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 la notificación 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.

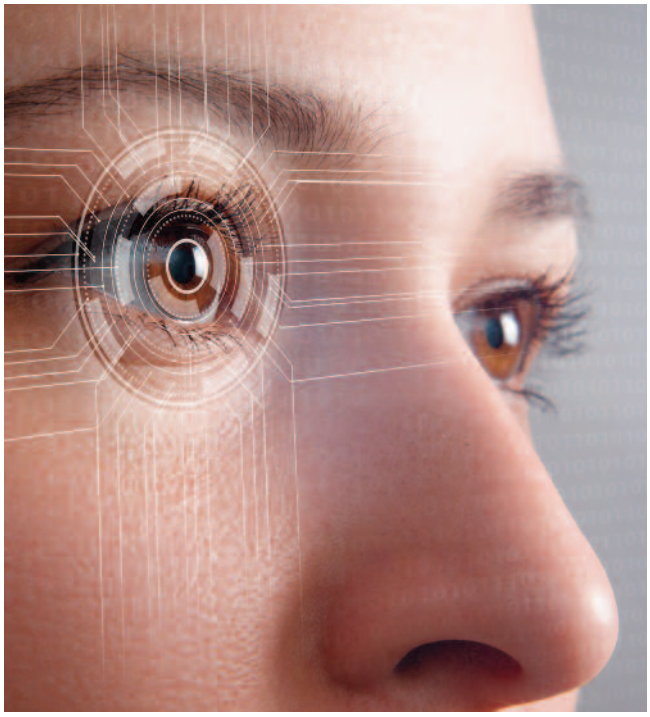
23. ***Infraestructura de datos e información de gestión.*** En una economía cada vez más impulsada por los datos, una de las áreas clave de desarrollo dentro del espacio de AML/CFT es la infraestructura de datos subyacente y la información de gestión utilizada para la toma de decisiones. Desde el punto 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 la notificación 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 sucursales 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 a la Dirección 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 Robótica Avanzada de Procesos (ARPA). 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 ARPA 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.