

# MANUAL DE POLÍTICAS Y PROCEDIMIENTOS PARA LA PREVENCIÓN DE BLANQUEO DE CAPITAL Y LA FINANCIACION DEL TERRORISMO

Noviembre 2017  
(edición 1)



- **Nombre o Razón social:** FRONTING CORREDURÍA DE SEGUROS Y REASEGUROS, S.L.
- **Domicilio:** Avda. Eduardo dato nº 44, planta 1, local 6, 41005
- **Inscripción en el Registro DGS:**
- **NIF:** B90335886
- **Descripción de la actividad:** Correduría de Seguros

|              |
|--------------|
| Índice (1/2) |
|--------------|

|  |           |
|--|-----------|
| <b>1. INTRODUCCIÓN .....</b>   | <b>4</b>  |
| 1.1. <b>Definición de Blanqueo de Capitales y financiación del terrorismo: .....</b> | <b>4</b>  |
| 1.2. <b>Entorno legal .....</b>  | <b>4</b>  |
| 1.3. <b>Objetivos del Manual y Justificación .....</b>                               | <b>6</b>  |
| 1.4. <b>Alcance del Manual.....</b>  | <b>7</b>  |
| 1.5. <b>Sujeto Obligado .....</b>  | <b>7</b>  |
| <b>2. POLÍTICA DEL GRUPO FRONTING .....</b>  | <b>9</b>  |
| 2.1. <b>Introducción.....</b>  | <b>9</b>  |
| 2.2. <b>Estructura Organizativa .....</b>  | <b>9</b>  |
| 2.3. <b>Política de admisión, identificación y conocimiento del cliente .....</b>    | <b>10</b> |
| 2.4. <b>Análisis de operativa inusual .....</b>                                      | <b>10</b> |
| 2.5. <b>Comunicación de operativa inusual.....</b>                                   | <b>11</b> |
| 2.6. <b>Conservación y archivo de documentación .....</b>                            | <b>11</b> |
| 2.7. <b>Formación .....</b>  | <b>12</b> |
| 2.8. <b>Informe de experto Externo / Auditoría Interna .....</b>                     | <b>12</b> |
| 2.9. <b>Régimen Sancionador .....</b>  | <b>13</b> |
| 2.10. <b>Normas complementarias de actuación.....</b>                                | <b>13</b> |
| <b>3. ESTRUCTURA ORGANIZATIVA.....</b>   | <b>14</b> |
| 3.1. <b>Introducción.....</b>  | <b>14</b> |
| 3.2. <b>Órgano de Control Interno (OCI) .....</b>                                    | <b>15</b> |
| 3.3. <b>Representante ante el SEPBLAC.....</b>                                       | <b>18</b> |
| 3.4. <b>Unidad de Prevención de Blanqueo de Capitales (UPBC).....</b>                | <b>20</b> |
| 3.5. <b>Canal de distribución .....</b>  | <b>21</b> |
| <b>4. POLÍTICA DE ADMISIÓN, IDENTIFICACIÓN Y CONOCIMIENTO .....</b>                  | <b>23</b> |
| 4.1. <b>Análisis de riesgo.....</b>  | <b>23</b> |
| 4.2. <b>Categorización de clientes por riesgo.....</b>                               | <b>23</b> |
| 4.3. <b>Identificación de clientes .....</b>   | <b>25</b> |

|             |  |           |
|-------------|--|-----------|
| <b>4.4.</b> | <b>Conocimiento de clientes</b> .....  | <b>28</b> |
| <b>4.5</b>  | <b>Identificación y conocimiento en Vida Colectivos</b> .....                | <b>28</b> |
| <b>5.</b>   | <b>ANÁLISIS DE OPERATIVA INUSUAL</b> .....                                   | <b>29</b> |
| <b>5.1.</b> | <b>Introducción</b> .....  | <b>29</b> |
| <b>5.2.</b> | <b>Canal descentralizado de detección de operativa inusual</b> .....         | <b>29</b> |
| <b>5.3.</b> | <b>Canal centralizado de detección de operativa inusual</b> .....            | <b>29</b> |
| <b>6.</b>   | <b>COMUNICACIÓN DE OPERATIVA SOSPECHOSA</b> .....                            | <b>31</b> |
| <b>6.1.</b> | <b>Introducción</b> .....  | <b>31</b> |
| <b>6.2.</b> | <b>Comunicación singular de operaciones</b> .....                            | <b>31</b> |
| <b>6.3.</b> | <b>Comunicación sistemática de operaciones</b> .....                         | <b>32</b> |
| <b>6.4.</b> | <b>Requerimientos de las Autoridades</b> .....                               | <b>32</b> |
| <b>7.</b>   | <b>CONSERVACIÓN Y CONFIDENCIALIDAD</b> .....                                 | <b>34</b> |
| <b>8.</b>   | <b>ANEXO I - PROCEDIMIENTOS INTERNOS</b> .....                               | <b>35</b> |
| <b>8.1.</b> | <b>Procedimientos internos en FRONTING Vida y Pensiones</b> .....            | <b>35</b> |
| 8.1.1.      | <i>Política de admisión, identificación y conocimiento de clientes</i> ..... | 35        |
| 8.1.2.      | <i>Detección y análisis de operativa sospechosa</i> .....                    | 42        |
| 8.1.3.      | <i>Reporting de operativa sospechosa</i> .....                               | 47        |
| <b>9.</b>   | <b>ANEXO II - PLANTILLAS COMUNICACIÓN INTERNA OPERATIVA INUSUAL</b> .....    | <b>50</b> |
| <b>10.</b>  | <b>ANEXO III – LISTADO DE OPERATIVA SUSCEPTIBLE DE SER SOSPECHOSA</b> .....  | <b>52</b> |

## 1. INTRODUCCIÓN

### 1.1. Definición de Blanqueo de Capitales y financiación del terrorismo:

Se entiende por **blanqueodecapitales:**

- ▬ a) *La conversión o la transferencia de bienes, a sabiendas de que dichos bienes proceden de una actividad delictiva o de la participación en una actividad delictiva, con el propósito de ocultar o encubrir el origen ilícito de los bienes o de ayudar a personas que estén implicadas a eludir las consecuencias jurídicas de sus actos.*
- ▬ b) *La ocultación o el encubrimiento de la naturaleza, el origen, la localización, la disposición, el movimiento o la propiedad real de bienes o derechos sobre bienes, a sabiendas de que dichos bienes proceden de una actividad delictiva o de la participación en una actividad delictiva.*
- ▬ c) *La adquisición, posesión o utilización de bienes, a sabiendas, en el momento de la recepción de los mismos, de que proceden de una actividad delictiva o de la participación en una actividad delictiva.*
- ▬ d) *La participación en alguna de las actividades mencionadas en las letras anteriores, la asociación para cometer este tipo de actos, las tentativas de perpetrarlas y el hecho de ayudar, instigar o aconsejar a alguien para realizarlas o facilitar su ejecución.*

Se considerará que hay blanqueo de capitales aun cuando las actividades que hayan generado los bienes se hubieren desarrollado en el territorio de otro Estado.

En consecuencia, el proceso de blanqueo de capitales consta de las siguientes fases:

**Colocación:** introducción del dinero procedente de actividades delictivas en el sistema económico. Se caracteriza por la utilización masiva de medios de pago líquidos (efectivo, medios de pago al portador, etc.).

**Encubrimiento:** desvinculación de los fondos de su origen delictivo mediante la realización de todo tipo de movimientos con el fin de fraccionar, acumular, ocultar o trasladar el dinero para que tenga una apariencia legal. Esta fase se caracteriza por la facilidad y rapidez operativa, así como por la posibilidad de realizar operaciones complejas y sofisticadas que permitan la movilización masiva y segura de los fondos.

**Integración:** Retorno del capital al patrimonio del blanqueador, como fondo aparentemente legítimo.

*Se entiende por financiación del terrorismo:*

*“el suministro, el depósito, la distribución o la recogida de fondos o bienes, por cualquier medio, de forma directa o indirecta, con la intención de utilizarlos o con el conocimiento de que serán utilizados, íntegramente o en parte, para la comisión de cualquiera de los delitos de terrorismo tipificados en el Código Penal.*

*Se considerará que existe financiación del terrorismo aun cuando el suministro o la recogida de fondos o bienes se hayan desarrollado en el territorio de otro Estado”.*

### 1.2 Entorno legal

La prevención del blanqueo de capitales y de la financiación del terrorismo está sujeta a la correcta aplicación de la Directiva 2005/60/CE del Parlamento Europeo y del Consejo, de 26 de octubre, relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales y para la financiación del terrorismo, y de la Directiva 2006/70/CE, de la Comisión de 1 de agosto, por la que se establecen disposiciones de aplicación de la Directiva 2005/60/CE. Adicionalmente, se tendrán en consideración las *Cuarenta Recomendaciones* publicadas por el Grupo de Acción Financiera Internacional (FATF-GAFI) en abril de 1990, complementadas por otras *Nueve Recomendaciones publicadas en junio de 2003*, como marco básico de la lucha contra el blanqueo de capitales a nivel internacional.

La principal legislación española en materia de prevención del blanqueo de capitales (PBC) y de financiación del terrorismo es la siguiente:

Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo, que transpone la Directiva 2005/60/CE y deroga la Ley 19/1993, de 28 de diciembre, sobre determinadas medidas de Prevención de Blanqueo de Capitales,

Real Decreto 925/1995, de 9 de Junio, que aprueba el Reglamento de la derogada Ley 19/1993.

Ley 19/2003, de 4 de julio, sobre régimen jurídico de los movimientos de capitales y de las transacciones económicas con el exterior.

Real Decreto 54/2005, de 21 de Enero, por el que se modifica el Reglamento 925/95 de la Ley 19/1993.

Ley 12/2003, de 21 de mayo, de bloqueo de la financiación del terrorismo.

Ley 36/2006, de 29 de noviembre, de medidas para la prevención de fraude fiscal que establece como sujeto obligado a los corredores de seguros.

Artículo 301 del Código Penal, que regula el delito de blanqueo.

Real Decreto 1080/1991, de 5 de julio, por el que se determinan los Países o Territorios a que se refieren los artículos 2, apartado 3, número 4, de la Ley 17/1991, de 27 de mayo, de Medidas Fiscales Urgentes, y 62 de la Ley 31/1990, de 27 de diciembre, de Presupuestos Generales del Estado para 1991, modificado por Real Decreto 116/2003, de 31 de enero.

Orden ECO/2652/2002, de 24 de octubre, por la que se desarrollan las obligaciones de comunicación de operaciones en relación con determinados países al Servicio Ejecutivo de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias, modificada por la Orden EHA/1464/2010, de 28 de mayo, por la que se incluye a la República Islámica de Irán en la lista de países afectados.

Orden Ministerial 2444/2007, de 31 de julio, en relación con el informe de experto externo sobre los procedimientos y órganos de control interno y comunicación establecidos para prevenir el blanqueo de capitales.

Resolución de 10 de septiembre de 2008, de la Dirección General del Tesoro y Política Financiera, por la que se publica el Acuerdo de 14 de julio de 2008, de la Comisión de Prevención de Blanqueo de Capitales e Infracciones Monetarias, por el que se determinan las jurisdicciones que establecen requisitos equivalentes a los de la legislación española de prevención de blanqueo de capitales.

### 1.3 Objetivos del Manual y Justificación

Como parte fundamental en el marco general del sistema de prevención del blanqueo de capitales y de la financiación del terrorismo el presente manual tiene, entre otros, los siguientes objetivos:

Establecer los criterios y procedimientos de estricto cumplimiento para toda la organización de FRONTING, con el fin de asegurar de forma responsable una alta capacidad para afrontar la amenaza que supone el blanqueo de capitales proveniente de actividades ilícitas y de la financiación del terrorismo.

Dar a conocer a todos los administradores, directivos, empleados y colaboradores de cada una de las entidades que conforman el Grupo, y en especial a los que están en contacto con el negocio de vida, el alcance de todas las obligaciones que impone la legislación y establecer los modos para su escrupuloso cumplimiento.

Concienciar a todos los empleados sobre la importancia de la labor de prevención y detección de operaciones sospechosas y la manera de proceder ante las mismas.

Detallar y establecer los efectivos mecanismos de control interno de cada una de las entidades componentes del Grupo FRONTING, para la prevención de blanqueo de capitales y financiación del terrorismo con el fin de reducir al máximo este riesgo.

El artículo 26 de la Ley 10/2010, de 28 de abril, de Prevención del Blanqueo de Capitales y de la Financiación del Terrorismo, bajo el epígrafe “Medidas de control interno”, establece, en su apartado 3, lo siguiente:

Los sujetos obligados, con las excepciones que se determinen reglamentariamente, deberán aprobar un manual adecuado de prevención del blanqueo de capitales y de la financiación del terrorismo, que se mantendrá actualizado, con información completa sobre las medidas de control interno a que se refieren los apartados anteriores. Para el ejercicio de su función de supervisión e inspección, el manual estará a disposición del Servicio Ejecutivo de la Comisión, que podrá proponer al Comité Permanente de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias la formulación de requerimientos instando a los sujetos obligados a adoptar las medidas correctoras oportunas. Los sujetos obligados podrán remitir voluntariamente su manual al Servicio Ejecutivo de la Comisión, a efectos de que por éste se determine la adecuación de las medidas de control interno establecidas, o que se propongan establecer. La conformidad del manual con las recomendaciones formuladas por el Servicio Ejecutivo de la Comisión permitirá entender cumplida la obligación establecida en el presente apartado.

