

POLÍTICAS EN MATERIA DE PREVENCIÓN DEL BLANQUEO DE CAPITALES Y DE LA FINANCIACIÓN DEL TERRORISMO



Versión Octubre 2018

INDICE

Introducción.....	3
1. Política de Aceptación de Clientes	3
2. Política de Identificación del Cliente.....	4
3. Política de Identificación de la Titularidad real.....	4
4. Política de Conocimiento del Cliente.....	4
5. Política de Aceptación de los Bancos Corresponsales.....	5
6. Plan de Formación.....	5
7. Comunicación Interna de Operaciones Sospechosas.....	6
8. Comunicación de Operaciones a las Autoridades.....	6
9. Conservación y Archivo de Documentos.....	6
10. Organización Interna	7
11. Auditoría Interna	7
12. Auditoría Externa	7
13. Patriot Act.	7
14. FACTA (Foreign Account Tax Compliance Act)	8

INTRODUCCIÓN

BMCE BANK INTERNATIONAL constituida en 1994 como entidad bancaria española y registrada en Banco de España con el número 0219, está supervisada en materia de prevención de capitales por el Servicio Ejecutivo de la Comisión para la Prevención del Blanqueo de Capitales e Infracciones Monetaria, adscrito al Banco de España.

España es un país miembro de la Unión Europea y como tal ha traspuesto a su legislación las Directivas CE relativas a la prevención del blanqueo de capitales y de la financiación del terrorismo. También España es miembro del Grupo de Acción Financiera Internacional (GAFI).

Como Banco europeo está sometido a todas las Directivas y Reglamentos europeos relativos a la prevención del blanqueo de capitales y la financiación del terrorismo. En España la principal regulación en la materia es:

- Ley 10/2010 de 28 de Abril de Prevención del blanqueo de capitales y financiación del terrorismo
- Real Decreto 304/2014 de 5 de Mayo

BMCE BANK INTERNATIONAL ha diseñado e implementado un programa de prevención de blanqueo de capitales y financiación del terrorismo basado en políticas y procedimientos de obligado cumplimiento en todas las áreas de nuestra entidad. Así mismo, se han integrado las Recomendaciones y Buenas prácticas del GAFI, Grupo Egmont, SEPBLAC y Banco de España.

1. PRINCIPIOS GENERALES DE LAS POLÍTICAS DE PBC/FT

Tal como queda recogido nuestro Manual de Prevención de Blanqueo de Capitales y Financiación del Terrorismo¹ y los Procedimientos técnicos de desarrollo e implantación, los principios que rigen nuestra actividad en la materia son:

1. **Enfoque riesgo**, mediante la elaboración de informes describiendo y evaluando la exposición al riesgo de PBC/FT con relación a nuestra actividad.
2. **Sensibilización de la alta dirección y el órgano de dirección**, que conocerán los riesgos en la materia y asegurarán que se toman las medidas adecuadas para mitigar dichos riesgos.
3. **Foco de la prevención generalizado**, que incluya no sólo a las unidades técnicas de prevención, sino la propia red de negocio como primer frente de protección.
4. **Retoolimentación derivada de la continua comunicación entre las unidades técnicas y las unidades de negocio**, con relación a los riesgos en los que se pueda estar incurriendo y las medidas necesarias para mitigarlos.

¹ Manual de Prevención de Blanqueo de Capitales recoge todas las políticas y procedimientos internos en materia de PBC/FT, de obligado cumplimiento y conocimiento por parte de todo el personal de la entidad.

