



Princípios Gerais da Política Corporativa de Prevenção de
Branqueamento de
Capitais e do Financiamento do Terrorismo e de Gestão
das Sanções e Contramedidas Financeiras
Internacionais do Grupo CaixaBank

setembro de 2021

Conteúdo

1.	Introdução	3
1.1	Antecedentes	3
1.2	Conceito do risco de Branqueamento de Capitais e Financiamento do Terrorismo e Sanções	3
1.3	Objetivo	4
2.	Âmbito de aplicação	5
3.	Quadro regulamentar. Legislação e padrões de aplicação	6
4.	Modelo de gestão de PBC/FT e Sanções	7
4.1	Avaliação de Riscos	7
4.2	Medidas de Diligência	7
4.3	Deteção, controlo e exame de operações	9
4.4	Comunicação de operação suspeita	9
4.5	Controlo de listas de Sanções e comunicação de deteções	9
4.6	Conservação da documentação	10
4.7	Formação	10
4.8	Gestão consolidada do risco	10

1. Introdução

1.1 Antecedentes

A CaixaBank, S.A. (doravante "CaixaBank"), como empresa-mãe das empresas que compõem o seu grupo (doravante "Grupo" ou "Grupo CaixaBank"), está firmemente empenhado na prevenção do branqueamento de capitais e na prevenção do financiamento de atividades terroristas (doravante "PBC/FT"), e no cumprimento dos Programas de Sanções e Contramedidas Financeiras internacionais (doravante "Sanções"), promovendo ativamente a aplicação dos mais elevados padrões internacionais nesta área.

A criminalidade financeira é um fenómeno universal e globalizado que tira partido do desaparecimento das barreiras comerciais e da internacionalização da economia para se materializar. A luta contra este fenómeno requer e exige uma resposta coordenada da comunidade internacional em geral e do setor financeiro em particular, a fim de evitar ser utilizado inadvertida e involuntariamente para fins ilícitos.

1.2 Conceito do risco de Branqueamento de Capitais e Financiamento do Terrorismo e Sanções

Para efeitos de interpretação e aplicação dos presentes Princípios Gerais, entende-se por:

Branqueamento de capitais

- A conversão ou transferência de bens, sabendo que tais bens provêm de atividade criminosa ou da participação em atividade criminosa, com o objetivo de ocultar ou encobrir a origem ilícita dos bens ou de ajudar pessoas envolvidas na fuga às consequências legais dos seus atos.
- A ocultação ou encobrimento da natureza, origem, localização, disposição, circulação ou propriedade reais de bens ou direitos sobre bens, sabendo que tais bens provêm de atividade criminosa ou da participação em atividade criminosa.
- A aquisição, posse ou utilização de bens, sabendo, no momento da receção dos mesmos, que provêm de atividade criminosa ou da participação em atividade criminosa.
- A participação em qualquer das atividades mencionadas nos parágrafos anteriores, a associação para cometer tais atos, as tentativas de as praticar e o facto de ajudar, instigar ou aconselhar qualquer pessoa a realizar tais atividades ou facilitar a sua execução.

Por bens provenientes de atividade criminosa entendem-se todos os tipos de ativos cuja aquisição ou posse tenha origem ilícita, quer sejam corpóreos ou incorpóreos, móveis ou imóveis, tangíveis ou intangíveis, bem como os documentos ou instrumentos legais sob qualquer forma, incluindo eletrónica ou digital, que comprovem a propriedade dos referidos ativos ou um direito sobre os mesmos, incluindo o montante defraudado no caso dos delitos fiscais.

Considera-se que existe branqueamento de capitais mesmo que as atividades que geraram os bens tenham sido realizadas no território de outro Estado.

Por último, há que destacar que, no processo de branqueamento de capitais, são habitualmente diferenciadas as seguintes fases:

- **Colocação ou ocultação:** Introdução do dinheiro em metálico procedente de atividades de delitos nos circuitos financeiros ou mudança para um ativo diferente.
- **Circulação:** Realização de transferências ou movimentos entre diferentes produtos ou serviços de uma ou de diferentes jurisdições com o fim de fracionar, acumular, ocultar, transladar os montantes e depositá-los em jurisdições menos rigorosas nas investigações sobre a origem das fortunas ou em contas onde a origem do dinheiro tiver uma aparência legal, ou realização de outras transações que impeçam rastrear a verdadeira origem.
- **Integração:** Incorporação dos capitais no sistema financeiro sob uma aparência de legitimidade.