Por su parte, el Artículo 52 de la Ley 10/2010 establece, entre las Infracciones graves, en su apartado 1. p), la siguiente:

*“El incumplimiento de la obligación de aprobar y mantener a disposición del Servicio Ejecutivo de la Comisión un manual adecuado y actualizado de prevención del blanqueo de capitales y de la financiación del terrorismo, en los términos del artículo 26.3.”*

Con el presente Manual, FRONTING CORREDURÍA DE SEGUROS Y REASEGUROS, S.L. (en adelante la Entidad) cumple lo previsto en el artículo 26.3 de la Ley 10/2010.

## 1.4 Alcance del Manual

El presente Manual de Prevención del Blanqueo de Capitales y de la Financiación del Terrorismo contempla la implantación del sistema de prevención del blanqueo de capitales y financiación del terrorismo en la entidad FRONTING, en lo relativo al ramo de Vida.

En consecuencia, este Manual desarrolla las obligaciones particulares y específicas que en estas materias debe considerar el Grupo FRONTING.

## 1.5 Sujeto Obligado

Los corredores de seguros (sujetos obligados según el Art. 2.1.b de la Ley 10/2010, de PBC y FT) no están incluidos en la exención a la que hace referencia, del Art. 31.1 Reglamento, que establece lo siguiente: *“Los sujetos obligados aprobarán por escrito y aplicarán políticas y procedimientos adecuados de prevención del blanqueo de capitales y de la financiación del terrorismo. Los corredores de comercio y los sujetos obligados comprendidos en el artículo 2.1 i) a u), ambos inclusive, que, con inclusión de los agentes, ocupen a menos de 10 personas y cuyo volumen de negocios anual o cuyo balance general anual no supere los 2 millones de euros, quedan exceptuados de las obligaciones referidas en este artículo y en los artículos 32, 33, 35, 38 (examen de experto externo) y 39. Estas excepciones no serán aplicables a los sujetos obligados integrados en un grupo empresarial que supere dichas cifras”*. Por lo tanto, los expertos externos, durante el mes siguiente al semestre de referencia, comunicarán al SEPBLAC las revisiones de experto externo realizadas a dichas entidades.

Asimismo, los corredores de seguros mantienen la obligación de comunicar al SEPBLAC cualquier indicio de Blanqueo, en el momento en que se tuviese conocimiento.

Independientemente de lo anterior, quedan exceptuados de la obligación de comunicación sistemática los corredores de seguros a los que se refiere el artículo 2.1 b) de la Ley 10/2010, de 28 de abril, las empresas de asesoramiento financiero y los sujetos obligados mencionados en los párrafos k) a y), ambos inclusive, del artículo 2.1 de la misma ley (Art.27.3 Reglamento).

Con respecto a la formación, los corredores no están exentos de realizar un plan anual de formación, debiendo recibir formación externa a tal efecto, y conservando los correspondientes certificados o justificantes de su efectiva realización, como prueba frente a un posible requerimiento de dicha información en el marco de una inspección.

Todas las actividades FRONTING se realizan conforme a las mejores prácticas y con estricto cumplimiento de la normativa vigente y su propósito es que no sea utilizado para realizar ninguna operación ilegal.

Todos los profesionales que integran la red de FRONTING y los administrativos y colaboradores que en ella trabajan conocen y cumplen las normas establecidas para conocer al cliente y detectar operaciones que puedan constituir indicios o certeza de blanqueo de capitales o de financiación del terrorismo.

La Ley 10/2010, de 28 de abril, de prevención del Blanqueo de Capitales y de la Financiación del Terrorismo establece determinadas obligaciones, previstas en la propia Ley, sin perjuicio de las especificaciones que se establezcan reglamentariamente, que deben cumplir los sujetos obligados incluidos en su artículo 2.

FRONTING, al integrarse como grupo empresarial y franquiciador supera el límite impuesto de 10 personas vinculadas al sector Vida y volumen de negocios anual o balance general anual superior a 2 millones de euros, por lo que, como sujeto obligado, asume las obligaciones en esta materia respecto de las operaciones realizadas, en su caso, a través de su personal, franquicias, sus colaboradores externos y otras personas físicas o jurídicas que actúen como mediadores o intermediarios de ella.

Este Manual regula las obligaciones, actuaciones y procedimientos que tiene FRONTING, dirigidos a impedir y prevenir la utilización de su actividad para el Blanqueo de Capitales y financiación del terrorismo e irá unido a otros documentos de la empresa como la política de admisión de clientes. En todo caso, además del presente Manual, el personal que presta sus servicios en FRONTING cuenta con el material de consulta facilitado como consecuencia del curso de formación impartido, así como con la información actualizada periódica que confeccione o reciba.

Dentro de las obligaciones exigidas por la normativa se trata de cumplir, en particular, con lo dispuesto en los siguientes grandes grupos de obligaciones con carácter general:

- Medidas de diligencia debida (normales, simplificadas o reforzadas).
- Medidas de control interno (examen externo, formación, protección e idoneidad de empleados, directivos y agentes, protección de datos de carácter personal).
- Obligaciones de información (examen especial, comunicaciones por indicio o sistemáticas, abstención de ejecución, prohibición de revelación, conservación de documentos y colaboración con autoridades).



## **2. POLÍTICA DEL GRUPO FRONTING**

### **2.1. Introducción**

El Grupo FRONTING se encuentra comprometido, de acuerdo con la normativa vigente, a seguir todas las iniciativas legales nacionales e internacionales para prevenir el blanqueo de capitales, la financiación del terrorismo y otros delitos financieros.

El Grupo está supervisado, en materia de prevención de blanqueo de capitales y financiación del terrorismo, por el Servicio Ejecutivo de la Comisión para la Prevención del Blanqueo de Capitales e Infracciones Monetarias (SEPBLAC).

Por este motivo, el Grupo ha diseñado e implementado un programa basado en el cumplimiento de la regulación española y de los estándares internacionales generalmente aceptados, adoptando, entre otros, los siguientes principios globales para impedir su utilización con propósitos delictivos:

Disponer de una estructura para la prevención de blanqueo de capitales y la financiación del terrorismo

Tener políticas y procedimientos internos de prevención de blanqueo de capitales y de la financiación del terrorismo.

Implementar estándares de identificación y conocimiento del cliente.

Prevenir e impedir la realización de operaciones sospechosas de blanqueo de capitales o relacionadas con la financiación de actividades terroristas, excepto cuando la abstención no sea posible o pueda dificultar la investigación.

Comunicar a las autoridades competentes aquellas operaciones con indicios de estar relacionadas con el blanqueo de capitales o con la financiación de actividades terroristas, así como cualesquiera que determine la legislación vigente en cada momento.

Organizar sesiones de formación a sus empleados y colaboradores

Someter sus políticas y procedimientos a revisiones de Auditoría Interna y Externa.

### **2.2. Estructura Organizativa**

El Grupo FRONTING dispone de una estructura interna (procedimientos y órganos de control, principalmente) para la prevención de blanqueo de capitales y la financiación del terrorismo cuyos objetivos generales son conocer, prevenir, impedir y comunicar las operaciones relacionadas con el blanqueo de capitales y la financiación del terrorismo.

Los principios básicos que basan el desarrollo de esta estructura son los de rapidez, seguridad, eficacia y coordinación, tanto en su funcionamiento interno, como en el análisis y comunicación de la información relevante al Servicio Ejecutivo.

Dicha estructura interna estará formada por: el Consejo de Administración, el Órgano de Control Interno (OCI), la Unidad de Prevención de Blanqueo de Capitales (UPBC), el Representante/s ante el SEPBLAC y los Empleados del canal de distribución, así como las funciones correspondientes de todos ellos, que se hacen extensibles a la totalidad de la entidad y que se detallan en los próximos apartados del presente Manual de PBC.

### **2.3. Política de admisión, identificación y conocimiento del cliente**

El presente Manual pretende incorporar unos procedimientos de admisión y controles internos que garanticen un eficaz y completo conocimiento de nuestros clientes, con el fin de:

Verificar la identidad de todos los clientes con los que mantenemos relaciones comerciales.

Verificar cualquier información adicional (verificación de la actividad, documentación de conocimiento, etc.) que sirva para evaluar los factores de riesgo establecidos.

Documentar los procesos de análisis de decisiones en la aceptación de nuestros clientes.

Los riesgos de un inadecuado conocimiento de nuestros clientes, que suponen, a su vez, el principal riesgo derivado del blanqueo de capitales o la financiación del terrorismo son:

Riesgo regulatorio: imposición de sanciones por parte de los órganos supervisores.

Riesgo reputacional: pérdida de imagen pública de nuestra entidad al vincularla con operaciones de blanqueo de capitales o de financiación de actividades terroristas.

Riesgo operativo: inexistencia o relajamiento de los controles “anti-blanqueo”.

Se considera fundamental para prevenir el blanqueo de capitales y la financiación del terrorismo la aceptación o no de los clientes en función de la evaluación del riesgo, definido conforme a sus características y actividad (la categorización de clientes por riesgo se detalla en el apartado 4.2 del presente documento).

### **2.4. Análisis de operativa inusual**

#### **Examen especial de operaciones**

Se examinará con cuidadosa atención cualquier operación, con independencia de su cuantía que, por su naturaleza, pueda estar aparentemente vinculada con el blanqueo de capitales o la financiación del terrorismo (el listado completo de operativa inusual o susceptible de ser sospechosa se adjunta en el anexo III del presente Manual).

El análisis y examen de operaciones tendrá como objetivos principales:

Detectar las operaciones inusuales o incoherentes.

Emprender las acciones adecuadas.

Informar a las autoridades de acuerdo con la legislación aplicable.

Cualquier empleado debe comunicar a la Unidad de Prevención de Blanqueo de Capitales, una operación inusual.

Como resultado de la investigación se determinará:

Continuar con normalidad la operación.

Establecer un seguimiento de la operación y las sucesivas del mismo cliente o relacionadas.

Comunicar como operación potencialmente sospechosa de estar relacionada con el blanqueo de capitales o la financiación del terrorismo al OCI, para que evalúe sobre la comunicación al regulador.

### **Abstención de ejecución de operaciones**

En todo caso, la Entidad se abstendrá de ejecutar cualquier operación respecto a la que exista indicio o certeza de que está relacionada con el blanqueo de capitales o la financiación del terrorismo sin haber efectuado previamente la comunicación al Servicio Ejecutivo a través de los órganos internos designados.

No obstante, cuando la abstención no sea posible o pueda dificultar la investigación de la operación, ésta se podrá llevar a cabo efectuando la comunicación inmediatamente después de su ejecución.

## **2.5. Comunicación de operativa inusual**

### **Comunicación de operaciones**

Cualquier empleado, directivo u órgano que, en el ejercicio de sus funciones, detecte cualquier operación relacionada con el blanqueo de capitales o la financiación del terrorismo, comunicará la misma a la UPBC utilizando el formulario del Anexo II.

### **Prohibición de revelación**

Las comunicaciones sobre operaciones inusuales tendrán un carácter estrictamente confidencial, así como la identidad de las personas que las hayan realizado.

### **Otras normas de actuación**

Se extremarán las precauciones respecto a las operaciones sucesivas que realicen los intervinientes vinculados a la operativa inusual que haya sido comunicada, informando a la Unidad de Prevención de Blanqueo de Capitales de cualquier hecho u operación relevante de dichos intervinientes que se produzca con posterioridad a la comunicación.

## **2.6. Conservación y archivo de documentación**

La Entidad conservará, durante como mínimo diez años, todos los documentos o registros correspondientes que, con fuerza probatoria, acrediten tanto la identificación como la adecuada realización de las operaciones y las relaciones de negocio con sus clientes, en soportes ópticos, magnéticos o electrónicos, garantizando su integridad, la correcta lectura de los datos, la imposibilidad de manipulación y su adecuada conservación y localización.

El plazo indicado en el párrafo anterior se contará a partir del día en que finalicen las relaciones con un cliente para los documentos relativos a su identificación o a partir de la ejecución de cada operación, para la conservación de los documentos o registros que la acreditan.

El procedimiento de conservación, debido a la naturaleza de la información contenida en estos documentos, será el adecuado para garantizar una fácil localización como la confidencialidad de la información.

Esta Entidad, además, deberá disponer de un procedimiento de archivo especial para toda la documentación relativa a la investigación de operaciones realizada por la UPBC, los requerimientos de autoridades y la relativa al OCI. Este archivo deberá cumplir igualmente con las medidas de seguridad y confidencialidad requeridas.

## **2.7. Formación**

De acuerdo con la normativa vigente, la formación continuada del personal en materia de prevención de blanqueo de capitales y financiación del terrorismo constituye uno de los objetivos fundamentales del Grupo, ya que es uno de los elementos que forman la base en la que se sustenta la eficacia de la política y procedimientos de la compañía.

Por ello, la UPBC organizará sobre dicha materia planes de formación anuales generales dirigidos a directivos y empleados de cada una de las entidades que conforman el grupo, así como cursos específicamente dirigidos al personal que esté más involucrado en el negocio de Vida, con el fin de lograr la capacitación adecuada para efectuar la detección de las operativas inusuales y dar a conocer la manera de proceder en tales casos. Estos cursos serán presenciales o a distancia.

El objetivo último de los planes de formación será lograr una cultura corporativa sobre el riesgo del blanqueo de capitales y financiación del terrorismo.

Los planes de formación se deberán ir adaptando hacia las nuevas formas de operar de las personas relacionadas con el blanqueo de capitales y la financiación del terrorismo, según se vayan conociendo a través de las publicaciones emitidas por el GAFI, el Servicio Ejecutivo, u otros órganos nacionales e internacionales relacionados con la lucha contra el blanqueo de capitales y la financiación del terrorismo, así como por la propia experiencia adquirida por las entidades del Grupo.

