Área de Riesgos y Cumplimiento

Marco General de Control

Abril 2023

cecabank

Índice

1. Introducción

El Consejo de Administración de Cecabank es el máximo responsable de los sistemas de control interno de la Entidad, asegurando que la estructura organizativa y operativa es adecuada y transparente y que fomenta y acredita la gestión prudente y eficaz de la Entidad. Igualmente, vela por que las funciones de control interno sean independientes de las líneas de negocio que controlan, con una segregación de funciones adecuada.

Cecabank ha implantado sistemas, procedimientos y mecanismos que garantizan la existencia de un marco de control y de gobierno interno completo, que abarca toda la organización y que incluye funciones de control de riesgos, de cumplimiento y de auditoría independientes, con la autoridad, el rango y los recursos suficientes para desempeñar su cometido correctamente.

El presente Marco General de Control tiene como finalidad describir y documentar el sistema de control interno, los canales de comunicación y la asignación de responsabilidades de forma clara y coherente.

2. Características del sistema de control interno

La estructura organizativa y los mecanismos de control interno desarrollados por la Alta Dirección están alineados con la naturaleza de la estrategia y del modelo de negocio de Cecabank, con líneas de responsabilidad bien definidas, transparentes y coherentes, y van dirigidos a garantizar:

- Una operativa eficaz y eficiente;
- Una gestión prudente del negocio;
- Una identificación, medición y mitigación adecuada de los riesgos;
- Una información financiera y no financiera publicada interna y externa fiable;
- Unos procedimientos administrativos y contables sólidos; y
- El cumplimiento de las leyes, normativas, requisitos en materia de supervisión y políticas, procesos, normas y decisiones internos de la Entidad.

Se caracteriza principalmente:

- Por estar basada en el modelo de tres líneas de defensa:
  - **Primera línea de defensa:** Compuesta por Unidades de Negocio y de Soporte que tienen la responsabilidad primaria de la gestión y control de los riesgos que afectan a la Entidad en el ejercicio continuo de su actividad. Los controles son establecidos y realizados en los propios departamentos.
  - **Segunda línea de defensa:** Conformada por el Área de Riesgos y Cumplimiento. Es la encargada de supervisar la actividad de la primera línea, asegurar la existencia de políticas y procedimientos de gestión y control de riesgos, y su adecuación con el nivel de apetito al riesgo definido por el Consejo.
  - **Tercera línea de defensa:** Formada por la función de Auditoría Interna. Esta función verifica de forma independiente y asegura de forma objetiva que todas las actividades y unidades de la Entidad, incluidas las actividades externalizadas, cumplen con las políticas y procedimientos internos y con la normativa y obligaciones legales y contractuales que debe cumplir la Entidad.
- Por garantizar la independencia de las unidades que realizan funciones de control con respecto a las áreas, unidades o funciones sobre las que gira su verificación.

- Por desarrollar una gestión integral y especializada. Existen unidades específicas de gestión y control de los distintos riesgos ubicadas en la primera y en la segunda línea de defensa.
- Por asegurar la adecuada coordinación en el control de los distintos riesgos y su visión integral, dando así cumplimiento a la estrategia de riesgos definida por el Consejo de Administración A este fin, se ha desarrollado una estructura de comités especializados.

3. Organigrama del control interno

La estructura organizativa del control interno está integrada por unidades especializadas con responsabilidades directas sobre su gestión y control, así como por una estructura de comités que favorece el sistema de reporte garantizando que tanto los órganos de administración como las líneas de negocio y unidades internas, puedan llevar a cabo sus funciones[1]:

A. Consejo de Administración y sus comisiones delegadas:
   - Comisión de Auditoría.
   - Comité de Riesgos.
   - Comité de Remuneraciones.
   - Comité de Nombramientos.

B. Comité de Dirección:
   - Comité de Precios.
   - Comité de Recursos.

C. Comités con responsabilidades directas sobre los riesgos:
   - Comité de Activos y Pasivos
   - Comité de Cumplimiento y Riesgo Operacional

