, la gestión de listas es una capacidad fundamental. Las organizaciones más maduras están implementando una plataforma de gestión de listas centralizada que agrega archivos de diferentes autoridades y proveedores, limpia los datos y luego los difunde entre todas las filiales de acuerdo con su normativa local y la política del grupo, eliminando duplicidades y aumentando la supervisión.

26. ***Conjuntos de datos heterogéneos.*** La naturaleza de los datos que se capturan es también muy variada y cambiante. Una taxonomía de datos estándar asociados a AML/CFT puede incluir, además de la información estándar sobre las transacciones, los identificadores electrónicos (por ejemplo, el eIDAS en la UE), la geolocalización, las direcciones IP o incluso el IMEI y el modelo de dispositivo de los aparatos utilizados en las transacciones de moneda virtual convertible. También listas que contengan direcciones IP no fiables, direcciones IP de jurisdicciones sancionadas o direcciones IP marcadas como sospechosas. Además, los archivos multimedia adversos y la información procedente de las redes sociales pueden incluir formato de audio o vídeo, lo que pone de manifiesto la demanda de información no estructurada y la correspondiente infraestructura subyacente para almacenarla y explotarla.



27. ***Capacidades de gestión de datos.*** Estas demandas de datos requieren el desarrollo de capacidades de gestión de datos. Una de ellas es la capacidad de calidad de datos para especificar de forma proactiva las reglas de negocio y los estándares de calidad de datos en torno a los datos críticos, y luego medir sistemáticamente esas reglas para identificar cualquier incumplimiento. También, un catálogo de datos que permite la armonización de la información en diferentes repositorios. Por último, las entidades financieras están invirtiendo mucho en capacidades de origen de datos para permitir la trazabilidad de los datos de principio a fin, desde el punto de origen hasta el punto de consumo.

28. ***Armonización de la infraestructura de datos.*** Uno de los principios más importantes en cuanto a la infraestructura de datos ha sido la convergencia hacia repositorios de datos únicos, de manera que todos los componentes tecnológicos o procesos de negocio implicados en el marco de AML/CFT consuman datos y los almacenen de vuelta en el mismo repositorio, poniéndolos inmediatamente a disposición del resto de componentes. Esta centralización puede producirse a nivel regional o incluso de grupo. Para obtener una visión holística del riesgo del cliente y estandarizar la investigación de alertas y la elaboración de informes, es indispensable consolidar los datos de KYC, escaneos, monitorización de transacciones y gestión de alertas y casos en una única plataforma. La consolidación de la información básica necesaria para una investigación antes de que se asigne la alerta mejora el tiempo por alerta, además de las notificaciones automáticas al departamento de Cumplimiento Normativo cuando una alerta está pendiente de autorización.

29. ***Procesos empresariales - Incorporación de clientes.*** En relación con los procesos de negocio para la incorporación de nuevos clientes y el KYC asociado, la evolución de los comportamientos de los clientes, acelerada por la pandemia del COVID-19, ha impulsado el dominio de los canales digitales en las interacciones financieras. Las entidades están invirtiendo en soluciones automatizadas de autoservicio a través de canales digitales, accionables por el usuario, utilizando una identificación digital y datos biométricos para capacitar a los clientes durante el proceso de incorporación, las revisiones periódicas y la recertificación. Además, permite una recopilación de información más específica sobre el riesgo (en el momento de la incorporación o siempre que haya un desencadenante) con cuestionarios dinámicos alineados con una segmentación predefinida. Estos procesos se conectan ahora directamente, a través de APIs y microservicios, a fuentes externas de datos para recuperarlos automáticamente y, por tanto, simplificar la experiencia del cliente, al tiempo que se validan de forma independiente los *inputs*. Estas soluciones también facilitan el registro automatizado de la asistencia al cliente durante el proceso de diligencia debida, lo que puede ser decisivo en un posible proceso de investigación.

30. **Procesos empresariales - Monitorización de las transacciones.** Otro proceso que las entidades financieras están mejorando drásticamente es la supervisión de las transacciones. Es muy exigente desde el punto de vista de los datos y del cómputo para calcular la probabilidad de cada

escenario. Las entidades financieras están invirtiendo en tecnología con mayor capacidad de cálculo, aprovechando la computación en la nube. Además, están afinando la ejecución de los escenarios en función de la segmentación de los clientes (en lugar de ejecutar todos los escenarios para todos los datos disponibles, se personalizan los escenarios para adaptarlos al perfil de riesgo de la entidad y a la realidad del negocio en términos de geografía, catálogo de productos, etc.). Otra opción para aumentar la eficiencia es realizar simulaciones (número de alertas, falsos positivos, falsos negativos, etc.) en un entorno *sandbox* antes de desplegar el escenario en producción o ejecutar los escenarios solo contra los clientes susceptibles al riesgo, omitiendo, por ejemplo, los organismos públicos y gubernamentales con muy bajo riesgo. Algunas instituciones ejecutan un escaneo *batch* retroactivo para identificar posibles vínculos con entidades sancionadas y marcar a esos clientes como individuos de alto riesgo que deben ser investigados.

31. ***Procesos comerciales - Evaluación en tiempo real.*** En lo que respecta al escaneo de los datos de los clientes (datos de identificación durante la incorporación o transacciones durante la actividad normal), la tendencia del mercado es que estos se ejecuten en tiempo real. Por lo tanto, hay exigencias estrictas en cuanto a los acuerdos de nivel de servicio para el mantenimiento de las listas, y un proceso técnico que garantice que las comprobaciones en línea no se vean afectadas por el reprocesamiento *batch* de todos los registros de clientes cada vez que se actualiza una lista. Además, la huella digital es un método en alza para la identificación de banderas rojas en el control de pagos. En las organizaciones más avanzadas, las direcciones IP recogidas durante las operaciones de los clientes, asociadas a las transacciones y a los inicios de sesión, se supervisan de forma rutinaria y se comparan con las introducidas durante la incorporación para detectar el uso indebido de una cuenta desde un país de alto riesgo/sancionado o el robo de cuentas. La detección de las direcciones IP asociadas a una red Tor (que anonimiza el tráfico web) es fundamental, ya que podría revelar conexiones entre el cliente y los delincuentes de la *darknet*.

32. ***Procesos empresariales - Reporting.*** Incluso cuando la detección de riesgos se implementa con éxito, la presentación de informes deficientes podría alterar el proceso. Las entidades financieras están mejorando sus procesos para garantizar el cumplimiento de los acuerdos de nivel de servicio previstos por sus unidades de inteligencia financiera locales (UIF) y la rápida incorporación de los cambios en los formatos y requisitos de información. Además, existen oportunidades de automatización en la ejecución de los pasos reglamentarios que no requieren intervención manual. Por último, los canales de comunicación entre las funciones de AML/CFT y las líneas de negocio deben ser muy dinámicos, para garantizar que la respuesta a las preguntas o la recopilación de más información se realice dentro de los plazos reglamentarios.

33. ***Machine learning.*** Como ya se ha comentado, las tecnologías de detección en tiempo real se están adoptando ampliamente para prevenir los riesgos asociados a errores inadvertidos y mejorar la experiencia del cliente. Para el escaneo transaccional y de nombres (o casos fuera del marco de AML/CFT, como la detección de fraude por audio) las instituciones más avanzadas están invirtiendo en librerías de *machine learning* para el Procesamiento del Lenguaje Natural (NLP) con el fin de recoger, analizar y almacenar información de audio y crear alertas a las líneas de negocio que interactúan con el cliente, finalizando la llamada inmediatamente para evitar compartir cualquier información personal.

34. ***Infraestructura tecnológica.*** Desde el punto de vista de la infraestructura tecnológica, el panorama de las herramientas de AML/CFT ya no puede depender únicamente de un *Data mart* relacional como base de datos central, ya que ahora recibe datos no estructurados (imagen, audio, vídeo...) en los que bases de datos NoSQL y *Data Lakes* resultan más eficaces.

35. ***Distributed ledger technology.*** Los avances tecnológicos también están mejorando los sistemas de gestión de listas, pasando de los clásicos sistemas de gestión de listas que administran tablas y archivos a la *Distributed Ledger Technology* (DLT) o Tecnología de registros distribuidos. La DLT ayuda a salvaguardar la integridad de los datos, la trazabilidad, la confidencialidad, el cifrado y el acuerdo entre los responsables. Además, permite a los reguladores auditar el libro de transacciones, que contiene la secuencia de cambios etiquetados con fecha de ocurrencia para validar el cumplimiento.

36. ***Robótica avanzada.*** Otra tendencia tecnológica que las entidades han estado utilizando para ganar eficiencia y mejorar la eficacia es la automatización a través de procesos robóticos (RPA). Los agentes virtuales, los *chat-bots* y los *call-bots* pueden asistir a los clientes con consultas estructuradas y repetitivas día y noche sin interrupción, poniéndolos en contacto con una persona para las consultas que son más complejas. El RPA es también una mejora crucial para la gestión de alertas y casos, ya que estos algoritmos pueden ingerir más datos de más fuentes con mayor rapidez que un investigador humano, lo que permite un análisis más rápido de una base de pruebas más amplia y, en última instancia, una resolución más precisa. Los sistemas más sofisticados automatizarán pasos o resultados basados en investigaciones y resultados anteriores.

37. ***Mejoras end to end.*** Todas esas mejoras tecnológicas combinadas conllevan la utilización de modelos de *machine learning* para puntuar las alertas, con el fin de discriminar los posibles falsos positivos. El departamento de Cumplimiento debería haber establecido un flujo de trabajo claramente definido y objetivo para la revisión de las alertas, con un criterio de priorización para analizarlas (por ejemplo, en función de los perfiles de riesgo, el importe de las transacciones o las puntuaciones de coincidencia). Este proceso solo es posible si lo llevan a cabo equipos especializados en AML/CFT que se encarguen de la detección de organizaciones complejas y de gestionar las listas blancas.

Definición del riesgo de delitos financieros y contexto regulatorio

"Durante demasiado tiempo, los delincuentes han calculado que el delito realmente paga"

Ronald Reagan[23]

El delito financiero se refiere a los actos ilegales cometidos por un individuo o grupo de individuos para obtener un beneficio económico personal utilizando los medios de los servicios financieros o los mercados financieros. Aunque existen diferentes definiciones de lo que es el delito financiero[24], bajo este concepto se consideran las acciones de ML/FT, soborno, abuso de mercado o fraude[25].

Se destacan dos definiciones de delito financiero de la Financial Conduct Authority (FCA, Autoridad de conducta financiera del Reino Unido) y la Federal Deposit Insurance Corporation (FDIC, Corporación Federal de Seguro de Depósitos de los Estados Unidos):

> *"Cualquier tipo de conducta delictiva relacionada con el dinero o con los servicios o mercados financieros, incluido cualquier delito que implique: a) fraude o deshonestidad; o b) conducta indebida en un mercado financiero o uso indebido de información relacionada con el mismo; o c) manejo de productos del delito; o d) financiación del terrorismo"* [26].

> *"Se puede abusar de las personas jurídicas para disfrazar la participación en la financiación del terrorismo, el blanqueo de capitales, la evasión fiscal, la corrupción, el fraude y otros delitos financieros"* [27].

La creación de medios para identificar y perseguir los delitos financieros en sus diferentes formas ha desencadenado la promulgación de diferentes iniciativas de supervisión y regulación. Las dos acciones fundamentales que promovieron una mayor coordinación mundial en materia de regulación del blanqueo de capitales fueron la constitución del Grupo de Acción Financiera (GAFI)[28] y la ratificación por parte de la ONU de la Convención sobre la Delincuencia Organizada Transnacional[29], el primer tratado de AML/CFT. Como parte del GAFI, los Estados miembros están obligados a cumplir las normas mundiales de prevención de estos riesgos. Estas normas[30] definen a grandes rasgos los componentes básicos de cualquier programa moderno de AML/CFT en cualquier institución financiera:

- Implantar medidas de verificación de la identidad de *"Know Your Customer"* (KYC).
- Implementar las medidas de diligencia debida recomendadas por el GAFI.
- Mantener registros adecuados de los clientes de alto riesgo.
- Supervisar periódicamente las cuentas para detectar actividades financieras sospechosas e informar de ellas a la autoridad nacional competente.
- Aplicar sanciones efectivas a las personas jurídicas y entidades obligadas que incumplan la normativa del GAFI.

Por otra parte, los principios del GAFI y los acuerdos de la Convención de la ONU crearon un consenso para empezar a trabajar en la identificación de las prácticas de AML/CFT y, lo que es más importante, para detenerlas.

Durante las últimas décadas, el concepto de AML/CFT ha evolucionado de forma diferente, así como las distintas normativas, en función, entre otras cosas, de la naturaleza cambiante de las actividades financieras. Las principales tendencias observadas internacionalmente de delito financiero son las siguientes:

[23] Ronald Wilson Reagan (1911-2004) fue el 40º presidente de los Estados Unidos (desde 1981 a 1989) y 33.er gobernador de California (desde 1967 a 1975).

[24] Algunos organismos reguladores o de supervisión, como la FCA, ofrecen una definición "cerrada" del término "delito financiero" y de las acciones que se consideran dentro de él, mientras que otros pueden reclamar la responsabilidad de evaluar, regular y supervisar determinados actos ilegales que podrían calificarse como delito financiero (por ejemplo, la FINCEN). No obstante, las acciones identificadas de ML y FT son fundamentales para cualquier programa de supervisión de delitos financieros.

[25] Otros actos ilegales con beneficios financieros implícitos que están sujetos a una regulación general son: la usurpación de identidad, la corrupción, la evasión de impuestos, la malversación, la falsificación.

[26] Autoridad de Conducta Financiera (2021).

[27] Apéndice A de § 1010.230-Certificación relativa a los beneficiarios finales de las personas jurídicas, FDIC Law, Regulations, Related Acts.

[28] GAFI (2019).

[29] Oficina de las Naciones Unidas contra la Droga y el Delito (2005).

[30] A pesar de la complejidad del tema y de la constante evolución de las técnicas de ML y de la tecnología disponible para ello, estas normas siguen siendo el núcleo de los programas de AML en todo el mundo y abordan los requisitos de evaluación de AML establecida por el sector: evaluación de la calificación del riesgo del cliente, programa de monitorización de las transacciones y programa de escaneo de sanciones. Las normas relativas a los clientes de alto riesgo son especialmente importantes, ya que el enfoque basado en el riesgo es la quintaesencia de la definición de cualquier programa de AML.

- Restricciones estrictas a las transacciones en la mayoría de las jurisdicciones, lo que aumenta el apetito de los delincuentes financieros por desviarse a otro tipo de actividades como las criptomonedas y las monedas digitales en fases incipientes de control y regulación.
- Las actitudes, preferencias y comportamientos de los clientes están cambiando, con una creciente atención a los servicios bancarios digitales[31], que serán el objetivo de los delincuentes financieros (por ejemplo, activos virtuales, carteras de custodia, monedas fiduciarias, tarjetas de prepago).
- El aumento de las actividades financieras internacionales facilitado por las tecnologías disponibles ha fomentado nuevas necesidades de consumo global, lo que crea nuevos canales para las actividades financieras ilícitas.

La complejidad del entorno actual está obligando a las autoridades reguladoras a tomar medidas y abordar la modernización de los programas de prevención del delito financiero a la luz de estos elementos transformadores.

Los cambios normativos asociados al delito financiero durante los últimos años (2021-2022) se han centrado en:

- Restricciones más estrictas para evitar el blanqueo en circuitos "no tradicionales", por ejemplo, nuevas normas para las transacciones digitales.
- Mayor atención a los fundamentos del programa KYC para controlar los riesgos y perfiles de los clientes y reforzar así la normativa AML/CFT.
- Introducción de nuevas tecnologías y análisis (por ejemplo, servicios en la nube, modelo de *machine learning/artificial intelligence,* analítica avanzada) para pasar a la identificación en tiempo real y al uso optimizado de los recursos.
- Coordinación entre jurisdicciones para mejorar los programas de prevención del delito financiero.
- Cooperación pública y privada y desarrollo de una plataforma para compartir información.

Una de las tendencias normativas más importantes ha sido el refuerzo de la colaboración interbancaria e interjurisdiccional con el objetivo de aumentar las capacidades de intercambio de datos e información sobre delitos financieros y crear normas homogéneas que puedan actuar en coordinación[32]. Aunque estas iniciativas se encuentran en una fase incipiente, están dando buenos resultados (como se ha visto, por ejemplo, en la reacción de distintas regiones a la invasión rusa de Ucrania, y las correspondientes sanciones impuestas a los intereses económicos rusos).

Panorama normativo en las distintas jurisdicciones

Estados Unidos lleva desarrollando una normativa al respecto desde 1970. Sin embargo, en los últimos años se ha publicado una nueva normativa para actualizar el corpus existente:

- La Ley AML de 2020[33] modernizó la Ley de 1970 (BSA/AML) incorporando elementos críticos para abordar la cuestión del blanqueo y el fraude en consonancia con las tendencias actuales.
- El mismo reglamento actuó sobre los requisitos para los beneficiarios finales. Los bancos tendrán una mejor visibilidad del beneficiario final de una transacción, lo que reforzará la diligencia debida con respecto al cliente y reducirá las actividades de blanqueo y fraude.
- Las bolsas de criptomonedas deben completar el proceso de KYC para cada cliente[34].

En el caso de la Unión Europea, la CE presentó un paquete con cuatro propuestas legislativas relacionadas con AML/CFT[35]. El objetivo de este nuevo paquete legislativo es abordar las diferencias entre las normativas nacionales y aumentar la coordinación entre los estados miembros.