5. **Universalidad** que garantice que los protocolos sean aplicados a todos los clientes, operaciones y ámbitos de negocio sin excepción.
6. **Adaptación al negocio** específico de nuestra entidad.
7. **Pilares de la prevención:** determinación de la titularidad real, el conocimiento del origen de los fondos y la coherencia de la operación.
8. **Seguimiento reforzado** de nuevos clientes, productos o servicios
9. **Documento práctico y ágil de implantación** de la normativa vigente.
10. **Revisores externos al sistema respecto de la efectividad** del sistema de PBC/FT.
11. **Actualizaciones y revisión de procedimientos registrados.**

2. POLÍTICA DE ACEPTACIÓN DE CLIENTES.

Por motivos de control de riesgo, **la Entidad no aceptará las siguientes categorías de clientes:**

- ✓ Personas que no estén debidamente identificadas o rehúsen facilitar información o la documentación requerida.
- ✓ Personas que tengan negocios cuya naturaleza haga imposible la verificación de la legitimidad de las actividades o la procedencia de los fondos.
- ✓ Personas incluidas en listas negras de la UE, OFAC, ONU u otras consideradas por la Entidad.
- ✓ Entidades financieras residentes en países o territorios en los que no tengan presencia física ("Shell Banks" o "Bancos Pantalla").
- ✓ Personas de las cuales tengamos sospecha o pruebas fehacientes que estén inmersos en procesos judiciales sobre blanqueo de capitales o de las cuales tengamos sospecha o pruebas fehacientes que participen en actividades delictivas, posean o adquieran bienes que procedan de una actividad delictiva.
- ✓ Casinos u otras actividades de juegos de azar o apuestas, así como personas o entidades que pretendan realizar operativa derivada de actividades relativas a juegos de azar, apuestas o actividades similares sin disponer de los requisitos necesarios, en especial la correspondiente autorización oficial. Tampoco será admitida la comercialización de loterías u otros juegos de azar respecto de las operaciones de pago de premios.
- ✓ Clientes relacionados con la producción o distribución de armas y otros elementos de carácter militar.
- ✓ Las personas físicas o jurídicas que tengan como objeto o actividad la promoción inmobiliaria, agencia, comisión o intermediación en la compraventa de inmuebles.
- ✓ Inversión filatélica y numismática.
- ✓ Personas menores de 18 años
- ✓ Personas jurídicas y otros instrumentos de jurisdicciones de riesgo su admisión será sometida a autorización expresa por la alta dirección.
- ✓ Cliente con insuficiencia de información o documentación

En su admisión, los clientes serán clasificados por el nivel de riesgo en 3 niveles (alto/medio/bajo), en función del riesgo de BC/FT inherentes a su personalidad y actividad. Así, en función del riesgo y en cumplimiento de las normas de diligencia debida, se establecerán las medidas necesarias de seguimiento de su actividad y actualización de su expediente y de la relación comercial. Las medidas de diligencia se adaptarán así a cada tipo de clientes en función de la asignación del riesgo (diligencia simplificada, normal o reforzada).

La documentación requerida para la apertura de cuenta para personas físicas y jurídicas pasa por identificar la persona inequívocamente, y su titular real en su caso, definición de su residencia fiscal, conocimiento de su actividad y origen de fondos, con el requerimiento documental de soporte adecuado a cada tipo de persona.

3. POLÍTICA DE IDENTIFICACIÓN DEL CLIENTE.

Existen normas y procedimientos específicos para asegurar la identificación y conocimiento del cliente.

Mencionar que la entidad tiene procedimientos específicos para identificar a personas expuestas políticamente (PEP's) o familiares directos o colaboradores cercanos al mismo, que como principio general no son individualmente admitidos.

Cuando hay una relación con un PEP (Persona de Responsabilidad Pública), las siguientes medidas de debida diligencia reforzada son tomadas: actualización de los datos obtenidos en el proceso de aceptación del cliente; refuerzo de periodicidad de revisión de la documentación; obtención de información adicional de la transacción (último beneficiario, propósito y naturaleza de la relación de negocio, origen de fondos, patrimonio del cliente, propósito de la operación); o, autorización jerárquica superior para establecer o mantener la relación de negocio o ejecutar la operación, entre otras.

