BUENAS PRÁCTICAS

Aplicación de listas de personas y entidades sujetas a sanciones y contramedidas financieras internacionales

Enero 2015

SEPBLAC

Servicio Ejecutivo de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias

Introducción

La Unión Europea, de acuerdo con los objetivos de la Política Exterior y de Seguridad Común, ha impuesto, por iniciativa propia o de acuerdo con las Resoluciones del Consejo de Seguridad de las Naciones Unidas, medidas restrictivas y sanciones de distinta naturaleza a determinados países y a las personas físicas y jurídicas que se enumeran expresamente en los instrumentos jurídicos correspondientes.

Entre las obligaciones impuestas destacan, entre otras, las de acordar la congelación o bloqueo de los fondos y recursos económicos de determinadas personas físicas o jurídicas, y la prohibición de ponerlos a su disposición o utilizarlos en su beneficio.

La normativa española de prevención del blanqueo de capitales y de la financiación del terrorismo recuerda expresamente que, aparte de las que pudieran acordarse por las autoridades nacionales, las medidas restrictivas y sanciones de la Unión Europea son de aplicación obligatoria, siendo su incumplimiento constitutivo de infracción grave o muy grave.

Uno de los aspectos prácticos más destacados en que se concreta el cumplimiento de estas obligaciones es el consistente en la verificación de que los clientes, o las personas con las que se realizan operaciones, no están incluidos en las listas de sanciones publicadas (en adelante, denominadas a veces simplemente “listas”).

El conocimiento adquirido por el Sepblac en su actividad como Unidad de Inteligencia Financiera se ha visto completado con la experiencia obtenida como Autoridad Supervisora en las inspecciones a entidades financieras. En este contexto y con el ánimo de servir de orientación a quienes estén obligados al cumplimiento de estas obligaciones, se ha decidido sistematizar en un documento público una serie de buenas prácticas en la aplicación práctica de listas de sanciones y contramedidas financieras.

Las entidades financieras, dado su volumen de operaciones y la consecuente necesidad de utilizar complejas aplicaciones informáticas, son quienes pueden encontrar mayor utilidad a estas buenas prácticas. No obstante, se entiende que también pueden ser utilizadas, con las necesarias adaptaciones, por el resto de personas sujetas a estas obligaciones.

Las medidas restrictivas aprobadas por la Unión Europea constituyen prohibiciones absolutas, por lo que la falta de congelación o bloqueo de fondos de personas o entidades designadas supone la comisión de una infracción administrativa. En este contexto, si bien no se configura como elemento bastante para exonerar la responsabilidad, la mejor calidad procedimental es un factor esencial encaminado a mitigar o eliminar el riesgo de incumplir la normativa.

Es importante indicar que la publicación de estas buenas prácticas no supone la imposición de obligaciones adicionales ni una intensificación de las previstas en la normativa aplicable en materia de sanciones y contramedidas financieras internacionales.

Cabe repetir que se publican con la intención fundamental de que puedan servir de orientación para el diseño e implantación de procedimientos de control interno adecuados. Asimismo, tampoco se trata de una relación cerrada e inamovible, sino que está abierta a modificaciones, sea para incorporar otras buenas prácticas o para adaptarlas a los cambios de todo tipo (normativos, tecnológicos, etc.) que puedan producirse en el futuro.

Por último, antes de reseñar de forma concisa estas buenas prácticas, debe hacerse una advertencia previa, aun cuando pudiera parecer innecesaria: de acuerdo con la experiencia del Sepblac, no es exacto que la probabilidad real de que se detecte un cliente incluido en listas internacionales sea nula o prácticamente nula. Si bien el número de casos de detección en los últimos años de personas incluidas en listas que eran clientes o intervenían en operaciones de entidades españolas es relativamente bajo, sí alcanza el nivel suficiente para poder afirmar que existe un riesgo que debe necesariamente ser controlado, máxime si se toman en consideración las repercusiones de toda índole que un fallo en esta materia tendría en la persona obligada.

