Marco General del Control

Comité de Dirección

ÍNDICE

I. CARACTERÍSTICAS DEL SISTEMA DE CONTROL INTERNO

II. ORGANIGRAMA DEL CONTROL INTERNO

III. PROTOCOLO DEL EURIBOR

IV. RELACIONES ENTRE LAS UNIDADES EN EL SISTEMA DE CONTROL

V. NORMATIVA COMPLEMENTARIA DEL SISTEMA DE CONTROL

I. CARACTERÍSTICAS DEL SISTEMA DE CONTROL INTERNO

La estructura organizativa y los mecanismos de control interno desarrollados por la Alta Dirección van dirigidos a garantizar que las actividades de la Entidad son eficientes y eficaces, que la información es de confianza, oportuna y completa y que se cumple con las leyes aplicables.

Se caracteriza principalmente:

- Por ser de gestión integral y especializada**.** Existen unidades específicas de gestión y control de los distintos riesgos, cuyo ámbito de actuación es integral y uniforme:
  - *El riesgo financiero* se gestiona desde el Área de Riesgos a través de las Divisiones de Mercado, Balance y Liquidez y Análisis y Control del Riesgo.
  - *El riesgo operacional y el riesgo reputacional* se gestionan desde el Área de Servicios Asociativos y Auditoría, a través de la División de Auditoría, Control y Cumplimiento y de la División de Recursos. Concretamente, hay unidades especializadas en:
    - El control del riesgo de cumplimiento
    - El control del riesgo del riesgo reputacional
    - El control del riesgo tecnológico
    - El control del riesgo operativo-contable
    - El control del riesgo de comisión de delitos penales
    - El control de la seguridad física
    - El control de la prevención (salud y seguridad laboral)
    - La gestión del riesgo operacional

- Por ser una estructura descentralizada pero con relaciones entre las unidades de gestión de riesgos guiadas por los principios de coordinación, cooperación e información recíproca.

  A pesar de que las diferentes unidades de control se ubican en el organigrama en áreas distintas de la Entidad, existen relaciones de cooperación entre ellas, formalizadas a través de la estructura de Comités, que aseguran una adecuada coordinación en la gestión de los distintos riesgos.

- Por ser una estructura que garantiza la independencia de las unidades que realizan funciones de control con respectos a las áreas, unidades o funciones sobre las que gira su verificación.

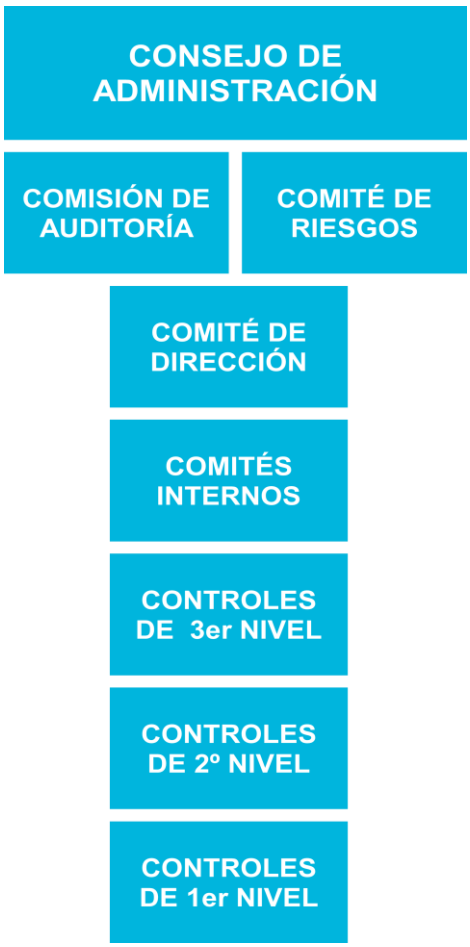
- Por la existencia de tres niveles de control**.** Existen distintos niveles de control que se clasifican en:
  - Primer nivel: Aquellos controles que son establecidos y realizados en los propios departamentos y que se denominan CONTROLES PRIMARIOS.
  - Segundo nivel: Aquellos controles ejercidos o realizados desde los departamentos con responsabilidades de control, y que se denominan CONTROLES SECUNDARIOS.
  - Tercer nivel: Aquellos controles que son realizados por el Departamento de Auditoría Interna y que se denominan CONTROLES TERCIARIOS.

II. ORGANIGRAMA DEL CONTROL INTERNO

En la estructura organizativa del control interno forman parte un amplio abanico de intervinientes con responsabilidades directas sobre su gestión. Dicha estructura es la siguiente:

- El Consejo de Administración y sus comisiones delegadas:
  - La Comisión de Auditoría y el Comité de Riesgos
- El Comité de Dirección
- Los Comités con responsabilidades directas sobre los riesgos: el Comité de Activos y Pasivos y el Comité de Cumplimiento y Riesgo Operacional.
- El departamento responsable del tercer nivel de control:
  - Auditoría Interna
- Los departamentos o Divisiones responsables del segundo nivel de control:
  - Control Interno
  - Riesgo Operacional
  - Cumplimiento Normativo
  - Seguridad Informática y riesgos tecnológicos
  - Organización
  - Seguridad Física
  - Riesgo de Mercado, Balance y Liquidez
  - Análisis y Control del Riesgo

- Los departamentos responsables del primer nivel de control (unidades de negocio y de soporte)



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 de integridad y valores éticos del más alto nivel, principios recogidos en el Código Ético de Cecabank.

COMISIÓN DE AUDITORÍA

Es la comisión delegada del Consejo responsable de supervisar la eficacia del control interno, la auditoría interna y los sistemas de gestión de riesgos llevados a cabo en la Organización, siguiendo las directrices marcadas por el Consejo de Administración y bajo el cumplimiento de la normativa establecida. La Comisión de Auditoría da cuenta de su actividad y del trabajo realizado al Consejo de Administración, y una vez al año elabora un informe sobre las actuaciones llevadas a cabo durante el ejercicio.