4. POLÍTICA DE IDENTIFICACIÓN DE LA TITULARIDAD REAL

En cumplimiento con la Ley 10/2010, de 28 de abril de Prevención de Blanqueo de Capitales y Financiación del Terrorismo, nuestra entidad tiene implementado un procedimiento de identificación de la titularidad real

La entidad adopta las medidas adecuadas con el fin de comprobar su identidad con carácter previo al establecimiento de relaciones de negocio o a la ejecución de cualquier operación, así como la valoración de posibles modificaciones posteriores a la entrada en relación.

5. POLÍTICA DE CONOCIMIENTO DEL CLIENTE.

Nuestra política de conocimiento de los clientes es un elemento básico de los procedimientos de gestión y control de riesgos del banco, el cual está basada en un enfoque riesgo y en una vigilancia continua, ayudándonos a gestionar con mayor prudencia.

Nuestra entidad cuenta con las normas, procedimientos y controles internos que permitan tener completo conocimiento de sus clientes, de sus actividades y del propósito de su relación de negocios.

Tanto por razones de negocio, como para prevenir determinada operativa sospechosa, las oficinas y los colaboradores comerciales deben conocer suficientemente la actividad desarrollada por la clientela y si la misma, puede justificar las operaciones y los flujos financieros que pasan a través del BMCE International.

Este conocimiento debe considerarse como una de las condiciones necesarias para el inicio de las relaciones comerciales con nuevos clientes, quedando así eliminadas las posibilidades de aperturas de cuentas espontáneas en el banco, sin previa información a la dirección de la Entidad.

Como ya se ha dicho nuestra Política PBC/FT incluye determinados clientes que por sus características no son admitidos. Una vez el cliente es admitido, el procedimiento interno incluye la identificación de los factores de riesgo y la metodología de categorización de clientes. De acuerdo con la categorización de riesgos del banco, los clientes son clasificados en los siguientes niveles de riesgo y frecuencias de revisión: Alto Riesgo (12 meses); Medio Riesgo (18 meses) y Bajo Riesgo (24 meses); Nuevos Clientes (6 meses desde la apertura).

Los factores considerados para realizar la clasificación de riesgos son el perfil de los clientes y sus actividades, países y áreas geográficas de negocio, productos y servicios contratados, canales de distribución y socios, complejidad y volumen de operaciones, desarrollo de nuevos productos y prácticas de negocio, origen de fondos, accionistas, cuentas anuales, participación en el capital y jurisdicción de riesgo.

Destacar que existen mecanismos automáticos para detectar la inclusión de personas en las lista negras de la UE, OFAC y ONU, tanto en el proceso de admisión del cliente como de modo diario, ante cualquier modificación de las mismas. Además, a partir de la experiencia propia, cabe la posibilidad de desarrollar listas propias.

6. POLÍTICA DE ACEPTACIÓN DE LOS BANCOS CORRESPONSALES.

Existen políticas de aceptación de los bancos con los que se establece corresponsalía. Dichas políticas y procesos abarcan desde la recopilación de información sobre los bancos corresponsales al análisis basado en el enfoque riesgo.

Para llevar a cabo el estudio de los bancos, se establece **la siguiente documentación a aportar:**

- Copia de su último reporte anual
- Copia de sus últimas cuentas auditadas
- Copia de su licencia de actividad expedida por el Banco Central de su país.
- Copia de su registro comercial
- Copia de sus estatutos
- Lista de sus accionistas y titulares reales.
- Lista de los miembros de su Consejo de Administración y de su Comité Ejecutivo, además su CVs y pasaportes.
- Copia de su política de PBC/CFT
- Cuestionario de nuestra entidad y el cuestionario Wolfsberg debidamente rellenos y firmados
- US Patriot Act Certification/ W8-BEN-E
- FATCA number

La entidad no podrá establecer o mantener relaciones de corresponsalía con bancos pantalla o con bancos de los que se conoce que permite el uso de sus cuentas por bancos pantalla (artículo 13 Ley 10/2010).

Tampoco se podrá establecer o mantener relaciones de corresponsalía que, directamente o través de una subcuenta, permitan ejecutar operaciones a los clientes de la entidad de crédito representada (artículo 13 Ley 10/2010).