Clasificación de las buenas prácticas

La definición e implantación de los procesos de verificación contra listas implican tener que adoptar una serie de decisiones. Las buenas prácticas que se recogen en este documento se presentan agrupadas en los cinco grandes bloques en que se pueden clasificar estas decisiones atendiendo a su orden cronológico de aplicación en la práctica:

- ámbito de aplicación: se trata básicamente de determinar qué bases de datos de clientes y qué tipo de operaciones, o transacciones, se van a contrastar contra listas;

- obtención de las listas: hay que decidir cuál va a ser la fuente que se va a emplear para disponer de listas actualizadas;

- proceso de aplicación: hay que definir detalladamente cómo va a ser el proceso de verificación; en especial, cuándo se va a hacer la verificación, o con qué periodicidad, y cuándo se entiende que puede existir una coincidencia y debe, por tanto, generarse una alerta para que se realice un análisis que confirme, o descarte, esa posible coincidencia;

- gestión de alertas: se debe definir un sistema de análisis de las alertas que conjugue la rapidez en la toma de decisiones sobre las posibles coincidencias detectadas con la necesidad de asegurar al máximo el acierto en esas decisiones;

- casos de coincidencia real con listas: cuando se concluya que un cliente, o un interviniente en una transacción, está incluido en listas no debe empezarse a estudiar en ese momento lo que ha de hacerse, sino que debe contarse con procedimientos establecidos con anterioridad que determinen claramente qué actuaciones deben seguirse en cada caso para cumplir estrictamente las obligaciones establecidas en los reglamentos comunitarios.

Buenas prácticas en la determinación de bases de datos y transacciones

BP 1 *Elaborar una relación de todas las bases de datos y tipos diferentes de operaciones o transacciones que puede realizar la entidad*

En el análisis de riesgo que deben hacer los sujetos obligados es buena práctica que se incluya una relación completa de las bases de datos y tipos diferentes de operaciones o transacciones de la entidad. Debe recordarse que el análisis de riesgo debe documentarse, así como que ha de ser revisado periódicamente o cuando se verifique un cambio significativo que pudiera influir en el perfil de riesgo del sujeto obligado.

En ese análisis es importante tener cuidado en incluir todas las áreas de negocio, entre ellas el área comercial, internacional, tesorería, gestión de carteras y gestión patrimonial (banca personal), depositaría, venta de inmuebles, y otras; los diferentes canales de distribución que se utilicen tales como los agentes bancarios, la banca telefónica, por internet, y otros; y todos los intervinientes en las operaciones.

El análisis de riesgo será la base de partida para diseñar, atendiendo al nivel de riesgo que se aprecie en que cada tipo de operación o base de datos, las medidas a implantar para dar cumplimiento a las obligaciones relativas a sanciones y contramedidas financieras internacionales.

BP 2 *Verificar contra listas todas las bases de datos y tipos de operaciones*

El punto de partida más acertado en la definición de bases de datos y de tipos de operaciones a verificar contra listas es afirmar que siempre procede realizar verificaciones, en vez de analizar caso a caso cuando procede realizar, o no, la verificación.

BP 3 *Decidir no verificar contra listas sólo cuando exista total certeza de "riesgo cero" por haberse realizado verificaciones anteriores*

Es buena práctica que la decisión de no verificar contra listas alguna base de datos u operación se tome sólo cuando exista certeza de que todos los intervinientes ya han sido verificados con anterioridad por estar incluidos en bases de datos que periódicamente son objeto de comprobación contra listas actualizadas.

Es importante documentar por escrito las razones que justifiquen que no se apliquen listas a determinadas bases de datos o tipos de operaciones.

BP 4 *Analizar y documentar el efecto en los procedimientos a implantar de la intervención de un tercero con obligación de cumplir con el régimen de sanciones y contramedidas financieras*

La intervención en las operaciones de un tercero sujeto a las obligaciones en esta materia es un factor atenuador del riesgo, si bien no hasta el grado de eliminarlo por completo. Es, por ejemplo, el caso de de una transferencia recibida de una entidad bancaria nacional o

de la Unión Europea. Es buena práctica analizar y documentar debidamente el efecto que la intervención de un tercero sujeto a las obligaciones tiene en los procedimientos implantados por el sujeto obligado.

En cualquier caso, ese efecto no puede consistir en no aplicar ninguna medida de verificación ya que, atendiendo a la norma, cuando se detecte que se ha operado con una persona incluida en listas, el que se hubiera decidido previamente no aplicar medida alguna de verificación, confiando en que los terceros no cometan errores, no eximiría a la entidad de la exigencia de responsabilidades por las autoridades.