COMITÉ DE RIESGOS

Como comisión delegada del Consejo de Administración, el Comité de Riesgos tiene como función, conocer y analizar periódicamente la situación de solvencia y liquidez de la Entidad. Asesora al Consejo de Administración sobre la estrategia global y la tolerancia/apetito por el riesgo general de la entidad, y vigila la implantación de dicha estrategia. En particular, le corresponde analizar el informe de autoevaluación del capital y el informe con relevancia prudencial antes de ser elevados al Consejo.

COMITÉ DE DIRECCIÓN

Al Comité de Dirección le corresponden las siguientes funciones:

- 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.

COMITÉS ESPECIALIZADOS

I. Comité de Activos y Pasivos

El COAP tiene como misión la aprobación, información, seguimiento y control del riesgo de crédito, de mercado y riesgo estructural de balance (riesgo de tipo de interés y riesgo de liquidez).

Para el desarrollo de las funciones que tienen encomendadas, cuenta como unidades de apoyo con los siguientes comités: Comité de Riesgos, Comité Financiero, Comité de Nuevos Productos Financieros y Comité de Contingencia de Liquidez.

II. Comité de Cumplimiento y Riesgo Operacional

El Comité de Cumplimiento y Riesgo Operacional tiene como misión la aprobación, información, seguimiento y control del riesgo operacional, incluyendo 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, el Comité Fiscal y el Comité de Seguridad y Riesgos Tecnológicos.

El Comité de Prevención de Blanqueo de Capitales y Financiación del Terrorismo es el órgano de control interno de CECABANK responsable de la aplicación de las políticas y procedimientos de la Entidad en materia de PBCFT, y, en general, de lo previsto en el manual de PBCyFT.

El 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.

El Comité de Seguridad Global y Riesgos Tecnológicos tiene como funciones 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). También analiza los proyectos tecnológicos vinculados al plan estratégico que le eleve el Comité de seguimiento del plan estratégico y los aspectos relevantes relativos a la gestión de riesgos tecnológicos dentro de cada uno de los diferentes proyectos analizados en el Comité del Área Tecnológica. 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.

III. Comité de Seguimiento del Código Ético

Su función es velar por el buen funcionamiento del canal de comunicación establecido en materias relacionadas con el Código Ético.
Este Comité no reporta al Comité de Cumplimiento y Riesgo Operacional, pero le informa cuando del análisis y resolución de las denuncias se determine que se ha producido un evento de pérdida de riesgo operacional. También le realiza las propuestas que considere oportunas para su elevación al Comité de Dirección cuando por su naturaleza se considere necesario.

IV. Comité de Seguridad y Salud

El Comité de Seguridad y Salud 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.
El Comité está formado por los Delegados de Prevención, de una parte, y por el empresario y/o sus representantes en número igual al de los Delegados de Prevención, de la otra.

CONTROL DE TERCER NIVEL: AUDITORÍA INTERNA

Auditoría Interna es responsable de garantizar a la Alta Dirección que el perfil de riesgos real de la Entidad es el que ella ha definido.

Sus actuaciones se dirigen, por un lado, a verificar que la estructura de control de segundo nivel cumple con sus funciones, y por otro, a dar cumplimiento a los requerimientos de auditorías internas establecidas normativa o contractualmente.

Hay establecido un sistema continuo de "feed back" con las unidades de control de segundo nivel, que garantiza que los procedimientos de auditoría son sólidos y adecuados, y aseguran que las políticas, procedimientos y sistemas establecidos para la gestión e información de los riesgos se cumplen y son apropiadas.

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

CONTROL DE SEGUNDO NIVEL

Se realizan a través de unidades especializadas de control, ubicadas en el organigrama[1]:

I. En el Área de Riesgos:

Función de control y seguimiento de los riesgos financieros.

Se ocupa de la identificación y el control los riesgos de crédito, mercado y estructurales del balance, asegurando que el perfil de riesgos se encuentra dentro de los niveles de tolerancia establecidos por el Consejo y el COAP. También es responsable de que el Consejo, directamente o a través del Comité de Riesgos, reciba una visión global de todos los riesgos relevantes, facilitando la información necesaria para entender el perfil de riesgo de la entidad. Participa en la elaboración de la estrategia de riesgos de la entidad y es responsable de implantar el marco de gestión definido por el Consejo y la alta dirección, desarrollando las políticas y las metodologías de medición de los riesgos dentro de su ámbito y participando en la implantación de éstas en las herramientas de control, de forma que se mantengan actualizadas y se adecúen a la complejidad y a los niveles de los riesgos asumidos.

Está conformado por tres divisiones, de las cuales participan en los procesos de gestión de riesgos las siguientes:

- 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.
- Análisis y Control del Riesgo: responsable del análisis y control del riesgo de crédito asociado a la actividad de las distintas unidades de negocio. Este análisis es la base para la toma de decisiones en el Comité de Riesgos Financieros y en el COAP.

II. En el Área de de Servicios Asociativos y Auditoría

Función de control y seguimiento de los riesgos operativos vinculados con la seguridad física y las relaciones laborales

El Departamento de Seguridad 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

[1] *Función de control y seguimiento de los riesgos tecnológicos:* el control secundario sobre los riesgos tecnológicos –excepto el riesgo de seguridad física- se recoge en el marco de control de las tecnologías de la información

coordinación con los Cuerpos y Fuerzas de Seguridad del Estado, y entre otras funciones establece los procedimientos de control para mitigar el riesgo derivado, por un lado, de desastres naturales, incendios accidentales, tormentas e inundaciones ó amenazas ocasionadas por el hombre y por otro, sabotajes internos y externos deliberados que pueden poner en peligro los recursos de la Entidad. Su función principal es evaluar y controlar permanentemente la seguridad física de las instalaciones.

