Área de Servicios Asociativos, Control y Recursos

Marco general del control

Mayo de 2019

cecabank

Índice

Características del sistema de Control Interno

01.Características del sistema de control interno

La independencia, la especialización y la gestión integral caracterizan el sistema de control interno de Cecabank.

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. Es una estructura alineada a la naturaleza de la estrategia de Cecabank, con líneas de responsabilidad bien definidas, transparentes y coherentes.

Se caracteriza principalmente:

A. Por ser de 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.
B. 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, asegurando la adecuada coordinación en la gestión de los distintos riesgos, una visión integral y el cumplimiento de la estrategia de riesgos definida por el Consejo de Administración.
C. 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.
D. 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.

Organigrama del Control Interno

02. 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:

A. El Consejo de Administración y sus comisiones delegadas:
   - La Comisión de Auditoría y el Comité de Riesgos

B. El Comité de Dirección

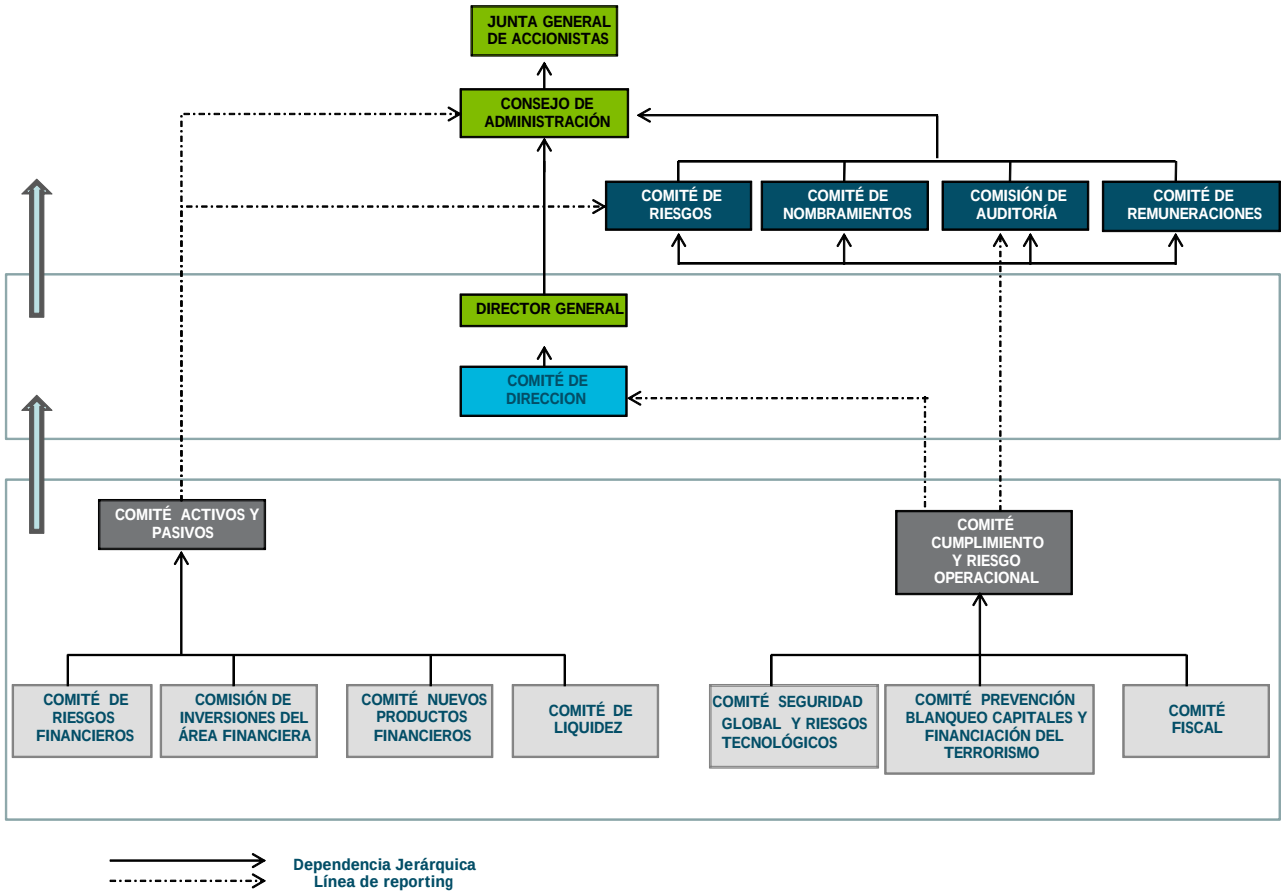
C. Los Comités con responsabilidades directas sobre los riesgos: el Comité de Activos y Pasivos y el Comité de Cumplimiento y Riesgo Operacional.

