



## Principios generales de la política corporativa de cumplimiento normativo

20 de febrero de 2025

## Contenido

<b>1. Introducción</b>	<b>3</b>
1.1 <i>Antecedentes</i> .....	3
1.2 <i>Alcance</i> .....	3
1.3 <i>Objetivo</i> .....	3
<b>2. Ámbito de aplicación</b>	<b>5</b>
<b>3. Marco normativo. Normativa y estándares de aplicación</b>	<b>6</b>
<b>4. Principios generales de la función de Cumplimiento normativo</b>	<b>9</b>
<b>5. Marco de gestión de la función de Cumplimiento normativo</b>	<b>11</b>
5.1 <b>Modelo de organización</b> .....	<b>11</b>
5.1.1 <i>La función de Cumplimiento normativo corporativa</i> .....	11
5.1.2 <i>La función de Cumplimiento normativo de CaixaBank</i> .....	12
5.1.3 <i>La función de Country Compliance</i> .....	13
5.1.4 <i>La función de Cumplimiento normativo en las sociedades del Grupo</i> .....	13
5.2 <b>Modelo de gestión</b> .....	<b>14</b>
5.2.1 <i>Taxonomía de riesgos de cumplimiento</i> .....	14
5.2.2 <i>Delimitación del ámbito de competencia de la función de Cumplimiento normativo en el entorno de control: el modelo de tres líneas de defensa</i> .....	15
5.3 <b>Elementos clave de la función de Cumplimiento normativo</b> .....	<b>15</b>
5.3.1 <i>Programa de cumplimiento</i> .....	15
5.3.1.1 <i>Políticas de cumplimiento normativo</i> .....	16
5.3.1.2 <i>Implementación y seguimiento de cambios normativos y regulatorios</i> .....	16
5.3.1.3 <i>Mapa de riesgos e indicadores</i> .....	16
5.3.1.4 <i>Asesoramiento</i> .....	16
5.3.1.5 <i>Evaluación periódica de los riesgos de cumplimiento</i> .....	16
5.3.1.6 <i>Monitorización y testeo</i> .....	16
5.3.1.7 <i>Formación y sensibilización</i> .....	17
5.3.1.8 <i>Comunicación e Información</i> .....	17
5.3.2 <i>Plan anual de cumplimiento</i> .....	17
5.3.3 <i>Proceso de identificación de deficiencias</i> .....	17

## 1. Introducción

### 1.1 Antecedentes

Son numerosas las disposiciones legislativas de diferente rango que exigen a las organizaciones contar con una función específica que desempeñe la función de cumplimiento normativo (en adelante Cumplimiento normativo, Cumplimiento o *Compliance*, indistintamente), y que se encargue de promover los principios éticos empresariales, reafirmar una cultura corporativa de respeto a la ley y verificar y evaluar regularmente la eficacia de los controles relacionados con el riesgo de incumplimiento de las obligaciones contenidas en ellas.

En este marco de actuación, el Consejo de Administración de CaixaBank, S.A. (en adelante, "CaixaBank" o "la Entidad") aprueba esta Política corporativa de cumplimiento normativo (en adelante, "la Política").

### 1.2 Alcance

En este escenario, resulta esencial disponer de una función de Cumplimiento normativo en la Entidad y garantizar que cuente con un modelo de organización y gestión que cumpla con la normativa de aplicación y con los más altos estándares nacionales e internacionales.

El cumplimiento normativo es responsabilidad de todos y cada uno de los miembros de la organización, es decir, a todos los empleados/as, directivos/as y miembros de los Órganos de Gobierno de CaixaBank.

En particular, corresponde a la **función de Cumplimiento normativo** velar de forma proactiva y autónoma por la correcta implementación de un sistema de gestión de *Compliance* en la Entidad. Para poder abordar esta correcta implementación la función se ejerce de forma autónoma, independiente y la Entidad la ha dotado de la autoridad y recursos humanos y técnicos necesarios, tal y como se establece en el apartado 4 de la presente Política.

Cumplimiento normativo

### 1.3 Objetivo

La presente Política tiene como objetivo definir la función de Cumplimiento normativo, la cual se concreta en identificar, evaluar, supervisar e informar de los riesgos de sanciones o pérdidas financieras a los que se encuentra expuesta la Entidad, como consecuencia del incumplimiento o cumplimiento defectuoso/inadecuado de las leyes, regulaciones, requerimientos judiciales o administrativos, códigos de conducta o estándares éticos y de buenas prácticas, relativos a su ámbito de actuación con referencia al riesgo legal y regulatorio y al riesgo de conducta y cumplimiento, (en adelante, "**los riesgos de cumplimiento**"); así como asesorar, informar y asistir a la alta dirección y a los órganos de gobierno en materia de cumplimiento normativo, promoviendo, a través de acciones de formación, información y sensibilización, una cultura de cumplimiento en toda la organización.

A tal efecto, la función de Cumplimiento normativo se articula a través de los siguientes objetivos:

- **La supervisión de los riesgos de cumplimiento** derivados de los procesos y actividades llevadas a cabo por la Entidad.
- **El fomento, impulso y promoción de los valores corporativos y los principios contenidos en el Código ético** que han de guiar la actuación de la Entidad.

- **La promoción de una cultura de control y cumplimiento de las leyes y de la normativa vigente** (tanto externa como interna) que permita y favorezca su integración en la gestión de toda la organización.