El Director de Seguridad es el interlocutor y enlace con la Administración, especialmente con las Fuerzas y Cuerpos de Seguridad, respecto de la función de seguridad integral de la Entidad, empresa o grupo empresarial que les tenga contratados, en relación con el cumplimiento normativo sobre gestión de todo tipo de riesgos.

El Servicio de Prevención de Riesgos Laborales, que depende jerárquicamente de la Dirección de Recursos, 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 a la consulta regular y periódica de las actuaciones de la empresa en materia de prevención de riesgos.

Función de control y seguimiento del riesgo de cumplimiento y del riesgo reputacional

Lo realiza Cumplimiento Normativo, que asume funciones de control en las siguientes áreas de actividad:

- Prevención del blanqueo de capitales y financiación del terrorismo,
- Cumplimiento de las normas del mercado de valores,
- Gobierno interno,
- Protección de datos de carácter personal,
- Riesgo reputacional,
- Grado de eficacia de los controles establecidos por Depositaría de Fondos en cumplimiento de las exigencias normativas,
- Sistema de prevención de los riesgos penales.

Función de control y seguimiento de los riesgos operativos-contables

Control Interno realiza actuaciones que permiten contrastar y verificar el grado de eficacia de los controles primarios operativo-contables previamente establecidos por cada departamento.

Función de gestión del riesgo operacional

La Unidad de Riesgo Operacional es responsable de los procesos de identificación, evaluación, seguimiento y control del riesgo operativo y también tiene asignada la elaboración de los mapas de riesgos de las distintas subcategorías del riesgo operacional (tecnológicos, de cumplimiento, penales) y del riesgo reputacional.

- El proceso de identificación se realiza a través del grupo de trabajo CIRO. Se constituye como un grupo de trabajo permanente cuya principal responsabilidad es la detección de los riesgos operacionales inherentes a los procesos, productos y sistemas de la Entidad. Su objetivo es la obtención de un inventario de riesgos operacionales así como la selección de los indicadores de riesgo y gestión para el adecuado seguimiento de los riesgos operacionales.

Su composición es la siguiente:

- Con carácter permanente: Un representante de Auditoría Interna, un representante de Organización, un representante de Control Interno y un representante de la Unidad de Riesgo Operacional.
- Con carácter transitorio y mientras se desarrolla el proceso de identificación de los riesgos de la unidad objeto de análisis, por la jefatura de cada departamento.

Para la gestión integral del riesgo operacional y su aplicación uniforme a todas las unidades de la Organización (de soporte y negocio), la Unidad de Riesgo Operacional cuenta con la colaboración de las Áreas y/o departamentos de soporte, y en especial el Departamento de Organización participa activamente en las funciones de análisis y modelización de procesos, con el fin de detectar los controles que se realizan en las Unidades.

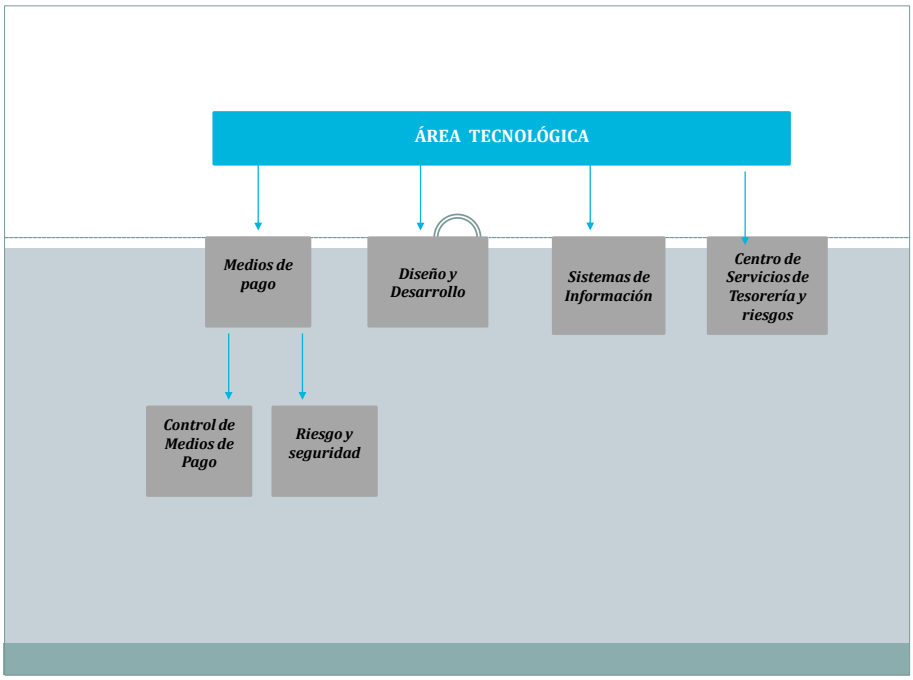
CONTROL DE PRIMER NIVEL

Son los controles establecidos y realizados en los propios departamentos. En ocasiones, existen unidades especializadas en su ejecución.

En particular, en el Área Tecnológica, la División de Medios de Pago cuenta con una unidad específica de control y coordinación y una Unidad de Seguridad y Riesgos, que realiza controles primarios sobre la seguridad del sistema de procesamiento.

Los proyectos de desarrollo que realizan la División de Diseño y Desarrollo y el Centro de Servicios de Tesorería y Riesgos, siguen la Metodología de Desarrollo Seguro, segregación de entornos y Protección de los Datos de Prueba, estableciendo controles primarios dirigidos a garantizar la realización de aplicaciones seguras y a mitigar el riesgo de cambios.

Sistemas de Información implementa los distintos elementos técnicos que conforman la infraestructura tecnológica y los modelo de datos, asociando roles y responsabilidades, clasificándolos de acuerdo a su sensibilidad y protegiéndolos para evitar modificaciones no autorizadas. Además protege los sistemas TIC de las amenazas de Internet y otras redes externas.