BP 5 *Aplicar las listas a todas las personas que intervengan*

La aplicación de listas no se ha de limitar, por ejemplo, a los titulares, sino que también se extenderá a todos los intervinientes: apoderados, autorizados, titulares reales, avalistas, etc.

BP 6 *En el caso de operaciones, verificar a quienes no son clientes*

En el caso, por ejemplo, de transferencias recibidas, es preciso verificar al ordenante, en la medida en que el beneficiario, que es cliente de la entidad, ya debe haber sido objeto de verificación. La decisión correcta sería la contraria en el caso de transferencias ordenadas.

BP 7 *En el caso de operaciones, verificar no sólo los campos relativos a los intervinientes, sino también los que recojan el "concepto" o contengan "observaciones"*

La verificación de que los campos "concepto" u otros que recojan observaciones no incluyen nombres de personas incluidas en listas es más compleja que cuando se trata de comprobar campos destinados específicamente a contener el nombre u otros datos de personas, pero no por ello deja de ser importante dado que, con independencia del campo en que formalmente vengan reflejadas, la responsabilidad se sustancia siempre que intervengan en la operación personas o entidades sujetas a sanciones o contramedidas financieras.

Buenas prácticas en la obtención de las listas a verificar

BP 8 *Conocer bien el contenido y la estructura de las listas*

El punto de partida en la valoración de las decisiones a adoptar respecto a cómo obtener las listas, y en su aplicación posterior, es conocer con cierta profundidad el contenido y la estructura de las listas publicadas.

Debe tenerse en cuenta que las listas aprobadas por Reglamentos comunitarios son obligatorias desde el momento de su publicación, por lo que las entidades deben encontrarse en condiciones de aplicar desde ese momento las sanciones y

contramedidas financieras previstas en los mismos. En el caso de los listados aprobados por Naciones Unidas, aunque no directamente obligatorios para los sujetos privados, son incorporados posteriormente por Reglamentos comunitarios, por lo que resulta buena práctica que las entidades tengan un conocimiento de los mismos, de tal manera que puedan anticipar su aplicación.

BP 9 *Justificar, en su caso, la conveniencia de contratar un determinado proveedor externo de listas*

Si bien las listas obligatorias son públicamente accesibles - las Naciones Unidas y la Unión Europea facilitan en sus páginas en internet[1] la relación actualizada de personas físicas y jurídicas incluidas en listas - muchas entidades prefieren acudir a proveedores externos que les facilitan estas listas. Al elegir un proveedor, se deberían tener en cuenta especialmente las garantías de servicio ininterrumpido que ofrece y su rapidez en la incorporación de las adiciones o modificaciones que se realicen en las listas oficiales.

Buenas prácticas en el proceso de aplicación

BP 10 *Valorar expresamente la conveniencia de desarrollar un sistema propio para realizar la verificación contra listas o, por el contrario, contratar una solución informática externa*

El contraste de forma segura y eficiente de las bases de datos y de las operaciones de una entidad frente a listas es una tarea que exige contar con aplicaciones informáticas complejas.

En primer término, es buena práctica sopesar detenidamente la conveniencia de desarrollar un sistema propio para realizar la verificación contra listas o, por el contrario, contratar una solución informática externa.

Es importante que las entidades que decidan contratar proveedores externos escojan al más conveniente sólo después de un análisis minucioso de sus necesidades, y que tengan en cuenta que con la contratación de esos servicios no pueden dar por resuelto el aspecto tecnológico del contraste de listas. Esto es, en los dos casos – desarrollo propio o solución externa – las buenas prácticas que a continuación se señalan son de aplicación en los mismos términos.

BP 11 *Fijar expresamente, y revisar periódicamente, los umbrales de aproximación a los nombres contenidos en listas cuya superación se considera que debe generar una alerta*

No es buena práctica que una entidad decida que, para que se genere una alerta, deba existir una coincidencia total entre la persona que se verifica y una incluida en listas. Por el

[1] http://www.un.org/spanish/sc/committees/consolidated.htm
http://eeas.europa.eu/cfsp/sanctions/consol-list/index_en.htm

contrario, los algoritmos de búsqueda que se empleen han de ser capaces, por ejemplo, de poder obviar errores en la introducción mecanográfica de nombres, transliteraciones alternativas o la utilización de abreviaturas diferentes a las que figuran en listas, etc.