Adicionalmente, las figuras clave de la función con mayor nivel de responsabilidad son:

- *Chief Compliance Officer* de Grupo: máximo responsable de la función de Cumplimiento normativo del Grupo.
- Country Compliance (Country Compliance Manager): máximo responsable de cumplimiento en cada jurisdicción. Ejerce la función de vigilancia, supervisión y coordinación de los riesgos de cumplimiento a nivel agregado cada jurisdicción.
- *Chief Compliance Officer o Director de Compliance*: responsable de la función de Cumplimiento de cada entidad (Caixabank, filiales, sucursales u oficina de representación - para el caso de EEUU-).
- *AML Manager*: máximo responsable de cumplimiento en materia de prevención de blanqueo de capitales.
- *AML Officer*: ejerce aquellas responsabilidades de cumplimiento en materia de prevención de blanqueo expresamente delegadas por el *AML Manager*.

El contenido de esta Política incluye, entre otros aspectos:

- Principios generales de la función de Cumplimiento normativo
- Marco de gobierno
- Marco de gestión de la función de Cumplimiento normativo
- Marco de control
- Marco de información

## 2. *Ámbito de aplicación*

La presente Política tiene carácter corporativo. En consecuencia, los principios de actuación definidos son aplicables a CaixaBank y todas sus sociedades dependientes (conjuntamente, "el Grupo CaixaBank" o "el Grupo") que realicen alguna de las actividades con exposición a los riesgos de cumplimiento. Los órganos de gobierno de estas sociedades adoptarán las decisiones oportunas con el objeto de integrar las disposiciones de esta Política adaptando, siguiendo el principio de proporcionalidad, el marco de gobierno a la idiosincrasia de su estructura de órganos de gobierno, comités y departamentos, y sus principios de actuación, metodologías y procesos a lo descrito en este documento.

Esta integración podrá suponer, entre otras decisiones, la aprobación de una política propia por parte de la filial. La aprobación será necesaria en aquellas sociedades del Grupo que precisen adaptar lo dispuesto en esta Política a sus especificidades propias, ya sea por materia, por jurisdicción o por relevancia del riesgo en la filial. En aquellos casos en los que las actividades de control y gestión del riesgo de la filial se realice directamente desde CaixaBank, ya sea por materialidad del riesgo en la filial, por razones de eficiencia o porque la filial haya externalizado en CaixaBank la gestión operativa de este riesgo, los órganos de gobierno de las sociedades del Grupo afectadas tomarán conocimiento de la existencia de esta Política corporativa y de su aplicación a dichas sociedades del Grupo. La adhesión a esta Política corporativa por parte de los órganos de gobierno de las sociedades del Grupo se realizará cuando, siendo aplicables los principios de actuación de la Política corporativa, la filial no elabore una política propia y el contenido de la Política corporativa establezca principios, obligaciones y actividades que tienen que realizarse directamente por la sociedad del Grupo.

En cualquier caso, la función de Cumplimiento normativo, dado su carácter corporativo, velará por que la integración de esta Política en las sociedades del Grupo sea proporcionada, que en caso de que las sociedades del Grupo aprueben políticas propias estas estén alineadas con la política corporativa, y por la consistencia en todo el Grupo CaixaBank.

Por último, la presente Política, además de ser corporativa, tiene la consideración de política individual de CaixaBank, matriz del Grupo CaixaBank.

A efectos de esta Política, configuran el **perímetro de Cumplimiento normativo** las sociedades del Grupo CaixaBank en las que concurren las siguientes condiciones:

- Gestión efectiva por parte de CaixaBank, es decir, que CaixaBank ostente la participación mayoritaria o el control de la sociedad
- Empresa activa y con vocación de permanencia<sup>1</sup> por parte de CaixaBank,
- Existencia de estructura en la sociedad, es decir, que la sociedad cuente con empleados
- Desarrollo de una actividad relacionada con la actividad de CaixaBank.

A su vez, **dentro de las sociedades del perímetro**, se distinguen:

- **Filiales con Función de Cumplimiento normativo propia:** sociedades que cuentan con función de Cumplimiento normativo propia en virtud de su criticidad dentro del Grupo o por la

<sup>1</sup> El condicionante de vocación de permanencia dejará de tener efecto si transcurridos dos años desde la decisión de su no inclusión en el Perímetro, la sociedad en cuestión continúa formando parte del Grupo

existencia de requerimientos específicos como consecuencia de estar sujetas a una regulación adicional a la regulación bancaria española y europea.

- **Filiales sin función de Cumplimiento normativo:** sociedades que no disponen de una unidad de Cumplimiento normativa propia al no estar sujetas a regulación adicional a la regulación bancaria o en las que el riesgo de cumplimiento es menor debido a la actividad desarrollada.

Las sociedades incluidas en el **Perímetro** deberán supervisar y coordinar la implantación del modelo de gestión y supervisión corporativo en las sociedades que, en su caso, dependan de ellas.

Por otro lado, **a nivel internacional**, se distinguen dentro del Perímetro otros dos tipos de sociedades:

- **Sucursales internacionales:** oficinas de CaixaBank establecidas en países diferentes a España que centran su ámbito de actividad básicamente en la financiación, la prestación de garantías y los servicios bancarios básicos. Como norma general, las sucursales cuentan con función de Cumplimiento normativa propia en base a los requerimientos de la legislación local.
- **Oficinas de representación:** oficinas de CaixaBank establecidas en países diferentes a España que centran su actividad en funciones de enlace y acompañamiento de las empresas españolas con actividad en el extranjero, así como de las empresas extranjeras con actividad en España. Como norma general no disponen de una unidad de Cumplimiento normativa propia puesto que su riesgo de cumplimiento es menor debido a la actividad desarrollada. Sin perjuicio de lo anterior, se designará un Compliance Officer propio en aquellas jurisdicciones que el regulador así lo establezca.