As entidades e sociedades do Grupo CaixaBank podem ser utilizadas em qualquer fase do processo descrito, fundamentalmente na fase de “colocação”, pelo que devem ser adotadas as medidas de controlo interno necessárias para gerir este risco.

Financiamento do terrorismo

O fornecimento, o depósito, a distribuição ou a recolha de fundos ou bens, por qualquer meio, de forma direta ou indireta, com a intenção de utilizá-los ou com o conhecimento de que serão utilizados, integralmente ou em parte, para a realização de qualquer um dos delitos de terrorismo classificados na normativa penal aplicável.

Será considerado que existe financiamento do terrorismo também quando o fornecimento ou a recolha de fundos ou bens se tiver desenvolvido no território de outro estado.

Programas de sanções e contramedidas financeiras internacionais

Instrumentos de natureza política, diplomática ou económica utilizada por países e organismos internacionais ou supranacionais com a finalidade de implementar medidas restritivas que impeçam violações do direito internacional, dos direitos humanos ou dos direitos e liberdades civis.

1.3 Objetivo

Este documento tem como objetivo estabelecer os princípios e as premissas que regulam a gestão do risco de branqueamento de capitais e financiamento do terrorismo (doravante BC/FT) e Sanções.

O objetivo destes Princípios Gerais da Política Corporativa de PBC/FT e Sanções (doravante, a “Política”) é estabelecer um quadro de cumprimento a nível do Grupo, que todas as sociedades devem aplicar no exercício das suas atividades, dos seus negócios e das suas relações, tanto nacional como

internacionalmente, para prevenir o branqueamento de capitais e o financiamento do terrorismo, bem como para o cumprimento dos diferentes programas de sanções e contramedidas financeiras internacionais que sejam aplicáveis.

2. Âmbito de aplicação

Os presentes Princípios Gerais têm caráter corporativo. Consequentemente, os princípios de ação definidos são aplicáveis a todas as empresas do Grupo CaixaBank que desenvolvam qualquer uma das atividades incluídas no seu âmbito. Os órgãos de governo destas sociedades tomarão as decisões adequadas para integrar as disposições desta Política, adaptando, seguindo o princípio da proporcionalidade, o modelo de governo às idiossincrasias da sua estrutura de órgãos de governo, comités e departamentos, e os seus princípios de ação, metodologias e processos ao que é descrito no presente documento.

Esta integração pode envolver, entre outras decisões, a aprovação de uma política própria por parte da sociedade. Será necessária a aprovação das sociedades que necessitem de adaptar as disposições desta Política às suas próprias especificidades, quer por assunto, jurisdição ou relevância do risco na sociedade. Neste caso, a função de Compliance da CaixaBank, dada a sua natureza corporativa, assegurará que estas políticas estejam alinhadas com a política empresarial e sejam consistentes em todo o Grupo CaixaBank.

Além disso, nos casos em que as atividades de controlo e gestão do risco da empresa são realizadas diretamente pela CaixaBank, quer devido à materialidade do risco na empresa, quer por razões de eficiência ou porque a empresa subcontratou a gestão operacional deste risco ao CaixaBank, os órgãos de governo das sociedades afetadas serão informados da existência desta Política Empresarial e da sua aplicação a essas sociedades.

3. Quadro regulamentar, Legislação e padrões de aplicação

Os presentes Princípios Gerais serão regidos pelas disposições na legislação espanhola aplicável em vigor, bem como por quaisquer regulamentos que a possam alterar ou substituir no futuro. Especificamente, na data da sua elaboração, a legislação em vigor aplicável à empresa-mãe do Grupo é a seguinte:

- Lei 10/2010, de 28 de abril, sobre a prevenção do branqueamento de capitais e do financiamento do terrorismo.
- Real Decreto 304/2014, de 5 de maio, que aprova o Regulamento da Lei 20/2010, de 28 de abril, sobre prevenção do branqueamento de capitais e do financiamento do terrorismo.