El gobierno del Reino Unido está trabajando activamente para cumplir con las normas internacionales de AML/CFT y considerando la introducción de prioridades nacionales en la Ley de AML[36]. El gobierno está avanzando en su Plan de Delitos Económicos 2019-2022[37] para reforzar los marcos de prevención de los delitos financieros. En su última declaración sobre el progreso de este Plan, se desarrollaron varias acciones básicas que se fundamentan en las acciones originales dentro del Plan de Delitos Económicos[38,39].

[31] Esta tendencia se ha agravado como consecuencia de la pandemia de COVID19.
[32] El GAFI incluyó en su agenda la iniciativa de asociación público-privada. Diferentes reguladores también han puesto en marcha iniciativas similares.
[33] FinCEN.gov (2020).
[34] Aparte de esta importante adición a las normas de KYC, la U.S. Securities and Exchange Commission, la Commodity Futures Trading Commission y la FinCEN emitieron otras normas sobre activos virtuales para reforzar el marco de control de estos activos en EE.UU.
[35] Reglamento por el que se crea una autoridad de la UE en materia AML/CFT; Regulación aplicable a AML/CFT (código normativo único) y a las entidades sujetas a ellas; Directiva 6 sobre AML/CFT (AMLD6), que sustituye a la anterior, y que debe incorporarse a la legislación nacional con normas para los supervisores nacionales y las UIF de los Estados miembros, y Reglamento sobre transferencias de fondos.
[36] El Instituto de Finanzas Internacionales y Deloitte (2021).
[37] Gobierno del Reino Unido (2019).
[38] Gobierno del Reino Unido (2021).
[39] i) Diseñar y poner en marcha un Plan de Acción contra el Fraude; ii) reforzar la acción operativa público-privada para hacer frente a las vulnerabilidades conocidas que permiten el flujo de finanzas ilícitas dentro y fuera del Reino Unido; iii) mejorar la eficacia y la eficiencia de la respuesta de todo el sistema a la delincuencia económica, aumentando la información de alto valor para la aplicación de la ley y reduciendo la actividad de bajo valor que cuesta a las empresas y ofrece poco beneficio; iv) continuar con la reforma de los RAS, incluidas las próximas fases de implantación de la nueva infraestructura informática y el aumento de la dotación de personal de la Unidad de Inteligencia Financiera del Reino Unido; v) finalizar el modelo de dotación de recursos sostenible para apoyar la reforma de la delincuencia económica, vi) desarrollar propuestas legislativas para abordar el fraude, el blanqueo de capitales, incautar más activos delictivos y reforzar la transparencia empresarial y vii) aprovechar la Presidencia del G7 para reforzar la respuesta internacional global a la financiación ilícita y la lucha contra la corrupción.

En China, el CBIRC emitió nuevas medidas[40] para alentar a las entidades financieras a cumplir eficazmente sus obligaciones en materia de AML/CFT y regular la supervisión y administración.

Japón ha publicado recientemente unas directrices en materia de AML/CFT[41] que también prescriben un enfoque basado en el riesgo que cumple con las normas internacionales, como las del GAFI.

En Singapur, la Ley de Servicios de Pago[42] se actualizó en enero de 2021. Esta normativa proporciona un marco flexible para los sistemas de pago y los proveedores de servicios de pago en el país. Recientemente, la Autoridad Monetaria de Singapur (MAS) también publicó dos documentos de consulta que pretenden reforzar el marco normativo en torno al blanqueo de capitales[43].

[40] Banco Popular de China (2020).
[41] Agencia de Servicios Financieros (2021).
[42] República de Singapur (2019).
[43] Ver: Consultation Paper on Proposed AML Notices for Cross-Border Business Arrangements of Capital Markets Intermediaries under Proposed Exemption Frameworks. Autoridad Monetaria de Singapur. 12 de mayo de 2021, y Consultation Paper on the FI-FI Information Sharing Platform for AML/CFT. Autoridad Monetaria de Singapur. Octubre de 2021.

La siguiente lista contiene los principales organismos de supervisión y regulación que actúan en la aplicación del programa de delito financiero y las principales normas y directrices. La evolución histórica explica la mayor atención prestada en AML/CFT.

Estados Unidos – Organismo regulador: FinCEN

- *Ley de Secreto Bancario (BSA), Ley de Información sobre Moneda y Transacciones Extranjeras de 1970* | 26-Oct-70. Define el marco normativo para que las entidades financieras estadounidenses ayuden a los organismos gubernamentales de Estados Unidos a detectar y prevenir el blanqueo de capitales, incluidas las transacciones que superen los 10.000 dólares, e informen de actividades sospechosas que puedan significar blanqueo de capitales, evasión fiscal u otras actividades delictivas.
- *Título III de la Ley USA PATRIOT de 2001* | 26-Oct-01. El artículo 314 contribuye a la identificación, desarticulación y prevención de actos terroristas y actividades de blanqueo de capitales.
- *Ley de transparencia empresarial de 2019* | 11-Jun-19. Exige a las entidades nuevas y existentes que comuniquen la información sobre la titularidad efectiva a la Red de Represión de Delito financiero ("FinCEN"), crea una base de datos sobre la titularidad efectiva e instituye sanciones civiles, multas y penales en caso de incumplimiento.
- *Ley AML de 2020 (US AMLA)* |1-Jan-21. Exige a la FinCEN que establezca prioridades nacionales en materia de AML/CFT para que las entidades financieras las incorporen a sus programas, y recopilen y reporten información adicional sobre los titulares de cuentas, incluyendo información sobre la propiedad real y control. Asimismo, requiere que los reguladores y examinadores las incorporen a sus normas, orientaciones y exámenes.
- *Prioridades nacionales contra el blanqueo de capitales y la financiación del terrorismo* | 30-Jun-21. Prioridades gubernamentales en materia de lucha contra el blanqueo de capitales y la financiación del terrorismo.

Reino Unido - Organismo regulador: Gobierno del Reino Unido

- *Ley sobre el producto del delito de 2002*| 24-Jul-02. Crea el Organismo de Recuperación de Activos y establece disposiciones sobre el nombramiento de su Director y sus funciones (incluidas las funciones en materia de ingresos) y fija el régimen legislativo para la recuperación de activos de origen delictivo.
- *Ley de finanzas penales de 2017* | 27-Apr-17. Ley para modificar la Ley de ganancias del delito de 2002; establecer disposiciones en relación con los bienes terroristas; crear delitos corporativos para los casos en los que una persona asociada a una entidad corporativa o sociedad facilite la comisión por parte de otra persona de un delito de evasión fiscal; y para fines relacionados.
- *El Reglamento sobre blanqueo de capitales, financiación del terrorismo y transferencia de fondos de 2017* | 28-Jun-17. El Tesoro Público está designado a los efectos del artículo 2(2) de la Ley de las Comunidades Europeas de 1972 en relación con la prevención del blanqueo de capitales y la financiación del terrorismo.

Reino Unido - Organismo regulador: FCA

- *Ley de Servicios Financieros de 2012* | 19-Dec-12. Ley para modificar la Ley del Banco de Inglaterra de 1998, la Ley de Servicios y Mercados Financieros de 2000 y la Ley de Banca de 2009; para adoptar otras disposiciones sobre los servicios y mercados financieros; para adoptar disposiciones sobre el ejercicio de determinadas funciones legales relativas a las sociedades de crédito hipotecario, las sociedades de socorros mutuos y otras sociedades mutuas; para modificar el artículo 785 de la Ley de Sociedades de 2006; para adoptar disposiciones que permitan al Director de Ahorros prestar servicios a otros organismos públicos; y para fines conexos.

Reino Unido - Organismo regulador: JMLSG

- *Orientaciones para la lucha contra el blanqueo de capitales y la financiación del terrorismo* |20-Dec-21. Establece lo que se espera de las empresas y de su personal en relación con la prevención del blanqueo de capitales y la financiación del terrorismo, pero les permite cierta discrecionalidad en cuanto a la forma de aplicar los requisitos del régimen británico de AML/CFT en las circunstancias particulares de la empresa, y de sus productos, servicios, transacciones y clientes.

Unión Europea - Organismo regulador: EC

- *Directiva contra el blanqueo de capitales* | 9-Jun-18. Establecen los factores que las empresas deben tener en cuenta al evaluar el riesgo de ML/FT asociado a una relación comercial o a una transacción ocasional. Además, proporcionan orientación sobre cómo las entidades financieras pueden ajustar sus medidas de diligencia debida con respecto al cliente para mitigar el riesgo de ML/FT que han identificado, de modo que sean más adecuadas y proporcionadas. Por último, apoyan los esfuerzos de supervisión de las autoridades competentes en materia de AML/CFT a la hora de evaluar la idoneidad de las evaluaciones de riesgo y de las políticas y procedimientos de AML/CFT de las empresas.
- *Reglamento Delegado de la Comisión (UE) 2019/758 (EU) 2019/758* | 31-Jan-19. Normas técnicas reglamentarias sobre la actuación mínima y el tipo de medidas adicionales que deben adoptar las entidades de crédito y financieras para mitigar el riesgo de blanqueo de capitales y financiación del terrorismo en determinados terceros países.
- *Propuesta de 6ª Directiva sobre Lucha contra el Blanqueo de Capitales y la Financiación del Terrorismo (AMLD 6)* | 20-Jul-21. Directiva relativa a los mecanismos que deben establecer los Estados miembros para la prevención de la utilización del sistema financiero para el blanqueo de capitales o la financiación del terrorismo y por la que se deroga la Directiva (UE) 2015/849.
- *Paquete legislativo contra el blanqueo de capitales y la financiación del terrorismo* | 20-Jul-21. El paquete incluye una propuesta de creación de una nueva autoridad de la UE para luchar contra el blanqueo de capitales. Forma parte del compromiso de la Comisión de proteger a los ciudadanos y al sistema financiero de la UE contra el blanqueo de capitales y la financiación del terrorismo. El objetivo es mejorar la detección de transacciones y actividades sospechosas, y cerrar las brechas utilizadas por los delincuentes para blanquear ingresos ilícitos o financiar actividades terroristas a través del sistema financiero.

Unión Europea - Organismo regulador: EBA

- *Directrices sobre políticas y procedimientos en relación con la gestión del cumplimiento y el papel y las responsabilidades del responsable de cumplimiento de AML/CFT.* | 14-Jun-22. Las directrices abordan de forma exhaustiva, por primera vez a nivel de la UE, toda la estructura de gobernanza en materia de AML/CFT. Estas directrices especifican el papel, las tareas y las responsabilidades del responsable del cumplimiento de AML/CFT, el órgano de dirección y el alto directivo encargado del cumplimiento de la AML/CFT, así como las políticas, los controles y los procedimientos internos. Complementan, pero no sustituyen, las directrices pertinentes publicadas por las Autoridades Europeas de Supervisión sobre acuerdos de gobernanza más amplios y controles de idoneidad

Unión Europea - Organismo regulador: ESMA

- *Informe anual de 2020 sobre las sanciones por abuso de mercado de la UE* | 20-Oct-21. El informe describe un aumento en el número de sanciones y medidas administrativas en 2020 en comparación con 2019, llegando a 541 desde 279 el año anterior. Sin embargo, también constata que las sanciones económicas impuestas son significativamente menores, alcanzando solo 17,5 millones de euros en 2020, frente a los 82 millones de euros de 2019.

- *Plan de acción para una política global de la Unión en materia de prevención del blanqueo de capitales y de la financiación del terrorismo* | 13-May-20. En su Comunicación "Hacia una mejor aplicación del marco de lucha contra el blanqueo de capitales y la financiación del terrorismo de la UE" y en los informes que la acompañan, de julio de 2019, la Comisión expuso las medidas necesarias para garantizar una política global de la UE en materia de prevención del blanqueo de capitales y lucha contra la financiación del terrorismo (AML/CFT). Estas incluyen una mejor aplicación de las normas existentes, un libro de normas más detallado y armonizado, una supervisión de alta calidad y coherente, incluso mediante la atribución de tareas de supervisión específicas a un organismo de la UE, la interconexión de los registros centralizados de cuentas bancarias y un mecanismo más fuerte para coordinar y apoyar el trabajo de las Unidades de Inteligencia Financiera (UIF).

China - Organismo regulador: CBIRC

- *Medidas de supervisión y administración de la lucha contra el blanqueo de capitales y la financiación del terrorismo de las instituciones financieras* | 1-Aug-21. Con el fin de que las entidades financieras cumplan eficazmente sus obligaciones en materia de lucha contra el blanqueo de capitales y la financiación del terrorismo y de regular la supervisión y administración de esta, el Banco Popular de China formuló las Medidas de supervisión y administración de la lucha contra el blanqueo de capitales y la financiación del terrorismo (las "Medidas") de conformidad con la Ley contra el blanqueo de capitales de la República Popular de China, la Ley bancaria de la República Popular de China y la Ley contra el terrorismo de la República Popular de China.

Japón - Organismo regulador: FSA

- *Directrices para la lucha contra el blanqueo de capitales y la financiación del terrorismo* | 19-Feb-21: La Agencia de Servicios Financieros ("FSA"), con las medidas de supervisión necesarias, supervisará las medidas AML/CFT de cada Institución Financiera, compartirá los resultados con las entidades financieras y las instará a mejorar la gestión de riesgos. Las Directrices aclaran las acciones requeridas y las acciones esperadas que deben ser implementadas por cada Institución Financiera y cómo la FSA llevará a cabo la supervisión en el futuro.

India - Organismo regulador: FIU

- *Ley de Prevención del Blanqueo de Capitales* | 17-Jan-03. Ley del Parlamento de la India promulgada por el gobierno del NDA para prevenir el blanqueo de dinero y disponer la confiscación de los bienes procedentes del blanqueo de dinero.

Australia - Organismo regulador: AUSTRAC

- *Ley de informes sobre transacciones financieras (FTR) de 1988* | 16-Apr-18. La Ley FTR se introdujo para ayudar a administrar y aplicar las leyes fiscales, así como otras leyes de la Commonwealth, los estados y los territorios.

- *Ley contra el blanqueo de capitales y la financiación del terrorismo* | 12-Dec-06. Prevé medidas para detectar, disuadir e interrumpir el blanqueo de capitales, la financiación del terrorismo y otros delitos financieros graves; y proporciona a los organismos gubernamentales australianos pertinentes y a sus homólogos internacionales la información que necesitan para investigar y perseguir este tipo de delitos, los delitos constitutivos de la financiación del terrorismo y otros delitos graves.

Sudáfrica - Organismo regulador: FIC

- *Ley del Centro de Inteligencia Financiera* | 28-Mar-03. Establece el Centro de Inteligencia Financiera del país (FIC) e introduce un marco básico para alinear la normativa del país en materia de AML/CFT con la de la comunidad internacional en general. Esta ley fue reforzada por la Ley de Enmienda número 1 del Centro de Inteligencia Financiera de 2017, que introduce un enfoque basado en el riesgo para la diligencia debida con respecto al cliente.

Global - Organismo regulador: ONU

- *Convención contra la Delincuencia Organizada Transnacional y sus Protocolos* | 15-Nov-00. El objetivo de este convenio es promover la cooperación para prevenir y combatir más eficazmente la delincuencia organizada transnacional.

Global - Organismo regulador: OCDE

- *Cooperación internacional contra los delitos fiscales y otros delitos financieros* | 14-Jun-12. Este informe de la OCDE contiene una recopilación de diversas normativas internacionales sobre delito financiero.

Global - Organismo regulador: GAFI

- *Recomendaciones del GAFI 2012* | Oct-21.Las Recomendaciones del GAFI establecen un marco exhaustivo y coherente de medidas que los países deben aplicar para combatir el blanqueo de capitales y la financiación del terrorismo, así como la financiación de la proliferación de armas de destrucción masiva. Los países tienen marcos jurídicos, administrativos y operativos diversos y sistemas financieros diferentes, por lo que no todos pueden adoptar medidas idénticas para contrarrestar estas amenazas.

- *Metodología del GAFI 2013* | *Nov-20.* El GAFI lleva a cabo evaluaciones mutuas de los niveles de aplicación de las Recomendaciones del GAFI por parte de sus miembros de forma continua. Se trata de evaluaciones entre pares, en las que miembros de diferentes países evalúan a otro país. La Metodología del GAFI para evaluar el cumplimiento de las Recomendaciones del GAFI y la eficacia de los sistemas de lucha contra el blanqueo de capitales y la financiación del terrorismo establece el proceso de evaluación.

- *Procedimientos para la Cuarta Ronda de Evaluaciones Mutuas AML/CFT del GAFI* | Jan-21. El GAFI está llevando a cabo una cuarta ronda de evaluaciones mutuas para sus miembros sobre la base de las Recomendaciones del GAFI (2012), y de la Metodología para evaluar el cumplimiento de las Recomendaciones del GAFI y la eficacia de los sistemas de AML/CFT (2013), con sus modificaciones periódicas. Este documento establece los procedimientos que constituyen la base de esa cuarta ronda de evaluaciones mutuas.

- *Procesos y procedimientos consolidados para las evaluaciones mutuas y el seguimiento* | Jan-21. Los Procesos y Procedimientos Consolidados para las Evaluaciones Mutuas y el Seguimiento establecen los elementos básicos que forman la base de todas las evaluaciones y se basan en los Procedimientos para la 4ª Ronda de Evaluaciones de AML/CFT del GAFI.