El contenido básico de las sesiones de formación en materia de prevención de blanqueo de capitales y de la financiación del terrorismo constará de los siguientes puntos principales:

- Concepto de blanqueo de capitales y fases
- Concepto de financiación del terrorismo
- Entorno legal
- Supervisor y competencias
- Principales obligaciones de FRONTING, sus empleados, directivos, asociados y colaboradores en esta materia
- Régimen de infracciones
- Régimen sancionador
- Catálogo ejemplificativo de operativa inusual en el sector asegurador

La UPBC controlará la asistencia a las sesiones de formación, recabarán justificantes de la misma, y evaluarán el aprovechamiento de las mismas por los asistentes a través de un cuestionario de evaluación.

Independientemente de los planes de formación, la UPBC deberá estar informada de todas las modificaciones normativas en esta materia, así como de todas las nuevas modalidades, técnicas o procedimientos que se detecten como de ser susceptibles de ser utilizados para la lucha contra el blanqueo de capitales y la financiación del terrorismo, e informar al OCI correspondiente de dichos cambios, con el fin de que se considere su adopción por parte de la política vigente.

## **2.8. Informe de experto Externo / Auditoría Interna**

De conformidad con la Orden Ministerial 2444/2007, de 31 de julio, por la que se desarrolla el Real Decreto 925/1995, de 9 de junio, en relación con el informe de experto externo sobre los procedimientos y órganos internos de control y comunicación establecidos para prevenir el blanqueo de capitales, los sujetos obligados serán objeto de examen anual por un experto externo. En base a este precepto se efectuará una revisión anual, que supervisará:

La eficacia del sistema de prevención del blanqueo de capitales y financiación del terrorismo.

La política, normas y procedimientos de obligado cumplimiento.

Las actividades se realizan de acuerdo con la normativa vigente contra el blanqueo de capitales.

Al margen de la revisión que se realizará con periodicidad anual por parte del experto externo, la propia Unidad de Prevención de Blanqueo de Capitales realizarán revisiones anuales sobre determinados aspectos del sistema de prevención de blanqueo de capitales implantado por la compañía, que incluirán, entre otros, los siguientes:

Procedimiento de gestión de pólizas de Vida

Formación en prevención de blanqueo de capitales y financiación del terrorismo.

Contratos con asociados, franquiciados y colaboradores

Procedimientos de FRONTING en relación a sus canales de distribución.

## **2.9. Régimen Sancionador**

La Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo, establece un cuadro sancionador común para todos los sujetos obligados.

Las infracciones administrativas previstas en la normativa se clasifican en muy graves, graves y leves, dependiendo del tipo de obligación incumplida.

En función de dicha clasificación de infracciones, la ley prevé la imposición de distintos tipos de sanciones, graduables según determinadas circunstancias.

Además de la responsabilidad que corresponda a la entidad obligada, quienes ejerzan en ella cargos de administración o dirección, sean unipersonales o colegiados, serán responsables de las infracciones, cuando éstas sean imputables a su conducta dolosa o negligente.

## **2.10. Normas complementarias de actuación**

El OCI de cada una de las entidades que conforman el Grupo FRONTING está expresamente facultado para el desarrollo de normas complementarias y procedimientos adicionales, o la actualización de este Manual, cuando sea necesario para el efectivo cumplimiento de las obligaciones en esta materia. En todo caso, deberá seguir las directrices establecidas al efecto en el presente Manual del Grupo.

### 3. ESTRUCTURA ORGANIZATIVA

#### 3.1. Introducción

La estructura del Grupo FRONTING engloba además de la gestión interna por sus empleados del ramo de Vida, la gestión de las diferentes empresas asociadas, franquicias y colaboradores, que deberán seguir las prescripciones del presente Manual.

Los diferentes acuerdos de distribución celebrados por FRONTING se muestran a continuación:

- a) En virtud del contrato denominado de ASOCIADO.
- b) Mediante los contratos de FRANQUICIA.
- c) Mediante los contratos de COLABORACIÓN.

Fruto de estos acuerdos, los Administradores, responsables o Consejos de Administración (CA) de cada una de las Entidades que conforman el Grupo FRONTING, se someten a los órganos de control de FRONTING a fin de conocer, prevenir e impedir la realización de operaciones relacionadas con el blanqueo de capitales y financiación del terrorismo y efectuar las comunicaciones establecidas por las leyes.

El **Consejo de Administración de FRONTING**, como el **más alto representante** de cada una de las Entidades en esta materia, será el máximo responsable de la función de prevención de blanqueo de capitales.

Las **funciones principales** del Consejo de Administración en materia de prevención de blanqueo de capitales serán:

**Aprobar** la constitución del OCI y **nombrar** a sus **miembros**.

**Nombrar** el **Representante ante el SEPBLAC**.

**Decidir** sobre aquellos aspectos claves en materia de prevención de blanqueo de capitales y financiación del terrorismo que hayan sido reportados por el OCI.

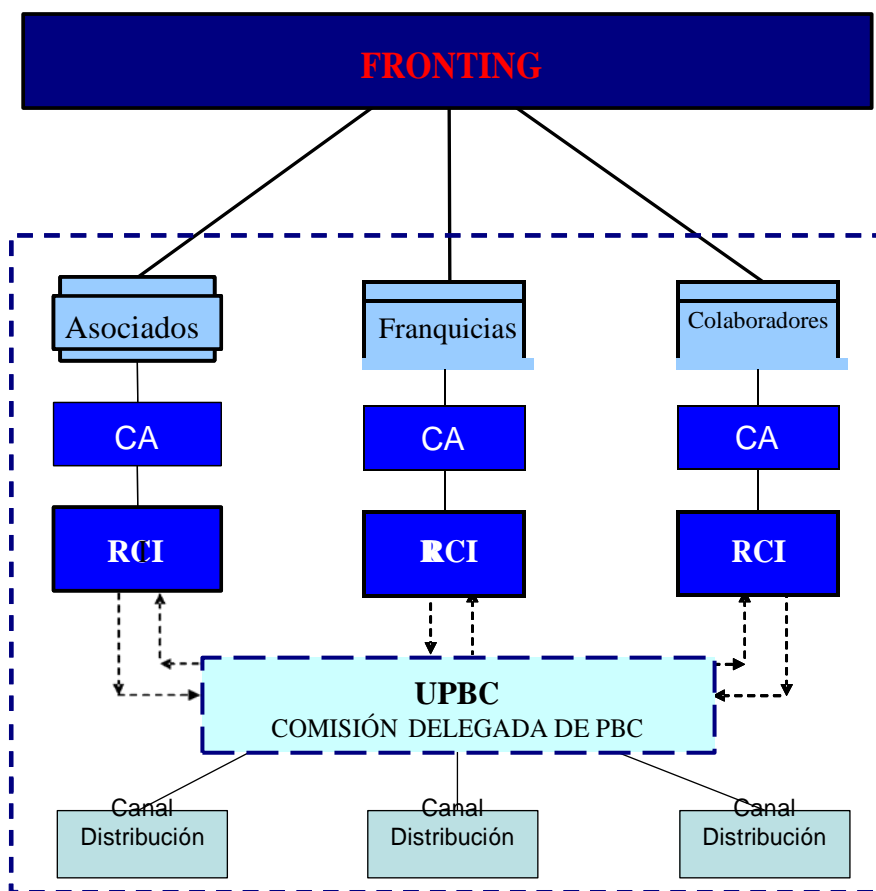
**Aprobar** el **manual de políticas y procedimientos** de la Entidad.

**Designar el Experto Externo** al que se refiere el artículo 28 de la Ley 10/2010, de 28 de abril, de prevención de blanqueo de capitales y financiación del terrorismo, así como sus condiciones de contratación.

La **estructura organizativa** necesaria para la prevención de blanqueo de capitales y financiación del terrorismo en las diferentes entidades deberá contener:

Responsable de Control Interno (RCI).

Estos organismos interrelacionados en las tareas de control y prevención de blanqueo de capitales y financiación del terrorismo llevadas a cabo en cada una de las entidades del Grupo FRONTING se muestran a continuación:



### 3.2. Órgano de Control Interno (OCI)

Conforme a la normativa aplicable, el OCI tendrá como misión principal analizar, controlar y comunicar al SEPBLAC todas las operaciones o hechos susceptibles de estar relacionados con el blanqueo de capitales y la financiación del terrorismo.

El OCI es el órgano de control interno creado por el Consejo de Administración para debatir y proponer a la Entidad la política a desarrollar para prevenir el blanqueo de capitales y financiación del terrorismo y mitigar con ello los riesgos inherentes existentes, principalmente los relacionados con el riesgo regulatorio y el de imagen o reputacional.

Este órgano se someterá a las prescripciones de las leyes locales y responderá a los principios de rapidez, seguridad, eficacia y coordinación, tanto en la transmisión interna como en el análisis y comunicación de las operaciones.

La composición del OCI es la que consta a continuación:

Representante titular ante el SEPBLAC

Secretario del OCI y Representante suplente ante el SEPBLAC

Responsable Unidad de Prevención de Blanqueo de Capitales de FRONTING.

Vocales respectivos responsable/s del canal de distribución de Vida de cada uno de los tres sujetos obligados (asociados, franquiciados y colaboradores).

Las **funciones principales** del OCI serán:

1. **Analizar** aquellas **operaciones** que, por comunicación interna de la UPBC, supongan un riesgo anormal, inusual y **potencialmente indicativas de actividades de blanqueo de capitales**, detectadas, comunicándoselas al SEPBLAC a través del representante cuando sea preciso y proporcionando a dicho Organismo la información y documentación que fuere necesaria para su investigación.
2. **Proponer** las **mejoras** de las **medidas de control** adecuadas para garantizar la prevención de blanqueo de capitales en la Entidad, velando por la actualización de la normativa interna de la Entidad y de su adaptación a las modificaciones legislativas, en su caso.
3. **Establecer políticas** adecuadas de **formación** y reciclaje para que el personal de los Sujetos Obligados tenga conocimiento de los procedimientos internos, de las exigencias derivadas de la normativa en materia de prevención del blanqueo de capitales, fomentando la continua actualización de los contenidos.
4. Podrá **programar cursos** o actividades de información y orientación sobre prevención de blanqueo de capitales, **dirigidos** a los **miembros del OCI**.
5. **Informar** en las reuniones del **Consejo de Administración** sobre cuestiones en materia de prevención de blanqueo de capitales, a través de su Presidente.
6. **Promover** las **relaciones institucionales con el SEPBLAC** a fin de trasladar a la Entidad las últimas tendencias y mejoras desarrolladas en el ámbito de la prevención de blanqueo de capitales.
7. Revisar el **manual de procedimientos** internos en materia de prevención de blanqueo de capitales.
8. Mantener **comunicación con el Experto Externo** y tratar todas aquellas cuestiones relacionadas con el desarrollo de su labor.
9. **Analizar** las **propuestas de mejora** que, en su caso, formule el **Experto Externo**, acordando las medidas necesarias para su cumplimiento.

Además de las funciones anteriormente descritas, el OCI dispone del siguiente **Régimen Interno de Funcionamiento**, o protocolo de actuación:



## **Nombramiento y cese de los miembros del OCI**

El Consejo de Administración nombrará y cesará a los miembros del Órgano de Control Interno, designando especialmente de entre ellos al Representante ante el SEPBLAC y el Representante o Representantes suplentes. Cualquier cese deberá acompañarse del nuevo nombramiento de representantes.

La propuesta de nombramiento de los miembros del OCI debe ser comunicada al Servicio Ejecutivo, en los términos previstos por el citado organismo, que podrá formular observaciones, si estima que los mismos no reúnen las condiciones necesarias.

Si el Servicio Ejecutivo no se pronuncia sobre la propuesta de nombramiento de los miembros del OCI, se entenderá la misma aceptada.

## **Convocatoria, quórum de asistencia y de adopción de acuerdos**

De manera ordinaria se realizarán reuniones semestrales y de manera extraordinaria cuando lo requieran al menos la cuarta parte de sus componentes.

El quórum mínimo será de la mitad más uno de los componentes del OCI para que la constitución del mismo sea válida. En los casos en los que el número de componentes sea una cifra impar, el quórum mínimo para una constitución válida será la cifra resultante de redondear a la alza la mitad del número de componentes.

La adopción de acuerdos será por mayoría simple de los asistentes, siempre y cuando el quórum sea completo y de 2/3 partes en cualquier otra circunstancia, con el voto de calidad del Presidente en caso de empate.

De forma ordinaria y, en concreto, serán objeto de tratamiento en el orden del día los temas siguientes:

- a) Lectura y aprobación, en su caso, del acta derivada de la reunión anterior.
- b) Análisis de operaciones inusuales.
- c) Otros (Informe de experto externo, plan de formación, novedades normativas, etc.)
- d) Ruegos y preguntas.

De forma no ordinaria, se incluirá cualquier asunto relevante en materia de prevención de blanqueo de capitales y financiación del terrorismo como novedades legislativas, cambios en procedimientos o cualquier otra circunstancia de naturaleza similar.

Sin perjuicio de ello, se celebrarán reuniones de carácter extraordinario, si hubiere temas que precisan de su tratamiento, debate o resolución con carácter más urgente con su correspondiente acta.

Las reuniones ordinarias a celebrar cada seis meses serán convocadas a través de correo electrónico por el Secretario del Órgano de Control, por orden del Presidente, comunicando los puntos del día a tratar.

Las reuniones extraordinarias serán convocadas a través de correo electrónico por el Secretario del OCI, a iniciativa propia o de cualquiera de los miembros del Órgano de Control Interno, especificando en cualquier caso los temas que motiven dichas reuniones.

Cualquier modificación en la estructura y funcionamiento del OCI deberá ser aprobada por el Consejo de Administración y comunicada al Servicio Ejecutivo.