D. Departamento responsable de la tercera línea de defensa:
   - Auditoría Interna.

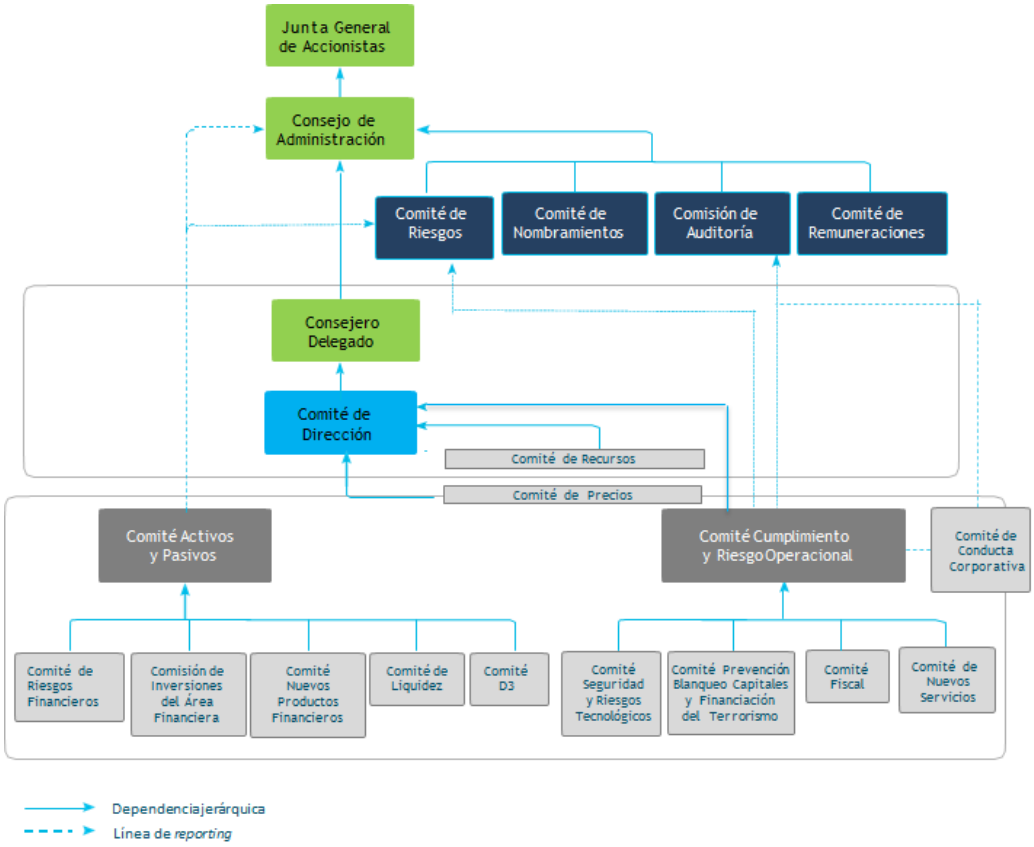
E. Departamentos o Divisiones responsables de la segunda línea de defensa que, a su vez, integran el Área de Riesgos y Cumplimiento:
   - División de Riesgos no Financieros y Cumplimiento, que a su vez engloba:
     - Cumplimiento Normativo.
     - Control Interno y Riesgo Operacional.
     - Seguridad de la Información y Riesgos Tecnológicos.
   - División de Riesgos financieros, que integra:
     - Riesgo de Mercado, Balance y Liquidez.
     - Riesgo de Crédito y Contraparte.
   - Unidad de Coordinación y Riesgos transversales.

F. Departamentos o divisiones que, si bien no son de segunda línea de defensa, realizan funciones vinculadas con el control de diferentes riesgos, especialmente los relacionados con Seguridad y Prevención de Riesgos Laborales.

G. Departamentos o Divisiones responsables de la primera línea de defensa:
   - División de Admisión de Riesgos y Control.
   - Unidades de negocio y soporte.

[1] Más información sobre los procedimientos establecidos para la identificación, medición, gestión y control de los riesgos se encuentra recogidos en la Información con Relevancia Prudencial de Cecabank (https://www.cecabank.es/).

3.1. Órganos de Gobiernos y estructura de Comités



Consejo de Administración

El Consejo de Administración, como máximo órgano de decisión, es el responsable de determinar las políticas generales de la Entidad en materia de riesgos. Ello incluye la definición de la naturaleza y los niveles de tolerancia al riesgo y la fijación de las políticas de asunción, seguimiento y control de los distintos riesgos incurridos, garantizando la adecuada correspondencia entre dicho nivel y el capital existente.

Igualmente, el Consejo es el primer impulsor de la cultura corporativa de riesgos, orientada a asegurar unos sistemas de control interno eficientes, unos procesos de gestión y medición completos y sustentada en un marco de integridad y valores éticos del más alto nivel, principios recogidos en el Código de Conducta Corporativa de Cecabank, garantizando la integridad de los sistemas de información contable y financiera, incluidos el control financiero y operativo y el cumplimiento de la legislación aplicable.

El régimen de funcionamiento interno del Consejo, sus principios de actuación y normas básicas de organización y funcionamiento están detallados en el Reglamento del Consejo, que se encuentra publicado en la web corporativa de la Entidad, en el apartado de información corporativa.

Comisión de Auditoría

Supervisa y valora la eficacia del control interno de la Entidad, la auditoría interna y los sistemas de gestión de riesgos; así mismo supervisa el proceso de elaboración y presentación de la información financiera regulada. En este marco es competente para supervisar el funcionamiento del canal de denuncias, el cumplimiento de los códigos de conducta y de sus normas de gobierno interno, realizando las propuestas de mejora que correspondan.

Le corresponde también evaluar y aprobar anualmente las funciones de auditoría interna y sus planes de actuación, supervisando su cumplimiento y el funcionamiento de la propia función de auditoría y el desempeño de su responsable. La dependencia funcional de Auditoría Interna de la Comisión de Auditoría salvaguarda la independencia de la función de control de tercer nivel.
El régimen de funcionamiento interno de esta Comisión, sus principios de actuación y normas básicas de organización y funcionamiento, así como las reglas de conducta de sus miembros, se encuentra recogido en el Reglamento de la Comisión de Auditoría, publicado en la web corporativa de la Entidad, en el apartado de información corporativa.

Comité de Riesgos

Como comisión delegada del Consejo de Administración, el Comité de Riesgos tiene, entre otras funciones, la de asesorar al Consejo de Administración sobre la propensión global al riesgo, actual y futura, de la Entidad y su estrategia en este ámbito, y asistirle en la vigilancia de la aplicación de esta estrategia. Así, deberá conocer y analizar periódicamente la situación de solvencia, liquidez y, en general, de los riesgos de la Entidad. En particular, le corresponde analizar el informe de autoevaluación del capital y de la liquidez y la información con relevancia prudencial antes de ser elevados al Consejo.

El régimen de funcionamiento interno de este Comité, sus principios de actuación y normas básicas de organización y funcionamiento, así como las reglas de conducta de sus miembros, se encuentra recogido en el Reglamento del Comité de Riesgos, publicado en la web corporativa de la Entidad, en el apartado de información corporativa.