Por otro lado, la definición de las sociedades del Grupo incluidas en las distintas taxonomías de Compliance (PBCFT, Penal, etc.) se realiza por parte de los equipos especialistas de cada uno de estos riesgos.

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

La presente Política se regirá por lo previsto en la normativa aplicable vigente, así como por aquella que la modifique o sustituya en el futuro. En concreto, a fecha de su elaboración, la normativa vigente aplicable a la función de Cumplimiento normativo es la siguiente:

- EEUU - US *Foreign Corrupt Practices Act* (FCPA), 1977
- Ley 35/2003, de 4 de noviembre, de instituciones de inversión colectiva.
- Circular 6/2009, de 9 de diciembre, de la Comisión Nacional del Mercado de Valores, sobre control interno de las sociedades gestoras de instituciones de inversión colectiva y sociedades de inversión.
- Ley Orgánica 5/2010, de 22 de junio, por la que se modifica la Ley 10/1995, de 23 de noviembre del Código penal y posteriores modificaciones (2010)
- UK Bribery Act (2010)
- Real Decreto 1082/2012, de 13 de julio, por el que se aprueba el Reglamento de desarrollo de la Ley 35/2003, de 4 de noviembre, de instituciones de inversión colectiva.
- Directiva (CRD IV) 2013-36-UE relativa al acceso a la actividad de las entidades de crédito y a la supervisión prudencial de las entidades de crédito y las empresas de inversión, por la que se modifica la Directiva 2002/87/CE y se derogan las Directivas 2006/48/CE y 2006/49/CE.
- Acuerdo entre el Reino de España y los Estados Unidos de América para la mejora del cumplimiento fiscal internacional y la implementación de la Foreign Account Tax Compliance Act - FATCA, hecho en Madrid el 14 de mayo de 2013
- Circular 1/2014 de 26 de febrero de la CNMV sobre los requisitos de organización interna y de las funciones de control de las entidades que prestan servicios de inversión.

- Directiva MIFID II 2014/65/EU de 15 de mayo de 2014 relativa a los mercados de instrumentos financieros y por la que se modifican la Directiva 2002/92/CE y la Directiva 2011/61/UE.
- Ley 10/2014, de 26 de junio, de ordenación, supervisión y solvencia de las entidades de crédito. (LOSS)
- Real Decreto 85/2015, de 13 de febrero, por el que se desarrolla la Ley 10/2014, de 26 de junio, de ordenación, supervisión y solvencia de entidades de crédito.
- Reglamento Delegado (UE) 2017/565 de la Comisión, de 25 de abril de 2016, por el que se completa la Directiva 2014/65/UE del Parlamento Europeo y del Consejo en lo relativo a los requisitos organizativos y las condiciones de funcionamiento de las empresas de servicios de inversión y términos definidos a efectos de dicha Directiva.
- Directiva relativa a la protección de las personas que informen sobre infracciones del Derecho de la Unión (2019).
- Ley 2/2023, de 20 de febrero, reguladora de la protección de las personas que informen sobre infracciones normativas y lucha contra la corrupción
- Reglamento (UE) 2024/1624 del Parlamento Europeo y del Consejo, de 31 de mayo de 2024, relativo a la prevención de la utilización del sistema financiero para el blanqueo de capitales o la financiación del terrorismo
- Directiva (UE) 2024/1640 del Parlamento Europeo y del Consejo, de 31 de mayo de 2024, relativa a los mecanismos que deben establecer los Estados miembros a efectos de la prevención de la utilización del sistema financiero para el blanqueo de capitales o la financiación del terrorismo, por la que se modifica la Directiva (UE) 2019/1937 y se modifica y deroga la Directiva (UE) 2015/849
- Directiva (UE) 2024/1654 del Parlamento Europeo y del Consejo, de 31 de mayo de 2024, por la que se modifica la Directiva (UE) 2019/1153 en lo que respecta al acceso de las autoridades competentes a los registros centralizados de cuentas bancarias a través del sistema de interconexión y a las medidas técnicas destinadas a facilitar el uso de los registros de operaciones

Resultan de aplicación igualmente las distintas directrices y criterios de supervisores, reguladores y autoridades, tales como:

- Directrices EBA sobre políticas de remuneración adecuadas en virtud de los artículos 74, apartado 3, y 75, apartado 2, de la Directiva 2013/36/UE y la divulgación de información en virtud del artículo 450 del Reglamento (UE) n.º 575/2013 (EBA/GL/2015/22).
- Circular 1/2016 de la Fiscalía General del Estado sobre la responsabilidad penal de la persona jurídica conforme a la reforma del Código penal efectuada por LO 1/2015 (2016)
- Guía de la EBA de 21 marzo 2018 sobre Gobierno interno EBA/GL/2017/11 (2017) adoptadas por el Banco de España como propias el 18 de mayo de 2018 y actualizadas con fecha 2 de julio de 2021 (EBA/GL/2021/05) con entrada en vigor a partir del 31 de diciembre de 2021
- Directrices sobre políticas y procedimientos en relación con la gestión del cumplimiento y sobre el papel y las responsabilidades del responsable del cumplimiento de la PBC/FT con arreglo al artículo 8 y al capítulo VI de la Directiva (UE) 2015/849 (2022)
- Qualified Intermediary Agreement-Revenue Procedure 2022-43.
- Reglamento (UE) 2024/1620 del Parlamento Europeo y del Consejo, de 31 de mayo de 2024, por el que se crea la Autoridad de Lucha contra el Blanqueo de Capitales y la Financiación del Terrorismo y se modifican los Reglamentos (UE) n.º 1093/2021, (UE) n.º 1094/2010 y (UE) n.º 1095/2010

