

Automatizando el Buen Gobierno en la prevención del blanqueo

**Luis Rodríguez Soler y
Juan Luis Escribano**
Socio Director y Gerente
de BROSETA Compliance

BROSETA

La globalización de los mercados, la internacionalización de la actividad bancaria y la mentalización por parte de los Gobiernos, han provocado que la prevención y la detección del Blanqueo de Capitales y la Financiación del Terrorismo en las entidades financieras se haya convertido en una necesidad estratégica en las organizaciones que son sujeto obligado a estos efectos.

De hecho, en España los procedimientos en esta materia pueden ser considerados referente para la prevención de otros delitos, en un ambiente regulatorio donde nuestro Código Penal ha recibido diversas revisiones desde 2010.

Todo este ambiente de mayor presión regulatoria, aterrizada en forma de nuevas leyes dentro de los estados, ha exigido a las entidades financieras elevadas inversiones, y a tener que adaptarse a los mismos en términos operativos y de organización.

En el caso español, y centrándonos exclusivamente en la Ley 10/2010 de 28 de abril y el RD 304/2014 de 15 de mayo, existen algunos conceptos interesantes a los que conviene prestar atención si queremos que nuestro sistema de Prevención esté alineado con lo que nos pide el regulador, máxime considerando que la prevención y detección de este tipo de actividades pueden constituir acciones atenuantes y eximentes en el ámbito penal por recoger dicho Código ambos delitos como críticos de cara a su prevención, y /o no comisión.

Conceptos como análisis de riesgo, control interno, diligencia debida, titularidad real, alerta, análisis estructurado, herramienta, seguimiento, producto, canal, operativa, y así algunos más, demuestran que la puesta en práctica y actualización constante de un completo y homogéneo sistema contra el blanqueo de capitales y la financiación del terrorismo es un desafío que exige la gestión de muchas variables y conceptos de forma simultánea y secuencial.

Según el Comité de Basilea, “*incumplimientos normativos*” pueden provocar riesgos legales, de reputación e integridad, operativos, de concentración o de solidez bancaria. Para la gestión de los mismos tenemos que establecer por ello adecuados sistemas preventivos, sistemas que han de basarse en:

- Buen Gobierno, materializado en una adecuada estructura evidenciada de control y políticas y procedimientos;
- Conocimiento del Cliente, a través del análisis del riesgo inherente de cada uno, de patrones operativos y de comportamiento;
- y Formación, indispensable cuando hablamos de personas que desarrollan su actividad dentro de la prevención y detección del blanqueo de capitales y financiación del terrorismo es indispensable.

Sistema automatizado

Según el RD 304/2014 de 5 de mayo, “*se procede a un redimensionamiento de las obligaciones de tipo procedimental exigidas a ciertos tipos de sujetos obligados. El objetivo es limitar las obligaciones procedimentales para los sujetos de tamaño más reducido, incrementando la exigencia en función de la dimensión y volumen de negocio del sujeto obligado. Un planteamiento que se justifica*

"Precisaremos disponer, para tranquilidad de la alta dirección, de un sistema integrado de gestión, documentación, seguimiento y control de todas las actividades preventivas y de detección, incluyendo la gestión de la documentación a enviar al Servicio Ejecutivo (SEPBLAC), resto de autoridades competentes, y los requerimientos a que éstos nos obliguen."

tanto desde el punto de vista económico como de gestión del riesgo, que en el caso de entidades de gran tamaño, requiere de un tratamiento centralizado, especializado y automatizado".

También en el artículo 23, referido a "Alertas", se hace referencia a que "en el caso de sujetos obligados cuyo número anual de operaciones exceda de 10.000, será preceptiva la implantación de modelos automatizados de generación y priorización de alertas".

Probablemente estemos pensando que por volumen y sector en el que operamos no es necesario que dispongamos de un modelo automatizado de control de alertas. Pero si nos hacemos preguntas como "¿Tengo acceso a la titularidad real de mis clientes?" "¿Conozco si mi cliente está en alguna lista negra o de riesgo?" "¿Tengo acceso a las alertas de manera automática?" "¿Puedo hacer un análisis estructurado y homogéneo de las operaciones?" "¿Mantengo una trazabilidad de quién ha hecho qué y cuándo en el análisis?" "¿Hago seguimiento de la relación de negocio?" "¿Soy capaz de detectar cambios de patrón de comportamiento?" "¿Llevo un registro de todas las operaciones según detalla la norma?", es posible que las respuestas no sean siempre satisfactorias.

La gran pregunta que subyace sería: "¿Tengo todos estos elementos en un mismo lugar o están dispersos en varias partes?" En definitiva, ¿puedo asegurar que mi sistema de prevención cumple con las prácticas razonables dentro del sector y permite centralizar el trabajo de la unidad especializada en materia de prevención?

La conclusión es que, si bien sí disponemos de un sistema, entendiendo como tal contar con políticas y procedimientos, algunas herramientas, algunas personas dedicadas a ello, seguramente no es lo suficientemente robusto, conectado, estructurado y homogéneo. Por tanto, precisaremos disponer, para tranquilidad de la alta dirección, de un sistema integrado de gestión, documentación, seguimiento y control de todas las actividades preventivas y de detección, incluyendo la gestión de la documentación a enviar al Servicio Ejecutivo (SEPBLAC), resto de autoridades competentes, y los requerimientos a que éstos nos obliguen.

Analizado en qué punto de madurez nos encontramos, tendremos que pensar cómo queremos que sea nuestro sistema, que ofrezca la seguridad casi total de que no se escapa nada, y que tenemos las herramientas en la mano suficientes para lograr que nuestra entidad esté cumpliendo con los requerimientos regulatorios.

No pensemos que un sistema automatizado de alertas que además permita gestionar aspectos como el conocimiento del cliente, la documentación a solicitar y su almacenamiento, el análisis de las operaciones, el establecimiento de patrones o la titularidad real, es algo sólo al alcance de grandes entidades.

Los sistemas automatizados evitan riesgos operativos por el componente manual de uso de la información y le proporcionan a la organización una información homogénea y estructurada. De igual manera, permiten a la unidad especializada en prevención centrar sus esfuerzos en la evaluación de los riesgos y en el análisis profundo de las operaciones.

Y la buena noticia es que la tecnología, a la par que ha evolucionado en el ámbito de nuestros dispositivos domésticos, también ha llegado al sector corporativo, habiendo en el mercado soluciones con una potencia ingente para presupuestos más razonables que en el pasado. La clave está en saber dimensionar nuestro universo y nuestras necesidades reales con un verdadero enfoque basado en riesgo. ■