Comité de Remuneraciones

A este Comité le corresponde asesorar al Consejo en lo relativo a las políticas retributivas de la Entidad, y el alineamiento de éstas con el mantenimiento de los niveles de tolerancia al riesgo. Así mismo, debe informar sobre la Política de Remuneraciones de los altos directivos, los empleados que asuman riesgos, los que ejercen funciones de control, y a todo trabajador que reciba una remuneración global que lo incluya en el mismo baremo de remuneración que el de los altos directivos y los empleados que asumen riesgos, cuyas actividades profesionales inciden de manera importante en su perfil de riesgo, supervisando directamente la remuneración de los altos directivos encargados de la gestión de riesgos y con funciones de cumplimiento de la Entidad.

El régimen de funcionamiento interno de este Comité, sus principios de actuación y normas básicas de organización y funcionamiento, así como las reglas de conducta de sus miembros, se encuentra recogido en el Reglamento del Comité de Remuneraciones, publicado en la web corporativa de la Entidad, en el apartado de información corporativa.

Comité de Nombramientos

A este Comité le corresponden, entre otras funciones, identificar y recomendar candidatos para proveer los puestos de vacantes en el Consejo, evaluar periódicamente la estructura, tamaño, composición y actuación del Consejo y la idoneidad de sus miembros y del Consejo en su conjunto y revisar periódicamente la política del Consejo en materia de selección y nombramiento de personal de la alta dirección.

El régimen de funcionamiento interno de este Comité, sus principios de actuación y normas básicas de organización y funcionamiento, así como las reglas de conducta de sus miembros, se encuentra recogido en el Reglamento del Comité de Nombramientos, publicado en la web corporativa de la Entidad, en el apartado de información corporativa.

Comité de Dirección

Al Comité de Dirección le corresponde promover el desarrollo de los sistemas y procedimientos de control interno que garanticen una correcta gestión de los riesgos corporativos, en base al marco de control definido por el Consejo de Administración.

El régimen de funcionamiento, así como sus responsabilidades, se encuentran recogidas en el Reglamento del Comité de Dirección.

Comités especializados

Comité de Recursos

Este Comité tiene por objetivo impulsar la transformación de la Entidad, a través de una adecuada estrategia de los recursos humanos y tecnológicos de Cecabank, de tal forma que permita dar respuesta a los requisitos, necesidades y estrategias del resto de unidades de la Entidad, acorde a los retos y principios marcados en los planes estratégicos vigentes y a la normativa y reglamentación vigente en cada momento.

En el ámbito tecnológico, es el responsable de definir la gobernanza tecnológica general de la Entidad de forma que se encuentre alineada su estrategia tecnológica y su estrategia de negocio. Puede solicitar al Comité de Seguridad y Riesgos Tecnológicos el análisis pormenorizado de aspectos de riesgo tecnológico que vayan más allá del análisis preliminar que el Comité de Recursos realice.

Este Comité informa periódicamente al Comité de Dirección, al que sirve de apoyo en aspectos como la estrategia y la inversión en tecnología y recursos humanos. Sus funciones aparecen detalladas en su Reglamento.

Este Comité elevará al Consejo de Administración, vía Comité de Dirección, el informe cuatrimestral de digitalización y tecnología.

Comité de Precios

Tiene como objetivo identificar y analizar los aspectos, tanto comerciales como de gestión o procedimiento, que puedan estar reduciendo la capacidad de la Entidad para maximizar sus ingresos. Entre sus funciones, detalladas en su Reglamento, están la de analizar y establecer los precios de los nuevos productos y servicios, atendiendo a las características específicas y de mercado, en línea con la estrategia de la Entidad.

Comité de Activos y Pasivos (COAP)

El COAP tiene como misión la aprobación, información, seguimiento y control primario de los riesgos financieros, dentro del esquema de gestión definido por el Consejo en el Marco de Tolerancia al Riesgo y en el Marco General de Gestión de Riesgos. Es el órgano de la Entidad a través del cual se vertebra la participación de la alta dirección en el seguimiento y control primario de los riesgos financieros y el desarrollo e implantación las políticas de riesgo que aseguren el mantenimiento del perfil de riesgos establecido en la Entidad.

Para el desarrollo de las funciones que tienen encomendadas, cuenta como unidades de apoyo con diferentes comités: Comité de Riesgos Financieros, Comité de Inversiones del Área Financiera, Comité de Nuevos Productos Financieros, Comité para la Disrupción, Diversificación y Dinamización (Comité D3) y Comité de Liquidez.

El régimen de funcionamiento, así como los objetivos y las responsabilidades del COAP y de sus comités de apoyo, se encuentran recogido en el Manual de COAP.

Comité de Cumplimiento y Riesgo Operacional (CCyRO)

El Comité de Cumplimiento y Riesgo Operacional tiene como misión la aprobación, información, seguimiento y control de los riesgos no financieros, incluyendo el riesgo operacional, el reputacional, el legal, el de cumplimiento y el tecnológico.

Para el desarrollo de las funciones que tienen encomendadas, cuenta como unidades de apoyo con los siguientes comités:

- Comité de Prevención de Blanqueo de Capitales y Financiación del Terrorismo: órgano de control interno responsable de la aplicación de las políticas y procedimientos de la Entidad en materia de PBCFT.
- Comité Fiscal: colabora en el análisis e interpretación de las normas fiscales que sean de aplicación en la actividad de Cecabank, en el control del cumplimiento de las obligaciones formales y en la investigación, evaluación y seguimiento de los posibles riesgos fiscales.
- Comité de Seguridad y Riesgos Tecnológicos: acuerda el establecimiento de las iniciativas que se consideren oportunas para la adecuada gestión de los riesgos tecnológicos (riesgo de seguridad lógica y física, riesgo de outsourcing, riesgo de cambios, riesgo de integridad de datos y riesgo de continuidad y contingencia). Este Comité tiene como finalidad hacer seguimiento a todos los proyectos de alcance en la Entidad que tengan por objeto la mejora del servicio tecnológico en procesos de negocio o soporte ya existentes o dar cobertura a nuevas líneas de actividad.
- Comité de Nuevos Servicios: analiza y en su caso, aprueba los nuevos servicios a prestar por la Entidad.