Finalmente, esta Política tiene en cuenta otros estándares nacionales e internacionales en la materia, como son:

- “Enterprise Risk Management - Integrated Framework” (COSO I, 1992)
- Convención contra el soborno/corrupción de la OCDE (1997) Convenio para combatir la corrupción de agentes públicos extranjeros en las transacciones económicas internacionales
- Principios de gobierno corporativo de la OCDE (1999)
- Convención de la ONU contra la corrupción (2003)
- Principios empresariales para contrarrestar el soborno. Transparencia internacional (2003).
- “Compliance and the Compliance function in Banks” (Comité de Supervisión Bancaria Basilea, 2005)
- “Enterprise Risk Management - Integrated Framework” (COSO II, 2004)
- Guidance to the US FCPA (2012) Guía de Recursos y compilación de información
- Principios de gobierno corporativo para Bancos (Comité de Supervisión Bancaria Basilea 2015)
- Principios de gobierno corporativo de la OCDE y del G20 (2016)
- Norma ISO 37001 de Sistemas de gestión antisoborno (2016)
- Informe final de EBA “ON THE APPLICATION OF THE GUIDELINES ON THE REMUNERATION OF SALES STAFF” Con el propósito de que las entidades sigan evolucionando en la protección de los clientes, EBA identifica 17 buenas prácticas detectadas a cumplir por las entidades en su aplicación práctica de las Directrices EBA 2016.
- Norma UNE 19601 sobre Sistemas de gestión de compliance penal (2017)
- Guía sobre el “COSO Enterprise Risk Management – Integrating with Strategy and Performance” (COSO III ERM, 2017)
- Guía de la CNMC sobre programas de *compliance* en relación con la defensa de la competencia (2020)
- Norma ISO 37301 de sistemas de gestión del compliance (2021)
- Directrices finales sobre la función de cumplimiento (compliance) de MiFID II - ESMA35-36-1952 (2021)
- Informe final emitido por ESMA en 2022 sobre “Las Directrices sobre políticas y prácticas de remuneración” El informe final emitido por ESMA en 2022 sobre “Las Directrices sobre políticas y prácticas de remuneración” que recoge las respuestas a la consulta pública planteada el año pasado y actualiza las directrices con objeto de mejorar la protección del cliente frente a conductas del personal de las entidades generadoras de posibles conflictos de interés o supuestos de malas praxis en la comercialización de productos y servicios
- Directrices ESMA35-43-3565 relativas a determinados aspectos de los requisitos de remuneración de la MiFID II

En el caso de sociedades del Grupo, o en su caso, sucursales sujetas a jurisdicciones extranjeras o normativa sectorial complementaria, las políticas y procedimientos que estas sociedades del Grupo o sucursales desarrollen tendrán en cuenta, además de su normativa propia, las obligaciones a nivel consolidado contenidas en la normativa antes referenciada en tanto no sean contradictorias con los requisitos específicos de la jurisdicción o normativa sectorial correspondiente.

Finalmente, en cada una de las sociedades del Grupo o, en su caso, en las sucursales se desarrollarán las normas, guías o procedimientos que sean necesarios para la correcta implementación, ejecución y cumplimiento de esta Política.

## 4. Principios generales de la función de Cumplimiento normativo

Los principios que regirán la actuación del Grupo CaixaBank para el control y la gestión de los riesgos de cumplimiento son:

### a) Autonomía

La función de Cumplimiento normativo es una función autónoma, lo que significa que debe tener la iniciativa suficiente para realizar sus funciones sin necesidad de recibir instrucciones concretas de otras áreas o actuar a instancias de ellas.

La función debe disponer de autonomía para tomar decisiones sin necesidad de que otra área o función de la organización aprueben o refrenden sus opiniones.

### b) Independencia

Para poder garantizar la objetividad de sus decisiones, la función de Cumplimiento normativo operará bajo el principio de independencia funcional con respecto de aquellas áreas o funciones sobre las que realiza la supervisión y monitorización de los riesgos de cumplimiento.

Asimismo, con el fin de garantizar su independencia, la función de Cumplimiento normativo no estará sujeta al cumplimiento de los objetivos comerciales, quedando únicamente sujeta a los de la actividad que le es propia y a los retos corporativos globales de la Entidad.

De igual forma, el nombramiento, cese, fijación de su remuneración (tanto fija como variable y la proporción entre ambas respetando siempre un principio de razonabilidad) y la evaluación del grado de consecución de sus objetivos o retos corresponderá, previo cumplimiento de los requerimientos legales aplicables, a los Órganos de Gobierno correspondientes.

Las personas que desempeñan la función de Cumplimiento normativo no podrán participar en la prestación de servicios y actividades que controlan con el fin de evitar una influencia indebida en el ejercicio de sus funciones.

La función de Cumplimiento normativo tendrá en todo caso acceso directo a los Órganos de Dirección y Gobierno en el desarrollo de sus funciones y responsabilidades.

### c) Autoridad

La función de Cumplimiento normativo se ubicará en todo momento dentro de los niveles jerárquicos más altos de la Organización de la entidad (Alta Dirección y otros puestos clave, tal y como se define en la Política corporativa de gobierno y control interno) y tendrá la autoridad suficiente para que sus líneas de actuación y decisiones sean asumidas por otras áreas de la entidad.