D. El departamento responsable del tercer nivel de control:
   - Auditoría Interna

E. Los departamentos o Divisiones responsables del segundo nivel de control:
   - Control Global de Riesgos
   - Control Interno
   - Riesgo Operacional
   - Cumplimiento Normativo
   - Seguridad Informática
   - Organización
   - Seguridad y Prevención de Riesgos Laborales

F. Los departamentos responsables del primer nivel de control:
   - Las unidades de negocio y de soporte
   - Riesgo de Mercado, Balance y Liquidez
   - Análisis y Control del Riesgo.

2.A. 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.

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. Asimismo supervisa el cumplimiento de los Códigos de conducta de la entidad, así como el funcionamiento del canal interno de denuncias de la entidad.

La dependencia funcional de Auditoría Interna de la Comisión de Auditoría, salvaguarda la independencia de la función de control de tercer nivel.

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 liquidez y el informe con relevancia prudencial antes de ser elevados al Consejo.

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.

Comités especializados

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, Comité D3 y Comité de Contingencia de Liquidez.

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.

Comité de Seguimiento del Código 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.

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.

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.

02.B. Estructura organizativa interna

Control de tercer nivel: Auditoría Interna

Auditoría Interna es responsable de garantizar a los Órganos de Gobierno y a la Alta Dirección que el perfil de riesgos real de la Entidad es el definido por el Consejo

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

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 a revisión externa (auditorías externas) por terceras partes independientes. Sus resultados y conclusiones se informan 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 en el Área de Servicios Asociativos, Control y Recursos

A. Función de control global de riesgos

Corresponde a la Unidad de Control Global de Riesgos ofrecer una visión integral de todos los riesgos al Consejo de Administración, directamente o a través del Comité de Riesgos, y velar por el adecuado cumplimiento de la estrategia de riesgos. Sus principales funciones son:

Funciones relacionadas con el apetito al riesgo:

- Colaborar en el diseño de la estrategia global de riesgos y el Marco de Tolerancia al Riesgo, así como en todas las decisiones importantes sobre gestión de riesgos, realizando las propuestas que se estimen necesarias para garantizar que abarca todos los productos, servicios, cambios normativos o nuevos riesgos.
- Realizar un seguimiento continuo de la situación y evolución de los riesgos financieros y no financieros de la entidad, garantizando el alineamiento de las decisiones de riesgo con el Marco de Tolerancia al Riesgo.

Funciones relacionadas con el marco de control:

- Verificar la adecuación del marco de controles primarios para todos los riesgos de la entidad, directamente o en cooperación con otras unidades de control secundario. En particular, velará por que se cuente con procesos efectivos, robustos y sostenibles de gestión y control de los riesgos.
- Participar en el proceso de revisión anual de los manuales de políticas y

procedimientos de las unidades de gestión de riesgos, verificando su correcta adaptación a los nuevos productos, servicios, límites, metodologías o normativas. Analizar los cambios que pudieran provocar en los sistemas internos de control.
- Coordinar la elaboración de los ejercicios de estrés.

Funciones relacionadas con control de riesgos:

- Validar la metodología de medición y análisis de todos los riesgos, incluidas sus herramientas de medición, que deberán estar actualizadas y alineadas con las mejores prácticas de mercado y permitir una evaluación adecuada de los diferentes factores de riesgos así como el riesgo global para el conjunto de las exposiciones (con la colaboración de terceros externos en el caso de que se estime necesario).
- Elaborar y efectuar seguimiento de los indicadores financieros y no financieros claves a fin de vigilar los cambios en la situación financiera y en el perfil de riesgo de la entidad y alertar sobre posibles situaciones de estrés.
- Valorar los incumplimientos de las estrategias y límites de riesgo y proponer medidas correctoras en el ámbito de los controles primarios.