7. ORGANIZACIÓN INTERNA.

BMCE BANK INTERNATIONAL dispone de una organización interna que permite garantizar el cumplimiento homogéneo de las políticas normativas en materia de PBC/FT:

- La **Unidad Técnica de PBC/FT (UTPBC)** es el órgano especializado en la materia y dedicado al tratamiento y análisis de la información relativa a políticas, procedimientos, clientes, operaciones y productos y servicios relevantes para la prevención y mitigación del riesgo PBC/FT.
- El **Órgano de Control Interno (OCI)**, como órgano de representación de las diferentes áreas de negocio afectadas por la normativa de PBC/FT junto con la Dirección de la Entidad, es responsable de la toma de decisiones en cuanto a directrices en la materia, admisión de clientes, análisis de operaciones sospechosas, decisión de comunicaciones al SEPBLAC,

colaboración con la Comisión del SEPBLAC, etc...así como la comprobación del adecuado funcionamiento y eficacia de las medidas y procedimientos.

- El **representante ante el SEPBLAC** es la persona de comunicación y contacto directo tanto a nivel técnico con el OCI como institucional con el SEPBLAC, con acceso global a toda la información y expedientes necesarios para sus labores de seguimiento y control de la materia.
- La **Alta Dirección** de la Entidad por su parte es la responsable última de las políticas y medidas implementadas en la materia, lo que implica tener pleno conocimiento de los riesgos específicos de la Entidad, así como formación en la materia. Además, **el Consejo de Administración y la Dirección General serán quienes aprueben, según se establezca**, los Manuales y procedimientos de PBC/FT, el Informe de autoevaluación del riesgo ante el BC/FT, la Memoria Anual, el Informe de verificación interna o cualquier otro que así se determine.

8. PLAN DE FORMACIÓN.

Tal y como establece la normativa, la formación continuada y permanente del personal en esta materia constituye uno de los objetivos fundamentales de la Entidad para aplicar adecuadas políticas de prevención de blanqueo.

Por ello, la Dirección, con la colaboración del Órgano de Control Interno (OCI), confecciona y promueve planes anuales de formación para sus empleados con el fin de dar a conocer las nuevas exigencias legales que vayan surgiendo, explicar los procedimientos internos en dicha materia y lograr la capacitación adecuada para efectuar la detección de las operativas relacionadas con el blanqueo de capitales.

Los programas de formación tendrán en cuenta las normas internacionales y la legislación local contra el blanqueo de capitales y la financiación del terrorismo, así como las normas y procedimientos internos destinados a combatir el blanqueo de capitales y la financiación del terrorismo, incluida la forma de reconocer las actividades sospechosas y comunicarlas.

El OCIC deberá aprobar el plan de formación y podrá informar a los empleados de las modificaciones normativas en esta materia, así como de todas las nuevas modalidades, técnicas o procedimientos que se detecten susceptibles de ser utilizados para la lucha contra el blanqueo de capitales.

9. CONTROLES INTERNOS Y EXTERNOS

La Entidad tiene encomendado a la Unidad de **Control Permanente** el seguimiento de los procesos y riesgos más inmediatos en la materia, detallado en su planificación, y reportando a las unidades afectadas, la Dirección y el OCI las recomendaciones, mejoras o correcciones que deban hacerse. Semestralmente, presentará un Informe al OCI que incluya estos elementos.

Por su parte, la **Auditoría interna** del banco en su Plan de auditoría supervisa y comprueba la aplicación de las directrices sobre los procedimientos establecidos, de la operativa y los procedimientos, concluyendo una opinión sobre su efectividad y ajuste.

Anualmente un **experto externo independiente** realiza un examen que valora la adecuación de las políticas, procedimiento y manuales en materia de la PBC/FT, conforme a los requisitos normativamente establecidos.