Podrá, en cualquier momento, plantear consultas, solicitar información, iniciar o requerir procesos de evaluación o verificación e investigaciones relativas a áreas o procesos que presenten riesgos reales o potenciales de incumplimiento que puedan poner en riesgo a la Entidad.

### d) Medios humanos y recursos técnicos

Debido a la importancia de la misión de la función de Cumplimiento normativo y de sus responsabilidades dentro de la organización, las áreas que desempeñan esta función deben contar con los recursos suficientes para acometer las actividades y responsabilidades asignadas en la presente política.

Así, deben asignarse los recursos materiales, informáticos y técnicos suficientes para que Cumplimiento normativo pueda ejercer de forma eficaz su función teniendo en cuenta la naturaleza, volumen y complejidad de las operaciones y la naturaleza de los riesgos asumidos por la Entidad.

A tal efecto, deberá contar con un presupuesto que le permita el desarrollo de sus actividades, acorde con el nivel de riesgo de incumplimiento al que está expuesta la Entidad.

e) **Aptitud y honorabilidad**

Todas las personas que ejerzan la función de Cumplimiento normativo deberán contar con los conocimientos, experiencia, cualificación y requisitos de honorabilidad profesional necesarios para ejercer con garantías sus cometidos en la Entidad y así garantizar una amplia cobertura de la función de Cumplimiento normativo con carácter permanente.

A tal fin, deberán establecerse programas de formación y certificación para el acceso y desempeño de la función, así como de planes que permitan su desarrollo profesional.

f) **Acceso a la información**

Cumplimiento normativo tendrá acceso a cuanta información y documentación sea necesaria para desarrollar adecuadamente su función; asimismo, deberá contar con la colaboración necesaria a todos los niveles para atender los requerimientos de información de los organismos supervisores dentro de los plazos establecidos.

g) **Enfoque basado en riesgo**

En el ejercicio de su actividad, todas las áreas involucradas en el cumplimiento de las normas, y en particular la función de Cumplimiento normativo, deben tener presente en todo momento un enfoque basado en riesgo, y por tanto, realizar una valoración continua de los riesgos de cumplimiento asociado a los principales procesos, para priorizar las actividades de supervisión y monitorización que le son propias, así como para llevar a cabo una adecuada asignación de los recursos en función de los riesgos identificados.

h) **Permanencia**

Con el objetivo de ejecutar la misión y las tareas que le son encomendadas por la normativa vigente, la función de Cumplimiento normativo debe existir y formar parte en todo momento de la estructura organizativa de la Entidad, independientemente de las personas concretas que formen parte de ella.

## 5. Marco de gestión de la función de Cumplimiento normativo

### 5.1 Modelo de organización

#### 5.1.1. La función de Cumplimiento normativo corporativa

La función de Cumplimiento normativo corporativa dependerá funcionalmente de la Presidencia de la Comisión de Riesgos de CaixaBank y jerárquicamente de la Dirección de Cumplimiento y Control y Public Affairs. Esta dependencia funcional supone que la Comisión de Riesgos de CaixaBank participe en el nombramiento y cese de su titular, el *Chief Compliance Officer* corporativo o de Grupo, así como en la fijación de objetivos, la evaluación de su desempeño y la remuneración fija y variable de este<sup>2</sup>.

El *Chief Compliance Officer* de Grupo es el máximo responsable de la función de Cumplimiento normativo corporativa y recae en la figura del *Chief Compliance Officer* o Director de Compliance de CaixaBank. El *Chief Compliance Officer* corporativo desarrolla sus funciones bajo los principios generales descritos en el apartado 4 de la presente Política, y en particular, de forma independiente y autónoma respecto del resto de órganos de la Entidad, por lo que no puede recibir instrucciones de ningún tipo en su ejercicio y dispone de todos los medios personales y materiales necesarios para llevarlas a cabo.

#### a) *Nombramiento*

Es responsabilidad del Consejo de Administración de la Entidad el nombramiento del *Chief Compliance Officer* corporativo. La designación debe realizarse:

- Cumpliendo lo establecido en la guía para la evaluación de la idoneidad del Banco Central Europeo.
- Teniendo en cuenta sus conocimientos, aptitudes y experiencia considerando que son adecuados para el desempeño de su cargo.

El nombramiento y cese del *Chief Compliance Officer corporativo se comunicará a las autoridades pertinentes*.

#### b) *Funciones*

El *Chief Compliance Officer* corporativo establecerá un marco de coordinación de las relaciones con las respectivas unidades de Cumplimiento normativo de las sociedades del Perímetro que permita la coordinación periódica entre la función de Cumplimiento normativo y estas, así como los flujos de Reporting. En este sentido, el marco determinará los mecanismos de coordinación oportunos en base a las competencias de la función corporativa que se describen a continuación:

- Establecimiento de las directrices generales para garantizar la adecuada gestión de los riesgos de cumplimiento y la implantación de la cultura de cumplimiento en el Grupo en coordinación con las áreas responsables de las sociedades del Grupo, así como el establecimiento de aquellas otras cuestiones que en relación con el Grupo se le pudieran

<sup>2</sup> En relación al nombramiento y cese la Comisión de riesgos asesora a la Comisión de Nombramientos y Sostenibilidad y por lo que hace referencia a su retribución asesora a la Comisión de Remuneraciones