Funciones relacionadas con el reporting:

- Coordinación de la elaboración de documentos legalmente requeridos ante supervisores y mercado (IACL, IRP, Plan de Recuperación).
- Informar al Comité de Riesgos sobre el cumplimiento de los límites de tolerancia al riesgo, de la evolución de las métricas que les dan soporte y alertar de posibles situaciones de estrés.

B. 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.

Para la gestión integral del riesgo operacional y su aplicación uniforme a todas las unidades de la entidad (de soporte y negocio), la Unidad de Riesgo Operacional cuenta con la colaboración de las Áreas y/o departamentos de soporte. 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.

Dentro del ámbito del riesgo operacional existen categorías específicas de riesgo que cuentan con mecanismos de seguimiento y gestión diferenciados:

- Riesgos tecnológicos. Esta función está definida en el Marco de Control de las Tecnologías de la Información. El Departamento de Seguridad Informática es la unidad de control secundario en este ámbito. En el caso específico del riesgo de continuidad de negocio, el Departamento de Organización asume también tareas de control y supervisión.

- Riesgos operativo-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.

- Riesgos 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 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 o 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.

- Riesgos de cumplimiento y reputacional. Cumplimiento Normativo 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.

Control de primer nivel

- Función de control de los riesgos financieros.

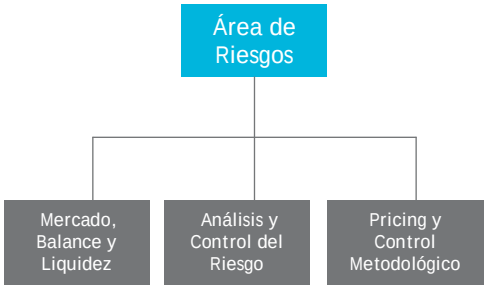
Sin perjuicio de las funciones y actividades de control secundario que le corresponden, el Área de Riesgos comparte con las unidades de negocio funciones de control primario. En particular, se ocupa de la identificación, evaluación, medición y el control los riesgos de crédito, mercado y estructurales 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 financieros, facilitando la información necesaria para entender el perfil de riesgo de la entidad.

El Área de Riesgos 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.

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. Sus precios se utilizan para la valoración contable de los distintos instrumentos financieros contratados por la División Financiera y Equity Sales. Además participa activamente con Depositaría de Fondos en la supervisión de los procedimientos de valoración utilizados por las gestoras en las posiciones de cartera.



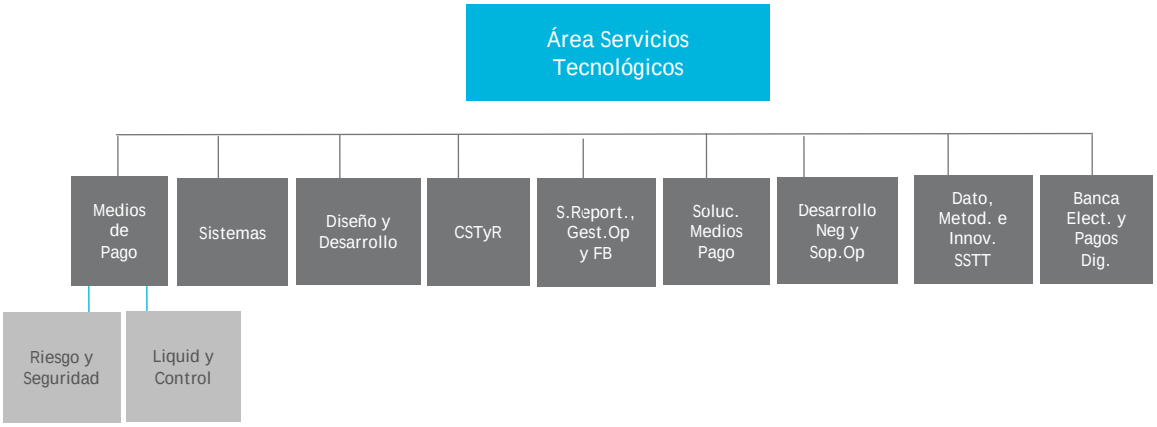
- Función de control de Riesgo operacional.