De igual forma asume directamente el seguimiento del riesgo penal.

El régimen de funcionamiento, así como los objetivos y las responsabilidades del Comité de Cumplimiento y Riesgo Operacional se encuentran recogido en el Reglamento del CCyRO.

Comité de Conducta Corporativa

Su función es velar por el buen funcionamiento del canal de comunicación establecido en materias relacionadas con el Código de Conducta Corporativa[2]. Este Comité informa al Comité de Cumplimiento y Riesgo Operacional cuando del análisis y resolución de las denuncias se determine que se ha producido un evento de pérdida de riesgo operacional, así como del funcionamiento del canal de denuncias desde el punto de vista de riesgo penal, su estado de tramitación y el resultado final de las actuaciones realizadas.

El presidente del Comité de Conducta Corporativa reporta con periodicidad, al menos anual, a la Comisión de Auditoría de la Entidad sobre el funcionamiento y utilización del Canal o cualquier otra iniciativa de seguimiento y aplicación del Código.

Comité de Seguridad y Salud

El Comité de Seguridad y Salud es un órgano autónomo de representación de la empresa y de los trabajadores, que tiene por objeto participar en la elaboración, puesta en práctica y evaluación de los planes y programas de prevención de riesgos de la empresa y promover iniciativas sobre métodos y procedimientos para la efectiva prevención de los riesgos, proponiendo a la empresa la mejora de las condiciones o la corrección de las deficiencias existentes.

3.2. Estructura organizativa interna

Primera línea de defensa

A. Áreas de negocio y soporte

Las diferentes Áreas donde se integran las líneas de negocio de la Entidad, así como las que les prestan soporte, asumen los riesgos en el ejercicio de su actividad, teniendo en cuenta el apetito al riesgo autorizado por el Consejo, los límites de riesgo autorizados y las políticas y procedimientos existentes.

Son responsables de desarrollar e implementar procesos y mecanismos de control para asegurar que se identifican, gestionan, miden, controlan, mitigan y reportan los principales riesgos que originan con sus actividades.

El proceso de identificación de los riesgos no financieros se realiza a través del grupo de trabajo CIRO, constituido como un grupo de trabajo permanente cuya principal responsabilidad es la detección de los riesgos no financieros inherentes a los procesos, productos y sistemas de la Entidad. Su objetivo es la obtención de un inventario de dichos riesgos, así como la selección de los indicadores de riesgo y gestión para el adecuado seguimiento de los mismos.

Su composición es la siguiente:

- Con carácter permanente, representantes de las siguientes unidades: Auditoría Interna, Organización, Control Interno, Riesgo Operacional y Seguridad y Riesgos Tecnológicos.
- Con carácter transitorio y mientras se desarrolla el proceso de identificación de los riesgos de la unidad objeto de análisis, por la dirección del departamento que corresponda.

[2] El Código de Conducta se encuentra publicado en la página web corporativa de la Entidad, en el apartado información corporativa (normas de conducta).

B. División de Medios Tecnológicos

De forma general, la función de primera línea de defensa es la de implantar y hacer seguimiento a los mecanismos primarios de control operativo necesarios para la mitigación de los riesgos identificados. En el caso de los riesgos tecnológicos, esta función está desempeñada por la División de Medios Tecnológicos. Sus funciones consisten en la implantación de las medidas de control que son a su vez supervisadas desde la segunda línea por Seguridad de la Información y Riesgos Tecnológicos, así como la monitorización y la atención temprana de los eventos de riesgo tecnológico de la Entidad.

C. División de admisión de riesgos y control

Esta división cubre las necesidades de análisis del riesgo de crédito de contrapartidas y negocios asociado a los procesos de admisión y seguimiento. Con independencia de la ubicación de este grupo dentro del Área financiera, da soporte trasversal a las necesidades de análisis del riesgo de crédito de todas las áreas operativas. Todo lo anterior implica, entre otros aspectos:

- Realizar el análisis y seguimiento del riesgo de crédito de contrapartidas y negocios.
- Participar en los procesos de toma de decisiones de inversión, desde el punto de vista del análisis de los riesgos incurridos.
- Apoyar en la definición de la política de inversiones, analizando el alineamiento con lo previsto en el Marco de Tolerancia al Riesgo.
- Definir y proponer el modelo de metodologías de riesgo de crédito empleadas por la Entidad para el seguimiento del riesgo de crédito.
- Participar en el desarrollo y evolución de los procesos y metodologías de gestión de riesgos y realizar propuestas de mejora en el ámbito de la gestión y control de los riesgos.
- Implementar los procedimientos y técnicas de admisión y seguimiento de riesgo de crédito adoptados.
- Asesorar en materia de riesgos a las distintas unidades de negocio.
- Detección de nuevos riesgos vinculados a las áreas de negocio en crecimiento y elaboración de propuestas para su mitigación.