Global - Organismo regulador: BCBS

- *Principios básicos para una supervisión bancaria eficaz* | Oct-06. Los países han utilizado los Principios Básicos como punto de referencia para evaluar la calidad de sus sistemas de supervisión y para identificar el trabajo futuro que debe realizarse para alcanzar un nivel de referencia de prácticas de supervisión sólidas.

- *Guías sobre la gestión prudencial de los riesgos relacionados con el blanqueo de dinero y la financiación del terrorismo (AML/CFT)* | Jul-20. Estas directrices tienen por objeto mejorar la eficacia de la supervisión de la gestión del riesgo de blanqueo de capitales y financiación del terrorismo (FT) de los bancos, en consonancia y como complemento de las metas y objetivos de las normas publicadas por el Grupo de Acción Financiera Internacional (GAFI) y los principios y directrices publicados por el Comité de Basilea.

- *Directrices actualizadas para un enfoque basado en el riesgo en relación con los activos virtuales y los proveedores de servicios de activos virtuales* | Oct-21. La Fuerza de Tarea de Acción Financiera (FATF) publicó en octubre de 2021 una serie de directrices que establecen cómo se deben aplicar las recomendaciones del GAFI en el contexto de la tecnología de contabilidad distribuida y las criptomonedas.

Tendencias y retos en la lucha contra el blanqueo de capitales y la financiación del terrorismo

"Las empresas deben aprovechar el poder de la ética, que está adquiriendo un nuevo nivel de importancia y poder "

James Joseph[44]

Existe un conjunto de capacidades que pueden considerarse dentro de un mapa de AML/CFT para las instituciones financieras, que tienen como objetivo permitir la identificación, gestión, control y supervisión de AML/CFT. Este mapa incluye (i) el marco y la gobernanza; (ii) la estructura organizativa; (iii) los procesos de negocio (incluyendo el KYC, la evaluación del riesgo del cliente, el escaneo de sancionados, así como la monitorización de transacciones o el escaneo de pagos, entre otros); (iv) la infraestructura tecnológica; y (v) la infraestructura de datos y las capacidades analíticas (ver figura 1).

Marco y gobernanza

En la base de sus programas de AML/CFT, las entidades financieras están mejorando su marco de riesgos y sus modelos de gobernanza para garantizar tanto un alcance exhaustivo como una integración efectiva en el negocio. Para ello, el marco incluye el proceso de evaluación de riesgos, el establecimiento de normas y políticas, y la garantía de una sólida gestión del riesgo a través de un modelo de tres líneas de defensa.

Evaluación de riesgos

La evaluación de riesgos es un mecanismo para comprender las fuentes de riesgo, y es uno de los componentes centrales del enfoque de una organización en materia de AML/CFT.

El proceso de evaluación de riesgos tiene cuatro componentes principales que pueden aplicarse: evaluación de riesgos contextuales, de negocio, del cliente y de terceros.

[44] James Joseph Sylvester (1814-1897) fue un matemático inglés que realizó importantes contribuciones al campo de las matrices (acuñó los términos matriz, invariante y discriminante, entre otros), así como a la teoría de los invariantes algebraicos (en colaboración con A. Cayley), a los determinantes, a la teoría de números, a las particiones y a la combinatoria.

Figura 1. Mapa genérico de las capacidades de AML/CFT en una institución financiera avanzada

Figura 2. Evaluación global de riesgos

Evaluación del riesgo contextual

El punto de partida de la Evaluación de Riesgos es un examen exhaustivo del modelo de negocio, así como del contexto en el que se desarrolla dicho negocio. Hay muchos factores que impulsan este análisis (véase la figura 2). Además, una aportación importante a este proceso es la Evaluación de Riesgos regional / local proporcionada por la autoridad reguladora correspondiente. En muchos países, la autoridad supervisora tiene el mandato de realizar una Evaluación de Riesgos exhaustiva sobre AML/CFT[45,46,47].

Evaluación del riesgo del negocio

La Evaluación de Riesgos a nivel de negocio es el mecanismo que permite a las entidades financieras evaluar, para cada parte de su negocio y dentro de él[48], dónde están los principales riesgos.

Además, la Evaluación de Riesgos en toda la organización proporciona el marco y el contexto en el que evaluar los riesgos de ML/FT en el diseño de nuevos productos, así como en las relaciones comerciales individuales, lo que permite una revisión exhaustiva de la relación a través de los diferentes factores de riesgo que afectan a la entidad.

El establecimiento de un proceso formal, la participación de los expertos en la materia adecuados en la organización y la garantía de que la evaluación de riesgos se revisa de forma continua son algunas de las prácticas del sector en las organizaciones más avanzadas[49].

Evaluación del riesgo del cliente

En el nivel más granular, las entidades financieras realizan Evaluaciones del Riesgo del Cliente individuales para analizar los riesgos que surgen en el punto de incorporación de un nuevo cliente, así como a lo largo del ciclo de vida del cliente. Esta evaluación incluirá un conjunto mínimo de factores, que los reguladores han proporcionado (por ejemplo, fuentes de riqueza y fondos o factores de riesgo específicos del país y del sector)[50,51].

Históricamente, los datos y las capacidades matemáticas dedicadas a esta evaluación han sido limitados, lo que ha provocado clasificaciones de clientes que no siempre discriminaban a los de alto riesgo, o que clasificaban de forma inadecuada a un gran número de clientes en categorías de riesgo medio o alto, con el correspondiente esfuerzo operativo requerido en la supervisión, y el impacto en la experiencia del cliente.

Como resultado, las entidades financieras han dedicado importantes inversiones para conseguir un enfoque más preciso basado en el riesgo y la gestión de este. En la actualidad, los esfuerzos se centran en simplificar la taxonomía de los modelos alineándolos con un conjunto común de familias de variables (por ejemplo, Cliente, Transacción, Canal, Producto, Región), que se utilizan de forma coherente en toda la organización, para garantizar la exhaustividad y la adecuada discriminación[52].

[45] Véase, por ejemplo, el artículo 6, apartado 5, de la (UE) 2015/849 (la cuarta Directiva de la UE contra el blanqueo de capitales), que exige a la EBA que emita un dictamen sobre los riesgos de blanqueo y financiación del terrorismo que afectan al sector financiero de la UE cada dos años.

[46] Véase el "Dictamen sobre los riesgos de blanqueo de capitales y financiación del terrorismo que afectan al sector financiero de la Unión Europea".

[47] GAFI. (2013). https://www.fatf-gafi.org/documents/documents/nationalmoneylaunderingandt e rroristfinancingriskassment.html

[48] Depende de su riesgo sectorial, de la escala de negocio, de los perfiles y la estructura de los clientes y los beneficiarios finales, de los tipos de productos y su complejidad, de los canales utilizados para la distribución o el servicio, de las transacciones y de las zonas geográficas.

[49] Este proceso permite incluir formalmente el AML/CFT en el marco de Apetito al Riesgo, ya que impulsa las actividades operativas en el negocio y las decisiones estratégicas en los comités de aprobación de nuevos productos, nuevas iniciativas de negocio (como fusiones, adquisiciones, etc.) y nuevos proyectos de transformación.

[50] EBA (2017a) https://www.eba.europa.eu/documents/10180/1890686/Final+Guidelines+on+Risk+Factors+%28JC+2017+37%29.pdf/66ec16d9-0c02-428b-a294-ad1e3d659e70

[51] FCA (2022), https://www.handbook.fca.org.uk/handbook/FCG.pdf

[52] Las entidades financieras más avanzadas ya utilizan algoritmos de aprendizaje automático y modelos de comportamiento para evaluar el riesgo del cliente. Estos algoritmos se entrenan y calibran con datos históricos y, cuando es necesario, con el juicio de los expertos, con mejoras significativas en la precisión frente a los modelos tradicionales que consideran fundamentalmente juicio experto.

Evaluación de riesgos de terceros

Por último, algunas entidades financieras dependen de terceros para ejecutar parte de sus actividades cotidianas, desde corredores e intermediarios hasta la externalización de actividades operativas, la prestación de servicios de formación, asesoramiento, infraestructura tecnológica, etc. Dependiendo de la naturaleza del negocio, estos terceros también pueden exponer a la organización al ML/FT[53] (u otra forma de delito financiero).

Por lo tanto, es una práctica común tener un enfoque totalmente integrado de la gestión del riesgo de proveedores terceros para evaluar los riesgos subyacentes de blanqueo de capitales y la financiación del terrorismo. Para ello, los equipos de compras realizan una formación específica para poder actuar como "primera línea de defensa" y realizar la evaluación integral.

Normas y políticas

Una documentación exhaustiva que especifique las normas que deben seguirse en toda la organización es uno de los pilares estratégicos de cualquier marco de AML/CFT, y uno de los mecanismos más eficaces para mitigar el riesgo.

Las organizaciones más avanzadas cuentan con los siguientes elementos:

- Una arquitectura de políticas que, partiendo de un marco de documentación, desciende progresivamente hacia normas específicas de la organización, así como hacia procedimientos e instrucciones de orientación[54].
- Mecanismos adecuados para comunicar e integrar eficazmente esas políticas en la actividad real de la organización. Esto puede incluir la existencia de un portal web en el que los empleados pertinentes puedan acceder a la documentación, junto con un programa exhaustivo de formación y concienciación y un proceso de comunicación eficaz que garantice que cualquier adición o cambio relevante en el panorama político se comunique inmediatamente en toda la organización.
- Un modelo operativo bien establecido que permita la revisión y actualización periódica de las políticas, de modo que la nueva normativa y los riesgos emergentes en el negocio o las lecciones aprendidas de los incidentes en materia de AML/CFT, se actualicen adecuada y oportunamente en los documentos, y se comuniquen a toda la organización. La alta dirección debe impulsar esta actualización y la integración efectiva de las políticas en los procesos de negocio[55].

El modelo de las tres líneas de defensa

Al igual que con otros riesgos, un modelo robusto de tres líneas de defensa (LOD) es uno de los pilares del marco de gestión de AML/CFT, ya que establece las responsabilidades para la identificación, gestión, control y supervisión de los riesgos subyacentes.

Las entidades financieras han reforzado su modelo de líneas de defensa realizando una división más granular de las responsabilidades y rendiciones de cuentas entre ellas.

[53] EBA (2017b). https://www.eba.europa.eu/documents/10180/1890686/Final+Guidelines+on+Risk+Factors+%28JC+2017+37%29.pdf/66ec16d9-0c02-428b-a294-ad1e3d659e70

[54] Cada documento contiene referencias a los riesgos a los que se refiere (conectadas a la Evaluación de Riesgos cuando es aplicable), así como a las referencias externas (regulación y legislación, orientación de la industria, etc.) que permiten el cumplimiento y la trazabilidad.

[55] EBA (2017c). https://www.eba.europa.eu/documents/10180/1890686/Final+Guidelines+on+Risk+Factors+%28JC+2017+37%29.pdf/66ec16d9-0c02-428b-a294-ad1e3d659e70

Primera línea de defensa

La primera línea de defensa es la responsable última de la identificación, gestión y control de los riesgos originados en el desarrollo de la actividad, así como del cumplimiento de la normativa interna y externa. Mantiene la relación con el cliente, lo que implica la realización de actividades básicas de KYC[56], y el seguimiento del perfil de riesgo[57]. Tambien es responsable de coordinar el *off-boarding* de clientes con el visto bueno de segunda línea.

Con el fin de garantizar la profesionalización, la normalización de las formas de trabajo y la dotación de recursos adecuada, las instituciones más avanzadas han formalizado el rol de una función o unidad de AML/CFT en la organización que apoya a los equipos de la entidad en el ejercicio de sus responsabilidades (véase la sección sobre la estructura organizativa).

Segunda línea de defensa

La segunda línea de defensa se encarga de establecer el marco de AML/CFT, emitir políticas (para adaptar la regulación externa a la realidad interna del negocio) y, finalmente, supervisar su adecuada aplicación. En la mayoría de las instituciones financieras, suele haber también un elemento de asesoramiento a la primera línea en casos complejos de incorporación y el *off-boarding* de clientes, así como en el caso de desarrollo de nuevos productos/servicios, etc.

En las entidades financieras avanzadas, la segunda línea de defensa desarrolla un plan de supervisión formal con diferentes acciones que combina la información obtenida de diferentes fuentes con el conocimiento especializado sobre el negocio y la evaluación de riesgos de toda la organización o las áreas de preocupación regulatoria. Las acciones del plan pueden incluir la emisión de nuevas políticas u orientaciones, una mayor frecuencia de información a la dirección sobre temas concretos, un mayor muestreo de casos o revisiones temáticas más "intrusivas" e inspecciones in situ especializadas.

La segunda línea de defensa también produce información de gestión e informes periódicos a los órganos de gobierno internos, para mantenerlos informados de la evolución del perfil de riesgo de la organización y de cualquier punto relevante para la escalada (por ejemplo, brechas en el entorno de control, nuevas relaciones de alto riesgo, etc.).

El responsable de la supervisión de AML/CFT suele depender de un nivel ejecutivo: Director de Riesgos, Director de Cumplimiento o Jefe de Asesoría Jurídica / Consejo General, o en su caso, un miembro del Consejo de Administración[58] o dentro de la alta dirección. Dicho funcionario designado[59] es un individuo con la responsabilidad última de la supervisión del marco y de toda la actividad asociada a AML/CFT. Esta persona y su equipo actúan como el punto central de referencia tanto para la impugnación independiente y efectiva, como para el asesoramiento en temas específicos y complejos.

Tercera línea de defensa

La tercera línea de defensa suele recaer en la función de Auditoría Interna de la organización. Al igual que el resto de riesgos, se trata de una función independiente del negocio y de la organización de riesgos, que depende directamente del Comité de Auditoría del Consejo, y que tiene la responsabilidad de evaluar y valorar la amplitud y eficacia del marco definido por la segunda línea de defensa, su nivel de adopción por parte de la primera línea y el nivel de supervisión independiente y desafío efectivo que realiza la segunda línea.

La tercera línea tiene su propio plan de auditoría independiente que parte de la información de gestión de primera y segunda línea de defensa, a partir del cual desarrolla su propio conjunto de auditorías.

Estructura organizativa

Funciones especializadas

En la última década, las entidades financieras se han visto sometidas a una intensa presión para reducir costes, dado el periodo sostenido de bajos tipos de interés al que han sido sometidas, y el impacto financiero añadido de la pandemia. Al mismo tiempo, se espera que mejoren la eficacia y la eficiencia de sus operaciones para aumentar el número de alertas productivas y la detección de intentos de blanqueo.

En términos de eficacia, existe una tendencia a profesionalizar aún más ciertas funciones dentro de la función propia de AML/CFT. Algunos ejemplos son:

1. La creación de equipos especializados de Control de Calidad / *Quality Assurance* en la primera línea de defensa, que utilizan un conjunto completo de técnicas para realizar muestreos avanzados con el fin de identificar fallos en el cumplimiento de las políticas y procedimientos y plantear recomendaciones de mejora.

2. La creación de funciones específicas de aseguramiento y supervisión en la segunda línea de defensa. En consonancia con lo expuesto anteriormente, estos equipos actúan como

[56] Por ejemplo, la recopilación, identificación y validación de la información sobre el cliente, la CDD (o la Diligencia Debida Reforzada, cuando se requiera) y la Evaluación del Riesgo del Cliente.

[57] Esto incluye la supervisión continua de las transacciones (utilizando en general modelos avanzados para detectar comportamientos atípicos y estrategias de blanqueo de capitales bien conocidas), el escaneo de los pagos con respecto a las listas de vigilancia, etc. Al igual que en el caso de la incorporación, el análisis y la eliminación de las alertas de bajo nivel suelen producirse también en negocio, y la escalada a la segunda línea sólo se produce en los casos de sospecha de verdaderos positivos.

[58] En algunas jurisdicciones se exige que la entidad designe formalmente a un miembro del Consejo de Administración o de la alta dirección como responsable último del cumplimiento de la normativa. Véanse, e.g. , las Directrices de la EBA sobre la función de los responsables del cumplimiento de la PBC/FT, EBA/CP/2021/31. Véase también The Financial Conduct Authority ML 7.1 The money laundering reporting officer

[59] El funcionario designado no se considera necesariamente una función formal. Por ejemplo , en la normativa del Reino Unido, reconoce la función de un "funcionario designado", al igual que la función de un funcionario encargado de informar sobre el blanqueo de capitales (ambas funciones pueden recaer en la misma persona, véase el Manual de la Autoridad de Conducta Financiera).

una capa de ejecución del plan de supervisión y realizan inmersiones profundas en forma de trabajos de revisiones detallados y especializados sobre temas específicos.

3. La creación de equipos de análisis de AML/CFT. Suelen incorporar otros sub-riesgos además del AML/CFT (por ejemplo, fraude) y suelen ser equipos muy orientados al negocio, que identifican cualquier nueva tendencia en el mercado.

4. La creación de capacidades especializadas en torno al cambio y la evolución en la empresa. El efecto combinado de los múltiples niveles de control y supervisión se traduce en un conjunto de recomendaciones, emitidas por los equipos de control de calidad, los equipos de auditoría interna y las revisiones de supervisión.

Centralización y creación de centros de excelencia

En relación con la búsqueda de una mayor eficiencia en las operaciones, varias grandes entidades financieras han tirado de la palanca de la centralización de algunas de las actividades operativas dentro de sus equipos de AML/CFT, creando centros de excelencia. Algunas de las actividades operativas que se han centralizado son la Diligencia Debida del Cliente, que incorpora las comprobaciones y controles en torno al KYC, la realización de la Evaluación del Riesgo del Cliente, etc[60]. Estos equipos suelen tener una especialización por *Retail* y *Corporate*, para dar cuenta de las diferencias en los procesos KYC / KYB *(Know Your Business)*. Algunas Instituciones tienen un equipo especializado en KYS *(Know your Supplier)* y realizan el AML/CFT así como la evaluación de Fraude y anti-soborno y corrupción (ABC, *Anti Brivery and Corruption*) de sus Proveedores en un solo equipo.

