



**Principios Xerais da Política Corporativa de Prevención do
Branqueo de Capitais e do Financiamento do Terrorismo e
Xestión de Sancións e Contramedidas Financeiras
Internacionais do Grupo CaixaBank**

Setembro 2021

Contido

1. Introducción	3
1.1 Antecedentes	3
1.2 Concepto de risco de Branqueo de Capitais e Financiamento do Terrorismo e Sancións	3
1.3 Obxectivo	4
2. Ámbito de aplicación	5
3. Marco normativo. Normativa e estándares de aplicación	6
4. Marco de xestión de PBC/FT e Sancións	7
4.1 Avaliación de riscos	7
4.2 Dilixencia debida	7
4.3 Detección, control e exame das operacións	9
4.4 Comunicación de operativa sospeitosa	9
4.5 Control das listaxes de Sancións e comunicación de deteccións	9
4.6 Retención da documentación	10
4.7 Formación	10
4.8 Xestión consolidada do risco	10

1. Introducción

1.1 Antecedentes

CaixaBank, S.A. (en adiante, «CaixaBank»), como sociedade matriz das empresas que integran o seu grupo (en adiante, «Grupo» ou «Grupo CaixaBank», indistintamente) está firmemente comprometida coa prevención do branqueo de capitais e a prevención do financiamento de actividades terroristas (en adiante, «PBC/FT») e o cumprimento dos Programas de Sancións e Contramedidas Financeiras Internacionais (en adiante, «Sancións»), promovendo activamente a aplicación dos máis altos estándares internacionais na materia.

A criminalidade financeira é un fenómeno universal e globalizado que aproveita a desaparición das barreiras comerciais e a internacionalización da economía para a súa materialización. A loita contra este fenómeno require e esixe unha resposta coordinada da comunidade internacional en xeral e do sector financeiro en particular, para evitar ser utilizados con fins ilícitos de forma inadvertida e involuntaria.

1.2 Concepto de risco de Branqueo de Capitais e Financiamento do Terrorismo e Sancións

Para os efectos da interpretación e aplicación destes Principios, enténdese por:

Branqueo de capitais

- A conversión ou a transferencia de bens, sabendo que eses bens proceden dunha actividade delituosa ou da participación nunha actividade delituosa, co propósito de ocultar ou encubrir a orixe ilícita dos bens ou de axudar a persoas implicadas en eludir as consecuencias xurídicas dos seus actos.
- A ocultación ou encubrimento da natureza, orixe, localización, disposición, movemento ou propiedade reais de bens ou dereitos sobre a bens, sabendo que eses bens proceden dunha actividade delituosa ou da participación nunha actividade delituosa.
- A adquisición, posesión ou utilización de bens, sabendo no momento da recepción dos mesmos que proceden dunha actividade delituosa ou da participación nunha actividade delituosa.
- A participación nalguna das actividades mencionadas nos parágrafos anteriores, a asociación para cometer este tipo de actos, as tentativas de perpetrarlas e o feito de axudar, instigar ou aconsellar a alguén para que os realice ou facilitar a súa execución.

Entenderase por bens procedentes dunha actividade delituosa todo tipo de activos cuxa adquisición ou posesión teña como orixe un delito, tanto materiais como inmateriais, mobles ou inmobiliarios, tanxibles ou intanxibles, así como os documentos ou instrumentos xurídicos con independencia da súa forma, incluídas a electrónica ou dixital, que acrediten a propiedade dos devanditos activos ou dun dereito sobre eles, incluída a cota defraudada no caso dos delitos contra a Facenda Pública.

Considerarase que existe branqueo de capitais aínda cando as actividades que xeraron os bens se desenvolveran no territorio doutro Estado.