El proceso de identificación de los riesgos operacionales 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, representantes de las siguientes unidades: Auditoría Interna, Organización, Control Interno, Riesgo Operacional y Seguridad Informática.
- Con carácter transitorio y mientras se desarrolla el proceso de identificación de los riesgos de la unidad objeto de análisis, por la dirección de cada departamento.

A. Área de Servicios Tecnológicos

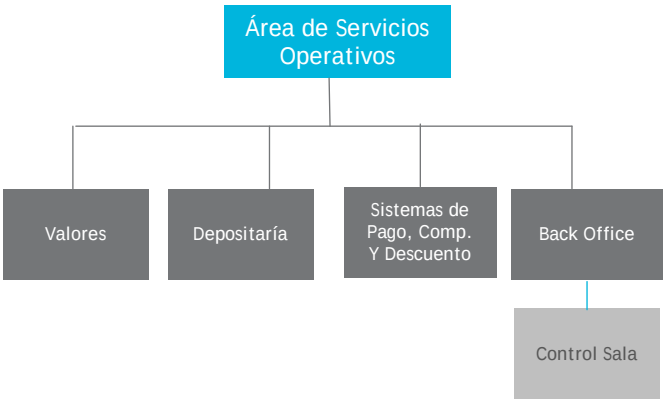


La División de Medios de Pago cuenta con una unidad específica de control y coordinación y una Unidad de Seguridad y Riesgos, que realiza controles primarios sobre la seguridad del sistema de procesamiento.

Los proyectos de desarrollo que realizan las distintas Divisiones 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 cambio.

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.

B. Área de Servicios Operativos



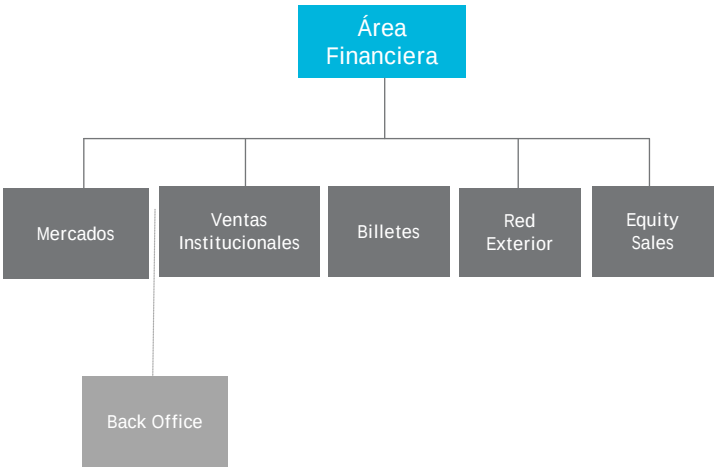
El Departamento de Back Office, organizado por tipo de operaciones, realiza todo el proceso de seguimiento, confirmación y liquidación de operaciones. Además cuenta con una unidad especializada en el control de la Sala de Mercado, cuyas funciones principales son:

- 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 Servicios Operativos 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 las Divisiones que realizan actividades de mercado del 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.

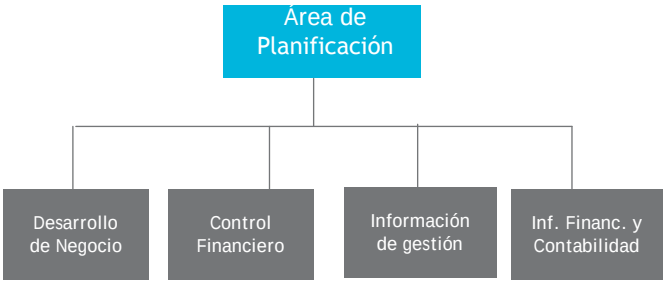
C. Área Financiera



Las divisiones identificadas como áreas separadas mantienen entre sí la debida separación con el objeto de impedir el flujo de información privilegiada y evitar conflictos de interés.

Back Office constituye la unidad de control primario de Tesorería y Equity Sales, estando ubicado en el Área de Servicios Operativos.