### **Régimen de Confidencialidad**

Por su contenido, los asuntos, deliberaciones y acuerdos del OCI están sujetos al deber de confidencialidad, sin perjuicio de las comunicaciones que se acuerde emitir o de la puesta en conocimiento de la Autoridad Judicial y Gubernativa de cuantos actos e informaciones fueran requeridos por aquéllas o de obligada o conveniente comunicación y dejando a salvo el ejercicio individual, por cada componente del OCI, de sus obligaciones legales en orden a la salvaguarda de su responsabilidad.

Toda comunicación de asuntos, informes, datos o acuerdos en materias tratadas por el OCI o de su competencia, deberá advertir al destinatario de la naturaleza y régimen legal de esta materia, con las advertencias de confidencialidad necesarias.

### **Régimen de Trabajos**

El OCI asignará a sus componentes las tareas que resulten necesarias y oportunas realizar, ya fuere en régimen de ponencia, para su examen y adopción de los acuerdos que procedan por el OCI, ya fuere en régimen ejecutivo, en conveniencia de los acuerdos adoptados.

### **Actas**

Se levantará la correspondiente acta por cada una de las reuniones, que será firmada por todos los asistentes y necesariamente por el Presidente y por el Secretario del OCI, aunque estos últimos no acudieren.

Al frente del OCI estará su Presidente, que será nombrado por el Consejo de Administración de la Entidad, el cual deberá reunir los siguientes requisitos:

Tener un comportamiento profesional que le cualifique como persona idónea para el ejercicio del cargo.

Poseer conocimiento y experiencia para ejercer las funciones propias del cargo.

En cualquier momento, a requerimiento del Presidente del OCI, podrá comparecer ante dicho Órgano cualquier directivo o empleado cuyo testimonio y/o explicaciones se juzguen convenientes por aquél para el esclarecimiento de determinadas operaciones al objeto de análisis, o para el establecimiento de políticas de prevención de blanqueo de capitales y financiación del terrorismo.

También habrá un Secretario del OCI. Las funciones de éste serán:

Tener a su cargo el tratamiento, archivo y custodia de la documentación del OCI.  
Mantener las relaciones documentales del OCI con las distintas áreas y dependencias de la Entidad, y el órgano supervisor.  
Control del cumplimiento de acuerdos del OCI.

Recibida por parte de la UPBC una comunicación de hechos u operaciones que revistan indicios o certeza de estar relacionados con el blanqueo de capitales o la financiación del terrorismo, se examinarán los hechos u operaciones comunicadas. Si del citado análisis se confirmaran los indicios o certeza que motivaron su remisión, el OCI decidirá su comunicación al SEPBLAC y adoptará las medidas necesarias relacionadas con los hechos acontecidos.

Posteriormente, el Representante ante el SEPBLAC procederá a su comunicación al SEPBLAC según el procedimiento establecido en el apartado 6 del manual.

En cualquier caso, el OCI tendrá conocimiento de las comunicaciones iniciadas, tanto las reportadas al SEPBLAC como las que no.

Se llevará un registro de todas las operaciones analizadas, aunque no se haya efectuado comunicación alguna por no encontrarle indicios de blanqueo de capitales después de realizar un completo estudio de las mismas, cuya custodia será responsabilidad del Secretario del OCI.

Las comunicaciones del OCI de hechos u operaciones presuntamente incurso en blanqueo de capitales o financiación del terrorismo serán archivadas y conservadas bajo su custodia durante un plazo mínimo de 10 años.

### **3.3. Representante ante el SEPBLAC**

De acuerdo con la legislación aplicable, los sujetos obligados designarán como representante ante el Servicio Ejecutivo de la Comisión a una persona que ejerza cargo de administración o dirección de la Entidad.

A este respecto, el RD 925/1995, y el RD 54/2005, indican que los sujetos obligados garantizarán la existencia de un representante ante el Servicio Ejecutivo.

Es la persona designada por el Consejo de Administración de la Entidad para ostentar la representación institucional ante el SEPBLAC a efectos de prevención del blanqueo de capitales y financiación del terrorismo.

Las **funciones** de los Representantes ante el SEPBLAC son:

**Canalizar** las **comunicaciones** existentes **entre** el **Servicio Ejecutivo y la Entidad**, especialmente las relativas a las comunicaciones relativas a operaciones incoherentes y sospechosas de blanqueo de capitales, así como otros requerimientos de las diferentes autoridades competentes.

**Participar en** las **reuniones que convoque el Servicio Ejecutivo** cuando éstas tengan una finalidad consultiva, bien con la Entidad, bien con el Sistema Financiero en general, o divulgativa sobre nuevos procedimientos a desarrollar por las Entidades Financieras.

**Asistir** a las **reuniones** periódicas del **OCI**, de manera permanente.

**Mantener constantemente informado al OCI** de cualquier circunstancia que pudiere o debiere alterar o modificar la política de prevención de blanqueo de capitales que realiza la Entidad. Para cumplir esta función, deberá estar permanentemente actualizado en relación con la normativa y procedimientos existentes en la prevención del blanqueo de capitales y financiación del terrorismo.

### 3.4. Unidad de Prevención de Blanqueo de Capitales (UPBC)

Conforme a la normativa aplicable, los sujetos obligados establecerán procedimientos y órganos adecuados de control interno para conocer, prevenir e impedir la realización de operaciones relacionadas con el blanqueo de capitales y la financiación del terrorismo.

La UPBC tiene como propósito garantizar el cumplimiento del régimen aplicable así como las recomendaciones y la comunicación con el regulador, así como las políticas internas de la compañía en la materia.

La UPBC está integrada en el Área de Legal y *Compliance*.

Las **funciones básicas** de esta Unidad son:

**Soporte técnico y operativo** a la Secretaría del **OCI** de la Entidad, en cuanto a:

1. Preparación de actas.
2. Control y cumplimiento de los acuerdos del OCI.
3. Tratamiento, archivo y custodia de la documentación del OCI.

**Soporte al mantenimiento** de las **relaciones documentales** del **OCI con las distintas áreas** y dependencias de la Entidad, y el órgano supervisor.

**Revisión y actualización** de los contenidos de **formación** impartidos en la Entidad, en materia de prevención de blanqueo de capitales y financiación de terrorismo.

**Revisión y actualización** de la **normativa y procedimientos internos** implantados en la Entidad, en materia de prevención de blanqueo de capitales y financiación de terrorismo.

**Estudio de operaciones inusuales:** análisis y elaboración de informes internos.

**Seguimiento** de las **operaciones** en estudio, que se ha estimado conveniente, y durante el período establecido.

**Comunicación** de **operaciones por indicios al SEPBLAC**, en modelo oficial de declaración F19-1.

**Chequeo de clientes:**

1. Gestión de la actualización de las listas públicas de terroristas, personas con responsabilidad pública (PRP), etc....
2. Análisis de los resultados del proceso de cotejo de clientes, no clientes, intervinientes, etc., de la Entidad con las listas públicas.
3. Comunicación al órgano competente, si el resultado es positivo.

**Presentación de las conclusiones del informe de experto externo** para el Consejo de Administración.

**Relaciones con otras entidades** del sector financiero (aseguradoras, bancos, cajas, etc....), en temas de prevención de blanqueo de capitales y financiación de terrorismo.

**Respuesta a los requerimientos del SEPBLAC**, o de otra autoridad administrativa al respecto de prevención de blanqueo de capitales o la financiación del terrorismo.

**Inspecciones del SEPBLAC o de otra autoridad administrativa** al respecto de prevención de blanqueo de capitales o la financiación del terrorismo.

### 3.5. Canal de distribución

El canal de distribución lo componen toda la red de comercialización del producto y su función principal será la de recabar información sobre el cliente. Si bien estas funciones están delegadas en el canal de distribución, la responsabilidad principal recae sobre el sujeto obligado.

Las **principales funciones** de estos serán:

**Cumplir** con la **política** de “**admisión de clientes**” establecida.

**Cumplir con las medidas de diligencia debida, con carácter previo al establecimiento de la relación de negocios o a la ejecución de cualesquiera operaciones.**

**Vigilar** de forma especial a aquellos **titulares**, contratos u operativas que estén consideradas **de mayor riesgo**, informando de cualquier modificación o movimiento significativo a la UPBC.

**Analizar** con detalle cualquier **operación / cliente** que muestre sospechas o **indicios de posible vinculación al blanqueo de capitales o a la financiación de terrorismo**, tal como éste sea definido en cada momento, comunicándolo con la mayor brevedad a la UPBC.

**Asistir** a los **cursos específicos de formación** sobre prevención del blanqueo de capitales y financiación del terrorismo, dentro de los programas de formación de Recursos Humanos, así como conocer y poner en práctica los procedimientos para prevenir el blanqueo de capitales propuestos por el OCI.

Mantener el deber de **confidencialidad** con respecto a todas las operaciones o clientes que hayan sido considerados como sospechosos de blanqueo de capitales o financiación del terrorismo.

En el apartado 8.1 del presente Manual de Procedimientos se describe los procedimientos del canal de distribución de FRONTING en lo relativo a Vida y Pensiones.

## 4. POLÍTICA DE ADMISIÓN, IDENTIFICACIÓN Y CONOCIMIENTO

### 4.1. Análisis de riesgo

Conforme al artículo 7 de la ley 10/2010, de 28 de abril, de prevención de blanqueo de capitales y financiación del terrorismo, las Entidades aplicarán cada una de las medidas de diligencia debida relativas a la identificación del titular real, del propósito e índole de la relación de negocios y al seguimiento continuo de la relación de negocios, pero podrán determinar el grado de aplicación de estas medidas en función del riesgo y dependiendo del tipo de cliente, relación de negocios, producto u operación.

En el punto 8.1.1 del presente Manual se incluye análisis de riesgo de FRONTING.

### 4.2. Categorización de clientes por riesgo

La **política de admisión de clientes<sup>1</sup> debe ser gradual**, atendiendo al perfil de riesgo que éstos presenten, a efectos de la normativa vigente en materia de prevención de blanqueo de capitales y financiación del terrorismo y, por tanto, se adoptarán precauciones reforzadas ante aquellos clientes que presenten un riesgo superior al riesgo promedio.

Con carácter previo al establecimiento de la relación de negocios o a la ejecución de cualquier operación, la Entidad comprobará la identidad de los clientes mediante documentos fehacientes.

Igualmente, la Entidad incorporará los procedimientos y controles internos que garanticen un eficaz y completo conocimiento de los clientes, con el fin de obtener información sobre su actividad profesional o empresarial y sobre el propósito e índole prevista de la relación de negocios de conformidad con lo establecido en la normativa actual y de acuerdo con el análisis de riesgo incluido en el apartado 8.1.1 del presente Manual.

Con el fin de disponer de una información completa y actualizada del cliente en relación a su identidad y su conocimiento, la Entidad establecerá determinadas medidas de seguimiento continuo de la relación de negocios, como de las operaciones efectuadas a lo largo de dicha relación a fin de comprobar que éstas coinciden con el conocimiento que tiene la Entidad sobre el cliente, su perfil empresarial y de riesgo.

La Entidad procederá a clasificar a los **clientes de forma gradual en tres categorías** según su perfil **de riesgo**. Con la salvedad de los clientes no admitidos, el perfil de riesgo de los clientes, una vez admitidos, será calificado como neutro o superior al promedio. Principalmente, se considerarán como factores determinantes de riesgo la residencia, nacionalidad, profesión o actividad.

La categorización de los clientes en base a riesgo establecida en la Entidad será la siguiente:

|                              |
|------------------------------|
| <b>CLIENTES NO ADMITIDOS</b> |
|------------------------------|

<sup>1</sup> En materia de prevención de blanqueo de capitales, se entenderá como cliente o "titular real":

- La persona o personas físicas por cuya cuenta se pretenda establecer una relación de negocios o intervenir en cualesquiera operaciones.
- La persona o personas físicas que en último término posean o controlen, directa o indirectamente, un porcentaje superior al 25 por 100 del capital o de los derechos de voto de una persona jurídica, o que por otros medios ejerzan el control, directo o indirecto, de la gestión de una persona jurídica. Se exceptúan las sociedades que coticen en un mercado regulado de la Unión Europea o de países terceros equivalentes.
- La persona o personas físicas que sean beneficiarias o controlen un porcentaje igual o superior al 25 por 100 de los bienes de una persona o instrumento jurídico que administre o distribuya fondos, o, cuando los beneficiarios estén aún por designar, la categoría de personas en beneficio de la cual se ha creado o actúa principalmente la persona o instrumento jurídico.

Se considera que los clientes que reúnan alguna de las siguientes particularidades o circunstancias tienen un perfil de riesgo inaceptable y por tanto, la Entidad no establecerá relaciones comerciales con éstos:

**Información y/o documentación insuficiente.** Personas físicas o jurídicas que rehúsen facilitar la información requerida en el momento de la contratación de una nueva póliza. En base a esta directriz, queda terminantemente prohibida la emisión de nuevas pólizas sin que, al menos, se haya obtenido la información y documentación requerida a efectos por las Políticas y Procedimientos de prevención de blanqueo de capitales y financiación del terrorismo de la Entidad.

**Actividades económicas o profesionales no aceptadas.** Entre estas actividades encontramos:

Personas o sociedades que tengan negocios cuya naturaleza haga imposible la verificación de la legitimidad de sus actividades o la procedencia de sus fondos.

Personas o sociedades que desarrollen una actividad profesional o económica que pueda encontrarse relacionada con el blanqueo de capitales y la financiación del terrorismo, o con otras actividades delictivas. Entre estas actividades encontramos:

Actividades relacionadas con la prostitución.

Actividades relacionadas con el tráfico de drogas.

Actividades relacionadas con las casas de cambio, locutorios, “money transfers” y otras empresas de servicios financieros o de intermediación no autorizadas oficialmente (entre ellas las entidades financieras sin la correspondiente autorización administrativa para operar que acepten depósitos reembolsables del público y aquellas sin presencia física donde desarrollen su actividad y que no pertenezcan a un grupo financiero regulado).