Por último, cómpre sinalar que no proceso de branqueo de capitais adoitan distinguirse as seguintes fases:

1. **Colocación ou ocultación:** Introducción dos cartos en efectivo procedentes de actividades delituosas en circuitos financeiros ou cambio a outro activo.
2. **Acumulación:** Realización de traspasos ou movementos entre distintos produtos ou servizos dunha ou de distintas xurisdicións co fin de fraccionar, acumular, ocultar, trasladar os importes e depositalos en xurisdicións menos rigorosas nas investigacións sobre a orixe das fortunas ou en contas onde a procedencia dos cartos teña unha aparencia legal, ou a realización doutras operacións que impidan rastrexar a verdadeira orixe.
3. **Integración:** Incorporación dos capitais no sistema financeiro baixo unha aparencia de lexitimidade.

As entidades e sociedades do Grupo CaixaBank poden utilizarse en calquera fase do proceso descrito, principalmente na fase de «colocación», polo que se deben adoptar as medidas de control interno necesarias para xestionar este risco.

Financiamento do terrorismo

A subministración, depósito, distribución ou recollida de fondos ou bens, por calquera medio, directa ou indirectamente, coa intención de utilizalos ou con coñecemento de que serán utilizados, total ou parcialmente, para a comisión de calquera dos delitos de terrorismo tipificados na normativa penal aplicable.

Considerarase que existe financiamento do terrorismo aínda cando a subministración ou a recollida de fondos ou bens se efectuase no territorio doutro Estado.

Programas de sancións e contramedidas financeiras internacionais

Instrumentos de natureza política, diplomática ou económica empregadas polos países e organizacións internacionais ou supranacionais para a implantación de medidas restritivas que eviten violacións do dereito internacional, dos dereitos humanos ou dos dereitos e liberdades civís.

1.3 Obxectivo

O obxectivo deste documento é recoller os principios e premisas que regulan o risco de branqueo de capitais e financiamento do terrorismo (en adiante, «BC/FT») e Sancións.

A finalidade destes Principios Xerais da Política Corporativa de PBC/FT e Sancións (en adiante, os «Principios») é establecer un marco de cumprimento a nivel de Grupo que todas as sociedades deben aplicar no exercicio das súas actividades, dos seus negocios e das súas relacións, tanto nacional coma internacionalmente, para previr o branqueo de capitais e o financiamento do terrorismo, así como para cumprir os distintos programas de sancións e contramedidas financeiras internacionais que sexan de aplicación.

2. Ámbito de aplicación

Estes Principios teñen carácter corporativo. En consecuencia, os principios de actuación definidos son aplicables a todas as sociedades do Grupo CaixaBank que realicen algunha das actividades incluídas no seu alcance. Os órganos de goberno destas sociedades adoptarán as decisións oportunas para integrar as disposicións destes Principios, adaptando, seguindo o principio de proporcionalidade, o marco de goberno á idiosincrasia da súa estrutura de órganos de goberno, comités e departamentos, e os seus principios de acción, metodoloxías e procesos ao descrito neste documento.

Esta integración poderá supoñer, entre outras decisións, a aprobación dunha política propia por parte da sociedade. A aprobación será necesaria naquelas sociedades que precisen adaptar o disposto nestes Principios ás súas propias especificidades, xa sexa por materia, por xurisdición ou pola relevancia do risco na sociedade. Neste caso, a función de Compliance de CaixaBank, dado o seu carácter corporativo, velará polo aliñamento destas políticas coa política corporativa e a súa consistencia en todo o Grupo CaixaBank.

Por outra banda, naqueles casos nos que as actividades de control e xestión do risco da sociedade se realicen directamente desde CaixaBank, xa sexa pola materialidade do risco na sociedade, por razóns de eficiencia ou ben porque a sociedade externalízase en CaixaBank a xestión operativa de este risco, porase en coñecemento dos órganos de goberno das sociedades afectadas a existencia desta Política Corporativa e a súa aplicación ás devanditas sociedades.

3. Marco normativo. Normativa e estándares de aplicación

Estes Principios rexeranse polo disposto na normativa aplicable vixente, así como pola que a modifique ou substitúa no futuro. En concreto, na data da súa elaboración, a normativa vixente aplicable á matriz do Grupo é a seguinte:

- Lei 10/2010, do 28 de abril, de prevención do branqueo de capitais e do financiamento do terrorismo.
- Real decreto 304/2014, do 5 de maio, polo que se aproba o Regulamento da Lei 10/2010, do 28 de abril, de prevención do branqueo de capitais e do financiamento do terrorismo.