Es buena práctica analizar con detalle el grado de aproximación o de similitud a los nombres contenidos en las listas que se exige para que genere una alerta. Evidentemente, ello implica que las entidades han tener un conocimiento adecuado del algoritmo de búsqueda empleado por las aplicaciones que utilizan.

BP 12 *Adoptar una decisión razonada sobre el momento de realización de las verificaciones*

Para cada proceso relativo a una base de datos y para cada tipo de operación, es buena práctica que se recojan por escrito los motivos que aconsejan realizar la verificación en tiempo real (en un proceso *online)* o, por el contrario, en un momento posterior (lo que se conoce como procesos en *batch*, generalmente ejecutados por la noche). En el caso de los procesos en *batch*, también es aconsejable que conste su periodicidad por escrito.

Esta buena práctica ha de leerse conjuntamente con la buena práctica señalada con el número 18.

BP 13 *Realizar verificaciones periódicas de las bases de datos para asegurar que las listas nuevas, o las modificaciones de listas anteriores, se aplican debidamente*

Sin perjuicio de los procesos *online* relativos a bases de datos – por ejemplo, los que se aplican al dar de alta a un nuevo cliente - la aplicación de procesos en *batch* a toda la base de datos permitiría asegurar que las listas nuevas, o las modificaciones de listas anteriores, se aplican debidamente.

Respecto a estos procesos en *batch*, la buena práctica aconsejaría ejecutarlos de forma rutinaria, y no solo cuando se tenga conocimiento de que se han modificado las listas.

BP 14 *Comprobar periódicamente el correcto funcionamiento del sistema de detección, en especial mediante la realización de simulaciones de altas de clientes o de operaciones que incluyan nombres de personas iguales o similares a los incluidos en listas*

Es buena práctica comprobar periódicamente el correcto funcionamiento del sistema de detección, para lo que es especialmente útil la realización de simulaciones de altas de clientes o de operaciones que incluyan nombres de personas iguales o similares a los incluidos en listas. Los simulacros son la mejor manera de poder asegurar el funcionamiento correcto del sistema - desde la detección de posibles coincidencias hasta la gestión de los casos de inclusión de un cliente en listas - y realizar, en su caso, las correcciones o adaptaciones necesarias.

BP 15 *Mantener un registro de las verificaciones realizadas*

En relación especialmente con los procesos en *batch*, es conveniente llevar un registro en el que se anoten todas sus ejecuciones.

BP 16 *Asegurar la intervención de los órganos de prevención del blanqueo de capitales y de la financiación del terrorismo en el diseño o modificación de los procesos informáticos.*

Es buena práctica que los órganos de prevención sean al menos informados, o mejor, que participen activamente, en las actuaciones de la entidad en el terreno informático que afecten a las bases de datos o a las operaciones sujetas a verificación contra listas.

Buenas prácticas en la gestión de alertas

BP 17 *Describir detalladamente las acciones a realizar cuando se produce una alerta sobre una posible coincidencia de nombres.*

Se comprueba que el sistema de gestión de alertas funciona mejor cuando los procedimientos escritos de actuación para el caso de que se genere ("salte") una alerta sobre una posible coincidencia entre la persona que se verifica y una incluida en listas son detallados y exhaustivos.

BP 18 *Impedir de forma automática que las operaciones se ejecuten hasta que se alcance la conclusión de que la alerta no responde a un caso real de coincidencia de nombres.*

En vez de presuponer que la entidad puede gestionar las alertas con rapidez y, en caso de coincidencia real de nombres, cancelar o retrotraer una operación ya ejecutada, la actuación más prudente es bloquear la operación e impedir su ejecución hasta que se resuelva la alerta.

BP 19 *Atribuir la capacidad de conocimiento y decisión final sobre las alertas a los órganos de prevención del blanqueo de capitales y de la financiación del terrorismo*

Sin perjuicio de la intervención en la gestión de las alertas de personas o departamentos de la entidad distintos de los órganos de prevención del blanqueo de capitales y de la financiación del terrorismo, la buena práctica es que el órgano de prevención: i) tenga conocimiento de todas las alertas generadas; y ii) intervenga necesariamente en su resolución de forma que, sin al menos su visto bueno, no pueda considerarse resuelta una alerta.

Por el contrario, es mala práctica que, por ejemplo, el empleado de la red comercial que está realizando una operación pueda, aun con conocimiento de su superior, dar por resuelta la posible alerta que se genere.