- encomendar en la normativa sectorial que resulte de aplicación (por ejemplo, en el ámbito de prevención del blanqueo de capitales y de la financiación del terrorismo).
- Supervisión de la definición del Plan de Cumplimiento de las sociedades del Perímetro de forma previa a su aprobación por parte de sus correspondientes Órganos de Gobierno, pudiendo solicitar la inclusión de nuevas actividades con el objetivo de que el Plan de cobertura a la supervisión de todos los riesgos de cumplimiento.
  - Propuesta en determinados ámbitos de la creación de órganos colegiados con alcance de Grupo (por ejemplo, el órgano de control interno de grupo en el ámbito de la prevención del blanqueo de capitales y de la financiación del terrorismo).
  - Participación en los procesos de nombramiento, cese, fijación y validación de retos, evaluación del desempeño y determinación de la remuneración fija y variable de los *Chief Compliance Officers* de las sociedades del Grupo.
  - Vela por que el personal involucrado en la gestión del Cumplimiento normativo en las sociedades del Grupo cuente con la competencia y experiencia adecuadas, y que la estructura de la función es adecuada para la gestión de los riesgos de cumplimiento que es proporcionada a la naturaleza, escala y complejidad de las actividades que desarrollan cada una de las sociedades del Grupo.

### 5.1.2 La función de Cumplimiento normativo de CaixaBank

El máximo responsable de la función de Cumplimiento normativo de CaixaBank es el *Chief Compliance Officer* de CaixaBank o Director de Compliance de CaixaBank que también ejerce la función de *Chief Compliance Officer* de Grupo.

Este cargo es compatible con el nombramiento de otras responsabilidades, así el *Chief Compliance Officer* de CaixaBank ha sido nombrado por el Consejo de Administración Responsable del Sistema Interno de información de Grupo, Responsable Officer FATCA, AML Officer ejerciendo las funciones propias y las delegadas del AML Manager, entre otros. Las funciones derivadas de cada uno de estos nombramientos se describen en las políticas que gestionan cada uno de estos riesgos.

#### a) *Nombramiento y retribución*

Los mismos criterios establecidos en el apartado 5.1.1. respecto al nombramiento del *Chief Compliance Officer* de Grupo son aplicables al *Chief Compliance Officer* de CaixaBank.

La remuneración del *Chief Compliance Officer* de CaixaBank y del personal de la función de Cumplimiento normativo no podrá estar ligada al beneficio de las áreas sobre las que ejerce su responsabilidad de vigilancia. Sin perjuicio de lo anterior, parte de la remuneración podrá estar compuesta por una retribución variable sujeta a la consecución de los objetivos globales de la Entidad, siendo estos siempre compatibles con una gestión adecuada y eficaz de los riesgos.

#### b) *Funciones*

El *Chief Compliance Officer* de CaixaBank es el responsable del correcto desarrollo del modelo de gestión de la Función de Cumplimiento normativo de CaixaBank y de ejecutar las acciones necesarias para desarrollar el presupuesto para que la Función cumpla con las tareas que tiene encomendadas. Sus principales responsabilidades son las siguientes:

- La aprobación y actualización del documento “Inventario marco normativo de Cumplimiento normativo”, que recoge la relación de los procedimientos, políticas y normativa interna de los riesgos de cumplimiento.
- Definir, implementar y mantener un programa de cumplimiento que garantice una correcta y eficaz implantación de la Política corporativa de cumplimiento normativo.
- Identificar, monitorizar y evaluar de forma continuada los riesgos de cumplimiento.
- Asegurar que los Órganos de Gobierno y la Alta Dirección de la Entidad son informados de los aspectos más relevantes de Cumplimiento normativo y de los planes de acción para resolver las debilidades detectadas/surgidas.
- Asistir y asesorar a la Alta Dirección y al resto de personal de CaixaBank y las sociedades del Grupo para la adecuada gestión de los riesgos de cumplimiento.
- Promover, coordinar, monitorizar y, en su caso, ejecutar los planes de formación a los empleados de la Entidad en el ámbito de Cumplimiento normativo.
- Mantener contacto permanente con los principales reguladores y supervisores con el objetivo de conocer sus expectativas y contribuir al mantenimiento de una comunicación fluida que incluya (el desarrollo de una relación basada en la cooperación mutua), manteniéndose informados de las principales iniciativas y proyectos regulatorios de CaixaBank.
- Liderar, juntamente con las áreas responsables de la Responsabilidad Social Corporativa, el proceso de difusión de los valores y principios incluidos en el Código ético de CaixaBank.
- Planificar, con un enfoque basado en riesgo, las actividades clave a realizar por la Función de Cumplimiento normativo durante el año, así como realizar el seguimiento de estas. Dicha planificación se refleja en el Plan anual de cumplimiento y se presenta para su aprobación al Consejo de Administración.
- Promover una cultura de cumplimiento de las normas dentro de la Organización, impulsando el establecimiento y el mantenimiento de un marco de gobierno adecuado que facilite el cumplimiento, a lo largo de toda la organización, de las regulaciones, políticas, procedimientos y estándares de conducta.

### 5.1.3. La función de Country Compliance

En aras a asegurar una adecuada gestión de los riesgos de cumplimiento en aquellas jurisdicciones donde operen más de un negocio del Grupo o más de una entidad supervisada, el *Chief Compliance Officer* corporativo nombrará como responsable de la función de Country Compliance (*Country Compliance Manager*) al *Chief Compliance Officer* de la sociedad del Grupo Cumplimiento normativo del principal negocio o entidad de la jurisdicción. El *Country Compliance Manager* ejercerá una función de vigilancia, supervisión y coordinación de los riesgos de cumplimiento a nivel agregado en dicha jurisdicción.

Dicha función no conllevará dependencias jerárquicas o funcionales adicionales a las definidas en esta Política.