Para los grandes grupos financieros internacionales, una evolución natural en su camino de centralización ha sido la regionalización de las actividades (es decir, la creación de centros de excelencia a nivel regional), con los correspondientes beneficios en términos de mejor gestión del conjunto de recursos, eliminación de duplicidades, racionalización de la estructura organizativa y mejores trayectorias profesionales y oportunidades de formación cruzada para la plantilla.

Aunque la externalización de algunas de las actividades operativas es una opción, hay una serie de factores que empujan a algunas entidades financieras a retomar las capacidades externalizadas y a desarrollar los conjuntos de habilidades dentro de la organización. Algunos de los factores son la creciente demanda de regulación en torno a las actividades subcontratadas que son críticas para la organización, la necesidad asociada de crear sólidas estructuras de supervisión y control en torno a los servicios subcontratados, el nivel de excelencia operativa que esperan las diferentes partes interesadas o el impacto reputacional de los fallos operativos.

[60]Existen otros ejemplos como: la ejecución del escaneo de nombres y el mantenimiento asociado de las listas de vigilancia; la realización de la supervisión de las transacciones (como en el caso de la CDD, con una división natural entre minoristas y empresas); la ejecución del escaneo de pagos; los procedimientos operativos asociados a las salidas de los clientes; la producción de información de gestión e informes estandarizados y algunas de las actividades especificadas anteriormente, incluyendo la *Quality Assurance*, el cambio y la corrección o el análisis de datos.

Enfoque integrado para la gestión del riesgo de delitos financieros.

Algunos de los casos recientes más complejos de delitos financieros implican una combinación de robo de credenciales y suplantación de identidad, uso ilícito de acceso privilegiado para cometer un fraude y múltiples mecanismos para blanquear los beneficios.

En este sentido, una tendencia común en algunas de las entidades financieras más avanzadas, según la recomendación regulatoria[1], consiste en lograr una convergencia hacia un modelo de Gobernanza unificado que incorpore todos los subtipos de riesgo (blanqueo de capitales, financiación de terrorismo, evasión fiscal, fraude y ciberdelincuencia) en un único marco.

Las sinergias naturales que surgen al abordar los diferentes subtipos de riesgo del delito financiero bajo un modelo unificado y la consiguiente oportunidad de eficiencia explican la adopción de este modelo:

- Hay un fuerte análisis de un nuevo cliente en el punto de origen de la relación, con una cantidad significativa de información común que abarca la identificación del cliente, la validación, el escaneo en listas, las evaluaciones de riesgo del cliente, etc.
- Existe un componente de seguimiento continuo, también con conjuntos de datos superpuestos en torno a la información sobre transacciones y pagos, que pueden fusionarse en un único repositorio de datos para su explotación.
- Por último, hay una investigación que requiere capacidades de herramientas de flujo de trabajo, un sólido mantenimiento de registros, documentación e informes.

En las grandes entidades financieras existe un cierto nivel de integración. Sin embargo, todavía hay margen de mejora para lograr la plena integración. Algunas de las mejores prácticas del sector son:

- Un marco único para la identificación, gestión y control de los riesgos, incluye una taxonomía de riesgos común a todos los tipos de riesgo, una autoevaluación de riesgos y controles común, etc.
- Infraestructura de datos subyacente común, con el objetivo de obtener una única "visión 360" del cliente y sus datos, junto con su transaccionalidad.
- Marco común e infraestructura tecnológica para la aplicación y detección de alertas, así como para su gestión.
- Organizaciones centralizadas, que incentivan el intercambio de información y un enfoque holístico de la propiedad y la gestión del riesgo, sin lagunas que los delincuentes financieros puedan aprovechar.
- Centros operativos de excelencia capaces de proporcionar capacidades operativas en los diferentes tipos de riesgo, con recursos con formación transversal capaces de gestionar esos casos.

Teniendo en cuenta el importante número de personas operativas que actualmente se encargan de la identificación y gestión de los diferentes equipos de delito financiero, y el enfoque natural de silos con el que fueron creados originalmente, las oportunidades de este viaje hacia la integración en términos de eliminación de la duplicación, el aumento de la eficiencia y la eficacia son especialmente significativas.

[1]Véase e.g. See FCA's A firm's guide to countering financial crime risks, https://www.handbook.fca.org.uk/handbook/FCG.pdf

Planificación de recursos humanos y competencias

Las entidades financieras más avanzadas han sido capaces de conectar su ambición en torno a AML/CFT, tal como se refleja en su estrategia y apetito al riesgo, con las necesidades de su personal. En esos casos, hay un análisis exhaustivo que:

i. Comienza con la Evaluación de Riesgos de toda la compañía, el crecimiento previsto de la organización y los cambios en el perfil de riesgo y las iniciativas estratégicas que se espera que cambien la forma de trabajar.

ii. Realiza una proyección informada de la capacidad necesaria para abordar la estrategia de AML/CFT[61]. Algunas de las mejores prácticas del sector implican la creación de modelos de dimensionamiento para que los equipos operativos puedan conectar, a nivel operativo, la demanda de capacidad con la oferta.

iii. A continuación, se diseña y aplica una estrategia para garantizar la existencia de dicha capacidad. Esto incluye la formación o el reciclaje del personal existente y la contratación de nuevos talentos.

En los últimos años, los ejercicios de planificación de la plantilla en algunas de las organizaciones más avanzadas han identificado la necesidad de reforzar los equipos con:

1. Perfiles cuantitativos y analíticos capaces de entender el negocio y los riesgos subyacentes y construir modelos matemáticos con técnicas de *machine learning*.
2. Conocimiento de las nuevas tecnologías de pago especializadas, incluidas las criptomonedas.
3. Personas polivalentes capaces de capitalizar la experiencia previa en diferentes subtipos de riesgo dentro del ámbito del delito financiero, que se convierten en expertos en materia de AML/CFT.

Procesos empresariales

Las entidades financieras han dedicado mucho tiempo y esfuerzo a racionalizar los procesos empresariales asociados a AML/CFT. La presión para reducir los costes y mejorar la eficiencia ha abierto la puerta a las tecnologías de automatización avanzadas, las plataformas de gestión de procesos empresariales y la modelización avanzada. Además, estas mejoras también tienen un impacto positivo en la experiencia del cliente, en "pedir las cosas una única vez", etc. Procesos como el de KYC se han simplificado y reforzado considerablemente.

KYC: Evaluación del riesgo, diligencia debida con el cliente y diligencia debida reforzada

Los canales de distribución han pasado de un modelo centrado en las sucursales a otro de autoservicio no presencial, fomentado por las tecnologías habilitadoras, las instituciones que persiguen la reducción de costes y la pandemia de COVID-19. La gestión digital del riesgo del cliente pasa de ser un factor penalizador a convertirse en el medio habitual de gestión, lo que exige un control más estricto de la comunicación banco-cliente. Desgraciadamente, a las entidades financieras les resulta más difícil verificar con quién están haciendo negocios y los propósitos reales de las relaciones comerciales. Las nuevas tecnologías y los procedimientos modernos permiten a las entidades financieras mitigar su exposición al blanqueo de capitales y la financiación del terrorismo mediante la mejora de los mecanismos de diligencia debida. No obstante, algunas de estas mejoras también se han vuelto extenuantes para el cliente debido a las constantes solicitudes de documentación, a menudo en papel y sin alternativa digital.

Las soluciones automatizadas de autoservicio[62] a través de canales digitales, accionables por el usuario, utilizando una identificación digital y datos biométricos, capacitan a los clientes durante el proceso de incorporación, las revisiones periódicas y la recertificación. Además, facilita el mantenimiento de registros automatizados de asistencia al cliente durante el proceso de diligencia debida, que puede ser determinante en un posible proceso de investigación. Asimismo, la identificación digital y los datos biométricos contrarrestan el fraude de identidad.

Estas soluciones de autoservicio reconocen la distribución de los clientes por segmentos, definidos y calculados por los departamentos de Cumplimiento Normativo con el apoyo de técnicas de IA. Como resultado, la segmentación de clientes puede mejorar la captura de información KYC con la ayuda de cuestionarios dinámicos de incorporación. En consecuencia, es fundamental perfeccionar el ciclo de desarrollo de la trayectoria del cliente, para garantizar una rápida comercialización de las nuevas mejoras en el proceso de KYC y adaptarse con agilidad a las nuevas normativas.

Las políticas y procedimientos de KYC deben revisarse periódicamente para mitigar el riesgo y aumentar la inclusión financiera. En este sentido, algunos ciudadanos no pueden abrir cuentas bancarias o acceder a ayudas públicas por la dificultad de reunir la identificación requerida. De ahí que las entidades financieras deban evitar las medidas de CDD rígidas y de marcado de casillas y apostar por las evaluaciones de comportamiento y contextuales.

Supervisión continua (monitorización de transacciones, escaneo de sanciones, escaneo de pagos)

La monitorización de las transacciones es un proceso muy pesado[63]. La agregación de todas las transacciones, cuentas y clientes para calcular la probabilidad de cada escenario requiere grandes cantidades de capacidad de cálculo y memoria. El análisis coste-beneficio es un tema controvertido entre los departamentos de Cumplimiento Normativo. Los sistemas heredados pueden mejorarse para hacer frente a las demandas de rendimiento, pero hay una necesidad creciente de

[61] Esta capacidad se articula en términos de número de personas, conjuntos de habilidades y experiencia, ubicaciones, etc.
[62] Véase la Guía de la EBA sobre el uso de soluciones de incorporación de clientes a distancia. https://www.eba.europa.eu/regulation-and-policy/anti-money-laundering-and-countering-financing-terrorism/guidelines-use-remote-customer-onboarding-solutions
[63] Autoridad Bancaria Europea (2021).

Elementos de la gestión de recursos humanos

Cultura y comportamientos

La cultura corporativa se refiere a las creencias e ideas que tiene una compañia y la forma en que afectan a su forma de hacer negocios y a la manera en que se comportan sus empleados [Diccionario de Cambridge].

La cultura, las formas de trabajar y los comportamientos del personal han sido identificados en varias revisiones temáticas y acciones de aplicación de la ley iniciadas por supervisores, reguladores y agencias nacionales como una de las causas fundamentales de las deficiencias en el marco de AML/CFT.

Por esta razón, las entidades financieras que tienen programas avanzados de AML/CFT tienden a incorporar una ambiciosa cultura, destinada a incorporar los comportamientos correctos en la conducción de los negocios. Algunos de los componentes del marco cultural de la organización incluyen capacidades en torno a los siguientes elementos:

Contratación y selección de personal

Antes de su incorporación, las personas que vayan a tener alguna responsabilidad asociada a AML/CFT (tanto el personal interno como un tercero) deben pasar por un proceso de investigación, para validar en la medida de lo posible que tienen la ética de trabajo y la integridad adecuadas, y que no hay nada en sus antecedentes que los exponga como objetivos de la delincuencia organizada[1].

Formación y certificación

Los programas de formación y concienciación incluyen cursos genéricos para todos los empleados del banco, formación específica para la función de lucha contra el blanqueo de capitales y formación para los miembros del Comité Ejecutivo y del Consejo de Administración, que abarcan toda la gama de delitos y estrategias delictivas que son pertinentes para la organización[2].

Compromiso de la dirección

La alta dirección desempeña un papel fundamental en la integración de la cultura. En las entidades financieras avanzadas, las personas que están cerca de los niveles operativos de ejecución del marco de riesgo se sienten seguras al plantear cuestiones y preocupaciones relacionadas con la actividad empresarial, y estas denuncias se tratan de forma anónima y diligente. Existen mecanismos de denuncia y los empleados los utilizan regularmente para plantear preocupaciones o debates constructivos en los foros de toma de decisiones.

A nivel del Consejo, en las entidades financieras avanzadas, los miembros del Consejo tienen tanto el conocimiento como la información de gestión para entender los riesgos de ML/FT y realizar un desafío efectivo a las funciones ejecutivas.

Incentivos y medición de resultados

Los mecanismos de incentivos y remuneración deben estar alineados con los comportamientos deseables de la plantilla y con un adecuado cumplimiento de las responsabilidades individuales según el modelo de gobierno de la organización. Además, el sistema de incentivos no debe fomentar la asunción de riesgos inaceptables que estén por encima del apetito de la compañía.

Las entidades financieras más avanzadas cuentan con un mecanismo de fijación de objetivos que incorpora indicadores clave de riesgo y de rendimiento asociados a AML/CFT, que son cuantificables, así como indicadores cualitativos que reflejan los comportamientos deseados.

Comunicaciones

Como uno de los mecanismos para propagar la cultura y aumentar la concienciación entre el personal, algunas entidades financieras construyen sólidos programas de comunicación en torno a su marco de AML/CFT. Estos programas se llevan a cabo como campañas de comunicación profesionales, con una clara segmentación de la audiencia, la selección de los contenidos que se dirigen a cada segmento de la audiencia, el canal de entrega, etc.

[1]Las instituciones más avanzadas cuentan con un proceso de investigación a medida para las diferentes funciones dentro de la organización, incluyendo diferentes niveles de antigüedad y responsabilidad, así como diferentes riesgos a los que estarán más expuestos dependiendo de su función (por ejemplo, clientes de cara al público, unidad de investigación financiera, especialista en segunda línea de defensa, etc.).

[2]Los programas de formación pueden incluir un proceso de revisión y mejora continua. Además, hay responsabilidades específicas para revisar formalmente los materiales de formación a fin de incorporar las nuevas evoluciones de la política interna y el panorama normativo, los riesgos emergentes, las nuevas publicaciones normativas, etc. También hay programas de certificaciones del sector, que pueden estar relacionados con las trayectorias profesionales y los incentivos para el desarrollo de la carrera.

tecnologías de vanguardia con mayor capacidad provisionada a medida que se integran más datos en los modelos.

Una configuración para aumentar el rendimiento sin inversión en infraestructura es la ejecución de escenarios basados en la segmentación de clientes, en lugar de ejecutar todos los escenarios para todos los datos disponibles. Esto se armoniza con un enfoque basado en riesgos, porque los escenarios se personalizan para adaptarse al perfil de riesgo de la institución y a la realidad del negocio (clientes, geografía, catálogo de productos, etc.). Otra opción para aumentar la eficiencia sin asignación de recursos adicionales es la simulación del rendimiento (número de alertas, falsos positivos, falsos negativos, etc.) en un entorno sandbox antes de desplegar el escenario en producción. Una tercera opción es ejecutar los escenarios solo contra clientes susceptibles al riesgo, omitiendo, por ejemplo, los organismos gubernamentales y públicos con un riesgo muy bajo. Por otra parte, los posibles vinculos con entidades o personas sancionadas podrían identificarse a través de un proceso batch de escaneo sobre la cartera completa de clientes, considerando a estos como individuos de alto riesgo que deben ser investigados.

Los procesos de negocio en torno a las sanciones han sufrido una importante transformación en los últimos meses, como consecuencia de la invasión rusa de Ucrania, y las acciones legislativas asociadas que tomaron la Unión Europea, Estados Unidos, el Reino Unido[64] y otras geografías. Las entidades financieras han invertido recursos tanto en la interpretación de las restricciones como en mejoras operativas en la gestión de las listas. En algunos casos, esto ha supuesto una aceleración de los programas destinados a implementar una Plataforma de Gestión de Listas Centralizada que agrega los archivos de los diferentes departamentos de tesorería y proveedores, limpia los datos y luego los difunde entre todas las entidades del grupo de acuerdo con su normativa local y la política del grupo, elimina duplicidades y aumenta la supervisión del programa de Sanciones[65].

El escaneo transaccional[66] y el escaneo de nombres de clientes durante la incorporación se ejecutarán en tiempo real. Por lo tanto, se requieren acuerdos de nivel de servicio (SLA) estrictos para la carga de listas, ya que la mayoría de los sistemas no pueden escanear durante la actualización de las listas. Por otro lado, cuando se actualizan las listas negras o grises, se requiere un escaneo batch a todos los registros de clientes contra los cambios en las listas. Este proceso no debe interferir con los procesos en línea y debe ejecutarse en una cola separada, ya que los cambios en las listas son muy frecuentes, incluso varias veces a la semana, y consumen mucho tiempo, dado el elevado número de registros de clientes.

Gestión e investigación de alertas

La implementación de una solución de un proveedor especializado por módulo, y a veces más de una herramienta por módulo de diferentes proveedores, aísla las alertas, ya que los sistemas de gestión de casos no están integrados. Además, los responsables de cumplimiento no tienen acceso a todos los datos y sus procedimientos pueden variar en función de su herramienta. Para obtener una visión holística del riesgo del cliente y estandarizar la investigación de las alertas y la elaboración de informes, es indispensable consolidar los datos de KYC, Escaneo, Monitorización de Transacciones y Gestión de Alertas y Casos en una única plataforma. La consolidación de la información básica necesaria para una investigación antes de que se asigne la alerta mejora el tiempo por alerta, además de las notificaciones automáticas a la función de cumplimiento cuando una alerta está pendiente de autorización.