Segunda línea de defensa

Aglutina las funciones de gestión de riesgos y función de cumplimiento establecidas en la Guía de la EBA de Gobierno Interno, asumiendo, entre otras, las siguientes funciones:

- Participar en la elaboración de la estrategia de riesgo de la Entidad, asegurando que tenga implantados procedimientos eficaces de gestión de riesgos.
- Proporcionar la información relevante en materia de riesgos que permita al Consejo de Administración establecer el apetito al riesgo de la Entidad.
- Proponer los límites de riesgo específico para garantizar el alineamiento de la actividad con el apetito al riesgo definido.

- Evaluar el impacto de transacciones excepcionales o cambios significativos en el riesgo global de la Entidad.
- Realizar el seguimiento periódico del perfil de riesgo de la Entidad en sus diferentes dimensiones, tanto financieras como no financieras y de cumplimiento, informando sobre su evolución a los órganos de gobierno.
- Analizar tendencias e identificará riesgos nuevos o emergentes.
- Asegurar que las políticas y normas internas permiten dar cumplimiento a las exigencias normativas aplicables, supervisando su respeto por la organización y proponiendo las mejoras que procedan.
- Asegurar que, con anterioridad al lanzamiento de nuevos productos o servicios, se han identificado los riesgos y las medidas para mitigarlos, y se da cumplimiento a las normas aplicables a los mismos.

Está constituida por las unidades especializadas de control, integradas en el Área de Riesgos y Cumplimiento.

A. División de Riesgos Financieros

Esta División está integrada por los departamentos de:

- **Control del Riesgo de Crédito y Contraparte**: responsable del control de segundo nivel del riesgo de crédito asociado a la actividad de las distintas unidades de negocio.
- **Riesgo de Mercado Balance y Liquidez:** se encarga de la medición y control del riesgo de mercado y del riesgo estructural de balance, así como de hacer el seguimiento de los resultados de gestión de la Sala de Tesorería.

B. División de Riesgos no Financieros y Cumplimiento

Esa División está a su vez integrada por los siguientes Departamentos:

- **Control Interno y Riesgo Operacional:**

  La Unidad de Riesgo Operacional tiene como función principal planificar, organizar e implantar en la Entidad el sistema de gestión del riesgo operacional, de acuerdo con las políticas y procedimientos aprobados, y comprobar que la primera línea de defensa identifique, evalúe, mida, controle, gestione y comunique adecuadamente todos los riesgos operativos.

  Así mismo es la unidad responsable de llevar a cabo el análisis del riesgo de las externalizaciones y del registro en Banco de España de las externalizaciones consideradas materiales, de acuerdo con lo establecido en la Política de externalización y contratación de servicios y funciones aprobada por el Consejo de Administración.

  La unidad de Control interno realiza actuaciones que permiten contrastar y verificar el grado de eficacia de los controles primarios operativo-contables previamente establecidos por cada departamento, con el fin de asegurar que se ha cumplido con dichos controles, que las transacciones se contabilizan y se reflejan de forma adecuada y que la información financiera suministrada es correcta. Así mismo, comprueba el cumplimiento de las normas internas de ámbito operativo, como las relativas a contratos.

- **Cumplimiento Normativo:**

  Su objetivo principal es asegurar una gestión eficiente del riesgo de cumplimiento, desarrollando los controles que permitan verificar que las normas y políticas internas son aplicadas por la primera línea.

  Sus principales ámbitos de actuación son la prevención del blanqueo de capitales, normas de conducta del Mercado de Valores (RIC y MiFID), la protección de datos de carácter personal, el gobierno corporativo y el riesgo penal.

- **Seguridad de la Información y Riesgos tecnológicos:**

  Es la unidad de control secundario en el ámbito de los riesgos de las tecnologías de la información y las comunicaciones (TIC). Atendiendo a las directrices de la Autoridad Bancaria Europea[3] (EBA), la unidad considera de forma específica los riesgos de seguridad, continuidad, integridad de datos y riesgo de cambio, así como el riesgo de outsourcing, si bien este último es analizado de forma conjunta con la Unidad de Riesgo Operacional, siguiendo las directrices fijadas por la Política de externalización y contratación de servicios y Funciones de la Entidad.

C. Unidad de Coordinación y Riesgos Transversales

Es la unidad responsable de la gestión y control de los riesgos transversales que afectan a la Entidad en su conjunto, y que se corresponden con riesgo reputacional, riesgos climáticos y medioambientales, riesgo de modelo y otros riesgos emergentes.

Adicionalmente, le corresponde la coordinación de la elaboración de documentos legalmente requeridos antes supervisores y mercado (IACL, IRP, Plan de Recuperación), así como la documentación solicitada por el supervisor a efectos de resolución. También es responsable de la coordinar la elaboración de Manuales y Políticas dentro del Área.

Dentro del ámbito de los riesgos operativos no financieros existen otras categorías específicas de riesgo que cuentan con mecanismos de seguimiento y gestión diferenciados, fuera del Área de Riesgos y Cumplimiento:

- Riesgos vinculados con la seguridad física y las relaciones laborales: El Departamento de Seguridad, integrado en la División de Talento, Cultura y Servicios Generales, está previsto en la Ley de Seguridad Privada como una obligación legal que tiene por objeto implantar la normativa relativa a la Seguridad Privada en coordinación con los Cuerpos y Fuerzas de Seguridad del Estado. Su función principal es evaluar y controlar permanentemente la seguridad física de las instalaciones.

- Por su parte, el Servicio de Prevención de Riesgos Laborales, integrado igualmente dentro en la División de Talento, Cultura y Servicios Generales, es el encargado de promover la integración de la prevención en la Entidad, mediante un servicio propio de Prevención de Riesgos Laborales y es el responsable de implantar las medidas legalmente establecidas en materia de prevención de riesgos laborales en todas las fases de actividad de la empresa, con el fin de evitar o disminuir los riesgos derivados del trabajo (salud y seguridad). El Comité de Seguridad y Salud es el órgano paritario y colegiado de participación destinado

[3] EBA/GL/2017/05, bajo el nombre de "Guidelines on ICT Risk Assessment under the Supervisory Review and Evaluation process (SREP)"

a la consulta regular y periódica de las actuaciones de la empresa en materia de prevención de riesgos.