D. Área de Planificación

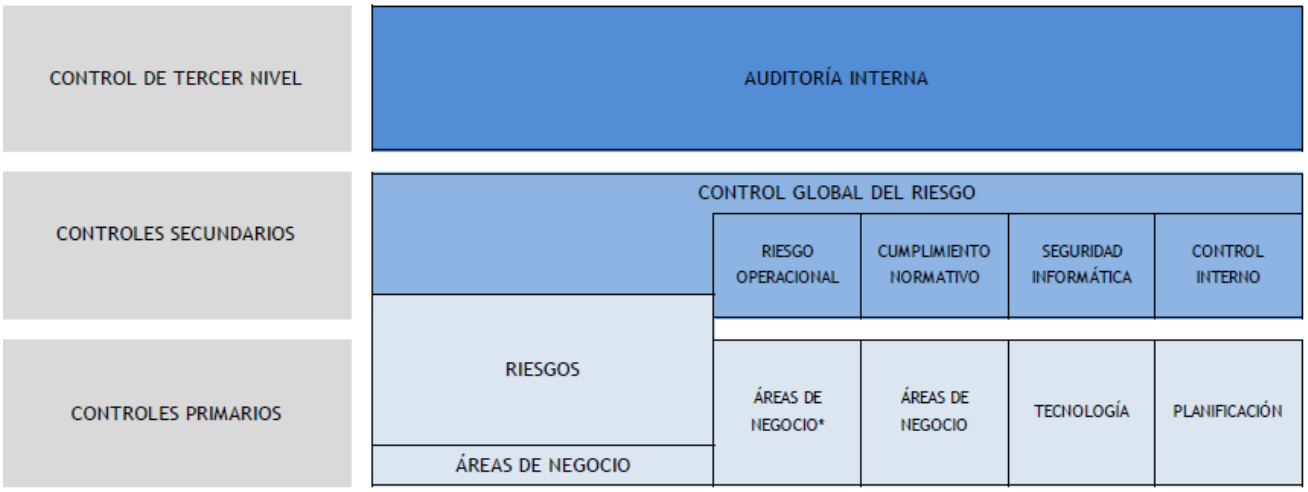


Es responsable de la elaboración de la información financiera. Define las pautas contables a seguir para garantizar la exactitud y seguridad en el registro y contabilización de operaciones y define los circuitos contables de cada nueva operativa. Además coordina y centraliza la elaboración de los presupuestos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

Relaciones entre las unidades en el sistema de control

03. 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 y la estructura de reporting, representada en el epígrafe 02.A., asegura la difusión de la información en todos los niveles de la Organización:



* Con la colaboración de la Unidad de Riesgo Operacional a través del grupo CIRO (ver apartado de controles primarios)

Normativa complementaria del sistema del control

04. Normativa complementaria del sistema del 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:

1. 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.

2. 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.

3. 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.

4. REGIMEN DE VIAJES. Regula el régimen a seguir en los desplazamientos a clientes, convenciones, reuniones, foros u otros eventos, tanto nacionales como Internacionales.

5. 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.

6. 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.

7. 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.

8. 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.

9. 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.

10. 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.

11. 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.

12. 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.

13. DOCUMENTO DE SEGURIDAD. Su finalidad es establecer las medidas de seguridad para la protección de la información de Cecabank.

14. 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.

15. 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.

16. 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.

17. 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.

18. GESTIÓN DE LOS ACCESOS A LAS APLICACIONES. Establece las responsabilidades en materia de seguridad de los accesos de las aplicaciones utilizadas en la Entidad.

19. 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.

20. 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.

21. 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.

22. 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.

23. 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.

24. 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.

25. 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.

26. 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.

27. 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.

28. 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.

29. 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).

30. 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.

31. 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.

32. DESARROLLO DE APLICACIONES SEGURAS. Establece las directrices a seguir en el desarrollo interno de aplicaciones de forma que resulten seguras en su utilización.

33. 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.

34. 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.

35. 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.

36. 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.

37. 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.

38. 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.

39. 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.

40. 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.

41. 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.