### 5.1.4. La función de Cumplimiento normativo en las sociedades del Grupo

Las personas que desarrollan sus actividades en la función de Cumplimiento normativo en las sociedades del Grupo actuarán siguiendo el modelo organizativo y de gobierno de codependencia que se describe a continuación:

- **Filiales, sucursales y oficinas de representación que cuentan con Función de Cumplimiento normativo propia:** El responsable de la función o *Compliance Officer* de cada una de estas entidades tendrá una doble dependencia: jerárquica, por un lado, del Consejero Delegado,

Director General o equivalente, o bien del Órgano de Gobierno directamente; y, por otro, funcional, del *Chief Compliance Officer* corporativo. En todo caso, las decisiones que afecten al nombramiento, cese, fijación de su remuneración (tanto fija como variable y la proporción entre ambas respetando siempre un principio de razonabilidad) y evaluación del cumplimiento de sus objetivos o retos corresponderá, previo cumplimiento de los requerimientos legales aplicables, al superior jerárquico que corresponda, juntamente con el *Chief Compliance Officer*. El Órgano de Gobierno, será informado de cualquier decisión que afecte a estas actuaciones.

Las funciones atribuidas a los *Compliance Officer* de las sociedades del Grupo, así como su retribución y nombramiento se determinarán en base a lo dispuesto en esta Política en el apartado 5.1.2 para el *Chief Compliance Officer* de CaixaBank, así como, en su caso, las funciones resultantes del nombramiento de otros cargos como AML Manager.

### Cumplimiento normativo

- **Filiales y oficinas de representación que no cuentan con personal dedicado a la función de Cumplimiento normativo:** La función se desempeñará desde la función de Cumplimiento de CaixaBank. La sociedad filial, sucursal, u oficina de representación designará una persona de la alta Dirección que haga de interlocutor entre CaixaBank y esta.

## 5.2 Modelo de gestión

El modelo de gestión de la función de Cumplimiento normativo se construye sobre dos pilares fundamentales:

- a) Taxonomía de los riesgos de cumplimiento
- b) Delimitación del ámbito de competencia de la función de Cumplimiento normativo en el entorno de control: el modelo de tres líneas de defensa

### 5.2.1 Taxonomía de riesgos de cumplimiento

La taxonomía de los riesgos de cumplimiento es una clasificación por categorías del riesgo de conducta y cumplimiento y del riesgo legal y regulatorio al que está expuesto el Grupo partiendo del catálogo corporativo de riesgos del Grupo CaixaBank.

La división de los riesgos de cumplimiento en diferentes categorías permite delimitar con mayor facilidad el ámbito de actuación de la función de Cumplimiento normativo y supone el punto de partida de la realización de un ejercicio de evaluación continuada de estos riesgos.

Asimismo, sirve de base para la identificación y priorización de las actividades en las que debe enfocarse la función de Cumplimiento normativo durante el año (Plan anual de cumplimiento), la actualización de la lista de debilidades y deficiencias de cumplimiento y la ejecución de las iniciativas y proyectos de la Dirección de Cumplimiento normativo.

De acuerdo con la Política corporativa de gobierno y control interno de CaixaBank, la función de Cumplimiento normativo es responsable de la supervisión de los siguientes riesgos, de entre los recogidos en el Catálogo corporativo de riesgos:

- Conducta y cumplimiento.
- Legal y Regulatorio.

Los riesgos para supervisar podrían variar por exigencia legal o criterio supervisor expreso, tal y como se prevé en el apartado 2 de la presente Política. Las subcategorías que conforman dicha taxonomía de riesgos de cumplimiento están sujetas a revisión anual por el Comité Global del Riesgo.

### 5.2.2. Delimitación del ámbito de competencia de la función de Cumplimiento normativo en el entorno de control: el modelo de tres líneas de defensa

Como parte del marco de control interno del Grupo y en línea con las directrices recogidas en la Política corporativa de gobierno interno y de control interno, la función de Cumplimiento normativo supervisa y gestiona el riesgo de conducta y cumplimiento y el riesgo legal y regulatorio ya identificados en la taxonomía de riesgos corporativos, siguiendo la estructura de tres líneas de defensa, en las que quedan delimitadas las funciones y responsabilidades de cada una de ellas.

La función de Cumplimiento normativo como función de control interno que constituye la segunda línea de defensa y de acuerdo con la Política corporativa de gobierno y control interno, realiza la identificación, medición, definición y seguimiento del apetito al riesgo de conducta y cumplimiento y del riesgo legal y regulatorio, siendo responsable de la revisión independiente de la aplicación de políticas y procedimientos por parte de la primera línea de defensa. La función de cumplimiento actúa de forma independiente de las unidades de negocio, asegurando la existencia de políticas de gestión y control de los riesgos de cumplimiento, monitorizando su aplicación, evaluando el entorno de control y reportando todos los riesgos materiales.

## 5.3 Elementos clave de la función de Cumplimiento normativo

La función de Cumplimiento normativo se sirve de los siguientes elementos clave para asegurar una adecuada cobertura de los riesgos de cumplimiento:

- Programa de cumplimiento
- Plan anual de cumplimiento
- Proceso de identificación de debilidades

### 5.3.1 Programa de cumplimiento

El programa de cumplimiento es el conjunto de procesos y actividades que, siguiendo una metodología generalmente aceptada a nivel internacional, racionalizan y sistematizan las principales actividades de la función de cumplimiento.

La aplicación del programa de cumplimiento está basada en la ejecución de una serie de actividades clave, como son:

### 5.3.1.1 Políticas de cumplimiento normativo

Un elemento fundamental del programa de cumplimiento de CaixaBank es la creación y mantenimiento de Políticas en el ámbito de Cumplimiento normativo que establezcan con claridad los requerimientos y criterios de actuación que debe seguir la Entidad en lo que se refiere a los riesgos de cumplimiento.