Tercera línea de defensa: Auditoría Interna

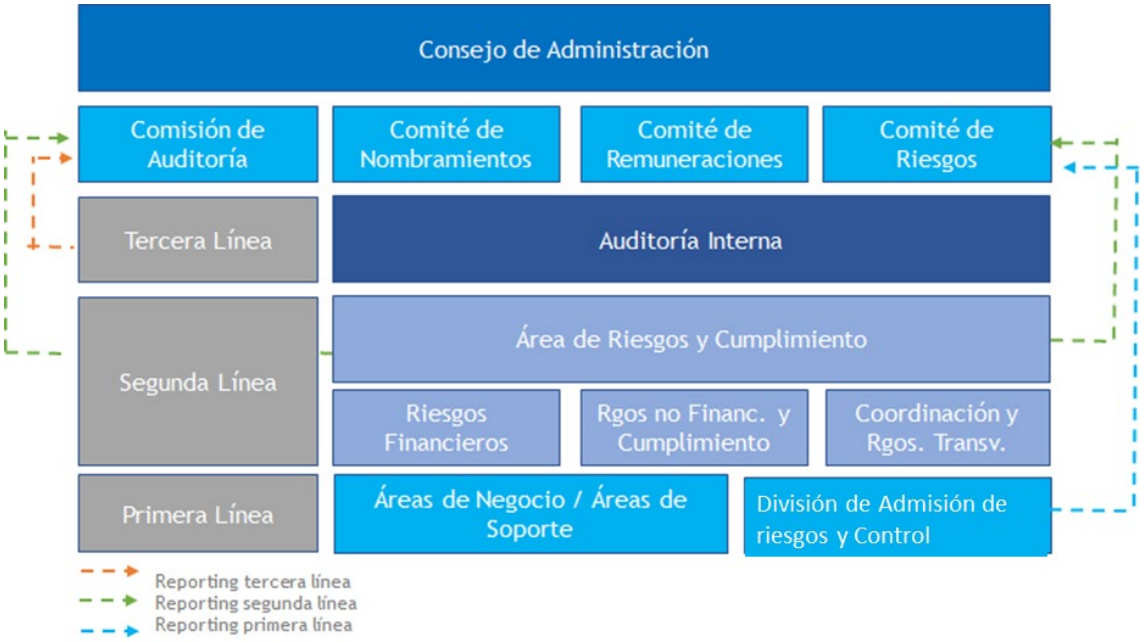
Auditoría Interna es una dirección independiente y objetiva cuya labor consiste en la supervisión de las funciones de control secundario y primario desarrolladas dentro del marco de gestión y control de riesgos de la actividad, evaluando de esta forma el marco de control interno de la Entidad.

Entre sus funciones se encuentra la de verificar el cumplimiento de la normativa interna y externa por parte de todas las actividades y unidades de la Entidad, incluyendo sus Sucursales y, en su caso, Sociedades participadas. Adicionalmente, Auditoría Interna revisa los procesos de evaluación del capital y de la liquidez (IACL), la Información con Relevancia Prudencial y la información financiera que la Entidad hace pública.

Con la finalidad de salvaguardar su independencia respecto de las funciones que audita, depende funcionalmente de la Comisión de Auditoría y orgánicamente del Consejero Delegado de la forma que éste determine.

Así mismo, determinados procesos y actividades se someten a revisión externa (auditorías externas) por terceras partes independientes. Sus resultados y conclusiones se informan a Auditoría Interna de la Entidad para su conocimiento y, en su caso, seguimiento de las recomendaciones propuestas.

Sus funciones están establecidas y reguladas en el Estatuto de Auditoría Interna.



4. Revisión y, en su caso, modificación del Marco General de Control

El Marco General de Control es revisado y, en caso de ser necesario, actualizado por parte del Comité de Dirección, siendo publicado en la página web corporativa (en el apartado Control Interno y Gestión de Riesgos), en aplicación de la Circular 2/2016 del Banco de España.

Forma parte como Anexo de los Informes anuales de Autoevaluación del Capital y de la Liquidez (IACL) y de la Información con Relevancia Prudencial (IRP), que analiza y aprueba el Consejo de Administración, a propuesta del Comité de Riesgos.

Anexo 1. Procedimientos Administrativos y contables

En Cecabank existe una estructura contable descentralizada, de forma que los departamentos de negocio contabilizan las operaciones asociadas a sus actividades, al igual que hacen los de soporte con relación a sus facturas emitidas y recibidas, si bien estas últimas son liquidadas por Administración.

La Entidad cuenta con los mecanismos necesarios con el fin de proporcionar seguridad razonable en cuanto a la fiabilidad de su información financiera. Para ello se asegura de que:

- Las transacciones existen y se han registrado en el momento adecuado (existencia y ocurrencia).
- La información refleja la totalidad de las transacciones (integridad).
- Las transacciones se registran y valoran de conformidad con la normativa aplicable (valoración).
- Se refleja, a la fecha correspondiente, los derechos y obligaciones a través de los correspondientes activos y pasivos, de conformidad con la normativa aplicable (derechos y obligaciones).

