



Principios xerais da Política corporativa de xestión do risco de  
prevención do branqueo de capitais e do financiamento  
do terrorismo e de xestión das sancións e contramedidas  
financeiras internacionais

29 de xuño de 2023

## Contido

|     |  |    |
|-----|--|----|
| 1.  | Introdución  | 3  |
| 1.1 | Antecedentes   | 3  |
| 1.2 | Concepto do risco de branqueo de capitais e financiamento do terrorismo e sancións | 3  |
| 1.3 | Obxectivo  | 4  |
| 2.  | Ámbito de aplicación   | 6  |
| 3.  | Marco normativo. Normativa e estándares de aplicación                              | 7  |
| 4.  | Marco de xestión de PBC/FT e Sancións  | 8  |
| 4.1 | Avaliación de riscos   | 8  |
| 4.2 | Dilixencia debida  | 8  |
| 4.3 | Detección, control e exame de operacións   | 11 |
| 4.4 | Comunicación de operativa sospeitosa   | 11 |
| 4.5 | Control de listaxes de Sancións e comunicación de deteccións                       | 12 |
| 4.6 | Retención da   | 12 |
| 4.7 | Formación  | 13 |
| 4.8 | Xestión consolidada do risco   | 14 |

## 1. *Introdución*

### 1.1 Antecedentes

Caixabank, S.A. (de agora en diante "CaixaBank"), como sociedade cabeceira das empresas que conforman o seu grupo (de agora en diante, "Grupo" ou "Grupo CaixaBank" indistintamente) está firmemente comprometida coa prevención do branqueo de capitais, e a prevención do financiamento do terrorismo (de agora en diante PBC/FT) e o cumprimento dos programas de sancións e contramedidas financeiras internacionais (de agora en diante "Sancións"), promovendo activamente a aplicación dos máis altos estándares internacionais na materia.

A criminalidade financeira é un fenómeno universal e globalizado que se aproveita da desaparición de barreiras comerciais e da 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 do 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, a sabendas de que os devanditos 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 as persoas que estean implicadas en eludir as consecuencias xurídicas dos seus actos.
- A ocultación ou o encubrimento da natureza, a orixe, a localización, a disposición, o movemento ou a propiedade real de bens ou dereitos sobre bens, a sabendas de que os devanditos bens proceden dunha actividade delituosa ou da participación nunha actividade delituosa.
- A adquisición, posesión ou utilización de bens, a sabendas, no momento da recepción destes, de que proceden dunha actividade delituosa ou da participación nunha actividade delituosa.
- A participación nalgunha das mencionadas nos parágrafos anteriores, a asociación para cometer este tipo de actos, as tentativas de perpetralas e o feito de axudar, instigar ou aconsellar alguén para realizalas ou facilitar a súa execución.

Entenderase por bens procedentes dunha actividade delituosa todo tipo de activos cuxa adquisición ou posesión teña a súa orixe nun delito, tanto materiais coma inmateriais, mobles ou inmobles, tanxibles ou intanxibles, así como os documentos ou instrumentos xurídicos con independencia da súa forma, incluídas a

electrónica ou a dixital, que acrediten a propiedade dos devanditos activos ou un dereito sobre estes, con inclusión da cota defraudada no caso dos delitos contra a Facenda pública.

Considerarase que hai branqueo de capitais aínda cando as actividades que xerasen os bens se desenvolvesen 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 do diñeiro en efectivo procedente de actividades delituosas nos circuitos financeiros ou cambio a un activo diferente.
2. **Acumulación:** Realización de traspasos ou movementos entre diferentes produtos ou servizos dunha ou de diferentes 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 orixe do diñeiro teña unha aparencia legal, ou realización doutras transaccións 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 ser utilizadas en calquera fase do proceso descrito, fundamentalmente na fase de "colocación", polo que deben ser adoptadas as medidas de control interno necesarias para xestionar este risco.

### **Financiamento do terrorismo**

A subministración, o depósito, a distribución ou a recollida de fondos ou bens, por calquera medio, de forma directa ou indirecta, coa intención de utilizalos ou co coñecemento de que serán utilizados, integramente ou en parte, 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 desenvolvesen no territorio doutro Estado.

### **Programas de sancións e contramedidas financeiras internacionais**

Instrumentos de natureza política, diplomática ou económica utilizados por países e organismos internacionais ou supranacionais coa finalidade de implantar medidas restritivas que impidan violacións do dereito internacional, dos dereitos humanos ou dos dereitos e liberdades civís.

## 1.3 Obxectivo

Este documento ten como obxectivo recoller os principios e premisas que regulan o risco de prevención de

branqueo de capitais e financiamento do terrorismo (de agora en diante PBC/FT) e Sancións.