No caso de sociedades sometidas a xurisdicións estranxeiras ou normativa sectorial complementaria, as políticas e procedementos que estas sociedades desenvolvan terán en conta, ademais da súa normativa propia, as obrigas de nivel consolidado contidas na normativa antes citada, sempre que non sexan contraditorias cos requisitos específicos da xurisdición ou normativa sectorial correspondente.

Finalmente, en cada unha das sociedades do Grupo desenvolveranse as normas, guías ou procedementos que sexan necesarios para a correcta implementación, execución e cumprimento destes Principios Xerais.

4. Marco de xestión de PBC/FT e Sancións

Os principais principios e estándares que constitúen o marco de prevención que regulan estes Principios son:

1. Avaliación de riscos
2. Dilixencia debida
3. Detección, control e exame das operacións
4. Comunicación de operativa sospeitosa.
5. Control das listaxes de Sancións e comunicación de deteccións
6. Retención da documentación
7. Formación
8. Xestión consolidada de riscos

4.1 Avaliación de riscos

A exposición das sociedades do Grupo aos riscos de branqueo de capitais, financiamento do terrorismo e Sancións está directamente relacionada co tipo de negocio ou actividade, os produtos comercializados, os servizos prestados, as canles de comercialización, o tipo e características dos clientes e/ou as xurisdicións nas que operen.

Co propósito de manter un marco de control e prevención adecuado cun enfoque baseado no risco, as Sociedades do Grupo deben ser categorizadas segundo o seu nivel de risco para garantir a aplicación dun maior grao de supervisión naquelas sociedades, segmentos, canles, xurisdicións ou produtos que presenten un nivel de risco máis elevado.

4.2 Dilixencia debida

A política de admisión de clientes e as medidas de dilixencia debida en ningún caso poderán supor a vulneración de dereitos nas xurisdicións onde a sociedade do Grupo desenvolve as súas actividades.

A política de admisión de clientes é dinámica e establece un marco de cumprimento a nivel de Grupo que pode variar en función do nivel de risco de determinados segmentos ou actividades segundo se derive da súa exposición a este en cada momento. A política de admisión debe cumprir os estándares internacionais e o principio de en inglés, KYC (Know Your Customer), con especial atención a garantir que se dispoña en todo momento dun bo coñecemento do cliente e das súas actividades.

O principio de Know Your Customer e as políticas de dilixencia debida aplicaranse sempre cun enfoque baseado no risco e garantirán que as medidas aplicadas sexan adecuadas ao risco subxacente de branqueo de capitais, de financiamento do terrorismo ou de Sancións.

Clasificación de clientes. Os clientes das sociedades do Grupo deben ser segmentados e clasificados en función do risco como un elemento que permita o deseño das medidas preventivas e de control que mitiguen a exposición ao risco, para que se apliquen medidas e controis máis estritos a aqueles clientes que presenten un nivel de risco superior.

Os controis e procedementos deberán garantir un seguimento adecuado e continuo da relación comercial co obxectivo de adaptar o nivel de risco e, polo tanto, as medidas a aplicar, ás circunstancias de risco do cliente en todo momento.

A valoración do nivel de risco documentarase nas sociedades do Grupo CaixaBank en función da súa actividade e operativa. Para determinar esta clasificación teranse en conta diversos factores en función da exposición ao risco da empresa e dos seus clientes ou provedores.

Como mínimo, as empresas do Grupo deberán utilizar a seguinte clasificación de clientes, segundo o grao de risco identificado:

Persoas cuxa admisión non está permitida: No se poderán admitir as relacións de negocio con persoas físicas ou xurídicas incluídas nas listaxes nacionais ou internacionais de Sancións ou ás que non lles fose posible aplicar as medidas de dilixencia debida establecidas na Lei 10/2010, así como calquera outro suposto previsto por un norma legal ou pola política interna da Entidade.

Persoas con risco superior á media: a súa aceptación como clientes está en todo caso condicionada á aplicación de medidas de dilixencia reforzada e requirirán aprobación centralizada.