Las actuaciones de control secundario que efectúa Control Interno tienen como principal finalidad asegurar la información financiera contable, el cumplimiento de los procedimientos y normativas internas y externas en el ámbito operativo y la salvaguarda de activos. Estas actuaciones se efectúan diariamente sobre todos los asientos contables que los departamentos registran, lo que implica una sistematización del análisis, consulta si procede, y envío de incidencias detectadas para su subsanación en el proceso contable siguiente.

Para efectuar estos controles, se aplican los principios de devengo (comprobar que el registro de los gastos y los ingresos se anota en el momento en que tiene lugar el intercambio comercial o la realización de un determinado servicio); uniformidad (comprobar que una vez que Cecabank ha adoptado un criterio o un método de valoración para elaborar los estados financieros, dentro del marco permitido, no lo cambia a no ser que cambien las condiciones por las que se aceptaron en su momento y lo aplica de la misma forma para todos los procesos y eventos); prudencia (comprobar que se valoran los elementos patrimoniales y los resultados con prudencia pero reflejando una imagen fie); no compensación (comprobar que no se compensan unas cuentas con otras, es decir, que no se compensa una partida de activo con una de pasivo en el balance general, ni gastos con ingresos en la cuenta de pérdidas y ganancias) y de importancia relativa (la aplicación de algunas normas contables puede omitirse cuando se trate de eventos que no poseen una importancia significativa para Cecabank).

Por su parte, el Área de Planificación es la responsable de la elaboración, presentación e integridad de la información financiera y de definir las pautas contables a seguir, de acuerdo con lo recogido en el Manual de Políticas Contables y en la normativa en vigor, para garantizar la exactitud y seguridad en el registro y contabilización de las operaciones. Además, define los circuitos contables de cada nueva operativa, coordinar y centralizar la elaboración de los presupuestos de la Entidad y la contabilización y el pago de todas las facturaciones por servicios, inversiones y aprovisionamiento.

Anexo 2: Principales políticas y otras normas o procedimientos referentes al ámbito de control

Nombre del documento	Objeto
MARCO DE TOLERANCIA AL RIESGO	Determina los riegos que el Consejo de Administración ha definido como relevantes para la Entidad, así como el nivel de riesgo que el banco está dispuesto y es capaz de asumir en el ejercicio de sus actividades.
MARCO GENERAL DE GESTIÓN DEL RIESGO	Documento que desarrolla el Marco de Tolerancia al Riesgo en cuanto a la definición de su apetito al riesgo y el marco de seguimiento y control de los riesgos de la entidad.
MARCO GENERAL DE CONTROL	Documento que describe el sistema de control interno, los mecanismos de control de la Entidad así como los canales de comunicación y la asignación de responsabilidades entre sus participantes. Define la estructura del control en la Entidad y los sistemas de relación entre sus participantes.
MANUAL DEL COAP	Su objetivo es describir las políticas, métodos, procedimientos y sistemas de gestión y control primario de los riesgos a los que se encuentra expuesta la Entidad, como consecuencia de la actividad financiera que realiza a través de sus distintas unidades operativas, delegados por el Consejo de Administración en el COAP (riesgo de crédito, riesgo de mercado y riesgos estructurales de balance).
MANUAL DE GESTION DE RIESGOS FINANCIEROS	Establece las políticas generales en materia de asunción de riesgos financieros, orientada a asegurar unos sistemas de control interno eficaces y unos procesos de gestión y medición de los riesgos.
MARCO DE CONTROL DE RIESGOS TECNOLÓGICOS	Establece un conjunto de estructuras organizativas, políticas, normas y procedimientos orientados al control de los riesgos de las tecnologías de la información y las comunicaciones.
POLÍTICA DE SEGURIDAD	Establece y comunica las líneas directrices que deberán seguirse en la organización para gestionar la seguridad y cumplir con los requerimientos regulatorios y de los clientes de la Entidad.
POLÍTICA DE CONTINUIDAD GLOBAL	Pretende facilitar un entorno seguro en el que Cecabank pueda desarrollar sus servicios minimizando el impacto ante situaciones de contingencia, protegiendo los activos, equipos y actividades de negocio, de forma permanente frente a los riesgos, velando especialmente por la seguridad de las personas, el cumplimiento normativo en la materia, la preservación de la buena reputación de la Entidad y la sostenibilidad de la misma.

PROCEDIMIENTO DE GESTIÓN DEL RIESGO OPERACIONAL	Contienen los procedimientos y prácticas que sirven de orientación y guía a la Unidad de Riesgo Operacional y al resto de la organización para una adecuada gestión del riesgo operacional, así como para el cumplimiento de las políticas de Identificación, evaluación, seguimiento y control/mitigación del riesgo operacional.
POLÍTICA DE EXTERNALIZACIÓN Y CONTRATACIÓN DE SERVICIOS Y FUNCIONES	Establece los principios, reglas y procedimientos de obligado cumplimiento en las distintas fases del proceso de externalización: propuesta y toma de la decisión; examen del proveedor; formalización contractual y determinación de acuerdos de nivel de servicio; implementación, supervisión y gestión de los acuerdos de externalización.
POLITICA DE SEGUIMIENTO DE LA CADENA DE CUSTODIA	Establece los principios, reglas y procedimientos de obligado cumplimiento en la selección de terceros custodios para salvaguardar los activos de clientes y minimizar el riesgo de pérdida y el mal uso de los mismos. Así mismo define un procedimiento riguroso y documentado de diligencia debida para la supervisión permanente del tercero en el que se deleguen las funciones de custodia, tal y como establece la normativa vigente.
MARCO GENERAL DE CONTROL DEL RIESGO OPERACIONAL DE LA ACTIVIDAD DE DEPOSITARIA	Principios y medidas de implantación específicos en relación al riesgo operacional para la actividad de depositaría.
POLITICA DE CUMPLIMIENTO Y ESTATUTO DE LA FUNCION DE CUMPLIMIENTO	Delimita las competencias de la función de Cumplimiento Normativo, distribuye las responsabilidades entre los distintos niveles de la organización, preserva su independencia y fija sus facultades y los niveles de cualificación requeridos.
POLÍTICA GENERAL DE REMUNERACIONES	Tiene por objeto sentar las bases retributivas de la Entidad a los efectos de establecer un sistema de remuneración que sea compatible con la estrategia empresarial, los objetivos, los valores y los intereses a largo plazo de Cecabank, sin perder su condición de elemento de motivación al esfuerzo. Con esta Política se pretende definir y controlar, de manera clara y concisa, las prácticas retributivas de la Entidad a fin de evitar que las mismas incentiven comportamientos de asunción excesiva de riesgos, todo ello de conformidad con lo establecido en la legislación vigente.
MARCO DE GESTION DEL RIESGO DE CUMPLIMIENTO	Diseño de un sistema de documentación, evaluación y control de los riesgos de cumplimiento, en materia de prevención del blanqueo de capitales, normas de conducta en los mercados de valores, protección de datos de carácter personal y penal.