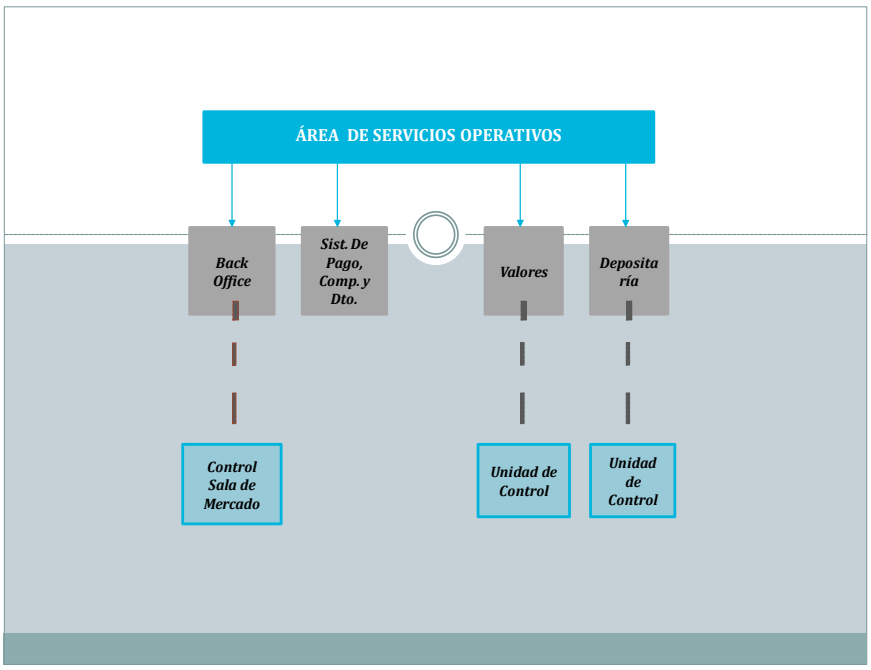


El Departamento de Back Office se sitúa en el Área de Operaciones para garantizar la independencia de la sala de Tesorería. Back Office, organizado por tipo de operaciones, realiza todo el proceso de seguimiento, confirmación y liquidación de operaciones. Además cuenta con una unidad especializada en el control de la Sala de Mercado, cuyas funciones principales son:

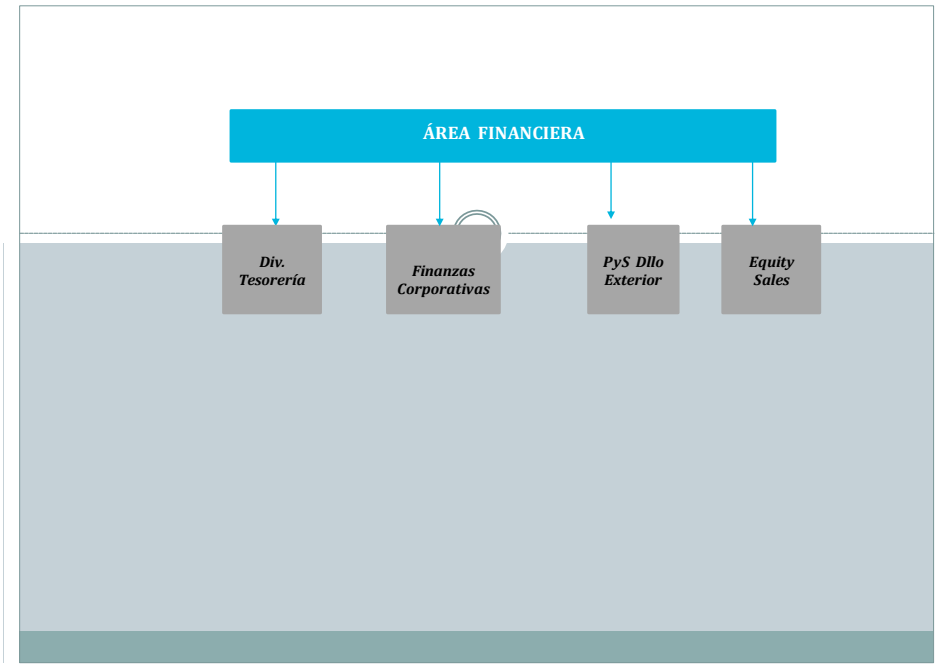
- Verificación y control de los procesos contables y operativos.
- Control de la facturación de brokers.
- Cuadres de posiciones y operaciones.
- Realización y seguimiento de presupuestos.

En el Área de Operaciones, también existe una segregación de las funciones de registro, depósito y administración de valores y las funciones de vigilancia y supervisión de las gestoras en los fondos depositados en la Entidad, al ser realizadas, respectivamente, por los departamentos de Valores y Depositaría de Fondos. Cada uno de estos departamentos cuenta con unidades de control específicas. Además el departamento de Valores está identificado como área separada al desarrollar actividades relacionadas con el mercado de valores, y por ello mantiene la debida separación con Tesorería y Mercado de Capitales, ubicados en el Área Financiera, con el objeto de impedir el flujo de información privilegiada y evitar conflictos de interés.