Casinos o entidades de apuestas no autorizadas legalmente.

Actividades relacionadas con cualquier otro tipo de delincuencia.

**Clientes no admitidos por la UPBC.** Aquellos clientes con riesgo superior al promedio que no hayan sido finalmente admitidos por la UPBC.

**Clientes personas jurídicas cuya estructura accionarial o de control no pueda determinarse y, en particular, sociedades cuyas acciones estén representadas mediante acciones al portador.**

**Personas físicas o jurídicas identificadas en listas de sospechosos de organismos oficiales.**

**Clientes residentes en países o territorios en los que las Entidades no están autorizadas para el ejercicio de la actividad aseguradora en libre prestación de servicios.**

#### **CLIENTES CON RIESGO SUPERIOR AL PROMEDIO**

Se considera que los clientes que reúnan alguna de las siguientes circunstancias contarán con un perfil de riesgo por encima del promedio y consecuentemente, su admisión precisará de unos controles complementarios o medidas reforzadas de diligencia debida. Por otro lado, la herramienta informática implementada por la compañía con el objetivo de prevenir y detectar operativa inusual o sospechosa de blanqueo de capitales incorpora parámetros específicos para detectar aquellas operaciones realizadas por clientes cuyo perfil de riesgo es superior al promedio.



Dentro de esta categoría encontramos:

**Actividades relacionadas con la producción armamentística.** Personas o sociedades relacionadas con la producción o distribución de armas, explosivos y otros productos militares deberán ser sometidos a un control más exhaustivo antes de ser admitidos por la entidad. En el caso de que sea la actividad principal y única del cliente, el cliente no será admitido.

**Personas físicas o jurídicas relacionadas con un paraíso fiscal.** En esta categoría de riesgo se encuentran:

Personas físicas de nacionalidad, residencia, residencia fiscal o nacimiento en paraísos fiscales.

Sociedades constituidas en paraísos fiscales.

**ONG's, sociedades fiduciarias, entidades religiosas, fundaciones y otras organizaciones similares.**

**Personas con responsabilidad pública (PRP):** Personas físicas que desempeñen o hayan desempeñado, en los últimos dos años, funciones públicas importantes, tanto a escala comunitaria como internacional, incluyendo los familiares más próximos, o sus allegados.

**Actividades en sectores potenciales de estar vinculados con el blanqueo de capitales.** Entre las cuales encontramos:

Casinos de juego, Bingos, entidades de apuestas, entidades cuya actividad sea la explotación de máquinas tragaperras y aquellas actividades relacionadas con la comercialización de loterías u otros juegos de azar vinculados con el pago de algún premio.

Empresas de servicios financieros o de intermediación, transmisores de dinero y casas de cambio siempre que se encuentren autorizados debidamente por la Administración.

Actividades de inversión relacionadas con el comercio de objetos de arte y antigüedades.

Actividades relacionadas con el comercio de joyas, piedras y metales preciosos.

Locutorios o sociedades que operen dentro de los sectores de telefonía, telecomunicaciones e informática que estén dirigidas o regentadas por personas de nacionalidad considerada de alto riesgo o que puedan considerarse susceptibles de estar vinculados con actividades sospechosas de blanqueo de capitales.

Bazares o actividades relacionadas con la restauración y venta al por menor de productos alimentarios regentados por personas de nacionalidad considerada de alto riesgo o que puedan considerarse susceptibles de estar vinculados con actividades sospechosas de blanqueo de capitales.

Clientes relacionados con actividades inmobiliarias.

Asociaciones y clubes deportivos.

Actividades de importación y exportación de vehículos.

Actividades de inversión filatélica y numismática.

|                                  |
|----------------------------------|
| <b>CLIENTES DE RIESGO NEUTRO</b> |
|----------------------------------|

Todos aquellos clientes actuales o potenciales no incluidos en las anteriores categorías.

Sin perjuicio de todo lo establecido anteriormente, la UPBC tiene la facultad de modificar la clasificación de riesgo de un cliente en el caso de que disponga o se le facilite información o documentación que justifique el cambio de categorización.

### 4.3. Identificación de clientes

La Entidad identificará a cuantas personas físicas o jurídicas pretendan establecer relaciones de negocio o intervenir en cualquier operación. La Entidad identificará al titular real y comprobará su identidad con carácter previo al establecimiento de relaciones de negocio o a la ejecución de cualesquiera obligaciones, en función del análisis de riesgo.

En ningún caso la Entidad mantendrá relaciones de negocio o realizará operaciones con personas físicas o jurídicas que no hayan sido debidamente identificadas.

Concretamente, la **documentación que, como mínimo<sup>2</sup>, deberá solicitar la entidad en función de la naturaleza del cliente será:**

- **Personas Físicas:**

Cuando el cliente sea persona física se deberá obtener una copia preferiblemente en soporte óptico, magnético o electrónico de:

**DNI o pasaporte**, si es de nacionalidad española.

Si es extranjero, el **NIE** otorgado a través de permiso de residencia expedido por el Ministerio de Justicia, **pasaporte o documentación identificativa oficial** del país de procedencia que incorpore fotografía de su titular (Art. 3.2 RD 925/1995).

Adicionalmente, en aquellos casos en que terceras personas actúen en nombre de otras (p.e: representante legal), se solicitarán los **poderes** de las personas que actúen en su nombre y su correspondiente identificación.

- **Personas Jurídicas:**

Cuando el cliente sea persona jurídica se deberá obtener una copia preferiblemente en soporte óptico, magnético o electrónico de:

**Documentación fehaciente (escritura) de denominación**, forma jurídica, domicilio social, objeto social y CIF.

**Tarjeta de identificación fiscal (CIF)** de la empresa (o similar, para las sociedades no registradas en España).

**DNI o pasaporte de los apoderados / administradores.**

Las personas que actúen en representación del titular deberán acreditar copia auténtica notarial de los **poderes** con que lo hacen.

---

<sup>2</sup> La Sección 1ª del Capítulo II de la ley 10/2010 (artículos 3 a 8) se refiere a determinadas medidas normales de diligencia debida que deben llevar a cabo los sujetos obligados. Reglamentariamente podrán establecerse criterios técnicos para la aplicación de medidas de diligencia simplificada respecto de otros clientes que comporten un riesgo escaso de blanqueo de capitales o de financiación del terrorismo (Sección 2ª, artículo 9). Por otro lado, las medidas de diligencia debida serán reforzadas en el caso de los clientes con riesgo superior al promedio, aplicándoles medidas reforzadas de diligencia debida (Sección 3ª, artículo 11).

Cuando existan indicios o certeza de que los clientes actúan en nombre de otros, de tal manera que pueda suscitarse una vinculación a actividades ilícitas, la Entidad recabará la información precisa a fin de conocer la identidad de las personas por cuenta de las cuales actúen.

En el ámbito del seguro de vida, la comprobación de la identidad del tomador y del asegurado deberá realizarse con carácter previo a la celebración del contrato. La comprobación de la identidad del beneficiario del seguro de vida, si es distinto del tomador, deberá realizarse en todo caso con carácter previo al pago de la prestación derivada del contrato o al ejercicio de los derechos de rescate, anticipo o pignoración conferidos por la póliza.

En cualquier caso, se deberán verificar los documentos aportados teniendo en cuenta los siguientes aspectos:

Comprobar que los documentos estén comprendidos entre los que se definen como apropiados y necesarios para la correcta identificación. (DNI, Pasaporte, escrituras, etc.).

Verificar que no están caducados.

Comprobar que todos los datos identificativos aportados a través de los distintos documentos coinciden (nombre, apellidos, fecha de nacimiento, dirección y cualquier otro tipo de información aportada por el cliente).

Observar la fotografía del titular y determinar si su aspecto y edad coincide con la fotografía y la fecha de nacimiento que aparecen en los documentos.

Cotejar la firma existente en los distintos documentos aportados por el solicitante.

Analizar los documentos observando tachaduras, distinto tipo de letra, partes escritas a máquina y a mano, etc.

La imagen escaneada debe obtenerse siempre de documentos originales.

La imagen escaneada de los documentos debe ser legible (anverso y reverso).

#### **4.4. Conocimiento de clientes**

La Entidad obtendrá información sobre el propósito e índole prevista de la relación de negocios de conformidad y en los casos establecidos por la normativa en vigor y las políticas de Grupo.

Durante el proceso de gestión de la nueva póliza de vida individual, con carácter previo al alta y en determinados casos, se deberá cumplimentar un cuestionario de conocimiento de cliente, en los cuales se especificarán, por ejemplo, los datos identificativos personales, la actividad, profesión, y otros datos económicos del cliente, además del motivo de contratación de la póliza y el origen de los fondos, titular real, estructura accionarial, etc.

Se aplicarán medidas de diligencia simplificada, normal o reforzada en función de la categorización de riesgo establecida. (Ver punto 8.1.1 del presente Manual).

#### **4.5 Identificación y conocimiento en Vida Colectivos.**

Ver punto 8.1.1.2.2 para las especificidades en relación con la aplicación de medidas de diligencia en cuanto a productos de Vida Colectivos.

## 5. ANÁLISIS DE OPERATIVA INUSUAL

### 5.1. Introducción

La Entidad examinará con cuidadosa atención cualquier operación inusual, independientemente de su cuantía, que por su naturaleza pueda encontrarse aparentemente relacionada a la actividad de blanqueo de capitales o bien con la financiación del terrorismo.

Consecuentemente, la Entidad ha establecido un **procedimiento de detección y análisis de operaciones inusuales o susceptibles de ser consideradas sospechosas** con el fin de cumplir con el ordenamiento vigente, analizando la forma de operar de sus clientes y las operaciones de estos, en particular, aquellas susceptibles de estar vinculadas con el blanqueo de capitales o la financiación del terrorismo.

La Entidad dispone de dos canales de identificación y detección de estas operaciones inusuales o susceptibles de ser consideradas sospechosas:

**Canal descentralizado:** Canal de detección vía empleados, asociados, franquiciados o colaboradores de la Entidad, los cuales, una vez identifiquen cualquier operación inusual o susceptible de ser sospechosa en el momento de contratación de un producto de Vida o Pensiones o en la posterior operativa del cliente, deberán comunicarla internamente a la UPBC a través de su responsable.

**Canal centralizado:** Canal de detección vía Unidad de Prevención de Blanqueo de Capitales, la cual analizará: operaciones derivadas de las alertas originadas por el sistema; requerimientos de las autoridades relacionados con clientes de la Entidad y aquellas operaciones que se extraigan de prensa y otras publicaciones.

### 5.2. Canal descentralizado de detección de operativa inusual

Cuando los empleados, asociados, franquiciados o colaboradores de la Entidad identifiquen cualquier operación de Vida o de Pensiones que presente indicios de encontrarse relacionada con el blanqueo de capitales o con la financiación de terrorismo, los mismos deberán abstenerse de ejecutar la operación y proceder a comunicarla inmediatamente a la UPBC a través de su responsable. En el Anexo II del presente documento figura el formulario a utilizar para realizar tales comunicaciones.

En el Anexo III se describe a modo ejemplificativo operativa potencialmente sospechosa de blanqueo de capitales.

Los empleados, asociados, franquiciados o colaboradores o directivos vinculados a la consulta de cualquier operación deberán garantizar la absoluta confidencialidad respecto a las operaciones analizadas, no revelando al cliente ni a terceros las actuaciones que estén realizando en relación con el análisis de dichas operaciones sospechosas.

### 5.3. Canal centralizado de detección de operativa inusual

La UPBC deberá analizar, con la diligencia exigida por la normativa actual vigente:

Las operaciones comunicadas por los empleados, asociados, franquiciados o colaboradores como presumibles de ser sospechosas.

Los requerimientos de las autoridades competentes,

Todas aquellas operaciones que se extraigan de prensa u otros medios de comunicación.

Cuando se tenga conocimiento de que el cliente podría estar relacionado con el blanqueo de capitales o la financiación del terrorismo a través de requerimientos de autoridades judiciales o cuerpos y fuerzas de seguridad.

Dicha revisión se llevará a cabo con el fin de determinar si éstas deberán ser comunicadas en primer término al OCI y posteriormente al SEPBLAC, o si bien, quedarán simplemente en indicios no confirmados.

Este examen especial de operaciones comprenderá, al menos, los siguientes aspectos:

Análisis de las relaciones con el cliente (operaciones, tipos, movimientos, antigüedad, etc.).

Análisis de la coherencia de la operativa realizada con la información que se dispone de la actividad del cliente y de sus antecedentes como cliente de la Entidad.

Conocimiento sobre el origen y destino de los fondos.

Valoración de su contenido económico y de la capacidad del cliente para el mismo.

Obtención de documentación adicional, bien obtenida del propio cliente, o bien de otras fuentes externas.

Cualquier otro análisis, investigación o valoración que determine el empleado o la UPBC.

La normativa de prevención del blanqueo de capitales y de la financiación del terrorismo califican como infracciones graves no realizar el examen especial de operaciones y no abstenerse de ejecutar operaciones sospechosas sin haber sido comunicadas previamente.

No obstante, cuando dicha abstención no sea posible o pueda dificultar la investigación, la Compañía podrá ejecutar la operación, efectuando seguidamente una comunicación al SEPBLAC con la información relativa a dicha operativa junto con los motivos que justificaron la ejecución de ésta.

## 6. COMUNICACIÓN DE OPERATIVA SOSPECHOSA

### 6.1. Introducción

La Entidad deberá colaborar con la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias y sus órganos, con el fin de mitigar cualquier hecho u operación que tenga relación con el blanqueo de capitales o la financiación del terrorismo.