O **resto de persoas** ou entidades quedarán suxeitos a medidas de dilixencia normais ou simplificadas segundo o establecido na normativa aplicable ou nas normas e procedementos internos.

Identificación formal dos clientes. As normas e procedementos que desenvolvan estes Principios deberán garantir nas sociedades do Grupo a adecuada identificación de todos os clientes de acordo coa lexislación aplicable en cada momento e en cada xurisdición, o que incluírá, en todo caso, a verificación da identidade mediante documentos válidos e vixentes.

En ningún caso se manterán relacións de negocio con persoas ás que non se puidese identificar, quedando tamén prohibida a contratación de produtos ou servizos de carácter anónimo, cifrado ou ficticio.

Con carácter previo ao establecemento de relacións de negocio ou á execución das operacións, deberase identificar ao titular real. Esta obriga implicará que no caso de existir indicios ou certeza de que os clientes non actúan por conta propia, deberá obterse información precisa para coñecer a identidade das persoas en cuxo nome actúan, así como documentación suficiente que acredite as facultades con que actúa.

Coñecemento da actividade e patrimonio do cliente. Antes de establecer unha relación de negocio, as sociedades do Grupo deberán recoller, como mínimo, información sobre a actividade profesional ou empresarial do cliente e a procedencia dos fondos ou patrimonio.

En función do nivel de risco asignado ao cliente, poderán adoptar medidas adicionais consistentes na verificación documental e a través de fontes externas fiables, da información facilitada polo cliente, especialmente en relación coa súa actividade profesional ou empresarial, a orixe dos fondos ou patrimonio e calquera outra información relevante de acordo coas normas e procedementos internos.

4.3 Detección, control e exame das operacións

As sociedades do Grupo deberán dispor de medios para a detección, control e exame das operacións. Estes medios aplicaranse en función do risco e conterán en todo caso os tres supostos básicos de detección de operacións:

- a. A comunicación interna por indicios realizada polos empregados do Grupo.
- b. A detección de posibles operacións sospeitosas a través dos sistemas de alertas establecidos (a nivel de cada sociedade do Grupo e/ou centralizados).
- c. As comunicacións dos organismos supervisores ou das autoridades policiais ou xudiciais.

A detección de operacións sospeitosas implicará a realización dunha análise detallada e de carácter integral destinada a determinar a existencia efectiva de indicios de branqueo de capitais e financiamento do terrorismo. A metodoloxía para a realización desta análise deberá incluírse nun procedemento específico denominado Procedemento de exame especial. A devandita análise centralizarase en todo caso nunha mesma unidade común para todas as sociedades do Grupo que operen na mesma xurisdición.

O seguimento será automatizado e revisarase a actividade en función dos patróns que a lei e as mellores prácticas identifiquen en cada momento.

4.4 Comunicación de operativa sospeitosa

As sociedades do Grupo comunicaranlle por iniciativa propia aos organismos supervisores e/ou de Intelixencia Financeira calquera feito ou operación, mesmo a simple tentativa, que unha vez concluído o exame especial cando determine que concorren na operativa, indicios ou certeza de relación co branqueo de capitais ou financiamento do terrorismo.

En particular, comunicaráselle aos organismos supervisores as operacións que amosen unha evidente falta de correspondencia coa natureza, volume de actividade ou antecedentes operativos dos clientes.

A decisión de comunicar será adoptada de xeito centralizado en cada xurisdición polas persoas ou órganos designados para o efecto e realizarase a través do representante habilitado perante as autoridades competentes. A comunicación efectuada incluírá, en todo caso, información sobre a decisión adoptada respecto da continuación ou non da relación de negocio, así como a xustificación desta decisión.

Sen prexuízo de efectuar a comunicación por indicio, a entidade adoptará inmediatamente medidas adicionais de xestión e mitigación do risco que deberán ter en conta o risco de revelación.

Os empregados do Grupo deberán absterse de realizar calquera operación respecto da cal exista indicio ou certeza de que estea relacionada co branqueo de capitais ou o financiamento do terrorismo.