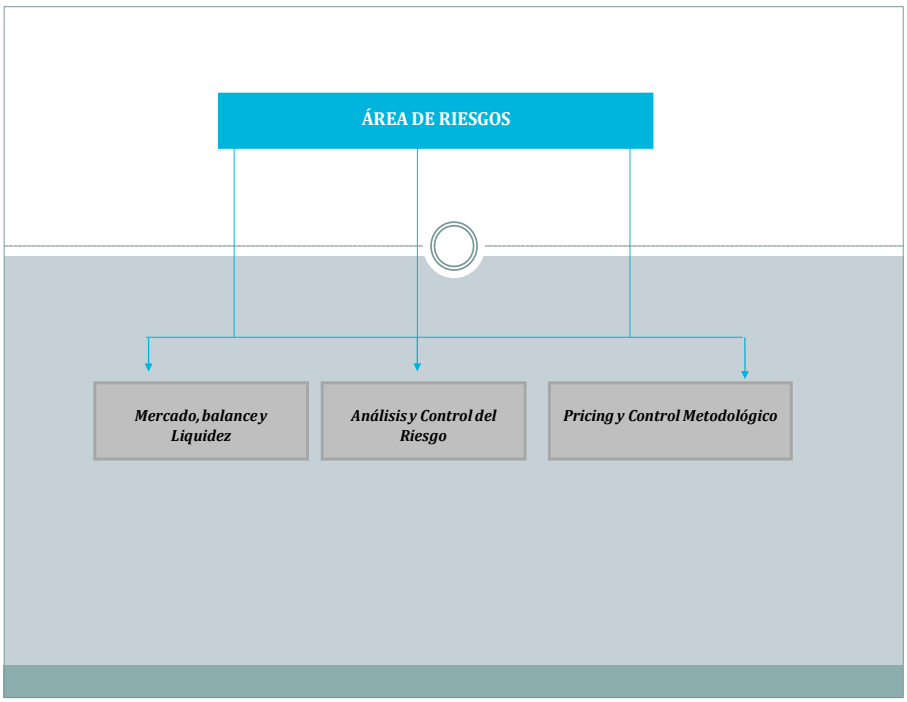
Todos los departamentos tienen perfectamente definidos los controles primarios que efectúan en sus procedimientos. En el Manual de procedimientos de la Entidad, se encuentran documentados los procesos y actividades que realizan y su relación de controles primarios.



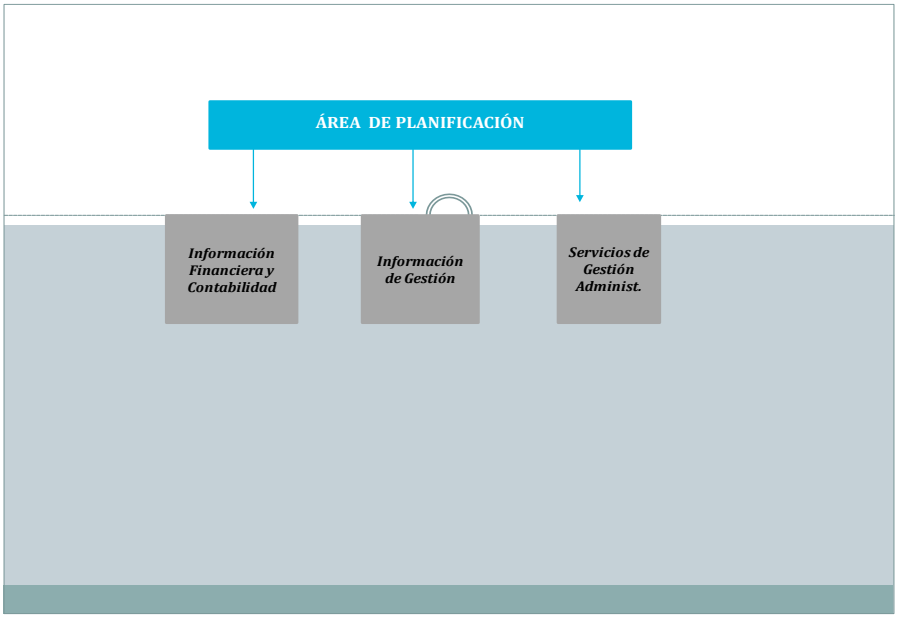
El Área Financiera se compone de cuatro Divisiones –Tesorería, Equity Sales, Finanzas Corporativas y Productos y Servicios-Desarrollo Exterior. Las tres primeras están identificadas como áreas separadas y por ello mantienen entre sí la debida separación con el objeto de impedir el flujo de información privilegiada y evitar conflictos de interés.



El Área de Riesgos, a efectos de garantizar una adecuada segregación de funciones, cuenta con una unidad encargada de valorar los productos ilíquidos del mercado, Pricing y Control Metodológico. Facilita estos precios a la División Financiera para la valoración de sus carteras y participa activamente con Depositaría de Fondos en la supervisión de los procedimientos de valoración utilizados por las gestoras en las posiciones de cartera.



El Área de Planificación es responsable de la elaboración de la información financiera. Define las pautas contables a seguir para garantizar la exactitud y seguridad en el registro y contabilización de operaciones y define los circuitos contables de cada nueva operativa. Además coordina y centraliza la elaboración de los presupuestos de la entidad y la contabilización y el pago de todas las facturaciones por servicios, inversiones y aprovisionamiento.



PROTOCOLO DEL EURIBOR.

El protocolo para la contribución a la fijación del Euribor, aprobado por el Consejo de Administración en Noviembre de 2013, establece el siguiente sistema de control con el fin de garantizar la integridad del índice y un entorno de control y revisión independiente del envío de las aportaciones:

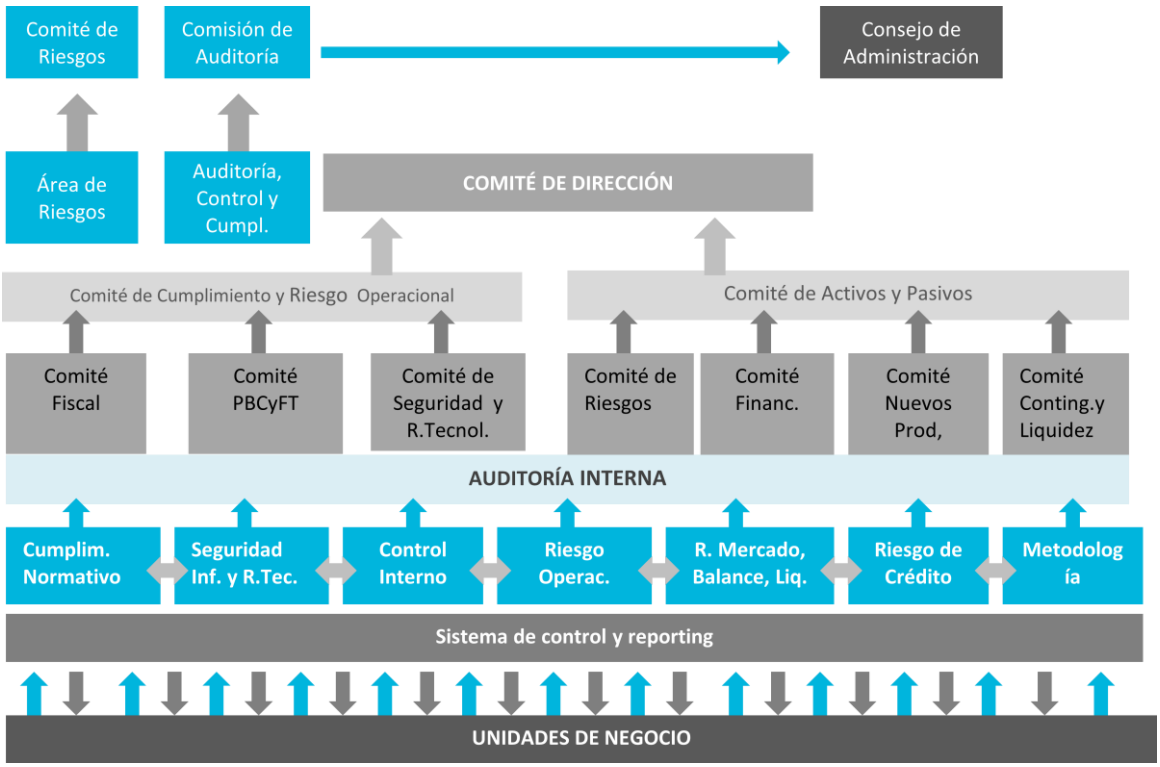
Control primario: elaboración del índice
Para garantizar la independencia y evitar conflictos de interés, la División de Pricing y control metodológico, ubicada en el Área de riesgos, es la responsable de realizar directamente la aportación de referencias para la formación del euribor. Queda separada, por tanto, de la Tesorería la responsabilidad relativa a su construcción.
En el citado protocolo se mencionan dos figuras, el proveedor y el verificador, que participan en la elaboración y que en ningún caso recaen en la misma persona.

Control secundario: controles sobre el envío de las referencias
El Departamento de Control Interno, ubicado en el Área de Servicios Asociativos y Auditoría, es el responsable de comprobar las aportaciones y analizar la razonabilidad de los envíos en relación a las condiciones de mercado, así como la información o datos de referencia usados en el cálculo por el proveedor.

Control terciario: supervisión anual
Auditoría Interna supervisa con carácter anual la actividad de las unidades anteriormente indicadas. Adicionalmente un Auditor Externo revisará el cumplimiento del protocolo con carácter anual.

III. RELACIONES ENTRE LAS UNIDADES EN EL SISTEMA DE CONTROL.

A continuación se adjunta un cuadro en el que gráficamente se aprecian las relaciones de cooperación entre las unidades de control primario, secundario y terciario, que aseguran una adecuada coordinación en la gestión de los distintos riesgos. La estructura de comités garantiza una perfecta integración, así como una estructura de reporting que asegura la difusión de la información en todos los niveles de la Organización:



V. NORMATIVA COMPLEMENTARIA DEL SISTEMA DE CONTROL

En la Entidad existe un procedimiento de emisión de Normas Internas que garantiza su divulgación y cumplimiento. Estas Normas establecen criterios específicos que complementan el sistema interno de control, destacando:

- CUMPLIMIENTO Y CONTROL DE LA NORMATIVA FISCAL. Su objetivo es velar por la existencia de sistemas de control que permitan un adecuado seguimiento del riesgo derivado de la fiscalidad de las operaciones y actividades.
- JUSTIFICACIÓN DE GASTOS DE REPRESENTACIÓN. Establece los principios básicos que deben seguir los empleados a la hora de realizar este tipo de gastos, determinando las pautas de justificación y liquidación.
- TARJETAS DE EMPRESA EMITIDAS POR Cecabank. Regula la solicitud, autorización, emisión, contabilización y control de las tarjetas de empresa emitidas por Cecabank para el pago de gastos.
- REGIMEN DE VIAJES. Regula el régimen a seguir en los desplazamientos a clientes, convenciones, reuniones, foros u otros eventos, tanto nacionales como Internacionales.
- PREVENCIÓN DEL BLANQUEO DE CAPITALES Y LA FINANCIACIÓN DEL TERRORISMO. Su finalidad es aplicar en la Entidad la normativa externa vigente relativa a la prevención del blanqueo de capitales, el bloqueo de capitales y la prevención de la financiación del terrorismo.
- REGLAS PARA LA PREVENCIÓN DEL ABUSO DEL MERCADO DE VALORES. El objeto de esta norma interna es facilitar a todas las personas que prestan sus servicios en Cecabank el conocimiento de las obligaciones.
- DECISIONES Y ACCIONES A REALIZAR EN MATERIA DE DEFENSA DE LA COMPETENCIA. Determinar las actuaciones a realizar en Cecabank para llevar a cabo la correcta aplicación y supervisión de sus prácticas en materia de derecho de la competencia.
- DOCUMENTACIÓN DE OPERACIONES CON VINCULADAS Y CON RESIDENTES EN PARAÍSOS FISCALES. El objeto de esta norma es describir las actuaciones que deben seguir los diferentes departamentos de la Entidad para la identificación, justificación y elaboración de la documentación exigida por la normativa del Impuesto de Sociedades que, por imperativo legal, tiene que estar a disposición de la Administración Tributaria.
- FORMALIZACIÓN Y CUSTODIA DE CONTRATOS. Esta Norma establece el procedimiento a seguir para formalizar y custodiar todo documento que genere para Cecabank algún tipo de compromiso, tanto económico como de cualquier otra naturaleza.
- ANALISIS DE CUENTAS TRANSITORIAS ALEATORIO - A.C.T.A. Su objetivo es mejorar el control y la seguridad de los movimientos de las cuentas transitorias.
- TRATAMIENTO DE IMPORTES A DISPOSICION DE TERCEROS CON ANTIGÜEDAD PREESTABLECIDA. Establece las normas básicas de funcionamiento que permitan asegurar la adecuada aplicación de estos fondos a disposición de terceros, para garantizar su seguridad y correcta aplicación.
- ASIENTOS MANUALES - PROCEDIMIENTO DE REALIZACIÓN. Tiene como objetivo mejorar el control y seguridad de los apuntes contables que no son originados de manera automatizada por aplicaciones o sistemas, mediante el establecimiento de las reglas de actuación y la regulación del procedimiento a seguir en su elaboración, formalización y firma.
- DOCUMENTO DE SEGURIDAD DE DATOS DE CARÁCTER PERSONAL. Su finalidad es cumplir lo establecido en la LOPD.
- COLABORACIÓN PARA LA SEGURIDAD DE LOS DATOS DE CARÁCTER PERSONAL SUJETOS A LA LOPD. Establece la colaboración que las unidades de la Entidad deberán proporcionar para el cumplimiento de la seguridad de los datos.
- GESTIÓN DE SOPORTES. Establece las medidas de seguridad necesarias para controlar y proteger los activos de soporte que contengan información propia o de cualquiera de sus clientes.
- DESTRUCCIÓN DE DOCUMENTOS Y SOPORTES EXTRAIBLES. Su objetivo es asegurar la destrucción segura y controlada de los soportes físicos (documentos y