POLITICA DE PREVENCIÓN DEL BLANQUEO DE CAPITALES Y DE LA FINANCIACIÓN DEL TERRORISMO	Establecer las líneas maestras que definen el modelo de prevención del blanqueo de capitales y la financiación del terrorismo.
MANUAL PARA LA PREVENCION DEL BLANQUEO DE CAPITALES Y LA FINANCIACIÓN DEL TERRORISMO	Tiene como objeto establecer las políticas y procedimientos establecidos por el Banco para luchar eficazmente contra el blanqueo de capitales y la financiación del terrorismo. Para ello, se aprueba en cumplimiento de lo previsto en el artículo 26.3 de la Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y la financiación del terrorismo.
MANUAL DE PROCEDIMIENTOS INTERNOS PARA EL CUMPLIMIENTO DE GDPR	Recogen los referidos procedimientos internos necesarios para un adecuado cumplimiento de las obligaciones derivadas de Reglamento General de Protección de Datos (GDPR).
REGLAMENTO INTERNO DE CONDUCTA EN EL ÁMBITO DEL MERCADO DE VALORES	Ajusta las actuaciones de Cecabank, de sus órganos de administración, empleados y representantes a las normas de conducta en el ejercicio de actividades relacionadas con el mercado de valores, con el objetivo de fomentar la transparencia en los mercados y preservar, en todo momento, el interés legítimo de los inversores.
POLITICA PARA LA PRESTACION DE SERVICIOS DE INVERSION	Tiene por objeto recopilar los principios, criterios, directrices y procedimientos de aplicación en la Entidad en aplicación de la normativa MiFID en lo relativo a los requisitos organizativos y las condiciones de funcionamiento de las empresas de inversión, y términos definidos a efectos de dicha directiva.
POLÍTICA DE TRANSPARENCIA EN LOS MERCADOS	Marco de actuación de la Entidad para dar cumplimiento a los requerimientos de transparencia previstos en MiFID II/MiFIR.
MANUAL PARA LA EJECUCION Y CONTROL DEL RIC	Establece los procedimientos de actuación en relación a las personas sujetas al Reglamento Interno de Conducta.
CÓDIGO DE CONDUCTA CORPORATIVA	Recoge una serie de principios y normas de actuación que deben guiar la conducta de los miembros de los órganos de gobierno y de todos los empleados en su desempeño profesional.
POLÍTICA DE CUMPLIMIENTO PENAL	Desarrolla lo establecido en el Código de Conducta Corporativa de Cecabank, definiendo un marco de principios en materia de Cumplimiento Penal.

DOCUMENTO VERTEBRADOR DEL SISTEMA DE ORGANZIACIÓN Y GESTIÓN DEL RIESGO PENAL	Establece el modelo de organización, prevención, gestión y control de riesgos penales de Cecabank
POLÍTICA DE RIESGO FISCAL	Desarrolla e implementa los principios rectores en materia tributaria detallando los principios y buenas prácticas, con base en los cuales, la Entidad desarrollará los procesos de naturaleza tributaria relacionados con la función fiscal, siendo de obligatoria aplicación a los miembros de la alta dirección y a todos los empleados de Cecabank, en especial, a todos aquellos involucrados directa o indirectamente en el ejercicio de los procesos de naturaleza tributaria relacionados con la función fiscal.
POLÍTICA DE TRANSPARENCIA	Regula los procedimientos de decisión y control respecto a la información a publicar.
MANUAL DE POLÍTICAS CONTABLES	Recoger las políticas contables utilizadas por Cecabank en el marco de la normativa vigente, para la elaboración de sus estados financieros.
MARCO DE CONTRATACIÓN INTERNA Y PROCEDIMIENTO DE OTORGAMIENTO DE PODERES	Establece los criterios, procedimientos y límites generales que definen la formalización y adquisiciones de recursos por la Entidad.
POLÍTICA DE SOSTENIBILIDAD	Identifica los ámbitos de actuación de Cecabank que contribuyen a construir relaciones duraderas con nuestros grupos de interés de forma que pueda maximizar la creación de valor.
POLÍTICA DE GOBIERNO DEL DATO	Establece los requisitos que deben contar los repositorios de información, en la medida en que esta debe ser validada y conciliada con la información contable (en el caso en el que a los datos le apliquen criterios contables), con reglas de calidad, con el máximo nivel de granularidad, con la profundidad histórica suficiente para su análisis y coherencia con otros ejes o visiones de información que pudieran existir.

cecabank