42. CANAL DE SEGUIMIENTO DEL CÓDIGO DE CONDUCTA CORPORATIVA. Establece las características del Canal de Seguimiento del Código de Conducta Corporativa, su funcionamiento y las implicaciones que conlleva, así como establecer la composición y funciones el Comité de Seguimiento del Código de Conducta Corporativa..

43. 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.

44. 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.

45. 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.

46. POLÍTICA DE CUMPLIMIENTO PENAL Y DOCUMENTO VERTEBRADOR. Desarrolla lo establecido en el Código de Conducta Corporativa de Cecabank, definiendo un marco de principios en materia de Cumplimiento Penal. El documento vertebrador sistematiza el sistema de gobernanza del riesgo penal, determinando los roles y responsabilidades que participan en la prevención y mitigación de la comisión de delitos en las distintas áreas de la Entidad.

47. 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.

48. 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.

49. 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.

50. 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.

51. 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.

52. 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.

53. GUÍA DE SEGURIDAD DE LA INFORMACIÓN PARA EL EMPLEADO

54. USO DE SERVICIOS DE ALMACENAMIENTO EN LA NUBE, cuyo objetivo es definir los requisitos de seguridad y mitigar los riesgos derivados del uso de servicios de almacenamiento en la nube.

55. REDES WIFI INTERNAS, que establece las directrices de seguridad para la utilización de las redes WIFI internas de Cecabank

56. CERTIFICADOS ELECTRÓNICOS DE COMPONENTES, cuyo objeto garantizar la correcta gestión y uso de los Certificados electrónicos de componentes utilizados en Cecabank.

57. EMISIÓN DE FACTURAS, cuyo objeto es establecer los criterios generales y las directrices que deberán seguirse en el proceso de emisión de facturas correspondientes al cobro de servicios prestados por la Entidad a sus clientes.

58. FORMALIZACIÓN DE CONTRATOS CON CLIENTES: establece los criterios generales y las directrices que deberán seguirse en el proceso de formalización de todo documento que genere para Cecabank algún tipo de compromiso con clientes, tanto económico como de cualquier otra naturaleza, para la prestación de servicios y productos por parte de Cecabank.

59. TRAMITACIÓN DE FACTURAS DE PROVEEDORES: establece el proceso de recepción, aprobación y pago de las facturas recibidas en la Entidad, procedentes de proveedores por la adquisición de elementos materiales, inmateriales, contratación de servicios y adquisición de recursos.

60. GESTIÓN DE CONTRATOS DE SERVICIOS Y PERSONAL SUBCONTRATADO: fija los criterios generales y las directrices que deberán seguirse en aquellos contratos con proveedores (en adelante también “contratistas”) con el fin de minimizar el riesgo de cesión ilegal de trabajadores a la empresa principal.

61. EJECUCIÓN DE GASTOS: establece el proceso general y las directrices que deberán seguirse para la formalización de compromisos con proveedores y ejecución de compras, realización de gastos y adquisición de recursos (de

cualquier tipo y por cualquier importe, definiendo las funciones y responsabilidades de todos los intervinientes del proceso.

62. POLÍTICA ENERGÉTICA: recoge el compromiso de la entidad con sociedad, al establecer un sistema de gestión eficiente de la energía consumida en los edificios donde se presta la actividad bancaria.

63. POLITICA DE EXTERNALIZACIÓN 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.

64. POLÍTICA DE TRANSPARENCIA: codifica las políticas internas de Cecabank en materia de divulgación externa de la información exigida por el supervisor, en los distintos ámbitos normativos y contempla, entre otros aspectos, el contenido de la información a publicar, la frecuencia y lugar de la publicación y la verificación de la información.

65. POLÍTICA DE PROTECCIÓN DE DATOS DE LA DIVISIÓN DE MEDIOS DE PAGO**:** su objeto es garantizar el cumplimiento de la legislación vigente y los estándares y normas de la industria en los distintos ámbitos de funcionamiento de las actividades realizadas por la División de Medios de Pago, así como la normativa interna de la entidad.

66. POLÍTICA DE SEGURIDAD PARA PAGOS POR INTERNET: su objeto es garantizar la seguridad de cualquier pago realizado a través de Internet mediante los Servicios de la Entidad.

67. POLÍTICA DE DELEGACIÓN DE LA FUNCIÓN 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.