Los modelos basados en *machine learning* son útiles para puntuar las alertas, con el fin de discriminar los posibles falsos positivos. A continuación, el departamento de Cumplimiento debe haber establecido un flujo de trabajo claramente definido y objetivo para la revisión de las alertas, con un criterio de priorización para analizarlas[67].

Compromiso con las fuerzas del orden e informes de actividades sospechosas

Incluso si la detección de riesgos se lleva a cabo con éxito, una mala presentación de informes podría alterar el proceso. Las entidades financieras deben cumplir los acuerdos de nivel de servicio previstos por su UIF, adaptando sus informes a un formato específico que está sujeto a cambios. Algunos pasos normativos que no requieren una intervención manual, por ejemplo, los informes sobre transacciones monetarias (CTR) de

[64] Véanse la Ley de Delitos Económicos (Transparencia y Ejecución) de 2022 (la Ley ECTE) en el Reino Unido, las preguntas frecuentes 1007 y 1010 de la OFAC, o los hasta ocho paquetes de sanciones impuestas por la UE a personas y empresas rusas.

[65] Las plataformas de sanciones necesitan reglas personalizadas para evitar el escaneo de valores irrelevantes (apartado de correos, #, dobles espacios...).

[66] Además del análisis de las transferencias de dinero, la huella digital es un método de uso creciente para identificar alertas rojas. Las direcciones IP recogidas durante las operaciones de los clientes, asociadas a las transacciones y a los inicios de sesión, se supervisarán de forma rutinaria y se compararán con las ingeridas durante el onboarding para detectar el uso indebido de una cuenta desde un país de alto riesgo/sancionado o el robo de cuentas. La detección de direcciones IP asociadas a Tor es fundamental, ya que podría revelar conexiones entre el cliente y los delincuentes de la darknet.

[67] Por ejemplo, en función de los perfiles de riesgo, el importe de las transacciones o las puntuaciones de coincidencia. Este proceso sólo es posible si lo llevan a cabo equipos especializados en AML para encargarse de la investigación de organizaciones complejas y gestionar las listas blancas.

aplicación en Estados Unidos, dejan margen para la automatización. Al mismo tiempo, la detección proactiva de las exenciones de los CTR es una mejora rápida de la función. No obstante, la dirección de la lucha contra el blanqueo de capitales debería revisar periódicamente el proceso de toma de decisiones de las excepciones para ganar en control y comprensión.

La comunicación con las líneas de negocio, que tienen un contacto directo con los clientes, exige canales dinámicos para resolver las dudas y transferir la documentación dentro de los plazos establecidos por el regulador, aplicando penalizaciones a los gestores de cliente en caso de que se repitan con frecuencia los errores en la recogida de información de los clientes. Por último, los avisos repetidos y los fundamentos de los informes rechazados exigen la detección y el perfilado de los datos para comprender la causa raíz y paliarla. Es importante asegurar la calidad de los datos entre las plataformas de los sistemas de ATMs y las bases de datos de los bancos con la información de los clientes previamente registrada, así como identificar errores y duplicidades de la información antes de presentarla al regulador.

Información y datos de gestión

Información sobre la gestión

La información de gestión sobre AML/CFT permite medir, visualizar, comunicar y gestionar eficazmente los riesgos subyacentes. En este sentido, las mejores prácticas del sector incluyen la adopción de normas del sector en torno a la gobernanza de los datos y las prácticas de gestión e información (por ejemplo, BCBS 239[68]).

La información de gestión producida debe detallar los cambios en la Evaluación de Riesgos a nivel de toda la organización, así como una representación de los riesgos asociados a las nuevas relaciones comerciales (incluyendo las nuevas relaciones comerciales por categoría de riesgo, cualquier nueva relación de alto riesgo, etc.). En el caso de las relaciones existentes, la alta dirección de la organización debe recibir información oportuna sobre los resultados de las actividades de supervisión en curso (por ejemplo, la supervisión de las transacciones, el control de los pagos, las revisiones periódicas de los clientes), así como el resumen de los informes de actividades sospechosas (*suspicious activity reports*, o SAR) y las estadísticas sobre los resultados positivos por encima y por debajo de un umbral específico. La estructura de los informes también debe contener la salida de las relaciones existentes, y su justificación.

En particular, las Entidades financieras más avanzadas incorporan, en los informes al Consejo, a los Comités delegados del Consejo y a los Comités Ejecutivos, un amplio conjunto de métricas e información cualitativa para garantizar que se tengan en cuenta todos los riesgos subyacentes asociados al negocio. Además, para los equipos más operativos, las instituciones han desarrollado cuadros de mando que contienen métricas KPI y KRI en tiempo real, con la opción de extraer información sobre los datos con más detalle para facilitar la identificación de los puntos débiles del proceso y elaborar estrategias a largo plazo.

Otras buenas prácticas del sector incluyen la incorporación, en la información de gestión periódica que se eleva a la alta dirección, de los problemas abiertos a nivel de cartera declarados por el Control de Calidad, la Auditoría Interna o la acción de investigación de la Supervisión[69]. Esta visión también se superpone, sobre la acción correctiva, a la información sobre la transformación estratégica de las operaciones de AML/CFT y proporciona de esta manera una visión única del cambio en toda la disciplina.

Gestión y calidad de los datos

Los datos han sido una de las áreas clave de evolución e inversión de las entidades financieras en los últimos años. Se reconoce que la insuficiencia o la mala calidad de los datos[70] es uno de los factores más relevantes que afectan a la capacidad de una institución financiera para identificar, gestionar y controlar los riesgos asociados a ML/FT. Además de la clásica corrección manual de la calidad de los datos, las entidades están haciendo un uso extensivo de técnicas avanzadas para el descubrimiento de datos, así como de métodos analíticos como la lógica difusa o el procesamiento del lenguaje natural para realizar el cotejo y la armonización de los datos.

Hay varias capacidades de gestión de datos que apoyan a las funciones de AML/CFT que son fundamentales. Una de ellas es la capacidad de calidad de datos para especificar proactivamente las reglas de negocio y los estándares de calidad de datos en torno a los elementos de datos críticos

[68] Comité de Basilea (2013a). https://www.bis.org/publ/bcbs239.pdf
[69] En las organizaciones más avanzadas, los informes a la alta dirección incluyen una sección sobre el enlace con la normativa o el compromiso con la industria. Suele contener un elemento de exploración del horizonte en busca de nuevas normativas o requisitos legales (y el impacto descendente previsto en la organización).
[70] Comité de Supervisión Bancaria de Basilea (2013b).

utilizados en la identificación y gestión de riesgos. También, un Catálogo de Datos que permita la armonización de los datos en diferentes repositorios y motores y permita a los administradores de datos comprender mejor el significado empresarial de los datos, clasificar los datos recogidos y consumidos en cada proceso y alertar a las partes interesadas apropiadas en caso de un problema de datos. Además, las entidades financieras están invirtiendo mucho en capacidades de linaje de datos para permitir la trazabilidad de los datos de principio a fin, desde el punto de uso hasta el punto de origen.

Incluso la detección automática de los sistemas AML/CFT más avanzados no son fiables si los datos son erróneos. Las reglas de calidad implementadas en los sistemas transaccionales y de *front-office* garantizarán la generación correcta de datos y las reglas de consistencia confirmarán que los datos correctos se introducen en los sistemas de AML/CFT.

Infraestructura de datos y exigencias de un modelo de datos de AML/CFT

La necesidad de información de gestión implica una exigente infraestructura de datos[71]. Es deseable capturar, almacenar, procesar y gestionar la información sensible con los más altos estándares. Los módulos tecnológicos utilizados para AML/CFT pueden sobresalir por sus capacidades analíticas, pero la duplicación de los flujos de datos hacia diferentes componentes tecnológicos aislados es muy ineficiente desde el punto de vista de la transmisión.

Por esta razón, es importante contar con un único repositorio de datos al que tengan acceso todos los componentes tecnológicos y los procesos de negocio implicados en el marco de AML/CFT. De este modo, cada proceso (por ejemplo, la calificación del riesgo del cliente, las alertas, los resultados de los casos, los SAR, etc.) utiliza los datos del repositorio central y almacena sus resultados, poniéndolos a disposición de otros procesos y de los diferentes implicados al instante. Las entidades financieras que operan en varios países pueden centralizar sus herramientas y repositorios para regiones enteras o incluso a nivel mundial. Estas soluciones mejorarán la supervisión del cumplimiento normativo y reducirán los costes en la duplicación de departamentos en las Entidades del Grupo, licencias de proveedores o infraestructura.

Aprovechar las fuentes precisas de información externa para complementar la información interna disponible es una tendencia en la mayoría de las instituciones financieras.

Sin embargo, las entidades financieras ya no pueden obtener por sí mismas toda la información necesaria para identificar y evaluar adecuadamente los posibles riesgos inherentes a su actividad. En un sector centrado en lo digital, los datos acumulados pueden venderse o compartirse con otras partes. Por ello, las fuentes externas, como las oficinas de reputación, los organismos nacionales de lucha contra la delincuencia, las sentencias judiciales y los registros públicos, son fuentes recomendables para el enriquecimiento del modelo.

Las tecnologías disruptivas, el comportamiento moderno de los clientes y las catástrofes mundiales exigen que las entidades financieras rediseñen sus estrategias de supervisión de las transacciones. Los modelos poco entrenados en las nuevas técnicas de AML/CFT no proporcionan la capacidad de responder rápidamente al riesgo de la delincuencia financiera. En consecuencia, ciertos escenarios deben ejecutarse automáticamente cuando se producen determinados acontecimientos externos (nuevos productos, cierres, catástrofes, conflictos, etc.).

El análisis histórico es una práctica clave en estos casos. Incluso si la institución financiera pasa por alto algún escenario durante una crisis, se pueden encontrar banderas rojas contra estos escenarios temporales y presentar los SAR. La monitorización del comportamiento es una de las tendencias actuales del sector, apoyada por las técnicas de *machine learning* más novedosas. La supervisión del comportamiento define en primer lugar cómo se espera que se utilicen los productos y servicios. En segundo lugar, examina el comportamiento histórico, el comportamiento esperado, el comportamiento del grupo de pares e identifica los cambios de comportamiento, consumiendo todos los datos disponibles para detectar el riesgo de delitos financieros.

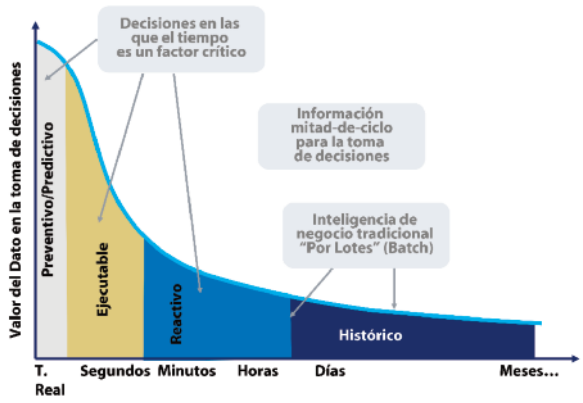
En el ámbito de la gestión de casos, el amplio uso de las redes sociales vuelve a exigir la ingestión de datos no estructurados y el uso de gráficos para encontrar posibles conexiones entre clientes y delincuentes. Por último, las plantillas estandarizadas para la presentación de informes que utilizan herramientas de agrupación de datos, que combinan conjuntos de datos procedentes de múltiples fuentes, y la generación automatizada de SAR se adaptarán a cualquier cambio de formato requerido por las UIF, reduciendo los rechazos.

Infraestructura tecnológica

Las herramientas AML/CFT ya no pueden depender únicamente de un *Data mart* relacional como base de datos central, ya que ahora se reciben datos no estructurados en los que las bases de datos NoSQL y los *Data Lakes* resultan más eficaces. Es de suma importancia implementar tecnologías de detección en tiempo real para prevenir los riesgos asociados a errores inadvertidos y mejorar la experiencia del cliente (ver figura 3). Las entidades financieras siguen confiando en los sistemas de gestión de colas y archivos para enviar transacciones y notificaciones entre aplicaciones. El escaneo transaccional y de nombres (o los casos ajenos a AML/CFT, como la detección de audio de fraude) se benefician del análisis en tiempo real. Para esto último, las librerías de *machine learning* para el Procesamiento del Lenguaje Natural (NLP) son apropiadas para recoger, analizar y almacenar la información de audio y crear alertas a las líneas de negocio que interactúan con el cliente, finalizando la llamada inmediatamente para evitar compartir cualquier información personal.

[71] Comité de Supervisión Bancaria de Basilea (2013c).

Figura 3. Reducción del tiempo de valor de los datos para la toma de decisiones



Source: Perishable insights, Mike Gualtieri, Forrester.

Las mejoras de los datos en tiempo real y no estructurados se traducen en picos de actividad de transmisión, procesamiento y almacenamiento, con importantes inversiones en nuevas opciones de almacenamiento y migración de datos. Por este motivo, la migración a una infraestructura en la nube es una solución sólida para acceder a las nuevas características de la gestión de datos.

En lo que respecta a la detección de direcciones IP, las entidades financieras deben coordinarse entre ellas y los reguladores para sistematizar la generación de listas que contengan direcciones IP no fiables, direcciones IP de jurisdicciones sancionadas o direcciones IP señaladas como sospechosas. Paralelamente, existen en el mercado herramientas analíticas para detectar si los clientes están utilizando una Red Privada Virtual (VPN) para distorsionar su ubicación real. Las *interfaces* de programación de aplicaciones (API) juegan un papel importante en esta nueva monitorización, ya que sus registros deben capturar datos de IP que pueden ser analizados en tiempo real, empleando herramientas como AWS OpenSearch o Splunk.

La automatización a través de procesos robóticos (RPA) es una de las principales tendencias tecnológicas que aumenta la experiencia del cliente a través de soluciones automatizadas de autoservicio. Los agentes virtuales, los *chat-bots* y los *call-bots* pueden asistir a los clientes con consultas estructuradas y repetitivas día y noche sin interrupción, poniéndolos en contacto con un recurso humano para las consultas que son más complejas. Los RPA son también una mejora crucial para la gestión de alertas y casos, ya que estos algoritmos pueden ingerir más datos de más fuentes con mayor rapidez que un investigador humano, lo que permite un análisis más rápido de una base de pruebas más amplia y, en última instancia, una resolución más precisa[72].

[72]Por ejemplo, la recopilación y agregación de los datos necesarios para una investigación ahorra tiempo al responsable de la lucha contra el blanqueo de capitales en la búsqueda de documentación. Otras tareas repetitivas son susceptibles de ser automatizadas, por ejemplo, marcar las alertas duplicadas de un mismo cliente. Los sistemas más sofisticados automatizarán los pasos o resultados basados en investigaciones y resultados anteriores.

Algunos ejemplos de requisitos y prácticas en materia de datos

Algunas jurisdicciones, como la de la UE (por ejemplo, el eIDAS), exigen a las entidades financieras de cualquier Estado miembro a que capturen y gestionen las identificaciones electrónicas a efectos de AML/CFT, lo que se espera que reduzca los costes y los errores humanos con una mejor experiencia del cliente. Esto es importante para los servicios fiduciarios, que se consideran de mayor riesgo debido a su estructura, ciclos de vida cortos y fines variados.

En este sentido, durante cualquier relación comercial, las entidades financieras recopilan información de geolocalización y direcciones IP para detectar posteriormente la actividad desde lugares no deseados o el robo de cuentas. Una sólida capacidad de integración de datos conecta correctamente los diferentes campos con las preguntas que aparecen en los cuestionarios dinámicos, segmentando así al cliente. FinCen[1] recomienda incluso recoger el IMEI *(International Mobile Equipment Identity)* es un número de identificación único de 15 dígitos que se asigna a cada teléfono móvil, y el modelo de dispositivo del teléfono móvil del cliente para las operaciones con moneda virtual convertible. Las entidades financieras almacenan sus interacciones digitales con los clientes desplegando bases de datos semiestructuradas y no estructuradas.

Como se ha mencionado, las entidades financieras tienen que integrar información de fuentes externas para enriquecer sus modelos. Parte de esta información es fácil de ingerir, como la marca del beneficiario final en los registros públicos o los registros de una lista PEP. Por el contrario, los registros de noticias negativas pueden incluir formato de audio o vídeo, lo que de nuevo pone de manifiesto la demanda de información no estructurada. Además, algunas jurisdicciones exigen mecanismos automatizados para informar de cualquier desajuste entre los registros públicos y los datos recogidos por las entidades obligadas.

En cuanto a las listas de control, también hay algunas buenas prácticas del sector que merece la pena destacar. Las listas negras no deben modificarse, salvo para su enriquecimiento y agregación, mientras que las listas blancas y grises deben ser actualizadas rápida y fácilmente por los departamentos de Cumplimiento para mejorar el rendimiento y cumplir con las políticas internas. Esta perspectiva debe reflejarse a la hora de construir un sistema de gestión de listas centralizado conjuntamente con notificaciones automáticas cuando se reciben, agregan y difunden las listas. Las estadísticas sobre el recuento de registros deben estar disponibles y el sistema debe esperar una notificación automática de los sistemas de detección, informando de los mismos recuentos de registros de listas cargados en sus bases de datos.

Aparte de eso, en 2018, la OFAC incluyó las primeras direcciones de monedas virtuales en la lista SDN *(Specially Designated Nationals and Blocked persons)*. Se trata de carteras digitales vinculadas a personas y empresas sancionadas con las que se prohíben los negocios, cuya estructura es la descrita.

A medida que más jurisdicciones incluyen listas de activos virtuales prohibidos, las entidades financieras deben escanear contra estas durante las transacciones de moneda virtual.