soportes extraíbles) con información confidencial de nivel medio o superior propiedad de la Entidad o sus clientes.

- GESTIÓN DE ACCESOS A BASES DE DATOS. Establece las medidas de seguridad necesarias para controlar y administrar los accesos a las bases de datos de la Entidad.
- GESTIÓN DE ACCESOS A FICHEROS DE DATOS. Establece las obligaciones en materia de seguridad sobre los ficheros de datos en producción existentes en la Entidad.
- GESTIÓN DE LOS ACCESOS A LAS APLICACIONES. Establece las responsabilidades en materia de seguridad de los accesos de las aplicaciones utilizadas en la Entidad.
- COPIAS DE SEGURIDAD DE ACTIVOS LÓGICOS. Establece las directrices para la realización y mantenimiento de copias de seguridad de la información de la Entidad, así como los mecanismos de restauración.
- CRIPTOGRAFÍA. Define las directrices de utilización de controles criptográficos sobre los activos de información y las comunicaciones de la Entidad, los requisitos de seguridad en el cifrado y los mecanismos de gestión de claves criptográficas.
- SEGREGACIÓN DE FUNCIONES EN EL USO DE APLICACIONES Y SISTEMAS. Su objetivo es el establecimiento de las directrices para garantizar un adecuado nivel de control sobre el acceso a los activos de información de la Entidad a través de aplicaciones y sistemas informáticos, mediante la aplicación de una adecuada segregación de funciones.
- SEGREGACIÓN DE ENTORNOS. Su finalidad es definir la estructura de entornos informáticos y las medidas de seguridad a implantar en los mismos para garantizar la seguridad de la información.
- GESTIÓN DE USUARIOS DE SISTEMAS. Tiene por objeto definir las pautas para gestionar de una forma segura los usuarios y sus identificadores así como los derechos de acceso a los sistemas de la Entidad.
- CONTROL DE CAMBIOS EN SISTEMAS. Su objetivo es establecer las directrices para garantizar que los procesos de realización de cambios en sistemas en la Entidad se llevan a cabo de manera fiable y segura.
- CONTROL DE CAMBIOS EN APLICACIONES. Su objetivo es garantizar que los procesos de gestión de cambios en aplicaciones desarrolladas internamente o por terceros utilizadas para el tratamiento y/o almacenamiento de activos de información en la Entidad, se llevan a cabo de manera fiable y segura.
- MONITORIZACIÓN DE SISTEMAS. Establece las directrices necesarias para llevar a cabo la monitorización y registro de eventos de seguridad que permitan detectar posibles desviaciones en las medidas de seguridad implantadas en los sistemas.
- GESTIÓN DE INCIDENCIAS DE SEGURIDAD EN SISTEMAS. Establece las directrices para la gestión de eventos e incidencias de seguridad que tengan lugar en los sistemas de información de la Entidad, así como el establecimiento de mecanismos de detección y corrección de vulnerabilidades de seguridad.
- PROTECCIÓN DE LAS REDES. Su objetivo es el establecimiento de las medidas técnicas relativas a la administración, configuración y supervisión de los elementos de comunicación de la Entidad así como los requisitos que deben cumplir las comunicaciones internas y externas para garantizar la seguridad e integridad de la información en tránsito a través de dichas redes.
- INFORMÁTICA MÓVIL Y ACCESO REMOTO A SISTEMAS. Establece los mecanismos y las medidas de seguridad a implantar para garantizar la seguridad de la información mediante los accesos remotos a los sistemas de la Entidad (empleo de ordenadores o dispositivos móviles).
- PROTECCIÓN CONTRA EL SOFTWARE MALICISOSO. Tiene por objetivo el establecimiento de las medidas de seguridad necesarias para garantizar la integridad y confidencialidad del software y de los activos de información de la Entidad y evitar el daño por software malicioso.
- DESARROLLO SEGURO DE APLICACIONES. Su finalidad es el establecimiento de las directrices y medidas de seguridad a seguir en todo proyecto de desarrollo de aplicaciones, tanto realizado internamente como por terceros, para garantizar la realización de aplicaciones seguras.
- DESARROLLO DE APLICACIONES SEGURAS. Establece las directrices a seguir en el desarrollo interno de aplicaciones de forma que resulten seguras en su utilización.

