Desafíos y tendencias 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 la expulsión 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 expulsión 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 ha esperado 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 una cartera 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 el asesoramiento regulatorio[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 de 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. Realizar 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 de canal 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 de provisión 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 AML/CFT 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, 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 y la notificación 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. Merece la pena 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, pero también para identificar los errores y duplicidades de las notificaciones antes de presentarlas 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 la notificación de actividades sospechosas 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 *Suspicious Activity Report*, 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 *Suspicious Activity Report*. 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.

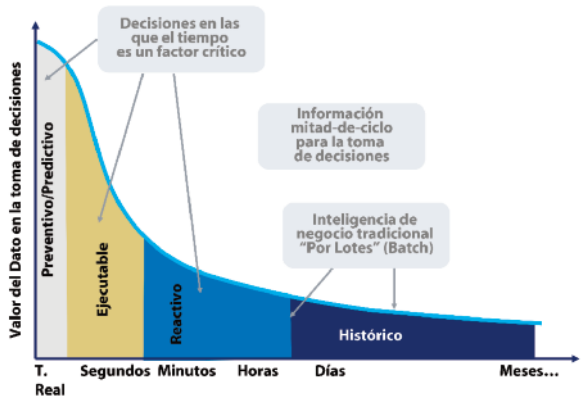
En el ámbito de la gestión de casos, el amplio uso de las redes sociales vuelve a exigir la ingestión de datos no estructurados y el uso de gráficos para encontrar posibles conexiones entre clientes y delincuentes. Por último, las plantillas estandarizadas para la presentación de informes que utilizan 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



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.