Por iniciativa propia, comunicará al Servicio Ejecutivo de la Comisión (SEPBLAC) cualquier hecho u operación, aun meramente intentado, respecto al que, tras el examen especial de operaciones, exista indicio o certeza de que está relacionado con el blanqueo de capitales o la financiación del terrorismo.

Finalmente, deberá facilitar la documentación e información que la Comisión, sus órganos u otras Autoridades competentes les requieran para el ejercicio de sus competencias.

### 6.2. Comunicación singular de operaciones

La Entidad comunicará al Servicio Ejecutivo de la Comisión cualquier hecho u operación, incluso la mera tentativa, que presente indicio o certeza de estar vinculado con el blanqueo de capitales o la financiación del terrorismo y, en concreto, las operaciones que muestren una falta de correspondencia ostensible con la naturaleza, volumen de actividad o antecedentes operativos de los clientes, siempre que no se aprecie justificación económica, profesional o de negocio para la realización de las operaciones.

Las **comunicaciones contendrán**, en todo caso, **la siguiente información**:

Relación e **identificación de las personas físicas o jurídicas** que participen en la operativa sospechosa de blanqueo y el concepto de su participación en ella.

La **actividad** conocida de las personas físicas o jurídicas que participa en las operaciones y la correspondencia entre la actividad y las operaciones realizadas.

**Relación de las operaciones y fechas** a que se refieren, con indicación de su naturaleza, moneda, importe, lugar o lugares de ejecución, instrumentos de pago o cobro utilizados y finalidad.

Las **gestiones realizadas por los sujetos obligados** comunicantes para investigar las operaciones comunicadas.

Exposición de todos los **hechos o circunstancias que den lugar a indicios de presunción de blanqueo de capitales** o de financiación del terrorismo o que pongan de manifiesto la falta de justificación económica, profesional o de negocio para la realización de las actividades.

**Cualquier otro dato relevante** para la prevención del blanqueo de capitales o la financiación del terrorismo que el Servicio Ejecutivo de la Comisión determine en el ejercicio de sus competencias.

En caso de que las operaciones detectadas se consideren susceptibles de estar relacionadas con el blanqueo de capitales o la financiación del terrorismo, tras el último y definitivo examen que realizará la UPBC o el OCI, en su caso, sobre ellas, **el representante ante el SEPBLAC** será el

**encargado de comunicar estas operaciones al Servicio Ejecutivo de la Comisión, mediante el expediente de comunicación F-19** (descargar modelo de este expediente de comunicación en [www.sepblac.es](http://www.sepblac.es)).

Los directivos o empleados de la Entidad podrán comunicar directamente al Servicio Ejecutivo de la Comisión las operaciones de que conocieran y respecto de las cuales estimen que concurren indicios o certeza de estar relacionadas con el blanqueo de capitales o con la financiación del terrorismo, en los casos en que, habiendo sido puestas de manifiesto internamente, la Entidad no hubiese informado al directivo o empleado comunicante del curso dado a su comunicación.

### **6.3. Comunicación sistemática de operaciones**

La Entidad tiene la **obligación de comunicar** al Servicio Ejecutivo de la Comisión, las **operaciones que se ajusten a la siguiente tipología por un importe superior a 30.000 € o su contravalor en moneda extranjera:**

**Operaciones con movimiento físico de moneda metálica**, billetes de banco, cheques de viaje, cheques u otros documentos al portador librados por entidades de crédito cualquiera que sea su importe, que no sean objeto de abono o cargo en la cuenta de un cliente.

**Operaciones donde intervengan personas físicas o jurídicas que sean residentes**, o actúen por cuenta de estas, en paraísos fiscales o territorios no cooperantes, así como las operaciones que impliquen transferencias de fondos a o desde dichos territorios o países, cualquiera que sea la residencia de las personas intervinientes.

Cualquier otra operación que, a propuesta de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias, se recojan en las disposiciones de aplicación del Reglamento de la Ley 19/1993 y sea de aplicación en las entidades que desarrollen las actividades descritas en el artículo 2.1 del citado precepto.

En esta comunicación se tendrán en consideración los posibles fraccionamientos de operaciones realizados por los clientes de la Entidad, procediéndose a acumular los importes de todas ellas y a su comunicación al SEPBLAC si se considera necesario.

Por otro lado, la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias podrá acordar la no inclusión de determinados clientes o grupos de clientes en las declaraciones mensuales de operaciones, de acuerdo con las condiciones que establezca en cada caso.

### **6.4. Requerimientos de las Autoridades**

La Entidad facilitará la documentación e información que la Comisión, sus órganos, o cualquier otra Autoridad competente (Policía, Juzgado, etc.) **le requiera** para el ejercicio de sus competencias.

Los requerimientos de información precisarán con toda claridad los aspectos que hayan de ser informados o la documentación que haya de ser aportada y el plazo en que hayan de ser atendidos.

Transcurrido el plazo para la remisión de la documentación o información requerida sin que ésta haya sido aportada o cuando se aporte de forma incompleta por omisión de datos que impidan examinar la situación en debida forma, se entenderá incumplida la obligación establecida.



Cabe destacar, que estará terminantemente prohibido poner en conocimiento del cliente o de terceros, salvo a los órganos internos especialmente designados y a las autoridades competentes, el hecho de que una operativa haya sido comunicada, o que se haya solicitado información sobre la misma por las autoridades o que se esté examinando por su posible vinculación al blanqueo de capitales. El incumplimiento por la Entidad de esta norma estará considerado como infracción muy grave.

## 7. CONSERVACIÓN Y CONFIDENCIALIDAD

La Entidad **conservará durante un período mínimo de diez años** la documentación en que se formalice el cumplimiento de las obligaciones establecidas en la ley.

En particular, se deberá conservar para su uso en toda investigación o análisis, en materia de posibles casos de blanqueo de capitales o de financiación del terrorismo, por parte del Servicio Ejecutivo de la Comisión o de cualquier otra autoridad competente:

- **Copia de los documentos exigibles en aplicación de las medidas de diligencia debida**, durante un periodo mínimo de diez años desde la terminación de la relación de negocios o la ejecución de la operación.
- **Original o copia de los documentos o registros que acrediten adecuadamente las operaciones, los intervinientes en las mismas y las relaciones de negocio**, durante un periodo mínimo de diez años desde la ejecución de la operación o la terminación de la relación de negocios.

La Entidad, con las excepciones que se determinen reglamentariamente, almacenará las copias exigidas de la **documentación de identificación y conocimiento de clientes** en soportes ópticos, magnéticos o electrónicos que garanticen su integridad, la correcta lectura de los datos, la imposibilidad de manipulación y su adecuada conservación y localización.

En todo caso, el sistema de archivo de la Entidad deberá asegurar la adecuada gestión y disponibilidad de la documentación, tanto a efectos de control interno, como de atención en tiempo y forma a los requerimientos de las autoridades.

La **documentación relativa al análisis y comunicación sistemática o singular de operaciones sospechosas o inusuales** tendrá un carácter estrictamente confidencial, debiendo permanecer en una localización distinta a la establecida para la documentación de identificación y conocimiento, y únicamente accesible por los integrantes de la UPBC y el OCI.

## 8. Anexo I - Procedimientos internos.

El objetivo del presente apartado es la descripción de los procedimientos internos que se llevarán a cabo en materia de prevención de blanqueo de capitales y la financiación del terrorismo en FRONTING.

### 8.1. Procedimientos internos en FRONTING ((Ramo Vida y Pensiones)

#### 8.1.1. Política de admisión, identificación y conocimiento de clientes

De conformidad con lo establecido en el artículo 7 al respecto de las medidas de diligencia debida así como lo establecido en el artículo 10 al respecto de las medidas de diligencia simplificada susceptibles de ser aplicables en algunos casos, en relación con lo establecido en los artículos 11 y siguientes de la Ley 10/2010, de 28 de abril, de prevención de blanqueo de capitales y financiación del terrorismo, al respecto de las medidas de diligencia reforzada, se establece la matriz siguiente resultado del análisis de riesgo realizado por FRONTING al respecto de los productos distribuidos por su red a clientes residentes teniendo en cuenta las variables perfil de cliente / tipo producto / canal de distribución / localización geográfica.

|   | Medidas Simplificadas <sup>(1)</sup> | Medidas Normales <sup>(2)</sup> | Medidas Reforzadas <sup>(3)</sup> |
|---|--------------------------------------|---------------------------------|-----------------------------------|
| <b>CLIENTES (PERFIL DE RIESGO)</b>  |                                      |                                 |                                   |
| Riesgo Neutro   | ✓                                    | ✓                               |                                   |
| Riesgo Alto – PRP's <sup>(4)</sup>  |                                      |                                 | ✓                                 |
| <b>PRODUCTOS</b>  |                                      |                                 |                                   |
| Vida Individual<br>(Prima anual/única = < 1.000 / 2.500 €)                              | ✓                                    |                                 |                                   |
| Vida Individual<br>(Prima anual/única > 1.000 / 2.500 €)                                |                                      | ✓                               |                                   |
| Vida Colectivos   | ✓                                    |                                 |                                   |
| <b>ÁMBITO</b>   |                                      |                                 |                                   |
| Nacional  | ✓                                    |                                 |                                   |
| Internacional   |                                      | ✓                               |                                   |
| Paraísos Fiscales / No cooperantes / Países restringidos ( <i>política Sanctions</i> ). |                                      |                                 | ✓                                 |
| <b>CANAL DE DISTRIBUCIÓN</b>  |                                      |                                 |                                   |
| Presencial  | ✓                                    | ✓                               | ✓                                 |
| No Presencial   | ---                                  | ---                             | ---                               |

- (1) *Identificación y Conocimiento del cliente mediante Cuestionario Simplificado o equivalente.*
- (2) *Identificación y Conocimiento del cliente mediante Cuestionario Completo.*
- (3) *Control de la operativa del cliente posteriormente a la contratación de la póliza o a la ejecución de la operación (medidas de diligencia reforzada).*
- (4) *Persona con Responsabilidad Pública.*

Las diferentes **actividades que integran el proceso de admisión**, identificación y conocimiento de clientes se describen en este apartado de manera cronológica, desde la solicitud de suscripción de una póliza, hasta el archivo de la documentación, definiéndose los procedimientos internos y los aspectos más relevantes de la distribución de los productos de FRONTING.

## ▪ **Solicitud de suscripción de una póliza de seguros**

### **1. Proceder a la solicitud de seguro realizada por el cliente**

Cuando un nuevo cliente solicite la suscripción de una, se procederá a efectuar el alta en función del nivel de atribuciones o competencias del canal de distribución (Gestor) al cual acuda este cliente:

Red de oficinas de FRONTING  
Asociados y Franquiciados  
Colaboradores

Atendiendo a los diferentes marcos de competencia designados para cada canal de distribución (gestor), el procedimiento de la Entidad para la suscripción o emisión de una póliza será el que se describe en este apartado y en los consiguientes:

Cuando el cliente acuda a un Gestor y solicite la contratación de una póliza, deberá rellenar la **solicitud de seguro** (o boletín de adhesión de seguro colectivo), firmándola en última instancia.

### **2. Recabar documentación de identificación y conocimiento**

#### 2.1 Respecto Vida Individual

Seguidamente, el Gestor deberá recabar toda la **información de identificación y conocimiento** del cliente (el documento identificativo del cliente así como el cuestionario de conocimiento debidamente cumplimentado).

Concretamente, deberán solicitarle al cliente todos aquellos documentos acreditativos de su identidad (ver más detalles de la documentación requerida para la identificación del cliente en el apartado 4.3 del presente manual):

Documento acreditativo de su identidad.

Como también toda aquella información de conocimiento a fin de conocer la naturaleza de su actividad profesional o empresarial (ver más detalles de la información requerida de conocimiento en el apartado 4.4 del presente manual):

Cuestionario de conocimiento.  
Documentos relativos al conocimiento del cliente (según su naturaleza o actividad).

## 2.2 Respecto Vida Colectivos

En caso de nuevas altas de pólizas de Vida Colectivos, se obtendrán los siguientes documentos previamente a la gestión o alta de la póliza. Los documentos se archivarán en soporte electrónico durante diez años:

- Copia de identificación fiscal del tomador;
- Copia de escrituras de constitución de la entidad tomador de la póliza, o en su caso;
- Copia de documentos identificativos de los representantes de la entidad tomador de la póliza, o en su caso;
- Copia de la escrituras de poder de los representantes.

### • Introducción de los datos en el Sistema

El Gestor introducirá en el sistema de la Entidad la información recabada de identificación y conocimiento relativa a los intervinientes:

Concretamente, el procedimiento que se debe seguir al introducir la información se muestra a continuación:

1. Se darán de alta a los intervinientes, introduciendo la siguiente información en la base de datos de personas (o se actualizarán los datos en caso de que ya sean clientes de la Entidad):

Primeramente, una vez se haya asignado automáticamente un código de filiación, se indicará el **Tipo de documento** que presenta cada interviniente (DNI, Pasaporte, NIE, CIF, etc.).

Seguidamente, se introducirá el **Número del documento**, que deberá ser el mismo que el facilitado por el cliente en la solicitud de seguro.

Se introducirán los **Datos Personales** relativos al nombre y apellidos, así como el sexo (para personas físicas), o nombre y razón social (personas jurídicas).

Se introducirá la **nacionalidad y país residencia**.

Seguidamente, se grabará en el sistema la **actividad (CNO / CNAE)**, que coincidirá con la declarada en la solicitud o boletín de adhesión.

2. Se introducirán los datos relativos a la nueva póliza suscrita en la base de datos de la póliza.

3. Se introducirán los datos relativos al conocimiento del cliente divididos en tres apartados:

**Datos Profesionales.** En este apartado se efectuarán preguntas como “empresa para la que trabaja”, “sector”, “antigüedad”, etc. En caso de persona jurídica se deberán introducir los datos del/los representantes legales, y en los casos pertinentes información de participación accionarial, detallando los titulares que posean una participación accionarial superior al 25% del capital social de la persona jurídica.