- POLÍTICA DE SEGURIDAD de Cecabank. Su objetivo es comunicar a la Entidad la Política de Seguridad, con el fin de asignar las responsabilidades correspondientes y exigir su cumplimiento.
- PLAN DE CONTINUIDAD GLOBAL DE Cecabank. Su objetivo es dar vigencia y comunicar a toda la Entidad el Plan de Continuidad, con el fin de asignar las responsabilidades correspondientes y exigir su cumplimiento.
- GESTIÓN DE ACTIVOS. Su objetivo es definir los tipos de activos de la Entidad de forma que se puedan aplicar sobre los mismos una protección adecuada y mantener su inventario.
- RELACIONES CON PROVEEDORES. Garantizar la seguridad en el acceso y/o tratamiento por parte de proveedores a los activos de información propiedad de la Entidad o de sus clientes.
- RELACIONES CON CLIENTES. Garantizar la seguridad en el acceso y/o tratamiento por parte de los clientes de los activos de información de su propiedad o de la Entidad.
- SEGURIDAD DE LAS APLICACIONES Y SERVICIOS INFORMÁTICOS PROPORCIONADOS POR PROVEEDORES. Establece las directrices en materia de seguridad que deberán seguirse en el proceso de adquisición o contratación de aplicaciones y/o servicios informáticos.
- CREACIÓN DE PISTAS DE AUDITORÍA. Desarrolla las Políticas de Seguridad en lo que se refiere al contenido de las pistas de auditoría a mantener por las aplicaciones de la Entidad.
- VALORACIÓN, CONTRATACIÓN Y GESTIÓN DE PÓLIZAS DE SEGURO. Su objeto es establecer los criterios generales y las directrices que se deberán seguir en el proceso de identificación, valoración y decisión sobre los riesgos susceptibles de ser asegurados, de manera que se garantice que se conocen y evalúan adecuadamente los riesgos de cualquier activo o servicio relacionado con el negocio susceptible de cubrirse por una póliza de seguro.
- SELECCIÓN Y EVALUACIÓN DE PROVEEDORES. Establece las directrices a considerar en el proceso de selección de un proveedor y su seguimiento, cuando esté catalogado como proveedor crítico.
- CANAL DE SEGUIMIENTO DEL CÓDIGO ÉTICO (CANAL ÉTICO). Establece las características del Canal de Seguimiento del Código Ético (en adelante Canal Ético), su funcionamiento y las implicaciones que conlleva, así como establecer la composición y funciones el Comité de Seguimiento del Código Ético.
- OTORGAMIENTO DE PODERES Y PROCESOS DE EJECUCIÓN. Regula las facultades y poderes en la confección y ejecución del presupuesto, formalización y custodia de contratos y procedimientos para compras, realización de gastos y adquisición de recursos.
- RECOGIDA Y CLASIFICACIÓN DE EVENTOS DE PÉRDIDA DE RIESGO OPERACIONAL. Su objetivo es establecer el procedimiento de registro de las pérdidas operacionales, las líneas maestras para abordar el análisis de la clasificación de los eventos, y determinar el alcance de pérdida por riesgo operacional, con el fin de unificar criterios dentro de la Entidad.
- EL CÓDIGO ÉTICO. 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.
- EL MANUAL DE PREVENCIÓN DE RIESGOS PENALES. Sistematiza los controles existentes en Cecabank y aquellos que, a raíz de la revisión realizada como consecuencia de la reforma del Código Penal, se han introducido para cumplir con la finalidad de prevenir y mitigar la comisión de delitos en las distintas áreas de la Entidad.
- EL PLAN DE PREVENCIÓN DE RIESGOS LABORALES. Recoge establece y formaliza la política de prevención de una empresa, recoge la normativa, la reglamentación y los procedimientos operativos, definiendo los objetivos de la prevención y la asignación de responsabilidades y funciones a los distintos niveles jerárquicos en lo que se refiere a la Prevención de Riesgos Laborales.
- MANUAL DE AUTOPROTECCION: Conforme a la normativa vigente en materia de protección civil, y tiene por objeto la organización de los medios humanos y materiales disponibles prevenir el riesgo de incendio o de cualquier otro equivalente, y garantizar la

evacuación y la intervención inmediata, haciendo cumplir la normativa vigente sobre seguridad, facilitar las inspecciones de los Servicios de Administración y preparar la posible intervención de ayudas exteriores en caso de emergencia.

- POLITICA DE CONTROL DE ACCESO: Define el sistema de control de acceso basado en los terminales de fichajes, accesos y tornos situados en todos y cada unos de los edificios de la Entidad.
- MANUAL DE PREVENCION DE RIESGOS LABORALES: tiene por objeto la integración de la Prevención de Riesgos Laborales en el sistema general de gestión de la Entidad, tanto en el conjunto de sus actividades como en todos los niveles jerárquicos de ésta.
- USO RESPONSABLE DE LA INFORMACIÓN Y LOS RECURSOS INFORMÁTICOS: tiene por objeto definir las obligaciones y restricciones, desde el punto de vista de la Seguridad de la información, en el uso y tratamiento de la información propiedad de la Entidad o de sus clientes o de terceros, en el puesto de trabajo y en el uso de los recursos informáticos de Cecabank, para mitigar los riesgos asociados a un uso indebido de la información a la Entidad.
- USO DE SERVICIOS DE ALMACENAMIENTO EN LA NUBE: su finalidad es definir los requisitos de seguridad y mitigar los riesgos derivados del uso de servicios de almacenamiento en la nube.
- GUÍA DE SEGURIDAD DE LA INFORMACIÓN PARA EL EMPLEADO