No caso de sociedades sujeitas a jurisdições estrangeiras ou legislação setorial complementar, as políticas e procedimentos que estas sociedades desenvolvem devem ter em conta, para além da sua própria legislação, as obrigações ao nível consolidado contidas na referida legislação, desde que não sejam contraditórias com os requisitos específicos da jurisdição ou legislação setorial correspondente.

Finalmente, em cada uma das sociedades do Grupo, serão desenvolvidas as regras, orientações ou procedimentos necessários para a correta implementação, execução e conformidade destes Princípios Gerais.

4. Modelo de gestão de PBC/FT e Sanções

Os principais princípios e normas que constituem o modelo de prevenção que esta Política regula são:

1. Avaliação de Riscos
2. Medidas de Diligência
3. Detecção, controlo e exame de operações
4. Comunicação de operação suspeita.
5. Controlo de listas de Sanções e Comunicação de deteções
6. Conservação da documentação
7. Formação
8. Gestão consolidada de riscos

4.1 Avaliação de Riscos

A exposição das sociedades do Grupo aos riscos de Branqueamento de Capitais, ao Financiamento do Terrorismo e às Sanções está diretamente relacionada com o tipo de negócio ou atividade, os produtos comercializados, os serviços prestados, os canais de comercialização, a tipologia e características dos clientes e/ou as jurisdições em que operem.

Com o objetivo de manter um modelo adequado de controlo e prevenção com um foco baseado em risco, as Sociedades do Grupo devem ser categorizadas segundo o seu nível de risco, para garantir a aplicação de maior grau de supervisão nessas sociedades, segmentos, canais, jurisdições ou produtos que apresentem um nível de risco mais elevado.

4.2 Medidas de Diligência

A política de aceitação de clientes e as medidas de diligência não poderão, em nenhum caso, representar violações de direitos nas jurisdições onde a sociedade do Grupo realizar as suas atividades.

A política de aceitação de clientes é dinâmica e estabelece um quadro de cumprimento ao nível do Grupo, que poderá variar em função do nível de risco de determinados segmentos ou atividades, conforme resultar da sua exposição ao mesmo em cada momento. A política de aceitação de clientes deve cumprir as normas internacionais e o princípio de “Conheça o seu Cliente” (também conhecido pelas suas siglas em inglês KYC, Know Your Customer), com especial foco em garantir que se dispõe sempre de um bom conhecimento do cliente e das suas atividades.

O princípio de Know Your Customer e as medidas de diligência serão aplicados sempre com um foco baseado no risco, e assegurarão que as medidas aplicadas são adequadas ao risco subjacente de branqueamento de capitais, de financiamento do terrorismo ou de Sanções.

[Classificação de clientes.](#) Os clientes das sociedades do Grupo devem ser segmentados e classificados em função do risco como elemento que permita a criação das medidas preventivas e de

controle que reduzam a exposição ao risco, e assim sejam aplicadas medidas e controles mais restritos aos clientes que apresentam um nível de risco superior.

Os controles e procedimentos devem garantir um seguimento adequado e contínuo da relação de negócio com o objetivo de adaptar o nível de risco e, portanto, as medidas a aplicar, às circunstâncias de risco do cliente em todos os momentos.

A avaliação do nível de risco será documentada nas sociedades do Grupo CaixaBank em função da sua atividade e operacionalidade. Para a determinação desta classificação terão sido em conta diversos fatores em função da exposição ao risco da sociedade e dos seus clientes ou fornecedores.

Como mínimo, as sociedades do Grupo devem utilizar a seguinte classificação de clientes, segundo o grau de risco identificado:

Pessoas cuja aceitação não é permitida: não são admissíveis relações de negócios com pessoas singulares ou coletivas a quem não foi possível aplicar as medidas de diligência previstas nestes Princípios, ou que se encontrem incluídas nas listas nacionais ou internacionais de Sanções e aquelas que não devem ser admitidas como clientes de acordo com os programas de Sanções definidos nos Presentes Princípios Gerais e nos regulamentos legais e internos aplicáveis.