Una de las tendencias más relevantes del sector es la adopción de la norma ISO20022 en los pagos SWIFT, que mejora el rendimiento de la detección y el control al incluir etiquetas XML. En contraste con los actuales mensajes de formato libre, los pagos SWIFT especificarán claramente el significado de los campos, reduciendo los falsos positivos. Las entidades financieras deben actualizar sus sistemas de detección y control para analizar estas nuevas etiquetas y almacenarlas en las tablas y columnas adecuadas de sus bases de datos.

Referencia de nuevas etiquetas XML de información en transacciones SWIFT

Digital Currency Address	XBT	158treVZBGMBThoaympxccPdZPtqUfYfT9
SDN list column	Currency	Wallet ID

[1]La Red de Aplicación de los Delitos Financieros de EE.UU. pretende salvaguardar el sistema financiero del uso ilícito, combatir el blanqueo de capitales y sus delitos conexos, incluido el terrorismo, y promover la seguridad nacional.

Modelización analítica y técnicas avanzadas para el AML/CFT

"Un modelo resulta siempre parcial, pero ofrece recursos para progresar en el conocimiento"
Jean-Pierre Changeux[73]

En esta sección se describen algunas de las tendencias y prácticas más innovadoras del sector basadas en la modelización analítica y en técnicas avanzadas para la identificación, gestión, control y supervisión del blanqueo de capitales.

El contexto para el enfoque analítico de la evaluación del AML/CFT

Con la aparición de una normativa más restrictiva, que busca una mejor y más rápida identificación del riesgo, y las nuevas tecnologías disponibles, las entidades financieras están avanzando en un nuevo viaje de transformación en lo que respecta a la implementación de la adopción de análisis avanzados de AML/CFT[74]. Las tres herramientas principales que se utilizan para detectar el blanqueo de capitales son la evaluación del riesgo del cliente, la monitorización de transacciones y el escaneo de sanciones.

Evaluación de riesgo del cliente

La evaluación del riesgo del cliente es un modelo basado en los factores de riesgo asociados a la identificación del blanqueo de capitales, como el país del cliente, la ocupación y el salario, los productos bancarios, etc.

Los modelos estadísticos se han convertido en la práctica habitual para la evaluación del riesgo de los clientes, mediante la aplicación de diferentes técnicas para resolver el problema de detección de anomalías. Sin embargo, este problema es complejo de identificar o reproducir, y produce muestras desbalanceadas.

La aplicación de métodos avanzados de datos permite superar estas limitaciones, mejora la precisión de la evaluación del riesgo del cliente y fomenta su relevancia a lo largo del programa de AML/CFT. La evaluación del riesgo del cliente evoluciona progresivamente hacia una evaluación del riesgo del cliente basada en el comportamiento, en la que se actualizan continuamente los datos y se enriquece el proceso de identificación del riesgo[75]. Además, los propios modelos están incorporando la ventaja de utilizar técnicas de aprendizaje automático. Los métodos de aprendizaje supervisado, como el *random forest*, son los primeros en aplicarse para desvelar las relaciones ocultas entre los factores de riesgo en un conjunto aumentado de factores.

A medida que aumenta la potencia de cálculo y la riqueza y profundidad de los datos, estos modelos de comportamiento también pueden incorporar desencadenantes de una posible estructuración de las transacciones, es decir, estrategias colectivas de blanqueo de dinero por parte de múltiples individuos a través de pequeñas cantidades, para evitar la detección por parte de las estrategias clásicas de detección estática. La capacidad de construir algoritmos y estrategias que se ejecutan no en base a un cliente individual o un cliente más una transacción, sino en conjuntos de clientes, permite la identificación de la agrupación de transacciones de una manera más proactiva y eficaz. Los llamados algoritmos gráficos[76,77] aprovechan las conexiones potenciales procedentes de diferentes fuentes de información[78]. Además, la capacidad de construir una representación de red completa de todos los clientes aporta el valor adicional de agilizar el proceso de investigación de alertas, entre otros.

[73] Jean-Pierre Changeux (b.1936) es un neurocientífico francés conocido por sus investigaciones en varios campos de la biología, desde la estructura y función de las proteínas, al desarrollo temprano del sistema nervioso hasta las funciones cognitivas.

[74] Sin embargo, no hay uniformidad en el grado de adopción de estas técnicas de análisis avanzadas. Mientras que algunas entidades financieras están experimentando con soluciones innovadoras, las aplicaciones simples son más habituales en el sector, y la dependencia del soporte analítico está en sus inicios para otras. No obstante, el presente y el futuro de los programas de AML/CFT no pueden entenderse sin examinar las nuevas tecnologías y metodologías disponibles.

[75] Por ejemplo, incorporando información procedente del seguimiento de las transacciones, el escaneo de pagos o el análisis de valores atípicos en torno a los canales, los volúmenes, la geolocalización, etc.

[76] Soltani, Reza & Nguyen, Uyen & Yang, Yang & Faghani, Mohammad & Yagoub, Alaa & An, Aijun (2016). 1-7. 10.1109/UEMCON.2016.7777919

[77] Aprendizaje gráfico escalable para la lucha contra el blanqueo de dinero: Un primer vistazo; Weber, M; Chen, J.; Suzumura, T.; Pareja, A.; Ma, T.; Kanezashi, H., Kaler, T.; Leisersen C.E.; Schardl, Tao B

[78] Por ejemplo, circuitos cerrados de transaccionalidad -transferencias periódicas-, a la titularidad de cuentas conjuntas, a la dirección única, a la sucursal elegida o a las sucursales o cajeros más visitados, al geoposicionamiento a través de la app móvil, a la coincidencia de comercios, etc.

Monitorización de transacciones

El enfoque más común para la monitorización de transacciones consiste en un sistema basado en reglas, al estilo de un árbol de decisiones. Cada regla está configurada para identificar un comportamiento definido que enmascara las posibles actividades de blanqueo de los clientes y las entidades implicadas en la transacción[79]. Estas reglas se identifican generalmente como "escenarios". Las reglas y los escenarios más complejos tratan de abordar la identificación de cuentas anidadas y de relaciones más sofisticadas entre las partes, pero la base de la identificación de valores atípicos sigue siendo, en general, el nivel de la transacción individual, examinando los datos recibidos durante el proceso transaccional. Cuando se identifica un valor atípico, se activa una alerta, que posteriormente requiere la evaluación de un experto[80].

En este proceso, el conjunto inicial de reglas se desglosa en una segmentación más profunda de los comportamientos en la que la línea de negocio, el nivel de actividad transaccional y la evaluación del riesgo del cliente determinan los valores atípicos finales del comportamiento, es decir, las alertas que se dispararían.

Los métodos de análisis de datos pueden aprovecharse para detectar más alertas de calidad, aumentando los verdaderos positivos y reduciendo los falsos negativos, es decir, se identifican más alertas verdaderas sin aumentar el ruido en la identificación. Las técnicas de análisis de datos y aprendizaje automático se implementan para optimizar la segmentación proporcionando una identificación más precisa de los patrones gracias a la exploración de los datos históricos[81].

No obstante, las entidades financieras que estén estudiando activamente la incorporación de métodos avanzados en su programa de AML/CFT podrían decidir centrarse en la priorización de las alertas. El enfoque de las reglas genera grandes cantidades de alertas incluso cuando se aplica un ajuste adecuado de los umbrales del escenario y se ha optimizado la segmentación. Para solucionar esto, muchos bancos implementan métodos de aprendizaje supervisado para clasificar las alertas en términos de productividad[82]. El aspecto clave que determina el éxito de este enfoque es la utilización de métricas diferenciales, más allá de las variables esperadas e inamovibles disponibles a nivel de transacción.

El enfoque más disruptivo para la identificación de los riesgos de AML/CFT consiste en abandonar el enfoque tradicional de las reglas individuales para desvelar la relación oculta con la analítica avanzada. Sin embargo, pocas entidades financieras están explorando la utilización de metodologías alternativas. Algunas de ellas son:

- La analítica de grafos, que está ocupando su espacio en la identificación de las relaciones de la red y es cada vez más determinante para las actividades de blanqueo en el mundo financiero interconectado.

- Técnicas de clustering, que ayudan a identificar los valores atípicos sin asumir comportamientos específicos; por lo tanto, capturando con mayor frecuencia nuevas actividades ilícitas potenciales.

Avanzar hacia un enfoque no basado en reglas no implica automáticamente abandonar las buenas prácticas de optimización previamente identificadas. De hecho, la utilización de análisis avanzados para mejorar la segmentación de clientes, combinada con la detección de redes y de valores atípicos, y la utilización de la priorización de alertas podría considerarse una solución integral.

[79] Este comportamiento sospechoso se basará muy probablemente en los valores atípicos de la ubicación, el recuento de transacciones o los importes de las mismas.

[80] Véase Scalable Graph Learning for Anti-Money Laundering: A First Look; Weber, Chen, Suzumura, Pareja, Ma, Kanezashi, Kaler, Leisersen Schardl, Tao.

[81] El ajuste de umbrales basado en datos permite optimizar los cubos de productividad creciente a lo largo de las variables utilizadas en los escenarios (más verdaderos positivos), al tiempo que proporciona medidas del riesgo potencial no identificado (limitando los falsos negativos). Estos enfoques comunes se basan en los motores existentes basados en reglas.

[82] Este enfoque puede considerarse como una imitación de la revisión de las alertas por parte de los analistas de nivel 1; sin embargo, podría ser una identificación más compleja de abordar y no todas las entidades tienen éxito en este esfuerzo.

Un ejemplo de evaluación nacional de riesgos

El gobierno del Reino Unido publica periódicamente una evaluación nacional de riesgos[1], que informa sobre los riesgos de delito financiero a los que se enfrenta a nivel nacional. A través de esta evaluación nacional de riesgos se aportan referencias sobre las técnicas más habituales utilizadas en el ML/FT y su nivel de implantación en el país y son una referencia importante para las propias entidades en su evaluación del riesgo.

Una compañía debe realizar una evaluación del riesgo de delito financiero y utilizarla para diseñar sus controles de AML/CFT. La evaluación del riesgo nacional sirve, por tanto, como una base sólida sobre la que construir esta evaluación, en la que la compañía toma medidas adicionales para comprender, de forma más específica, los riesgos a los que se enfrenta.

Esto tendría en cuenta, entre otras cosas, su cartera de clientes y los productos que tienen: las cuentas corrientes personales sirven como medio de evasión fiscal para muchas pequeñas empresas, además de introducir la exposición a muchas otras técnicas de blanqueo de capitales debido a su capacidad para realizar transferencias rápidas de fondos y aceptar transacciones en efectivo. Además, una revisión de la actividad delictiva histórica puede ayudar a comprender cualquier tipología adicional a la que se enfrente el banco.

Las transacciones en efectivo, que entran y salen de las cuentas, son una forma fácil para los blanqueadores de dinero de romper los rastros de las transacciones. Aunque el uso de efectivo en el blanqueo de capitales está muy extendido y se incluye en muchas de las estrategias utilizadas, los controles en torno a los riesgos del efectivo suelen ser los más sencillos, en gran medida debido a la poca información disponible sobre las transacciones en efectivo.

Las mulas de dinero son terceras partes que se utilizan, consciente o inconscientemente, para realizar transacciones adicionales en efectivo y transferencias de fondos que enmascaran los rastros de las transacciones. Esto puede utilizarse junto con otras estrategias, por ejemplo, la compra de activos de alto valor y revendibles, para eliminar casi por completo las sospechas sobre el origen de los fondos, cuando las cuentas temporales podrían ser las de una red de mulas. Esto es difícil de detectar utilizando los métodos tradicionales, ya que ninguna cuenta, ni ningún cliente, puede ser utilizado para grandes volúmenes de las transacciones utilizadas en cualquier etapa de este proceso.

Del mismo modo, los negocios con gran cantidad de dinero en efectivo suponen otro reto para los métodos de detección tradicionales. Negocios como los salones de belleza, los quioscos de prensa y los lavaderos de coches son utilizados por los blanqueadores de capitales para documentar el dinero en efectivo procedente de actividades delictivas como ingresos comerciales legítimos, de modo que grandes volúmenes de los fondos ilícitos de las redes delictivas puedan centralizarse en una sola cuenta. Esto resulta difícil de detectar, ya que los ingresos en efectivo del negocio pueden parecer coherentes con su propio historial, así como con los ingresos de sus compañeros, y por lo tanto es posible que las transacciones en efectivo del negocio no levanten sospechas. Sin embargo, estas empresas suelen estar también vinculadas a la trata de personas y a la esclavitud moderna, que incluyen sus propios comportamientos transaccionales que pueden ser más fáciles de detectar. Al igual que con el uso de mulas de dinero, estas tipologías suelen implicar una red de terceros aparentemente no relacionados. Estos terceros pueden ser los facilitadores o incluso las víctimas de estos delitos y, por lo tanto, hay comportamientos específicos que uno esperaría ver. Las transacciones en varias ciudades diferentes, especialmente en ciudades con centros de transporte, el uso intensivo de restaurantes de comida rápida, las transacciones múltiples en el mismo hotel en el mismo día, los pagos múltiples a proveedores de telefonía móvil, las transferencias de fondos entre cuentas con comportamientos similares y las transacciones internacionales, especialmente las transferencias de efectivo y de fondos, son fuertes indicadores de estas tipologías. Si se puede vincular a estas partes con el negocio de uso intensivo de efectivo, se podría descubrir la red completa.

Las transacciones internacionales son otra operación de alto riesgo identificada en la evaluación nacional de riesgos. Se observan en una variedad de técnicas de blanqueo de capitales, además de presentar un riesgo en otros aspectos de la delincuencia financiera. Esto se ve en el tráfico de personas, que se estima que es uno de los mayores generadores de ganancias criminales a nivel mundial. El tráfico de personas requiere el envío al extranjero de los miembros de la banda de delincuencia organizada asociada en los países relacionados con el tráfico. Esto puede ser en forma de dinero en efectivo retirado en el Reino Unido y trasladado físicamente al extranjero o a través de mulas de dinero de manera similar al comportamiento asociado con los depósitos en efectivo descritos anteriormente.

La financiación del terrorismo está identificada como una tipología de alto riesgo en el Reino Unido. La recaudación y el movimiento de fondos no se consideran un objetivo primordial de los terroristas, especialmente porque la mayoría de los recientes atentados terroristas han sido de bajo presupuesto y poca sofisticación, y con frecuencia han sido planificados, financiados y realizados por un individuo. La financiación del terrorismo se utiliza habitualmente para trasladar fondos al extranjero a través de métodos relativamente sencillos, como el traslado físico de dinero en efectivo al extranjero o el empleo de empresas de servicios monetarios (MSB). Por lo tanto, la detección de la financiación del terrorismo requiere una recopilación de indicadores clave de la misma manera que se requiere para el uso de empresas con gran cantidad de efectivo en el blanqueo de capitales.

El riesgo asociado a los criptoactivos crece año tras año a medida que los criptoactivos se vuelven más comunes y de fácil acceso, pero los controles en torno a ellos siguen siendo relativamente nuevos, ya que el Reino Unido no introdujo normas sobre el uso de criptoactivos para el blanqueo de capitales hasta enero de 2020. Las bandas criminales organizadas utilizan los criptoactivos para el blanqueo de dinero comprando primero los criptoactivos con sus fondos ilícitos, potencialmente después de una etapa inicial de estratificación, antes de vender los activos para proporcionar una fuente legal de sus fondos. Además, los criptoactivos pueden moverse fácilmente a través de las fronteras, lo que permite a los delincuentes mover importantes fondos a nivel internacional con gran facilidad en comparación con las monedas fiduciarias.

Este es un ejemplo de los nuevos riesgos que surgen en el ámbito del delito financiero y que suponen un nuevo reto para las entidades, que deben desarrollar y poner en práctica nuevos controles de forma regular para mantenerse al día con los cambios y la evolución de los blanqueadores de capitales.

[1]HM Treasury: National risk assessment of money laundering and terrorist financing 2020. December 2020.

Escaneo de sanciones

Los motores de escaneo de sanciones comparan a las personas o empresas con la lista de sanciones designada utilizando técnicas de coincidencia difusa. Los enfoques más sencillos se basan en una amplia gama de transformaciones aplicadas a los "nombres" (cambio de orden del nombre, iniciales, transliteración, errores vocales o consonánticos comunes, etc.). Los nombres transformados se normalizan como cadenas y se comparan con los nombres de la lista de sanciones, también normalizados siguiendo las mismas reglas. Las reglas o lógicas de comparación miden el grado de separación entre las dos cadenas. El motor puede devolver una puntuación de la coincidencia, o una alerta basada en una regla de coincidencia predefinida, sin embargo, la lógica subyacente es la misma, es decir, las dos cadenas son lo suficientemente similares como para conceder una revisión de expertos.

Como en el caso de la monitorización de transacciones, estas reglas producen un gran número de falsos positivos[83]. Además, el potencial de optimización basado en el ajuste es menor que en el caso de la monitorización de transacciones.

Por ello, las entidades están explorando métodos alternativos para mejorar la calidad de la identificación basados en tecnologías de traducción y transliteración, y en la aplicación de tecnologías de procesamiento de lenguaje natural (NLP) para mejorar la coincidencia de nombres. La mejora de los métodos analíticos para el escaneo de sanciones va en paralelo a la exploración de estas técnicas en la identificación de noticias negativas.