La intervención de los órganos de prevención en los términos antes señalados presupone que el número de alertas que se generan es razonable, para lo que es importante que el algoritmo de búsqueda esté bien definido.

BP 20 *Facilitar a los órganos de prevención del blanqueo de capitales y de la financiación del terrorismo acceso directo a toda la información necesaria.*

Para que puedan realizar su tarea de la forma más eficaz, los órganos de prevención deberían tener acceso directo a toda la información, externa o interna a la entidad, que necesiten.

BP 21 *Dotar a los órganos de prevención del blanqueo de capitales y de la financiación del terrorismo con personas dedicadas exclusivamente a sanciones y contramedidas financieras*

En el caso de entidades financieras es buena práctica que, dentro de las unidades de prevención, uno o más empleados estén dedicados en exclusiva a sanciones y contramedidas financieras. Ello permitiría asegurar que se cuenta con personas debidamente especializadas.

Al respecto, debe tenerse en cuenta que las listas son solo una parte de la actividad exigida por las normas en relación con sanciones y contramedidas financieras, existiendo otras limitaciones o prohibiciones, como las relativas a la exportación o importación de determinados productos o la prestación de ciertos tipos de servicios, que requieren del desarrollo de los adecuados controles por parte de la entidad.

BP 22 *Mantener un archivo integral de todas las alertas*

La buena práctica aconseja mantener un archivo único con todas las alertas que se han analizado en el tiempo, en el que se registrará toda la información relevante: datos de la operación, persona potencialmente incluida en listas, fecha de generación de la alerta, fecha de resolución, motivos, documentación soporte, etc.

BP 23 *Definir criterios para impedir reiteradas alertas idénticas*

Los procedimientos del sistema de alertas pueden prever que no se generen nuevas alertas sobre personas concretas respecto de las que ya se ha comprobado con certeza que no son las personas incluidas en listas.

Ello puede reducir de forma apreciable la carga de trabajo asociada a la gestión de alertas.

BP 24 *Aplicar medidas de diligencia debida reforzada a las personas sobre las que no se puede afirmar con certeza que no están incluidas en listas*

En algunos casos puede ser difícil asegurar que la persona analizada no está incluida en listas. Puede pensarse, por ejemplo, en los casos de homonimia, en los que, si bien puede concluirse con razonable seguridad que se trata de ese caso y que la persona no está incluida en listas, se carece de información suficiente para poderlo afirmar con total certeza. En estos supuestos, la buena práctica aconseja establecer medidas de diligencia debida reforzada a esas personas (en particular, el seguimiento reforzado).

Buenas prácticas en el tratamiento de los casos de coincidencia real con listas

BP 25 *Describir detalladamente las acciones a realizar cuando se concluye que un cliente o un interviniente en una operación está incluido en listas.*

Cuando se concluye que un cliente, o un interviniente en una operación, están incluidos en listas, no parece prudente que se empiece en ese momento a estudiar la actuación a seguir atendiendo al instrumento jurídico correspondiente.

Por el contrario, es buena práctica que los procedimientos precisen de antemano, con el mayor detalle posible, todos los pasos y decisiones que se deben adoptar para dar cumplimiento efectivo a la obligación de bloqueo de los fondos y comunicación a las autoridades.

Al respecto, dada la naturaleza de la materia, debería analizarse la oportunidad de que los servicios jurídicos de la entidad participen en la elaboración y actualización de los procedimientos.

BP 26 *Examinar las operaciones anteriores realizadas por un cliente que ha sido incluido en listas.*

Sin perjuicio de que se adopten las medidas necesarias para dar cumplimiento a las obligaciones legales, cuando se comprueba que un cliente ha sido incluido en listas la buena práctica es realizar un examen especial de su actividad anterior. También deberían ser examinadas las operaciones de otras personas relacionadas con el cliente.

BP 27 *En el caso de que una persona incluida en listas aparezca como contraparte en una operación con un cliente de la entidad, examinar todas las operaciones del cliente aunque no aparezcan en principio relacionadas con la persona en listas*

Como en la buena práctica anterior, también procede realizar examen especial en estos casos.

BP 28 *Considerar la aplicación de listas un proceso permanente*

La aplicación de listas no debería considerarse un proceso cerrado, en el que las decisiones se toman una vez y luego sólo es necesario ponerlas en práctica. Por el contrario, es recomendable que cada cierto tiempo se revise de forma global todo el proceso de verificación de listas.

* * * * *