**Datos Económicos.** Este será un apartado siempre visible, ya que incluso en los casos en que NO es obligatoria su cumplimentación, sí es recomendable cumplimentarlos. Se cumplimentará el apartado de “Datos Económicos” en función de la prima aportada, por tanto:

**No será obligatorio** cumplimentar este apartado, aunque sí RECOMENDABLE, en el caso de que la prima periódica anual NO EXCEDA de 1.000 euros o cuando la prima única NO EXCEDA de 2.500 euros.

**Sí será obligatorio** cumplimentar este apartado para primas anuales que EXCEDAN de 1.000 euros o cuya prima única EXCEDA de 2.500 euros.

Asimismo en este apartado habrá una pregunta obligatoria con el fin de conocer la procedencia de los fondos que el cliente utilizará para el pago de la prima.

**Otros.** En este apartado se efectuarán dos cuestiones, ambas obligatorias, destinadas a conocer los motivos de contratación de la póliza y para la detección de PRPs.

Con carácter opcional y en función del riesgo del cliente, en este apartado podrán aparecer otras preguntas destinadas al gestor que variarán en función de que el cliente sea una persona física o jurídica.

En cuanto a aquellas nuevas altas que resulten de la reinversión de pólizas previamente contratadas por el mismo tomador, será recomendable cumplimentar los campos correspondientes al cuestionario de conocimiento aunque no obligatorio (únicamente se deberán cumplimentar dichos campos con la palabra “reinversión”).

#### ▪ Indexación de la documentación

La obtención de toda la documentación relativa a la identificación del cliente y la solicitud o el boletín de adhesión debidamente firmado, será un requisito indispensable para poder proceder con el proceso de alta y emisión de la póliza. Dicha documentación deberá ser indexada al sistema, ya que de no ser así aparecerá un mensaje en pantalla recordándole al usuario este hecho y dejando paralizada la emisión de la póliza.

Como criterio general, en caso de negativa por parte del cliente a facilitar los documentos o los datos necesarios de identificación para realizar la operación, no se procederá a la admisión del mismo y se clasificará al cliente como no admitido.

#### ▪ Aprobación de la solicitud

En algunos casos la emisión de la póliza podrá quedar paralizada si se cumple alguno de los siguientes supuestos:

- El tomador de la póliza tiene su nacionalidad o residencia en alguno de los países especialmente designados por la política de *Sanciones Comerciales y Económicas*
- El tomador de la póliza es un PRP de ámbito internacional.
- El tomador haya sido clasificado previamente como No Admitido (apartado 4.2 del presente manual).

Ante estos casos, el sistema generará automáticamente un aviso que notificará al gestor que debe ponerse en contacto con la UPBC. En estos casos el usuario deberá facilitar la información necesaria para que la UPBC pueda hacer las gestiones correspondientes para la admisión o no del cliente.

#### ▪ Medios de pago de prima por parte del tomador

El pago de las contraprestaciones por parte del cliente se realizará **como regla general** mediante domiciliación bancaria en **cuenta corriente titularidad del tomador**.

Cualquier otro medio de pago, se considera no admitido, excepto aprobación por parte del OCI documentada en acta de reunión ordinaria o extraordinaria.

**No se consideran incluidas en esta obligación las reinversiones en otros productos de vida ni las inversiones constituidas en seguros de vida con origen en indemnizaciones a perjudicados en un siniestro de circulación.**

La documentación se conservará durante 10 años, en formato electrónico, todos los documentos o registros correspondientes que, con fuerza probatoria, acrediten tanto la identificación como la adecuada realización de las operaciones y las relaciones de negocio con los clientes de la Entidad.

En todos los casos, el procedimiento de conservación, debido a la naturaleza de la información contenida en estos documentos, deberá ser el adecuado para garantizar una fácil localización como su confidencialidad.

#### ▪ Actualización de la información

Durante la operativa del cliente, se deberá tener en cuenta la actualización periódica de la información suministrada por el mismo, para garantizar que se esté cumpliendo con la política y los procedimientos internos establecidos en la Entidad en materia de prevención de blanqueo de capitales.

Concretamente, los datos que deberán considerarse para su actualización, según su naturaleza serán:

Datos relativos a la de identificación del cliente (tomador y/o beneficiario):

Control de caducidad del DNI/NIE/Pasaporte (de una persona física o de los administradores / apoderados de una empresa): en caso de que se tenga constancia de que el documento acreditativo de identidad del tomador y beneficiario/s del seguro no está actualizado, se solicitará el documento identificativo en vigor para su indexación.

Datos relativos a contratos con menores de edad: en caso de que conste que tomador o el beneficiario han llegado a su mayoría de edad, se reclamará dicha documentación.

Modificación de la naturaleza jurídica de una empresa: Se deberán actualizar los datos relativos a las personas jurídicas, en caso de que se tenga constancia que se han producido cambios en los apoderados, administradores o representantes de la empresa, cambios en el accionariado, o se tenga constancia de un cambio de denominación.

Datos relativos al conocimiento del cliente (tomador):

Modificación de la profesión / actividad del cliente, con la consecuente actualización de los documentos relacionados (documentación de carácter económico, cuestionario de conocimiento, información adicional de conocimiento, etc.).

Información económica del cliente: Se deberán obtener los datos de conocimiento del cliente, según el perfil de riesgo de éste.

Cualquier cambio que afecte a la BBDD's de personas: los de datos de contacto, país de residencia, nacionalidad, etc., se deberán mantener actualizados en cuanto se tenga constancia de algún cambio.



Cambios en el perfil del cliente: cuando fruto de la modificación en la actividad o la residencia del tomador, se tenga conocimiento de que el perfil de riesgo de éste puede haber variado, se deberán adoptar las medidas inherentes al nuevo perfil.

Actualización de datos de la póliza suscrita (ver más detalles en el documento “*Normas de Contratación.doc*”): Dichos cambios pueden ser de distinta naturaleza:

Cambios en los intervinientes (beneficiario, tomador o asegurado).

Cambios en las condiciones del producto contratado (suplementos).

Etc.

En este sentido cualquier empleado o miembro de la red de FRONTING que conociera de cualquier variación relevante en la operativa de los clientes, actualizará dicha información.

## **8.1.2. Detección y análisis de operativa sospechosa**

### **▪ Canal descentralizado de detección de operativa sospechosa**

El procedimiento que se seguirá para la detección y análisis de operativa sospechosa mediante el canal centralizado será el siguiente:

#### **1. Detección de operativa sospechosa**

FRONTING cuenta con un catálogo de todas aquellas operaciones que pueden presentar indicios de estar vinculadas con la actividad de blanqueo de capitales y sobre las cuales deberá llevarse a cabo un examen especial por si llegaran a confirmarse dichos indicios (ver listado en el Anexo III del presente Manual).

Cuando en la red de oficinas (o bien por la vía del mediador) se identifique alguna operación de las recogidas en este listado, o bien, cualquier otra que presente indicios de encontrarse relacionada con el blanqueo de capitales, el empleado o miembro de la red deberá **abstenerse de ejecutar la operación** y procederá a comunicarla inmediatamente a la UPBC.

#### **2. Comunicación interna entre el empleado y la UPBC**

Esta comunicación podrá realizarse mediante el uso de la Plantilla de Comunicación de Operaciones Sospechosas adjuntada en el apartado 10 (Anexo II) de este manual, en la cual deberá describirse la operación y facilitarse información básica sobre el cliente.

#### **3. Análisis de la operativa sospechosa**

En el caso de que la operación sospechosa detectada y comunicada por parte de los empleados o miembros de la red muestre indicios de estar relacionada con actividades vinculadas con el blanqueo de capitales, la UPBC solicitará del empleado toda aquella información adicional posible que se encuentre relacionada. Éste deberá recopilar toda la información que permita justificar la sospecha, realizará fotocopias de la documentación referente a la operación como toda la información identificativa del cliente, y, adicionalmente, deberá:

Informar de la relación e identificación de las personas físicas o jurídicas que participen en la operación y el concepto de su participación.

Comunicar la relación de las operaciones y fechas a las que se refieren, con indicación de su naturaleza, cuantía, lugar o lugares de ejecución, finalidad y medios de pago o cobro utilizados.

Exponer todas aquellas circunstancias de las que pueda inferirse el indicio o la certeza de vinculación al blanqueo de capitales.

Comunicar cualquier otro dato que se considere oportuno informar.

#### **4. Seguimiento de la relación de negocios**

En las relaciones de negocio u operaciones de personas con responsabilidad pública (PRP), así como en los demás casos de clientes de Riesgo Alto, la UPBC llevará a cabo un seguimiento reforzado y permanente de la relación de negocios.

### **5. Toma de decisión por la UPBC**

La UPBC ante la información que la red le haya remitido y, una vez la haya analizado, podrá actuar de la siguiente manera:

Solicitando aclaración sobre la información recibida. Cuando la UPBC considere que la información recibida no es lo suficientemente completa, clara, o consistente para la toma de decisión, podrá solicitar más información de soporte con el fin de poder decidir sobre la operación consultada.

Desestimando la sospecha. Cuando tras el análisis de la información relativa a la operación sospechosa se considere que no se desprenden indicios reales sobre la relación de la operación con actividades relacionadas con el Blanqueo de Capitales, la UPBC se abstendrá de comunicar la sospecha al SEPBLAC. Dicha abstención deberá ser documentada, exponiéndose los motivos principales por los cuales se considere que la operación detectada no es indicio de blanqueo de capitales. Todo ello, con el fin de garantizar la objetividad como la transparencia en la toma de decisión sobre una operación que posteriormente, podría acabar siendo realmente sospechosa.

Manteniendo vigilancia especial. Cuando la UPBC considere que la información recibida del empleado no dispone de la base suficiente para decidir sobre la necesidad de informar al SEPLAC sobre la operación o bien, desestimar la sospecha, ésta podrá comunicar al empleado que emitió la consulta que mantenga una “vigilancia especial” sobre el cliente que haya efectuado la operación considerada como potencialmente sospechosa. El periodo de vigilancia no podrá superar los 3 meses y tendrá como finalidad obtener mayor información, para poder decidir finalmente si se deberá comunicar o no al SEPBLAC la operación de la cual se sospecha.

Considerando la Operativa (Cliente) sospechosa. Cuando la UPBC considere que de la información recibida del empleado que realizó la suscripción de la póliza) puede determinarse que hay indicios de que se trata de una operación relacionada con la actividad de blanqueo de capitales, procederá a establecer aquellas medidas cautelares que se hayan acordado instaurar ante esta casuística (como p.ej. el bloqueo de la operativa del cliente) y deberá ser comunicado al OCI con urgencia con el fin de que éste, tras las investigaciones exigidas, verifique la necesidad de comunicar al SEPBLAC sobre esta operación (cliente) sospechosa, mediante el procedimiento de reporting detallado en el apartado 8.1.3 del presente manual.

### **6. Toma de decisión por el OCI**

Cuando la UPBC considere, tras el análisis, que la operación debe ser remitida al OCI por encontrar indicios claros de ser una operación vinculada a la actividad de blanqueo de capitales, se someterá al análisis de este órgano en la reunión inmediatamente siguiente, con el fin de que el OCI pueda emitir decisión concluyente sobre la comunicación o no de la operación consultada al SEPBLAC.

En caso de que el OCI concluya que dicha operación presenta indicios determinantes de vinculación al blanqueo de capitales, deberá procederse al envío del expediente de comunicación al SEPBLAC mediante el procedimiento descrito en el apartado 8.1.3. En caso contrario, se procederá al archivo de toda la documentación relacionada con la investigación de esta operación mediante el proceso descrito en el apartado siguiente, finalizando con el análisis de la operación consultada por el empleado.

## **7. Archivo de la documentación relativa a las operaciones sospechosas**

Una vez finalizado el análisis, éste, independientemente de cuál haya sido la decisión que se haya tomado sobre ella, deberá ser adecuadamente documentado y archivado. Cada operación deberá contar con un expediente y se le asignará un número secuencial de archivo.

El procedimiento que se seguirá para la detección y análisis de operativa sospechosa mediante el canal centralizado será el siguiente:

### **1. Análisis de operaciones sospechosas vía detección de empleados y red**

Esta vía de detección de operativa sospechosa corresponde al canal descentralizado de identificación de operaciones descrito en el apartado anterior “Canal descentralizado de detección de operativa sospechosa”, del presente manual.

### **2. Análisis de operaciones sospechosas vía UPBC**

La UPBC analizará todas las operaciones sospechosas.

Adicionalmente, se establecen unas **reglas fijas** basadas en diferentes casuísticas o perfiles de operativa sospechosa. Éstas generarán alarmas las cuales deberán considerarse de revisión obligatoria. Estas **reglas fijas** son:

- **Operatoria desfavorable:** Serán identificados como “operativa desfavorable” todos aquellos movimientos de productos de vida donde se produzca un rescate en un periodo inferior a un determinado número de días desde la fecha de emisión de la póliza.
- **Incrementos de capital:** Serán identificados como “incrementos de capital” todos aquellos movimientos de incrementos de aportación o prima donde el capital de la operación sea superior a un determinado importe respecto a la última prima o aportación.
- **Método de pago distinto a domiciliación bancaria:** Se identificará cualquier pago en efectivo o mediante cualquier otro método de pago distinto a la domiciliación bancaria a partir de un determinado importe.

- **Profesión de riesgo para prima elevada:** profesiones consideradas de alto riesgo (ver apartado 4.2 Categorización) con prima establecida a partir de un determinado importe.
- **Domiciliación bancaria en cuenta del agente:** coincidencia entre cuenta de domiciliación bancaria del clientes con cuenta bancaria de mediador registrada en Administración, para importes superiores a una determinada cantidad.