Los próximos pasos en los enfoques analíticos de la evaluación de AML/CFT

La aplicación de métodos y tecnologías innovadoras no se detiene en las destacadas anteriormente. El procesamiento extendido del lenguaje natural y el aprendizaje profundo, las aplicaciones de blockchain, la verificación electrónica de la identidad, el reconocimiento de voz y del habla, la biometría o la geolocalización son otras tecnologías que pueden contribuir a la identificación de actividades ilícitas.

Detrás de todos estos posibles enfoques, se encuentran varias tendencias en el análisis de AML/CFT:

- Se implementa un análisis más profundo de los datos tanto de la transacción, como del cliente y sus relaciones. Algunas de las opciones analíticas señaladas anteriormente se vuelven impotentes si no se dispone de datos diferenciales y se incorporan al análisis.

- Se requieren datos complementarios de las fuentes internas y de las diferentes dimensiones del programa de AML/CFT (es decir, calificación del riesgo del cliente, diligencia debida, escaneo de sanciones, transacciones) y fuentes externas (datos públicos sobre PEP, relaciones de propiedad, fuentes de reputación, búsquedas abiertas) para crear un enfoque holístico de la identificación del riesgo de ML/FT.

- Las tecnologías y los métodos pueden ser tan complejos como lo permita la innovación, pero dimensionar los más adecuados a la naturaleza del negocio y a la evaluación de riesgos de la entidad es fundamental para optimizar el uso de los recursos tecnológicos y humanos, al tiempo que se garantiza el cumplimiento de la normativa.

Los supervisores y reguladores son en general reacios a los cambios repentinos y favorecen las metodologías bien

[83] Los motores pueden ser más o menos complejos en la incorporación de transformaciones innovadoras aplicadas a los nombres, o incorporar más fuentes de sanción de calidad mejoradas con información PEP, sin embargo, todos presentan las mismas debilidades.

establecidas antes de adoptar plenamente los cambios revolucionarios. Sin embargo, para aquellas instituciones que están dispuestas a embarcarse en un programa de transformación total de la analítica de AML/CFT, se han producido una serie de avances en los últimos años[84]: desde desarrollos específicos de aplicaciones de coincidencia difusa o de detección de PEP en colaboraciones conjuntas, hasta la constitución de centros de innovación y *sandboxes*.

En el camino hacia una identificación de riesgos más sofisticada, la interpretabilidad y el control adecuado de los riesgos siguen siendo el centro de las preocupaciones del regulador (y de las instituciones).

El uso de la analítica avanzada en el programa de AML/CFT está vinculado a que las reglas implementadas se consideren modelos y estén por tanto, sujetos a las prácticas de identificación, monitorización y control que las entidades han desplegado bajo la función de Gestión del riesgo de modelo (MRM). Mientras que la distinción para la calificación del riesgo de cliente es clara, ya que cumple todas las condiciones típicamente establecidas en el marco de la gestión del riesgo de modelo (MRM) para ser un modelo o, al menos, una herramienta de usuario que debe ser supervisada, los motores de AML/CFT no han sido considerados como modelos inicialmente. La asimilación de los motores de reglas de AML/CFT en la disciplina de la gestión del riesgo de modelo no se ha producido de manera uniforme en todas las jurisdicciones y los principales actores quieren evitar la carga de un escrutinio incremental de los programas de AML/CFT[85].

Sin embargo, las tecnologías de *machine learning* para mejorar la identificación de riesgos están ampliando la concepción de lo que se entiende como modelo sujeto a MRM. A pesar de su voluntad de fomentar su aplicación a los programas de AML/CFT, los supervisores dejan clara la necesidad de garantizar un grado adecuado de comprensión e interpretabilidad de las metodologías aplicadas y los resultados obtenidos. Hay que evitar los modelos de caja negra. Los modelos de *machine learning* pueden adolecer de falta de transparencia en la selección y explicación de las características, la evaluación del rendimiento del modelo, etc. Una documentación adecuada, la comprobación del modelo, los módulos de interpretabilidad; los principios básicos de un marco robusto de MRM apoyarán la adecuación de estos modelos para el uso de AML/CFT.

Caso práctico: mejorar la detección de patrones sospechosos mediante el análisis de redes

Una de las técnicas aplicadas con éxito para detectar el fraude es el denominado análisis de redes. Esta técnica puede ayudar a identificar, detectar y caracterizar comportamientos sospechosos utilizando métricas, técnicas de aprendizaje automático y algoritmos difusos.

Para desarrollar el análisis de redes, hay que dar tres pasos relevantes: (i) recopilar datos relevantes y construir un gráfico que represente las relaciones entre las entidades; (ii) decidir la estrategia de identificación que permita identificar el cluster de entidades y relaciones sospechosas; y (iii) caracterizar esos clusters mediante métricas apropiadas que se utilizarán como características de los modelos de detección (véase figura 4).

Etapa 1. Representación de la red

Una red permite examinar relaciones complejas entre entidades relacionadas, ya sea mediante vínculos de datos internos, como transacciones, o externos, como direcciones y titularidades

Figura 4. Etapas para la detección mediante el análisis de redes.

[84] En palabras del reciente documento publicado por el GAFI, "las nuevas tecnologías tienen el potencial de hacer que las medidas de AML/CFT sean más rápidas, baratas y eficaces". Además, el GAFI enumera las múltiples iniciativas de supervisores y entidades de todo el mundo que constituyen la vanguardia de la evolución del sector Ver: Opportunities and challenges of new technologies for AML/CFT, disponible en https://www.fatf-gafi.org/media/fatf/documents/reports/Opportunities-Challenges-of-New-Technologies-for-AML-CTF.pdf

[85] Una declaración conjunta de la FRS, la FDIC y la OCC abordó las preguntas del sector sobre cómo deben aplicarse las directrices del MRM a los modelos de cumplimiento de la BSA/AML. Los supervisores consideran que no se requiere que todos los sistemas se clasifiquen como modelos, y que el propio banco puede categorizar los modelos como considere oportuno. Y lo que es más importante, afirmaron que los bancos no están obligados a tener procesos duplicados ni a llevar a cabo actividades de prueba duplicadas para cumplir con la normativa BSA. Aunque proporciona cierto grado de maniobra a las instituciones financieras, la declaración refuerza la opinión de que el banco debe abordar los riesgos asociados a los sistemas de AML (con modelos o sin ellos).

(véase la figura 5). La construcción de las redes requiere computar suficientes puntos de datos granulares que puedan conectar las entidades con diferentes objetos, como empresas, direcciones, usos digitales, etc., y considerar la fuerza de estas relaciones (por ejemplo, conexión transaccional). Esta red puede estructurarse como un grafo (tanto dirigido como no dirigido, y ponderado o no ponderado). La red construida y la información contenida en ella determinarán la idoneidad de determinadas técnicas (por ejemplo, un grafo no dirigido ponderado podría tratarse en los pasos siguientes mediante técnicas de agrupación, como la agrupación espectral).

Etapa 2. Estrategia de identificación

Se necesita una estrategia de identificación para descubrir posibles pautas de blanqueo de capitales u otras actividades ilícitas dentro de la red identificada. Existen diferentes estrategias que pueden utilizarse, por ejemplo:

- Enfoques heurísticos basados en la proximidad a casos o entidades sospechosos confirmados.
- Enfoques probabilísticos y reconocimiento de patrones.
- Enfoque de detección de comunidades basado en técnicas de aprendizaje automático.

Al aplicar el enfoque de detección de comunidades, es necesario descubrir las distintas comunidades. Una comunidad es un subgrafo de la red con un mayor número y una relación más intensa entre los miembros de la comunidad en comparación con subgrafos aleatorios y poco informativos (véase la figura 6). La detección de comunidades es un enfoque útil para detectar y caracterizar las estructuras objetivo, que puede requerir el uso de algoritmos como *k-means*, *clustering* jerárquico, *clustering* espectral, algoritmos evolutivos u optimización de la modularidad[86].

Para encontrar las comunidades óptimas, se optimiza una función específica: la función de modularidad. Dada una red representada como un grafo ponderado y particionada en comunidades o módulos, esta fórmula depende de la estructura específica de la representación gráfica, y expresa la definición matemática de modularidad en términos de pesos:

$$Q = \frac{1}{2w}\sum_i\sum_j\left(w_{ij} - \frac{w_i w_j}{2w}\right)\delta(C_i, C_j)$$

Donde C_i es la comunidad a la que está asignado el nodo i, w_{ij} representa el valor del peso en el enlace entre los nodos i y j (0 si no existe enlace), $w_i = \sum_j w_{ij}$, y $w = \sum_i w_i$. Por último, la función δ corresponde a la función delta de kronecker: $\delta(i,j)$ toma el valor 1 si los nodos i y j están en el mismo módulo y 0 en caso contrario.

Etapa 3. Uso de funciones

Una vez identificadas las comunidades objetivo dentro de la red, pueden definirse métricas o características específicas para evaluar la profundidad e importancia de las relaciones o el riesgo de las conexiones entre entidades. Estas características pueden utilizarse en reglas o algoritmos de aprendizaje automático para mejorar la capacidad predictiva de los modelos reduciendo los falsos positivos e identificando mejor los patrones sospechosos. El enfoque basado en reglas que incorporan características "enriquecidas" puede ser útil para producir alertas cualitativas, ya que incorporan nueva información aparte de la base transaccional tradicional

[86] Varios autores han desarrollado algoritmos óptimos para la detección de patrones. Véase L. Alsedà, A. Awasthi, Jörg Lässig (2012).

Figura 5. Representación del algoritmo de detección de comunidades (pasos (a) a (d)) utilizando la optimización de la modularidad.
La comunidad superior contiene un comportamiento sospechoso (objetivo) que corresponde en este caso de uso a la red del Cliente A de la Etapa 1 (representado en la figura 7 en la página siguiente).

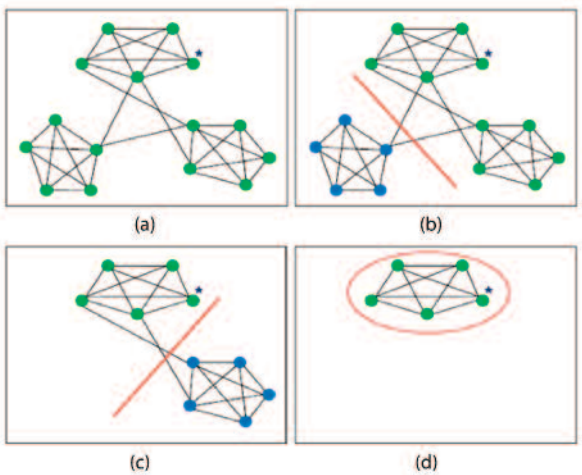
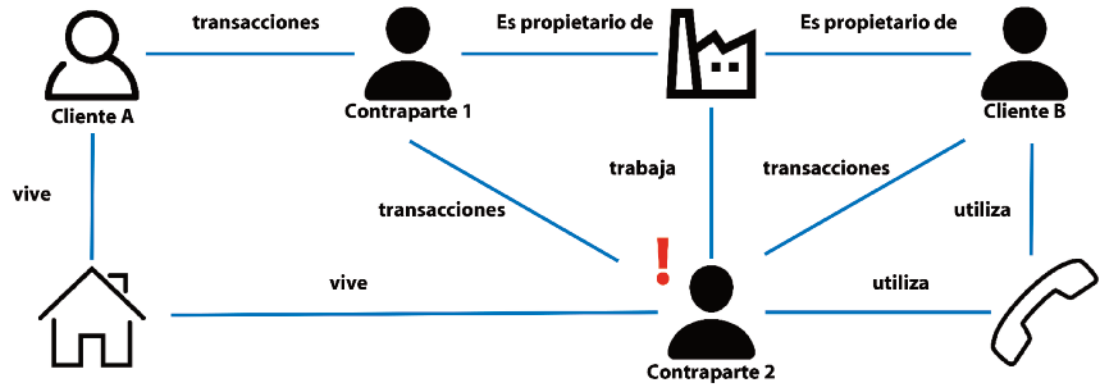


Figura 6. Lógica simplificada para un escenario basado en características obtenidas mediante el análisis de la red. Otras características, como los importes de las transacciones, pueden incorporarse en función del patrón o la combinación de patrones que se desee detectar. Este ejemplo es meramente ilustrativo.

Lógica y parametrización de reglas de detección con características de red

- Si el tipo de entidad = **Individual**
- Si la comunidad sospechosa identificada: conexiones sospechosas identificadas = **Sí**
- Si el número de rutas al nodo sospechoso >= **num_rutas_a_nodo_sospechoso**
- Si la distancia al nodo sospechoso es <= **distancia_máxima_a_nodo_sospechoso**
- Si las conexiones primarias al nodo sospechoso = **tipo_conexión_principal**

Figura 7. Representación de una red con las relaciones del cliente A, donde se incluye un nodo sospechoso (la contraparte 2 está en una lista negra) y posibles entidades sintéticas (nodos relacionados con la empresa)



relacionada con el cliente (véase la figura 8). Sin embargo, las técnicas de aprendizaje automático pueden desvelar relaciones más sólidas que permitan separar las alertas positivas verdaderas de las falsas.

En el ejemplo de la figura 7, cuya información de redes se presenta en la figura 8, el cliente A y el cliente B pertenecen al mismo *cluster* sospechoso con conexiones a la entidad sospechosa (Contraparte 2), pero el cliente B tiene la relación más fuerte, tanto personal como profesionalmente con la Contraparte 2. Basándonos en este escenario, si los umbrales se calibran para que sean *num_rutas_a_nodo_sospechoso* = 1, *distancia_máxima_a_nodo_sospechoso* = 5 y *tipo_conexión_principal* = "all" (ya sea transaccional, personal o de cualquier tipo), entonces tanto el Cliente A como el B serán marcados como entidades sospechosas (o sus transacciones relacionadas, etc.). Sin embargo, considerando un enfoque más tradicional, sin el análisis de redes, sólo el cliente B sería marcado como tal; el cliente A no tiene conexiones transaccionales con la Contraparte 2.

Se pueden evaluar características complejas y entrenar distintos tipos de algoritmos de aprendizaje automático, lo que permite asignar un mayor riesgo al cliente B y a las transacciones asociadas. La incorporación de nuevas características a los modelos permite también aumentar la precisión y detectar más comportamientos potencialmente arriesgados (reduciendo las falsas alertas negativas), al tiempo que se discrimina mejor el riesgo entre esos comportamientos identificados (reduciendo las falsas alertas positivas).

Figura 8. Información sobre los clientes para la identificación de conexiones sospechosas

Empresa	Distancia mínima al nodo sospechoso	Conexión fundamental al nodo sospechoso	Conexión de datos personales	Número de rutas hacia el nodo sospechoso	Cluster identificado	Conexiones sospechosas identificadas
Cliente A	2	Transaccional	Sí	2	1	Sí
Cliente B	1	Transaccional	Sí	4	1	Sí

Conclusiones

Los delitos financieros (en su sentido amplio, que incluye el blanqueo de capitales, la financiación del terrorismo, el incumplimiento de sanciones económicas, el soborno y la corrupción, el fraude y el abuso de mercado) siguen siendo una gran amenaza para el sector financiero en todo el mundo, y en concreto, el blanqueo de capitales como una la de las áreas a la que prestar mayor atención. Según la Oficina de las Naciones Unidas contra la Droga y el Delito, se calcula que la cantidad de dinero blanqueado en el mundo en un año alcanza entre el 2% y el 5% del PIB mundial, es decir, entre 800.000 millones y 2 billones de dólares estadounidenses actuales. Sin embargo, menos del 1% de ese dinero es incautado o congelado por las fuerzas del orden.

Las entidades financieras, los reguladores y los organismos de lucha contra la delincuencia están colaborando para aprovechar una mayor capacidad de cálculo, una modelización matemática más avanzada, una mayor concienciación de los altos cargos y una coordinación más estrecha para luchar contra el blanqueo de capitales en todas las jurisdicciones a fin de combatir este delito económico.

En este contexto, las entidades financieras están inviertiendo en mejorar sus capacidades para poder identificar, gestionar, medir, controlar y supervisar sus riesgos:

1. Marco y gobernanza, con evaluaciones de riesgos más formales y exhaustivas, normas y políticas más detalladas, un modelo de tres líneas de defensa mejor definido y más coordinado, y enfoques más integrados para la gestión de riesgos (entre los diferentes riesgos de delitos económicos).

2. Estructura organizativa, con equipos especializados y plenamente dedicados dirigidos por expertos en la materia. También la centralización de capacidades para garantizar una actuación eficiente y eficaz, y la planificación estratégica de la plantilla que garantice no solo la oferta actual de expertos en la materia, sino la identificación de las necesidades futuras de competencias (por ejemplo, científico de datos). Las entidades financieras también están invirtiendo fuertemente en asegurar la adecuada interiorización de la cultura y los comportamientos adecuados para hacer frente a este delito.