Os empregados, directivos ou axentes do Grupo non lle revelarán ao cliente nin a terceiros que se comunicou información aos órganos de control interno ou ao organismo supervisor nin que se está a examinar ou pode examinarse algunha operación por se puidese estar relacionada co branqueo de capitais ou co financiamento do terrorismo.

4.5 Control das listaxes de Sancións e comunicación de deteccións

Para cumprir coas restricións impostas polos programas de Sancións, as sociedades do Grupo deberán:

- Identificar e seguir os programas de Sancións instaurados polas Nacións Unidas (ONU), a Unión Europea (UE), a OFAC e os programas locais que sexan de aplicación nas xurisdicións nas que operan as sociedades do Grupo.
- Avaliar os riscos asociados ás actividades relacionadas cos Programas de Sancións para determinar os riscos de participar ou intervir en actividades restrinxidas ou prohibidas polas Sancións.
- Absterse de executar ou participar en operacións ou transaccións con persoas sancionadas.
- Cumprir as prohibicións e restricións na execución de transaccións, pagamentos ou relacións comerciais e absterse de executalas cando supoñan un incumprimento dos programas de Sancións.
- Bloquear activos e fondos cando así o requiran os programas de Sancións e comunicándolle esa circunstancia ás autoridades que administran os programas de Sancións.
- Implantar procedementos de control interno e mecanismos de prevención que permitan un axeitado cumprimento das obrigas das empresas do Grupo, o que incluírá procedementos e ferramentas de filtrado automatizado (screening).

4.6 Retención da documentación

As sociedades do Grupo CaixaBank establecerán políticas de conservación da documentación que cumpran cos requirimentos legais aplicables en cada xurisdición, sendo o período mínimo de conservación o que determine en cada momento a lexislación na materia e nunca inferior a 10 anos.

4.7 Formación

A sensibilización sobre os riscos asociados a estes delitos é un elemento fundamental na loita contra o branqueo de capitais e o terrorismo.

As sociedades do Grupo CaixaBank deberán definir, manter e aplicar programas de formación dos seus empregados para garantir un adecuado nivel de sensibilización de todo o persoal, tal e como esixen as leis, e establecerán políticas que garantan a formación obrigatoria en materia de prevención de branqueo de capitais, financiamento do terrorismo e Sancións de todo o seu persoal (incluíndo a alta dirección e os órganos administrativos) de forma periódica e adecuada ao nivel de exposición ao risco da súa actividade na sociedade.

Os programas de formación PBC/FT e Sancións de todas as sociedades do Grupo CaixaBank deberán ser validados pola Unidade de Cumprimento Normativo de CaixaBank como unidade especializada do Grupo, unha vez validados polos departamentos competentes en materia de formación e cumprimento da sociedade, levando rexistros e constancia da formación impartida, dos seus contidos e dos empregados que a recibiron e a superaron.

4.8 Xestión consolidada do risco

CaixaBank considera que a mellor forma de combater os riscos asociados a estes Principios é a súa xestión consolidada e a xestión uniforme e agregada da información relacionada coa xestión destes riscos a nivel de Grupo, con independencia da xurisdición na que operen as sociedades que o integran.

O principio de xestión agregada ou consolidada constitúe así un pilar fundamental do modelo de prevención e permite coordinar de xeito uniforme os esforzos de todas as sociedades do Grupo, así como avaliar e xestionar os riscos de forma agregada.

Por este motivo, todas as entidades que integran o Grupo manterán a CaixaBank informada puntualmente sobre relacións de alto risco, datos sobre actividades sensibles e os seus riscos asociados, atendendo con prontitude calquera solicitude de información que CaixaBank poida formular sobre a xestión do risco regulatorio e reputacional relacionado co branqueo de capitais, o financiamento do terrorismo e as Sancións.

En todo caso, estas obrigas enténdense sen prexuízo do estrito cumprimento da normativa aplicable, e moi especialmente da de protección de datos e privacidade. CaixaBank e as sociedades do Grupo adoptarán as medidas necesarias para preservar a confidencialidade e privacidade dos datos comunicados desta forma entre as entidades do Grupo.