Cada cliente en función de las ponderaciones de las operaciones que haya realizado y de los elementos referidos al perfil de riesgo del que conste, tendrá un porcentaje de riesgo, que podrá llegar a ser del 100%.

A partir de las ponderaciones y las reglas fijas de la herramienta, la UPBC revisará las alertas relacionadas con clientes no analizados y sus operaciones.

Cualquier situación anómala detectada por parte de la UPBC será investigada, y en caso de que exista sospecha de estar vinculada con el blanqueo de capitales y financiación del terrorismo deberá realizarse un control exhaustivo de la operativa del cliente, pudiendo escalar cada caso al OCI cuando proceda.

### **3. Análisis de operaciones sospechosas vía los requerimientos de las autoridades**

Las autoridades podrán requerir información y documentación de clientes (y no clientes) de la Entidad. A partir de estos requerimientos, la UPBC deberá preparar la comunicación a las autoridades, con la mayor celeridad posible, acerca de la información sobre aquellas personas con indicios de ser sospechosas.

El procedimiento de detección y análisis de estas operaciones será el mismo que el del resto de vías de detección de operaciones sospechosas.

#### **4. Análisis de operaciones sospechosas vía estudio de prensa y medios de comunicación.**

Las operaciones con indicios de estar vinculadas con actividades de blanqueo de capitales o de financiación del terrorismo también podrán identificarse vía el estudio de prensa y otro tipo de publicaciones. Mediante estas fuentes de información podrá ampliarse el conocimiento sobre determinados clientes o bien, sobre operaciones que requieren de un examen especial.

Así, una vez se identifiquen operaciones relacionadas con algún cliente de la Entidad, de nuevo, deberá iniciarse el proceso de análisis de la operación por la UPBC.

### 8.1.3. Reporting de operativa sospechosa

#### **▪ Comunicación singular de operaciones**

El OCI será el último receptor de todas las comunicaciones de operaciones inusuales o incoherentes que provengan de las diferentes fuentes de detección ya comentadas en el apartado 8.1.2 del presente manual.

El representante ante el SEPBLAC será el encargado de comunicar estas operaciones al Servicio Ejecutivo, en caso de que las operaciones detectadas se consideren susceptibles de estar relacionadas con el blanqueo de capitales y financiación del terrorismo, tras el último y definitivo examen que realizará éste organismo sobre ellas.

Concretamente, el procedimiento que se seguirá para la comunicación de operativa sospechosa al SEPBLAC será el siguiente:

#### 1. Decisión de comunicación al SEPBLAC

Una vez la UPBC haya analizado e investigado una operación o un cliente inusual, ésta procederá a decidir si existen o no los indicios suficientes para declararla como susceptible de estar relacionada con el blanqueo de capitales y la financiación del terrorismo o si bien, esta operativa detectada es simplemente un “falso indicio”.

**En aquellos casos en los que se considere la operación como sospechosa, la UPBC lo comunicará al OCI y éste decidirá si definitivamente esta operativa debe ser comunicada al Servicio Ejecutivo o no.**

#### 2. Introducción en el Sistema y generación de un expediente

Cuando se haya decidido definitivamente comunicar al SEPBLAC la operación o cliente sospechoso, la UPBC cumplimentará el formulario F-19, en el cual incluirá toda la información requerida de manera obligatoria por el SEPBLAC respecto a la operación a comunicar, además de aquella que la UPBC, de manera adicional, haya considerado oportuna para una mayor clarificación de la comunicación enviada. Además, en este expediente también podrán anexarse ficheros con documentación adicional. Concretamente, la información y/o documentación a incluir en el expediente se encuentra detallada en el apartado 6.2 del presente manual.

Una vez cumplimentado el expediente, se guardará una copia del Expediente de Comunicación en el archivo de la UPBC.

#### 3. Envío al SEPBLAC de operación o cliente sospechoso

La UPBC enviará al Representante ante el SEPBLAC el Expediente de Comunicación (formulario F-19) cumplimentado para que sea firmado, y enviado por éste último al SEPBLAC.

El procedimiento establecido para dar respuesta a los requerimientos de las autoridades que sean recibidos en la Entidad es el siguiente:

### **1. Atender a los requerimientos recibidos**

La recepción de estos requerimientos deberá ser revisada por la UPBC de FRONTING o, en su caso, por el área Legal y *Compliance*, con el fin de detectar con la mayor brevedad posible cualquier nuevo requerimiento por parte del SEPBLAC o bien de cualquier otra Autoridad oficial al cual deba atenderse.

La UPBC, una vez recibido el requerimiento, deberá iniciar las investigaciones y la correspondiente recopilación de información necesaria para poder atender este requerimiento.

### **2. Análisis del requerimiento por la UPBC y recopilación de la información**

La UPBC analizará el requerimiento de información recibida por la Entidad y procederá a iniciar todas las medidas que sean necesarias con el fin de recabar toda la documentación e información relacionada y poder hacer frente al requerimiento en el tiempo y forma que hayan sido exigidos.

Estos requerimientos podrán ser de cualquier dato o conocimiento obtenido por la Entidad de las operaciones que haya realizado un cliente o no de la entidad.

### **3. Envío de la documentación a la Autoridad**

Una vez recabada toda la documentación por la Entidad, la UPBC remitirá ésta al Representante ante el SEPBLAC de la Entidad, o bien, su suplente, el cual será el encargado de responder al requerimiento enviando esta documentación. Posteriormente, se informará al OCI sobre los requerimientos recibidos.



#### **4. Archivo de la comunicación realizada**

Tras el envío, la UPBC será el encargado de establecer las medidas adecuadas para la conservación de esta información, bajo total confidencialidad.

La UPBC conservará en un lugar restringido el archivo documental de todas las comunicaciones recibidas por parte de las autoridades, junto con toda la documentación recabada por la Entidad. Todo ello, con el fin de que esta documentación pueda ser localizada y utilizada cuando sea preciso.

## 9. Anexo II - Plantillas comunicación interna operativa inusual

### Informes sobre indicios de blanqueo de capitales o de financiación de terrorismo

Fecha: --/--/----

Nº Empleado:

Oficina:

Localidad:

Provincia:

¿Es el primer informe que se envía sobre este asunto?  Sí  No

Titular de la cuenta u ordenante de la operación:

Documento Identificativo (Tipo y Número):

Población:

Provincia:

Cód. Postal:

Otros domicilios conocidos:

CÓDIGO CUENTA CLIENTE (C.C.C)

| Entidad | Oficina | Control | Número de Cuenta | Fecha de apertura |
|---------|---------|---------|------------------|-------------------|
| 0000    | 0000    | 00      | 0000000000       | --/--/----        |

Identificación de todos los intervinientes en la/s operación/es (titulares, autorizados, apoderados y otros relacionados directa o indirectamente) e identificación de las relaciones con la Caja de los intervinientes indicados (cuentas, préstamos, créditos, cajas de seguridad, tarjetas):

.....

Conocimiento de los intervinientes en las operaciones (antigüedad como cliente, relaciones, conocimiento, comportamiento, actividades del cliente):

.....

Descripción de las operaciones (fecha, moneda, importe, lugar de ejecución, finalidad, instrumento de pago o cobro, forma de operar, motivos que conozca por los que se realiza este tipo de operativa, correspondencia o no entre volumen de operaciones y actividad del cliente):

....

Indicios de blanqueo de capitales o financiación de terrorismo (motivos por los cuales se considera operación sospechoso/a):

- 1. Por indicios o certeza de vinculación al blanqueo de capitales o a la financiación de terrorismo.
- 2. Por manifestar una falta de justificación económica, profesional o de negocio para la realización de las actividades.
- 3. Por considerar la operación como compleja, inusual, o sin propósito económico o lícito aparente.

Indicar los motivos de la elección:

....

Gestiones y comprobaciones realizadas (si ha visitado alguna vez las instalaciones del cliente, impresión o comentarios al respecto):

.....

Documentación remitida. Relación de documentos que se adjuntan (copias de los documentos generados, tales como documentos de identificación, justificantes de operaciones, poderes, estados financieros):

....

## **10. Anexo III – Listado de operativa susceptible de ser sospechosa**

### **1. Riesgo asociado a los intervinientes o clientes (tomador, asegurado o beneficiario)**

Imposibilidad de conocer o verificar los datos sobre la actividad de los intervinientes debido a la negativa por parte del cliente a facilitar información o por facilitar datos erróneos, falsos o difíciles de verificar, tanto en la contratación como en el momento de verificarse el pago de la prestación.

Intervinientes residentes en paraísos fiscales, en países o territorios no cooperantes en la lucha contra el blanqueo de capitales y la financiación del terrorismo, en jurisdicciones no reguladas o escasamente reguladas, o en Estados donde se tiene conocimiento de la existencia de organizaciones criminales particularmente activas (por ejemplo, tráfico de drogas, actividades terroristas, delincuencia organizada o tráfico de seres humanos).

Intervinientes con antecedentes policiales o penales de conocimiento público, o relacionados con personas sometidas a prohibición de operar o vinculadas a actividades de financiación del terrorismo.

Intervinientes vinculados con el mundo político o PRP (Personas con responsabilidad pública), tanto de fuera de España como nacionales.

Pólizas individuales en las que no coincide la identidad de los intervinientes o hay datos erróneos.

Pólizas en las que los intervinientes están cruzados (por ejemplo, el tomador de una póliza es el asegurado de otra póliza en la que figura como tomador el asegurado de la primera póliza) y no se aprecian razones que lo justifiquen.

Pólizas en las que alguno de los intervinientes es una sociedad interpuesta.

Tomadores individuales que mantengan varias pólizas en iguales o diferentes productos y que la suma total de las primas superen los 30.000 € u otro umbral que, atendiendo a su perfil de negocio, establezca la entidad.

Pólizas en las que, poco antes del cobro de la prestación, hay un cambio de beneficiario.

Pólizas que cubren el fallecimiento, y éste se produce en el extranjero.

Cliente que facilita el mismo domicilio o número de teléfono que otro cliente, con quien aparentemente no parece tener relación.

Cliente que procede a cancelar la póliza al ser requerido para que facilite información.

Existencia de una misma cuenta corriente como receptora de los recibos de diferentes Tomadores.

Pluralidad de pólizas con un único beneficiario.

Solicitud de una póliza de un potencial cliente residente en una localidad distinta a la correspondiente a la oficina, cuando éste podría obtener una póliza similar en su lugar de residencia.

Solicitud de negocio fuera del patrón normal de conducta del tomador de la póliza (por ejemplo, solicitud de adquisición de un producto de pago único cuando el

comportamiento anterior del tomador se basaba en la contratación de productos con pequeños pagos regulares).

El cliente muestra poco interés por los beneficios del seguro y en cambio se muestra muy interesado por las condiciones de cancelación anticipada del contrato.

El cliente utiliza datos de contacto de difícil verificación (p.ej. el cliente facilita una dirección de correspondencia fuera de España y, tras varios intentos de verificación, se constata que la dirección es inexistente, el número telefónico facilitado por el cliente está permanentemente desconectado o no es válido, etc.).

## **2. Riesgo asociado a las primas, aportaciones o prestaciones**

Pago en moneda metálica, billetes de banco, cheques al portador u otros instrumentos anónimos.

Pago mediante transferencia internacional o transferencia nacional de importe elevado en la que no se contenga la identidad del ordenante o el número de la cuenta de origen.

Pago procedente de paraísos fiscales, países o territorios no cooperantes en la lucha contra el blanqueo de capitales y la financiación del terrorismo, jurisdicciones no reguladas o pobremente reguladas, o Estados donde se tiene conocimiento de la existencia de organizaciones criminales particularmente activas (por ejemplo, tráfico de drogas, actividades terroristas, delincuencia organizada o tráfico de seres humanos).

Fraccionamiento en el pago con el fin de eludir el umbral de comunicación (primas únicas sucesivas, primas periódicas fraccionadas o aportaciones extraordinarias).

Primas asumidas por el tomador desproporcionadas con relación a su patrimonio aparente.

Cobro de la renta a través de cuentas en países extranjeros por parte del beneficiario.

## **3. Riesgo asociado a la operativa**

Rescate anticipado de seguros de vida en un intervalo relativamente corto de tiempo desde la contratación.

Anticipos a cuenta de la provisión matemática constituida solicitados al poco tiempo de haber contratado el seguro.

Anulación de un seguro de vida en el plazo de 30 días sin penalización ni indicación de los motivos.

Extornos por anulación de póliza por emisión errónea o sin efecto y que posteriormente no se contrata nueva póliza.

Seguros de vida contratados con condiciones fuera del mercado (por ejemplo, seguros que garantiza una rentabilidad de 0,1% en caso de supervivencia a 10 años).

Póliza contratada con prima periódica de pequeño importe que recibe una aportación extraordinaria de gran importe.

Terminación anticipada de un producto, especialmente si ello ocasiona una pérdida y la devolución del dinero es solicitada en efectivo o a nombre de un tercero.

Aceptación por parte de un cliente de condiciones desfavorables en la suscripción de una póliza, teniendo en cuenta su edad o estado de salud.

#### **4. Riesgo asociado a los empleados, asociados, franquiciados o colaboradores**

Estilo de vida suntuoso o que no se corresponda con sus ingresos aparentes.

Negativa o resistencia a disfrutar vacaciones o permisos.

Negativa o resistencia a cambios en sus responsabilidades profesionales, especialmente si son favorables (promociones o ascensos).

Incremento notable e inesperado de sus ventas o resultados.

Nivel desproporcionado de negocios a prima única.

Incumplimiento reiterado de las normas internas de prevención.

Pago de la prima del cliente mediante cuenta del agente o corredor.