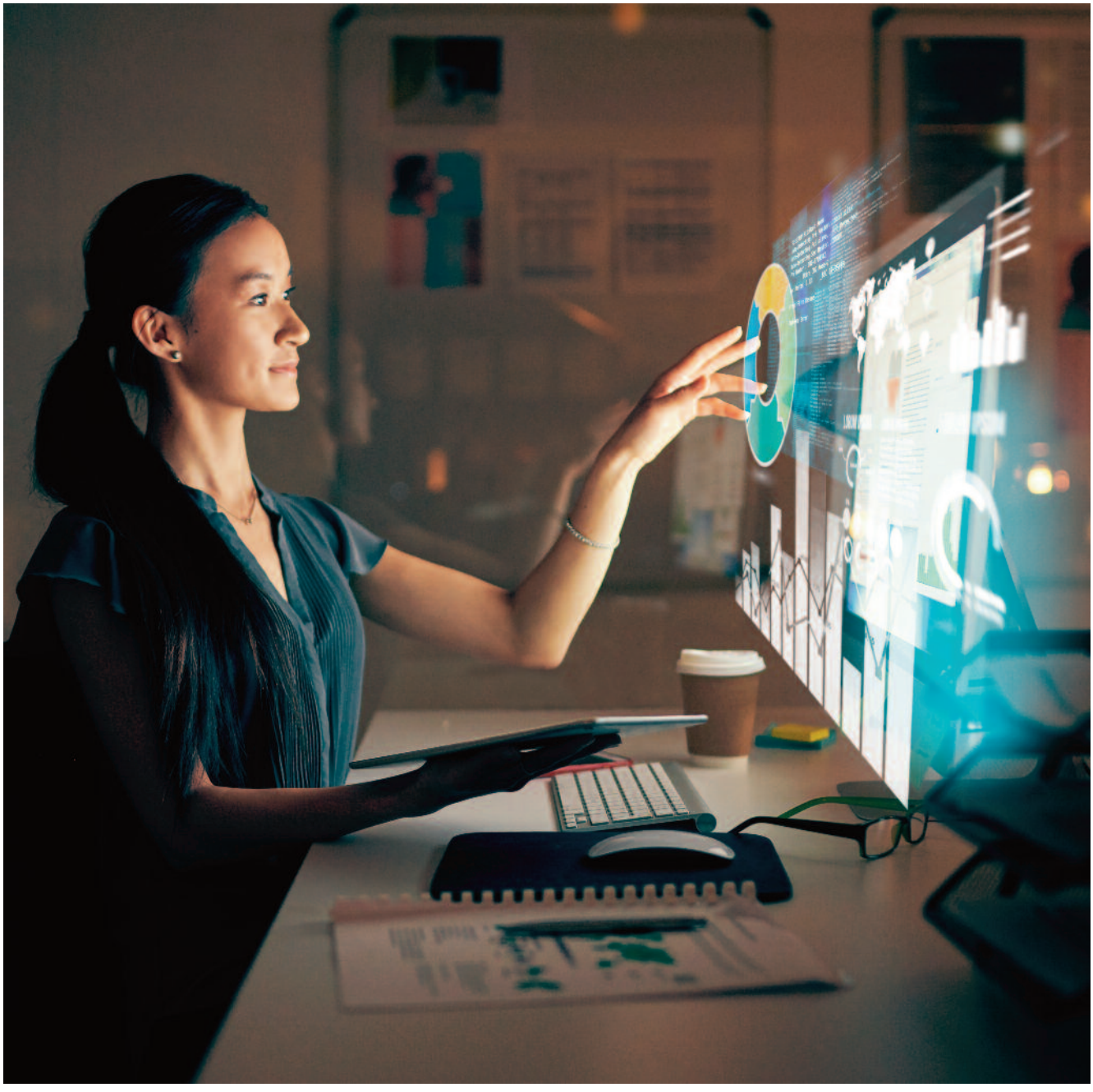
3. Procesos empresariales, incluidas las evaluaciones de riesgos en toda la empresa, así como la diligencia debida y la evaluación de riesgos de cada cliente. También la inversión en la racionalización y el fortalecimiento de la supervisión de las transacciones, la detección de sanciones y pagos, la investigación de la gestión de alertas, así como la colaboración con las fuerzas y cuerpos de seguridad.

4. Mejora del entramado de datos subyacente que respalda la identificación y medición de riesgos, incluidas la mejora de las fuentes de datos, la mejora de la calidad de los datos y las capacidades de gobernanza de datos.

5. Inversión en la infraestructura tecnológica, con especial atención a poder hacer frente a nuevas amenazas como el blanqueo de capitales a través de criptomonedas, además de aumentar las capacidades y automatizar los procesos tecnológicos.

Una de las principales áreas de inversión, que también está demostrando ser una de las más eficaces, es el desarrollo de modelos analíticos avanzados para aumentar la eficacia de la detección de amenazas. Este es uno de los pilares del futuro de una función eficaz contra el blanqueo de capitales (y la delincuencia financiera en general): una función en la que los datos y los modelos y análisis avanzados sean capaces de identificar patrones casi en tiempo real y desencadenar alertas productivas y respuestas automatizadas.

Glosario



AML: significa Anti Money Laundering, se utiliza principalmente en el sector financiero, legal y de cumplimiento para referirse a los controles estándar que las empresas y organizaciones deben tener para prevenir, identificar y reportar comportamientos sospechosos de lavado de dinero.

BPM: Business Process Management. BPM es una metodología de trabajo basada en un sistema de gestión que se encarga de controlar el modelado, visibilidad y gestión de los procesos productivos de la empresa.

BSA (Bank Secrecy Act): de 1970, es una de las primeras leyes de lucha contra el blanqueo de capitales en Estados Unidos. La BSA exige a las empresas que mantengan registros y presenten informes que se determinen con un alto grado de utilidad en materia penal, fiscal y reglamentaria.

CFT (Countering the Financing of Terrorism): este término implica la utilización de fondos que pueden ser de origen lícito o ilícito y el uso de estos fondos para apoyar la actividad terrorista.

Convención sobre la Delincuencia Organizada Transnacional: fue adoptada por la resolución 55/25 de la Asamblea General, de 15 de noviembre de 2000, y es el principal instrumento internacional en la lucha contra la delincuencia organizada transnacional.

Escaneo: es un proceso que tiene como objetivo identificar y llevar a cabo la debida diligencia de los clientes sobre cualquier persona políticamente expuesta como parte de un sólido programa de Anti-Lavado de Dinero y Know Your Customer (AML/KYC).

Escaneo de sanciones: es una combinación de políticas, procedimientos y tecnologías que permiten a una institución financiera garantizar que no presta ningún tipo de servicio a partes sancionadas, directa o indirectamente.

Evaluación de la calificación del riesgo del cliente: es una de las tres herramientas principales utilizadas por las entidades financieras para detectar el blanqueo de capitales. Los modelos desplegados por la mayoría de las instituciones hoy en día se basan en una evaluación de factores de riesgo como la ocupación del cliente, su salario y los productos bancarios que utiliza.

GAFI (Grupo de Acción Financiera Internacional): es una institución intergubernamental creada en 1989 por el entonces G8. El objetivo del GAFI es desarrollar políticas que ayuden a combatir el blanqueo de capitales y la financiación del terrorismo.

KCI (Key Control Indicator): indicador clave de control.

KYB (Know Your Business): estas estrategias se centran en el establecimiento de relaciones óptimas con otras empresas que pueden ser clientes o proveedores, para mitigar el riesgo de hacer negocios con una entidad poco fiable o que haya estado involucrada en una situación comprometida en el pasado.

KYC (Know Your Customer): estos procedimientos se establecen en torno a un proceso de identificación y verificación de la identidad de un cliente en el que se aplican una serie de controles y comprobaciones para evitar las relaciones comerciales con personas vinculadas al terrorismo, la corrupción o el blanqueo de capitales.

KYS (Know your Supplier): esta práctica proporciona más información y transparencia sobre los proveedores y los riesgos relacionados con la cadena de suministro, con el fin de abordar temas como el rendimiento de los proveedores, la continuidad del negocio, la sostenibilidad, el fraude y el soborno, el riesgo de seguridad, el blanqueo de dinero, el trabajo infantil y otros requisitos de cumplimiento legal/organizativo.

KRI (Key Risk Indicator): indicador clave de riesgo.

Modelo de líneas de defensa: las tres líneas de defensa representan un enfoque para proporcionar una estructura en torno a la gestión de riesgos y los controles internos dentro de una organización mediante la definición de funciones y responsabilidades en diferentes áreas y la relación entre esas diferentes áreas.

Mula de dinero: persona que transfiere o mueve dinero adquirido ilegalmente en nombre de otra persona.

PEP: Politically Exposed Person. persona políticamente expuesta.

Programa de monitorizacion de transacciones: ayuda a las entidades financieras a detectar automáticamente las transacciones sospechosas, como los depósitos en efectivo de alto valor o la actividad inusual en las cuentas.

Unidades de Inteligencia Financiera (UIF): unidades de investigación establecidas por los distintos países para centralizar la recopilación de informes de actividades sospechosas relacionadas con la actividad financiera delictiva y compartir los resultados del análisis con los organismos gubernamentales pertinentes.

Bibliografía

Autoridad de Conducta Financiera (n.d). Manual de la FCA. https://www.handbook.fca.org.uk/handbook/glossary/G416.html

Oficina de las Naciones Unidas contra la Droga y el Delito (s.f.). Blanqueo de capitales. https://www.unodc.org/unodc/en/moneylaundering/overview.html

Foro Económico Mundial (n.d). Coalición Mundial para la Lucha contra la Delincuencia Financiera. https://www.weforum.org/projects/coalition-to-fight-financial-crime

Lexis Nexis Risk Solutions (2021). Coste global del cumplimiento.

Paesano, F. (2021). Las criptomonedas y las investigaciones sobre el blanqueo de capitales. Instituto de Gobernanza de Basilea.

Europol. (2018). Detenido en España el autor intelectual de un robo cibernético de 1.000 millones de euros. https://www.europol.europa.eu/media-press/newsroom/news/mastermind-behind-eur-1-billion-cyber-bank-robbery-arrested-in-spain#downloads

Escáner de sanciones. (2021). Multas contra el blanqueo de capitales (AML) de 2021. https://sanctionscanner.com/blog/anti-money-laundering-aml-fines-of-2021-561

Comisión Europea. (2019). Informe de la Comisión al Parlamento Europeo y al Consejo sobre la evaluación de los recientes casos de presunto blanqueo de capitales en los que están implicadas entidades de crédito de la UE.

Parlamento Europeo y Consejo. (2015). Directiva (UE) 2015/849.

Autoridad Bancaria Europea. (2021). Directrices sobre la cooperación y el intercambio de información entre los supervisores prudenciales, los supervisores de AML/CFT y las unidades de inteligencia financiera en virtud de la Directiva 2013/36/UE.

Mersch, Y. (2019). La lucha contra el blanqueo de capitales y la financiación del terrorismo: iniciativas recientes y el papel del ECB. https://www.bankingsupervision.europa.eu/press/speeches/date/2019/html/ssm.sp191115~a435dd398e.es.html

Autoridad bancaria europea. (2019). Dictamen de la Autoridad Bancaria Europea sobre las comunicaciones a las entidades supervisadas en relación con los riesgos de blanqueo de capitales y financiación del terrorismo en la supervisión prudencial.

Parlamento Europeo. (2021). Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la información que acompaña a las transferencias de fondos y a determinados criptoactivos (refundición).

Grupo de Acción Financiera Internacional. (2014). Virtual Currencies Key Definitions and Potential AML/CFT Risks.

Parlamento Europeo. (2021). Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se crea la Autoridad Europea de Lucha contra el Blanqueo de Capitales y la Financiación del Terrorismo y por el que se modifican los Reglamentos (UE) nº 1093/2010, (UE) 1094/2010, (UE) 1095/2010.

Holman, D.; Stettner, B. (2018). Regulación antilavado de dinero de la criptodivisa: Enfoques estadounidenses y globales. Allen & Overy, LLP.

Autoridad Bancaria Europea. (2021). Informe final sobre los proyectos de normas técnicas de regulación con arreglo al artículo 9 bis, apartados 1 y 3, del Reglamento (UE) nº 1093/2010.CFT.

Autoridad de Conducta Financiera (2022). Empresas aceptadas por el Regulatory Sandbox. https://www.fca.org.uk/firms/innovation/regulatory-sandbox/accepted-firms

Junta de Gobernadores del Sistema de la Reserva Federal (2018). Declaración conjunta sobre los esfuerzos innovadores para combatir el blanqueo de capitales y la financiación del terrorismo. https://www.fca.org.uk/firms/innovation/regulatory-sandbox/accepted-firms

Junta de Gobernadores del Sistema de la Reserva Federal (2021). Request for Information and Comment on Financial Institutions' Use of artificial intelligence, including machine learning. https://www.federalregister.gov/documents/2021/03/31/2021-06607/request-for-information-and-comment-on-financial-institutions-use-of-artificial-intelligence

Corporación Federal de Seguros de Depósitos (2021). Apéndice 1010.230 Requisitos de propiedad efectiva para clientes con personalidad jurídica. Ley de la FDIC, reglamentos, leyes relacionadas.

Grupo de Acción Financiera Internacional. (2019). Los ministros del GAFI otorgan a este organismo un mandato de duración indefinida.

Oficina de las Naciones Unidas contra la Droga y el Delito. (2005). Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional y sus Protocolos.

Oficina de las Naciones Unidas contra la Droga y el delito (2011). Estimación de los flujos financieros ilícitos resultantes del tráfico de drogas y otros delitos organizados transnacionales. Informe de investigación. Octubre de 2011.

Red de Ejecución de Delitos Financieros. (2020). Ley contra el blanqueo de capitales de 2020.

Instituto de Finanzas Internacionales; Deloitte. (2021). La eficacia de la reforma de la gestión del riesgo de los delitos financieros y los próximos pasos a nivel mundial.

Banco Popular de China. (2021). Medidas para la supervisión y administración de la lucha contra el blanqueo de capitales y la financiación del terrorismo de las instituciones financieras.

Agencia de Servicios Financieros. (2021). Directrices para la lucha contra el blanqueo de capitales y la financiación del terrorismo.

República de Singapur. (2019). Ley de servicios de pago.

Autoridad Monetaria de Singapur. (2021). Documento de consulta sobre los avisos de AML propuestos para los acuerdos comerciales transfronterizos de los intermediarios de los mercados de capitales en virtud de los marcos de exención propuestos.

Autoridad Bancaria Europea. (2021). Dictamen de la Autoridad Bancaria Europea sobre los riesgos de blanqueo de capitales y financiación del terrorismo que afectan al sector financiero de la Unión Europea.

Grupo de Acción Financiera Internacional. (2013). Evaluación del riesgo nacional de blanqueo de capitales y financiación del terrorismo.

Autoridad Bancaria Europea. (2022). Directrices sobre la función de los responsables del cumplimiento de las normas de AML/CFT.

Autoridad Bancaria Europea. (2021). Directrices sobre el uso de soluciones de incorporación de clientes a distancia.

Comité de Supervisión Bancaria de Basilea. (2013). Principios para una eficaz agregación de datos sobre riesgos y presentación de informes sobre riesgos.

Soltani, R.; Nguyen, U.; Yang, Y.; Faghani, M. (2013). Un nuevo algoritmo para la detección del blanqueo de dinero basado en la similitud estructural.

Weber, M; Chen, J.; Suzumura, T.; Pareja, A.; Ma, T.; Kanezashi, H., Kaler, T.; Leisersen C.E.; Schardl, Tao B. (2018). Aprendizaje gráfico escalable para la lucha contra el blanqueo de dinero.

HM Treasury: National risk assessment of money laundering and terrorist financing. December 2020.

Nuestro objetivo es superar las expectativas de nuestros clientes convirtiéndonos en socios de confianza

Management Solutions es una firma internacional de servicios de consultoría centrada en el asesoramiento de negocio, finanzas, riesgos, organización y procesos, tanto en sus componentes funcionales como en la implantación de sus tecnologías relacionadas.

Con un equipo multidisciplinar (funcionales, matemáticos, técnicos, etc.) de más de 3.300 profesionales, Management Solutions desarrolla su actividad a través de 41 oficinas (17 en Europa, 20 en América, 2 en Asia, 1 en África y 1 en Oceanía).

Para dar cobertura a las necesidades de sus clientes, Management Solutions tiene estructuradas sus prácticas por industrias (Entidades Financieras, Energía, Telecomunicaciones y Otras industrias) y por líneas de actividad que agrupan una amplia gama de competencias: Estrategia, Gestión Comercial y Marketing, Gestión y Control de Riesgos, Información de Gestión y Financiera, Transformación: Organización y Procesos, y Nuevas Tecnologías.

El área de I+D da servicio a los profesionales de Management Solutions y a sus clientes en aspectos cuantitativos necesarios para acometer los proyectos con rigor y excelencia, a través de la aplicación de las mejores prácticas y de la prospección continua de las últimas tendencias en metodologías de medición en el ámbito de la sostenibilidad (ambiental y social).

Juan G. Cascales
Socio de Management Solutions
juan.garcia.cascales@msunitedkingdom.com

Antonio Tazón
Socio de Management Solutions
antonio.tazon@msnorthamerica.com

Patricia Pajuelo
Director de Management Solutions
patricia.pajuelo@msnorthamerica.com

Luke Harrison
Experienced Senior de Management Solutions
luke.harrison@msunitedkingdom.com

Management Solutions, servicios profesionales de consultoría

Management Solutions es una firma internacional de consultoría centrada en el asesoramiento de negocio, finanzas, riesgos, organización, tecnología y procesos,

Para más información visita **www.managementsolutions.com**

Síguenos en:

© Management Solutions. 2023
Todos los derechos reservados

www.managementsolutions.com

Madrid Barcelona Bilbao Coruña London Frankfurt Düsseldorf Paris Amsterdam Copenhagen Oslo Warszawa Zürich Milano Roma Bologna Lisboa Beijing Istanbul Johannesburgo Sydney Toronto New York New Jersey Boston Pittsburgh Atlanta Birmingham Houston San Juan de Puerto Rico San José Ciudad de México Monterrey Querétaro Medellín Bogotá Quito São Paulo Lima Santiago de Chile Buenos Aires