10. COMUNICACIÓN INTERNA DE OPERACIONES SOSPECHOSAS.

Siguiendo las normas y procedimientos internos de comunicación, cualquier empleado que detecte una operación sospechosa de blanqueo deberá comunicarlo al OCI, tras el pertinente análisis de la UTPBC, y determinará su comunicación al SEPBLAC cuando presente indicios de ser sospechosa.

11. COMUNICACIÓN DE OPERACIONES A LAS AUTORIDADES.

Mensualmente se remitirá al SEPBLAC la **comunicación sistemática** de operaciones, según las definiciones normativamente establecidas, a propuesta de la UTPBC.

Por su parte, ante la detección de una posible operación sospechosa, según lo indicado anteriormente, se procederá a la comunicación por indicio, conforme a la legislación en vigor. Asimismo, UTPBC desarrollará y pondrá en práctica los controles adecuados con el fin de detectar cualquier operación susceptible de ser sospechosa.

Para generar dicha información, la UTPBC se valdrá de un sistema de alertas y filtros definidos, además de una catalogación o registro de tipologías de operaciones que puedan tener relación con el BC/FT, con el fin de detectar cualquier posible operación con indicios o relacionada con BC/FT.

Los Sistemas informáticos de BMCE han parametrizado una serie de alertas en operaciones y clientes que han sido definidas internamente por el equipo de Compliance. Si se detecta que un cliente u operación se desvía del comportamiento esperado, el Sistema notifica al Departamento de Compliance para analizar la operación. También se analizan operaciones sospechosas recibidas de los departamentos internos. Cuando el departamento de Compliance recibe una operación sospechosa (del sistema o de los departamentos) su misión consiste en investigar con más detalle los casos sospechosos. Mientras lleva a cabo su investigación y análisis, el equipo de Compliance puede requerir información adicional. La operación puede ser elevada al OCI (Órgano de Control Interno) con toda la información obtenida. El responsable de Compliance presentará la operación al OCI que estudiará la operación y en caso que se aprecie indicio de blanqueo de capitales, el caso será inmediatamente reportado al SEPBLAC (Regulador español).

12. CONSERVACIÓN Y ARCHIVO DE DOCUMENTOS.

El plazo de conservación establecido de la documentación es de diez años, cumpliendo con lo establecido en la Ley 10/2010. La referida documentación o información se archivará adecuadamente de forma que se facilite su localización y se garantice su confidencialidad.

La Entidad realiza copias de seguridad mensualmente, conservándose dichas copias con la diligencia debida.

13. PATRIOT ACT.

Conforme a los requerimientos establecidos por la Ley Norteamericana "USA PATRIOT ACT"², todas aquellas entidades bancarias que estén domiciliadas fuera de Estados Unidos y que deseen entablar o mantener relaciones de corresponsalía internacional con una entidad bancaria o un broker/dealer norteamericano, tienen la obligación de aportar cierta información sobre la naturaleza de sus negocios y el grado de supervisión al que está sometido.

Para dar cumplimiento a este requisito, BMCE BANK INTERNATIONAL ha preparado un Certificado Global USA PATRIOT ACT, que podrá ser utilizado por todas aquellas instituciones financieras que lo precisen y que encontrarán en formato PDF en nuestra página web.

14. FACTA (Foreign Account Tax Compliance Act)

De acuerdo a lo establecido en la Ley de EE.UU. para el Cumplimiento Fiscal de las Cuentas en el Extranjero, FATCA (Foreign Account Tax Compliance Act), nuestra entidad ha realizado el registro en el IRS (Internal Revenue Service) como institución financiera participante.

El Número de Identificación de Intermediario Global - GIIN3, otorgado a nuestra entidad es el *47CQP3.00010.ME.724*.

² Certificado correspondiente al USA Patriot Act, amparando en las normas 313 y 319 de la Patriot Act (Ley Pública 107-56)

³ <http://www.irs.gov/Businesses/Corporations/FATCA-Foreign-Financial-Institution-List-Search-and-Download-Tool>