O propósito destes Principios Xerais da Política corporativa de PBC/FT e Sancións (de agora en diante os "Principios") é establecer un marco de cumprimento no Grupo, que todas as sociedades deben aplicar no exercicio das súas actividades, os seus negocios e as súas relacións, tanto nacional coma internacionalmente para previr o branqueo de capitais e o financiamento do terrorismo así como para cumprir cos diferentes programas de sancións e contramedidas financeiras internacionais que resulten de aplicación.

## 2. *Ámbito de aplicación*

Os presentes 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 co obxecto de 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 actuación, metodoloxías e procesos ao descrito neste documento.

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

Por outra banda, naqueles casos en que as actividades de control e xestión do risco da sociedade se realice directamente desde CaixaBank, xa sexa por materialidade do risco na sociedade, por razóns de eficiencia ou porque a sociedade externalízase en CaixaBank a xestión operativa deste risco, os órganos de goberno das sociedades afectadas tomarán coñecemento da existencia desta política corporativa e da súa aplicación ás devanditas sociedades.

### 3. Marco normativo. Normativa e estándares de aplicación

Estes Principios rexeranse polo previsto na normativa aplicable vixente, así como por aquela 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, de 5 de maio, polo que se aproba o Regulamento da Lei 10/2010, de 28 de abril, de prevención do branqueo de capitais e do financiamento do terrorismo.
- Lei 12/2003, do 21 de maio de bloqueo do financiamento do terrorismo.
- Regulamentos da Unión Europea relacionados coa aplicación de normativa de prevención de branqueo de capitais.
- Regulamentos da Unión Europea relacionados coa aplicación de sancións financeiras internacionais.
- Estándares de organismos internacionais principalmente representados polas Recomendacións do Grupo de Acción Financeira Internacional (GAFI).

No caso de sociedades ou se é o caso, sucursais suxeitas 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 a nivel consolidado contidas na normativa antes referida en tanto non sexan contraditorias cos requisitos específicos da xurisdición ou normativa sectorial correspondente.

Finalmente, en cada unha das sociedades do Grupo ou, se é o caso, sucursais desenvolveranse os marcos, normas, guías ou procedementos que sexan necesarios para a correcta implantación, execución e cumprimento destes principios.

## 4. Marco de xestión de PBC/FT e Sancións

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

1. Avaliación de riscos
2. Dilixencia debida
3. Detección, control e exame de operacións
4. Comunicación de operativa sospeitosa.
5. Control de listas 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, ao financiamento do terrorismo e ás Sancións está directamente relacionada co tipo de negocio ou actividade, os produtos comercializados, os servizos prestados, as canles de comercialización, a tipoloxía e características dos clientes e/ou as xurisdicións en que operen.

Co propósito de manter un axeitado marco de control e prevención cun enfoque baseado en risco, as sociedades do Grupo deben ser categorizadas segundo o seu nivel de risco de xeito que se garanta a aplicación de 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 non poderán en ningún caso supor a vulneración de dereitos nas xurisdicións onde a sociedade do Grupo leve a cabo as súas actividades.

A política de admisión de clientes é dinámica e establece un marco de cumprimento no Grupo que poderá 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 "Coñece o teu cliente" (tamén coñecido polas súas siglas en inglés KYC, (*Know Your Customer*), con especial foco en garantir que se dispón en todo momento dun bo coñecemento do cliente e as súas actividades.

O principio de *Know Your Customer* e as políticas de dilixencia debida aplicaranse sempre cun enfoque baseado no risco, e asegurarán que as medidas aplicadas son axeitadas 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 elemento que permita o deseño das medidas preventivas e de control que mitiguen a exposición ao risco, de xeito que se apliquen medidas e controis máis estritos a aqueles clientes que presentan un nivel de risco superior.

Os controis e procedementos deben garantir un axeitado e continuo seguimento da relación de negocio co obxectivo de adaptar o nivel de risco e, polo tanto, as medidas que hai que 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 a determinación desta clasificación teranse en conta diversos factores en función da exposición ao risco da sociedade e os seus clientes ou provedores e como mínimo, incluírá a análise dos seguintes factores:

- Características do cliente:
  - Actividade.
  - Zona xeográfica.
  - Persoa de responsabilidade pública (PRP).
  - Identidade do titular real.
  - Estrutura de propiedade ou control.
- Características de produtos ou servizos:
  - Tipo de produto.
  - Segmento de negocio.
  - Canle de relación.
- Características da operativa:
  - Orixe dos fondos.
  - Transaccións.