Pessoas de risco acima da média: a sua aceitação como clientes está, em qualquer caso, condicionada à aplicação de medidas de diligência reforçada e exigirá uma aprovação centralizada. As seguintes pessoas ou entidades serão incluídas nesta categoria.

As **restantes pessoas** ou entidades ficarão sujeitas a medidas de diligência normais ou simplificadas, segundo o estabelecido na legislação aplicável ou nas regras e procedimentos internos.

Identificação formal de clientes. As regras e procedimentos de aplicação da presente Política devem garantir nas sociedades do Grupo a correta identificação de todos os clientes, de acordo com a legislação aplicável em todos os momentos e em cada jurisdição, o que incluirá, em todos os casos, a verificação da identidade mediante documentos válidos e em vigor.

Em caso algum serão mantidas relações de negócio com pessoas que não tenham sido identificadas, sendo também proibida a contratação de produtos ou serviços de natureza anónima, encriptada ou fictícia.

Antes do estabelecimento de relações de negócios ou da execução das operações, o beneficiário efetivo deverá ser identificado. Esta obrigação implicará que, perante a existência de indícios ou certeza de que os clientes não agem por conta própria, deverá ser solicitada informação precisa, com o fim de conhecer a identidade das pessoas por conta das quais agem. Assim como documentação suficiente que certifique as procurações com as quais opera.

Conhecimento da atividade e património do cliente. Antes do estabelecimento de uma relação de negócios, as sociedades do Grupo deverão solicitar, pelo menos, informação sobre a atividade profissional ou empresarial do cliente e a origem dos fundos ou património.

Em função do nível de risco atribuído ao cliente poderão ser adotadas medidas adicionais consistentes na verificação de documentos e através de fontes externas confiáveis, da informação fornecida pelo cliente, especialmente em relação à sua atividade profissional ou empresarial, a origem dos fundos ou património e qualquer outra informação relevante de acordo com as normas e procedimentos internos.

4.3 Detecção, controlo e exame de operações

As sociedades do Grupo deverão dispor de meios para a deteção, controlo e exame de operações. Estes meios serão aplicados em função do risco e conterão sempre os três pressupostos básicos de deteção de operações:

- a) A comunicação interna por indícios realizados pelos empregados do Grupo.
- b) A deteção de possíveis operações suspeitas através dos sistemas de alertas estabelecidos (ao nível de cada sociedade do Grupo e/ou centralizados).
- c) As comunicações dos órgãos de supervisão ou das autoridades policiais ou judiciais.

A deteção de operações suspeitas acarretará a realização de uma análise detalhada e de carácter integral, destinada à determinação da existência efetiva de indícios de branqueamento de capitais e do financiamento ao terrorismo. As metodologias para a realização desta análise deverão ser registadas num procedimento específico denominado Procedimento de exame especial. Essa análise estará sempre centralizada na mesma unidade comum para todas as sociedades do Grupo que operem na mesma jurisdição.

A monitorização será automatizada e reverá a atividade com base nos padrões que a lei e as melhores práticas identificarem em cada momento.

4.4 Comunicação de operação suspeita

As sociedades do Grupo comunicarão, por iniciativa própria, aos órgãos de supervisão e/ou de Inteligência Financeira, qualquer facto ou operação, incluindo a mera tentativa, depois de concluído o exame especial quando determinar que ocorrem na operação, indícios ou certeza de relação com o branqueamento de capitais ou o financiamento do terrorismo.

Em particular, serão comunicadas aos órgãos de supervisão as operações que mostrarem uma evidente falta de correspondência com a natureza, volume de atividade ou antecedentes operacionais dos clientes.

A decisão de comunicar será adotada centralmente em cada jurisdição pelas pessoas ou órgãos designados para esse efeito e será realizada através do representante capacitado perante as autoridades competentes.

Na comunicação efetuada, em qualquer caso, será incluída informação sobre a decisão adotada quanto à continuação ou não da relação de negócios, bem como a justificação desta decisão. Sem prejuízo de efetuar a comunicação por indício, a entidade adotará imediatamente medidas adicionais de gestão e mitigação do risco, as quais devem ter em conta o risco de divulgação.

Os funcionários do grupo devem abster-se de executar qualquer operação para a qual exista qualquer indício ou certeza de que está relacionada com branqueamento de capitais ou financiamento do terrorismo.