### 5.3.1.2. Implementación y seguimiento de cambios normativos y regulatorios

Consiste bien en la implementación de normativas que impactan en el ámbito de los riesgos de cumplimiento, o bien en su seguimiento cuando dicha implementación corresponda a otras áreas afectadas.

### 5.3.1.3 Mapa de riesgos e indicadores

Supone la creación y mantenimiento de un inventario de regulaciones clave que afectan a la actividad de CaixaBank, vinculadas a la taxonomía de los riesgos de cumplimiento, así como la identificación, implantación y seguimiento de indicadores que permitan monitorizar, detectar y mitigar dichos riesgos.

### 5.3.1.4 Asesoramiento

Tal y como se ha descrito anteriormente, la función de cumplimiento tiene encomendada la labor fundamental de asesorar al Órgano de Gobierno, a la Alta Dirección y al resto de la organización en todos los aspectos relevantes relacionados con la misión de Cumplimiento normativo. En el desempeño de dicha función, la función de cumplimiento deberá contar, en su caso, con el apoyo de otras áreas especializadas en la Entidad en función de la materia.

### 5.3.1.5 Evaluación periódica de los riesgos de cumplimiento

Uno de los elementos clave dentro del Programa de cumplimiento de la entidad es la realización periódica de una evaluación de los riesgos de cumplimiento, que sirva de herramienta para priorizar las actividades a desarrollar por la función de cumplimiento, así como para fijar la criticidad de las mismas y la asignación de recursos.

En la evaluación de los riesgos de cumplimiento se deberán tener en cuenta el riesgo inherente a la actividad, junto con el resultado de la supervisión del entorno de control, así como las conclusiones relevantes de las auditorías internas o externas y las de los organismos supervisores, y la actividad del Servicio de Atención al Cliente o las consultas o comunicaciones que se presenten en los canales habilitados al efecto y cuya gestión tiene atribuida la función de cumplimiento.

### 5.3.1.6 Monitorización y testeo

La función de Cumplimiento normativo se vale de las técnicas de monitorización y testeo para valorar el entorno de control relacionado con los riesgos de cumplimiento con un enfoque basado en el riesgo.

La monitorización implica el seguimiento y revisión recurrente de actividades basadas en indicadores de riesgo (KRIs) o de decisiones internas para la detección temprana de desviaciones o actuaciones incorrectas que se derivan del incumplimiento de las normas.

El testeo consiste en la validación del cumplimiento de la normativa relacionada con los riesgos de cumplimiento en los procesos ordinarios de la entidad mediante técnicas de verificación independiente como muestreos, revisiones de procesos, o cualquier otro tipo de pruebas.

### 5.3.1.7 Formación y sensibilización

Con el fin de cumplir con la misión que le tiene encomendada, la función de Cumplimiento normativo desarrolla de forma continua programas de formación, comunicación y sensibilización a toda la plantilla para promover una cultura de cumplimiento y el conocimiento de las obligaciones y responsabilidades de Cumplimiento. Dichas acciones de formación se recogerán en el Plan anual de formación realizado en estrecha colaboración con Recursos Humanos.

### 5.3.1.8 Comunicación e Información

La función de Cumplimiento normativo debe favorecer un marco de gobierno adecuado para elevar y reportar, de manera temprana y eficaz, a los Órganos de Gobierno de la entidad cualquier debilidad de control significativa relacionada con los riesgos de cumplimiento.

Reportará de forma periódica a Órganos de Gobierno.

### 5.3.2 Plan anual de cumplimiento

El Plan anual de cumplimiento, aprobado por el Consejo de Administración, contiene la relación de las actividades de la función de Cumplimiento normativo durante el período al que se refiere (año natural), junto con una planificación para su ejecución, y todo ello, con el fin de garantizar que de forma periódica las actividades con exposición a riesgo son objeto de revisión, valoración y comunicación.

Para su definición y priorización se aplican los principios de proporcionalidad y de enfoque basado en riesgo, de forma que, en función de los resultados de la evaluación de riesgos, los riesgos identificados con anterioridad y la previsión de las actuaciones supervisoras, se construyen y planifican las actividades claves que se desarrollarán a lo largo del año.

Periódicamente, se realizará un seguimiento del Plan anual de cumplimiento con el objetivo de informar a los Órganos de Dirección y de Gobierno de las principales conclusiones del Plan, del grado de ejecución respecto a la planificación inicial y de las variaciones más relevantes que hayan podido surgir.

### 5.3.3 Proceso de identificación de deficiencias

El proceso de identificación de deficiencias es el elemento clave del que dispone la función de Cumplimiento normativo para cumplir con el mandato de segunda línea de defensa de los riesgos de cumplimiento y para informar a la Alta Dirección.

Las deficiencias de Cumplimiento son cualquier debilidad identificada en el entorno de control asociado a los riesgos de cumplimiento, que derive en:

- Incumplimiento de la legislación o normativa vigente en relación con los riesgos gestionados por la función de cumplimiento
- Prácticas de negocio inadecuadas o contrarias al *Código Ético y normativa de desarrollo* por parte de la Entidad o sus empleados

Las deficiencias detectadas pueden surgir de la aplicación de cualquiera de las actividades clave que integran el Programa de cumplimiento, y que normalmente tienen su reflejo en el Plan anual de cumplimiento, así como de aquellas actuaciones (comprobaciones/inspecciones) realizadas por los supervisores y los auditores internos y externos en las que identifiquen deficiencias en el entorno de control.