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

**Persoas cuxa admisión non está permitida:** Non poderán ser admitidas as relacións de negocio coas persoas físicas ou xurídicas que se encontren nalgunha das seguintes situacións:

- Persoas ás que con ocasión do seu proceso de admisión non se lles puidesen aplicar as medidas de dilixencia debida previstas nesta política.
- Persoas incluídas nas listaxes nacionais ou internacionais de Sancións e aquelas que non se deban admitir como clientes de conformidade cos programas de Sancións definidos na presente política e na normativa legal aplicable nesa materia.
- Persoas que teñan negocios cuxa natureza faga imposible a verificación da lexitimidade das operacións ou a procedencia dos fondos.
- Persoas que refusen facilitar a documentación que permita realizar unha plena identificación formal do titular e/ou beneficiario real ou, que, aínda que a facilitaron, se neguen a que a Entidade conserve unha copia dixitalizada desta.
- Persoas que acheguen documentos manifestamente falsos ou que alberguen serias dúbidas sobre a súa legalidade, lexitimidade, non manipulación, ou que non ofrezan garantías suficientes.
- Persoas que refusen facilitar información ou documentación requirida relativa á verificación das actividades declaradas ou a procedencia dos fondos, como acerca do propósito e natureza da relación comercial coa Entidade.
- Persoas e instrumentos xurídicos sobre as que non se poida determinar a estrutura de propiedade ou control ou ben en sociedades en que non se poida determinar o seu titular real.
- Bancos pantalla e aquelas entidades financeiras que operen con este tipo de entidades.
- Persoas ou entidades cuxa actividade consista na emisión ou intermediación de

“criptomoedas” ou “criptoactivos” en xeral.

- Persoas ou entidades que pretendan realizar unha operativa correspondente a actividades financeiras, xogos de azar, apostas, entidades de pagamento, cambio de moeda, entidades de pagamento ou outras actividades sen dispor da correspondente autorización oficial ou outros requisitos legalmente esixibles.
- Calquera outra categoría non prevista nas anteriores e que cumpra rexeitar á vista do previsto por unha norma xurídica ou por política interna da sociedade.
- Persoas físicas ou xurídicas que foron nalgún momento clientes do Grupo e deixaron de selo en aplicación da presente política.

**Persoas de risco superior ao termo medio:** a súa aceptación como clientes está, en todo caso, condicionada á aplicación de medidas de dilixencia reforzada e requirirán a aprobación centralizada. Inclúiranse nesta categoría as seguintes persoas ou entidades:

- Persoas físicas nacionais e estranxeiras con responsabilidade pública.
- Persoas xurídicas nacionais e estranxeiras cuxo titular real sexan persoas con responsabilidade pública (PRP), tanto nacionais coma estranxeiras.
- Persoas físicas ou xurídicas con residencia ou nacionalidade nunha xurisdición de risco, así como aquelas que, sen estaren nesa situación, estean controladas por persoas ou entidades de xurisdicións de risco.
- Clientes de banca privada.
- Relacións de correspondencia.
- Clientes relacionados coa produción, comercialización, distribución e venda de armas e outros elementos de carácter militar.
- Entidades de diñeiro electrónico e entidades de pagamento cando realicen actividade de envío de diñeiro e/ou cambio de moeda estranxeira
- Casinos, sociedades de explotación de xogos recreativos e outras sociedades vinculadas a xogos de azar que dispoñan da correspondente autorización oficial ou outros requisitos legalmente esixibles, así como calquera outro sector de risco cando así o requiran os seus correspondentes procedementos específicos.
- Sociedades con títulos ao portador, unha vez determinada a súa estrutura de propiedade ou de control.
- Calquera persoa física ou xurídica que, polas súas características ou operatoria, a UPBC conclúa que sexa aconsellable someter á súa propia consideración a súa aceptación como cliente ou a súa clasificación por risco.

O **resto de persoas** ou entidades quedarán suxeitas a medidas de dilixencia normais ou simplificadas segundo se estableza na normativa aplicable ou nas normas e procedementos internos.

**Identificación formal de clientes.** As normas e procedementos que desenvolvan os presentes Principios deben garantir nas sociedades do Grupo a axeitada 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 que non puidesen ser identificadas. Igualmente, queda 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 o titular real. Esta obriga implicará que ante a existencia de indicios ou certeza de que os clientes non actúan por conta propia, deberá obterse información precisa co fin de coñecer a identidade das persoas por conta das cales actúan. Así como documentación suficiente que acredite os poderes cos que actúa.

Coñecemento da actividade e patrimonio do cliente. Con anterioridade ao establecemento dunha relación de negocio, as sociedades do Grupo deberán conseguir, polo menos, información sobre a actividade profesional ou empresarial do cliente e a orixe 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 de operacións

As sociedades do Grupo deberán dispor de medios para a detección, control e exame de 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 (por cada sociedade do Grupo e/ou centralizados).
- c. As comunicacións dos organismos supervisores ou das autoridades policiais ou xudiciais.