Os funcionários, diretores ou agentes do Grupo não devem revelar ao cliente ou a terceiros que as informações foram comunicadas aos órgãos de controlo interno ou ao organismo de supervisão, ou que qualquer operação está a ser ou pode ser examinada para verificar eventual branqueamento de capitais ou financiamento do terrorismo.

4.5 Controlo de listas de Sanções e comunicação de deteções

Para cumprir as restrições impostas pelos programas de Sanções, as sociedades do Grupo devem:

- Identificar e seguir os programas de Sanções implementados pelas Nações Unidas (ONU), pela União Europeia (UE), OFAC pelos programas locais aplicáveis nas jurisdições em que as sociedades do Grupo operam.
- Avaliar os riscos associados às atividades relacionadas com os Programas de Sanções para determinar os riscos de participação ou envolvimento em atividades restritas ou proibidas pelas Sanções.
- Abster-se de executar ou participar em operações ou transações com pessoas sancionadas.
- Cumprir as proibições e restrições na execução de transações, pagamentos ou relações comerciais e abster-se de as executar quando impliquem o incumprimento dos programas de Sanções.
- Bloquear ativos e fundos quando exigido pelos programas de Sanções e comunicar tal situação às autoridades que gerem os programas de Sanções.
- Implementar procedimentos de controlo interno e mecanismos de prevenção para assegurar o cumprimento adequado das obrigações das sociedades do Grupo, incluindo procedimentos e ferramentas de filtragem automatizada (*screening*).

4.6 Conservação da documentação

As sociedades do Grupo CaixaBank devem estabelecer políticas de conservação da documentação que cumpram os requisitos legais aplicáveis em cada jurisdição, sendo o período mínimo de conservação determinado em qualquer momento pela legislação na matéria, e nunca inferior a 10 anos.

4.7 Formação

A sensibilização nos riscos associados a estes delitos é um elemento fundamental na luta contra o branqueamento de capitais e o financiamento ao terrorismo.

As sociedades do Grupo CaixaBank devem definir, manter e aplicar programas de formação para os seus funcionários, de modo a assegurar um nível adequado de sensibilização de todo o pessoal, tal como exigido por lei, e estabelecer políticas para assegurar uma formação obrigatória na prevenção do branqueamento de capitais, financiamento do terrorismo e Sanções para todo o seu pessoal (incluindo a alta direção e os órgãos de administração) numa base regular e adequada ao nível de exposição do risco da sua atividade na sociedade.

Os programas de formação de PBC/FT e Sanções de todas as sociedades do Grupo CaixaBank devem ser validados pela unidade de Cumprimento Normativo do CaixaBank como unidade especializada do Grupo, uma vez validados pelos departamentos responsáveis de formação e cumprimento da sociedade, mantendo registos e provas da formação fornecida, dos seus conteúdos e dos funcionários que a receberam e que obtiveram aprovação.

4.8 Gestão consolidada do risco

O CaixaBank considera que a melhor forma de combater os riscos associados a esta Política é geri-los numa base consolidada e gerir as informações relacionadas com a gestão destes riscos a nível do Grupo de forma uniforme e agregada, independentemente da jurisdição em que as sociedades que a compõem operam.

O princípio de gestão agregada ou consolidada é assim um pilar fundamental do modelo de prevenção e permite coordenar os esforços de todas as sociedades do Grupo de forma uniforme, bem como avaliar e gerir os riscos numa base agregada.

Por conseguinte, todas as entidades que constituem o Grupo manterão a CaixaBank frequentemente informada das relações de alto risco, dos dados de atividades sensíveis e dos seus riscos associados,

atendendo de forma rápida qualquer pedido de informação que o CaixaBank possa fazer na gestão do risco regulamentar e de reputação relacionado com o branqueamento de capitais, o financiamento do terrorismo e as Sanções.

Em qualquer caso, essas obrigações são entendidas sem prejuízo do cumprimento restrito da normativa aplicável, e muito especialmente, da de proteção de dados e privacidade.

A CaixaBank e as sociedades do Grupo adotarão as medidas necessárias para preservar a confidencialidade e privacidade dos dados, assim comunicados entre entidades do Grupo.