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

A monitorización será automatizada e revisará a actividade segundo os padróns que a lei e as mellores prácticas identifiquen en cada momento.

### 4.4 Comunicación de operativa sospeitosa

As sociedades do Grupo comunicarán por iniciativa propia aos organismos supervisores e/ou de intelixencia financeira calquera feito ou operación, incluso 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 o financiamento do terrorismo.

En particular, comunicaranse aos organismos supervisores as operacións que mostren unha falta de correspondencia ostensible coa natureza, volume de actividade ou antecedentes operativos dos clientes.

A decisión de comunicar será adoptada centralizadamente en cada xurisdición polas persoas ou órganos designados para ese fin e realizarase a través do representante habilitado ante as autoridades competentes. Na comunicación efectuada, en todo caso, incluírase 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 con carácter inmediato medidas adicionais de xestión e mitigación do risco que deberán ter en consideración o risco de revelación.

Os empregados do Grupo deberán absterse de executar calquera operación sobre a que exista indicio ou certeza de que está relacionada co branqueo de capitais ou o financiamento do terrorismo.

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

#### 4.5 Control de listas de Sancións e comunicación de deteccións

Para o cumprimento das restricións que impoñen os programas de Sancións, as sociedades do Grupo deberán:

- Identificar e seguir os programas de Sancións instaurados polas Nacións Unidas (UN), a Unión Europea (UE), OFAC e os programas locais que sexan de aplicación nas xurisdicións en que operan as sociedades do Grupo.
- Avaliar os riscos asociados ás actividades relacionadas cos programas de Sancións para a determinación dos 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 comunicar tal 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 sociedades 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 mínimo período de conservación o que en cada momento determine a lexislación na materia, e nunca inferior a 10 anos.

A documentación que se debe conservar de acordo coas leis de prevención inclúe como mínimo, os seguintes aspectos:

- En particular conservará para o seu uso en toda investigación ou análise en materia de posibles casos de prevención, por parte dos supervisores ou de calquera outra autoridade competente.
- Copia dos documentos esixibles en aplicación das medidas de dilixencia debida, con inclusión, en particular, das copias dos documentos fidedignos de identificación, as declaracións do cliente, a documentación información achegada polo cliente ou obtida de fontes fiables independentes.
- Orixinal ou copia con forza probatoria dos documentos ou rexistros que acrediten axeitadamente as operacións, os intervenientes nelas e as relacións de negocio.
- Toda aquela documentación en que se formalice o cumprimento das súas obrigas de comunicación e de control interno:
  - Comunicacions aos organismos supervisores.
  - Comunicación do nomeamento de representantes ante as autoridades de Intelixencia Financeira.
  - Expedientes de exame especial.
  - Comunicacions de operativa sospeitosa enviadas aos organismos supervisores e documentación relacionada con estas.
  - Requirimentos de información e solicitudes de rastrexo recibidos dos organismos supervisores.
  - Informes anuais do exame de experto externo e documentos relacionados.
  - Actas das reunións dos órganos de control interno, conservándose tamén as actas e documentos doutros órganos con respecto a aqueles aspectos con impacto en materia de prevención.

## 4.7 Formación

A sensibilización nos riscos asociados a estes delitos é un elemento clave na loita contra o branqueo e o terrorismo.

As sociedades do Grupo CaixaBank deberán definir, manter e aplicar programas de formación dos seus empregados para garantir un axeitado nivel de sensibilización por 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 de administración) de forma periódica e axeitada ao nivel de exposición do risco da súa actividade na sociedade.

Os programas de formación de PBC/FT e Sancións de todas as sociedades do Grupo CaixaBank deberán ser validados pola unidade de Cumprimento Normativo de CaixaBank como unidade especializada no Grupo, unha vez que estes fosen validados polos departamentos responsables de formación e cumprimento da sociedade, gardando rexistro e evidencia da formación impartida, os seus contidos, e dos empregados que a recibiron e superaron.

#### 4.8 Xestión consolidada do risco

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

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

Por iso todas as entidades que forman o Grupo manterán puntualmente informada a CaixaBank sobre relacións de alto risco, datos de actividades sensibles e os seus riscos asociados, atendendo de forma rápida calquera solicitude de información que CaixaBank lle poida formular na xestión do risco regulador e reputacional relacionado co branqueo de capitais, o financiamento do terrorismo e as Sancións.

En todo caso, as devanditas 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 así comunicados entre entidades do Grupo.