BANCO DE ESPAÑA
Eurosistema

Directrices sobre gobierno interno

(EBA/GL/2017/11)

Estas Directrices de la Autoridad Bancaria Europea (EBA por sus siglas en inglés) van dirigidas a las autoridades competentes según se definen en el artículo 4, apartado 1, punto 40, del Reglamento (UE) n.º 575/20133, y a las entidades definidas en el artículo 4, apartado 1, punto 3, del Reglamento (UE) n.º 575/2013.

Las Directrices tienen por objeto especificar los sistemas, procedimientos y mecanismos de gobierno interno que las entidades de crédito y las empresas de inversión deben implementar de conformidad con el artículo 74, apartado 1, de la Directiva 2013/36/UE para garantizar una gestión eficaz y prudente de la entidad.

Concretamente, estas Directrices detallan las obligaciones, responsabilidades y requisitos de organización interna de los órganos de gestión de las entidades, incluyendo la necesidad de establecer estructuras transparentes. Se distribuyen en un total de siete títulos relativos al principio de proporcionalidad, las funciones y composición del órgano de administración y de los comités, el marco de gobierno, la cultura de riesgos y conducta profesional, el marco y los mecanismos de control interno, la gestión de la continuidad del negocio y la transparencia.

Estas Directrices, cuya aplicación tendrá en cuenta el principio de proporcionalidad, han sido desarrolladas por la EBA de acuerdo con lo señalado en el artículo 16 del Reglamento (UE) No 1093/2010. La EBA publicó la versión en inglés de mismas el 26 de septiembre de 2017 y la versión en español el 21 de marzo de 2018. Se aplicarán a partir del 30 de junio de 2018.

La Comisión Ejecutiva del Banco de España, en su calidad de autoridad competente de la supervisión directa de las entidades de crédito menos significativas, adoptó estas Directrices como propias el día 18 de mayo de 2018, con el límite y sin perjuicio de las disposiciones españolas que implementan la CRDIV, y con la excepción de lo previsto en la directriz 65 que prevé que las entidades no significativas CRD puedan constituir un comité conjunto de riesgos y nombramientos.

EBA/GL/2017/11

21/03/2018

Directrices

sobre gobierno interno

1. Obligaciones de cumplimiento y de notificación

Rango jurídico de las presentes directrices

1. El presente documento contiene directrices emitidas en virtud del artículo 16 del Reglamento (UE) nº 1093/2010[1]. De conformidad con el artículo 16, apartado 3, del Reglamento (UE) nº 1093/2010, las autoridades competentes y las entidades financieras harán todo lo posible para atenerse a ellas.

2. En las directrices se expone el punto de vista de la ABE sobre las prácticas de supervisión más adecuadas en el marco del Sistema Europeo de Supervisión Financiera o sobre cómo debería aplicarse el Derecho de la Unión en un determinado ámbito. Las autoridades competentes definidas en el artículo 4, apartado 2, del Reglamento (UE) nº 1093/2010 a las que sean de aplicación las directrices deberían cumplirlas incorporándolas a sus prácticas de la forma más apropiada (modificando, por ejemplo, su marco jurídico o sus procedimientos de supervisión), incluso en aquellos casos en los que las directrices vayan dirigidas principalmente a las entidades.

Requisitos de notificación

3. De conformidad con el artículo 16, apartado 3, del Reglamento (UE) nº 1093/2010, las autoridades competentes deberán notificar a la ABE, a más tardar el 21/05/2018 si cumplen o se proponen cumplir estas directrices indicando, en caso negativo, los motivos para no cumplirlas. A falta de notificación en dicho plazo, la ABE considerará que las autoridades competentes no las cumplen. Las notificaciones se presentarán remitiendo el modelo que se encuentra disponible en el sitio web de la ABE a compliance@eba.europa.eu, con la referencia «EBA/GL/2017/11». Las notificaciones serán presentadas por personas debidamente facultadas para comunicar el cumplimiento en nombre de las respectivas autoridades competentes. Cualquier cambio en la situación de cumplimiento de las directrices deberá notificarse igualmente a la ABE.

4. Las notificaciones se publicarán en el sitio web de la ABE, tal y como contempla el artículo 16, apartado 3.

[1] Reglamento (UE) nº 1093/2010 del Parlamento Europeo y del Consejo, de 24 de noviembre de 2010, por el que se crea una Autoridad Europea de Supervisión (Autoridad Bancaria Europea), se modifica la Decisión nº 716/2009/CE y se deroga la Decisión nº 2009/78/CE de la Comisión, (DO L 331 de 15.12.2010, p. 12).

2. Objeto, ámbito de aplicación y definiciones

Objeto

5. Las presentes directrices especifican los sistemas, procedimientos y mecanismos de gobierno interno que las entidades de crédito y las empresas de inversión deben implementar de conformidad con el artículo 74, apartado 1, de la Directiva 2013/36/UE[2] para garantizar una gestión eficaz y prudente de la entidad.

Destinatarios

6. Estas directrices están dirigidas a las autoridades competentes según se definen en el artículo 4, apartado 1, punto 40, del Reglamento (UE) n.º 575/2013[3], incluido el Banco Central Europeo para los asuntos relacionados con las tareas que le encomienda el Reglamento (UE) n.º 1024/2013, y a las entidades definidas en el artículo 4, apartado 1, punto 3, del Reglamento (UE) n.º 575/2013.

Ámbito de aplicación

7. Las presentes directrices se aplican en relación con los sistemas de gobierno de las entidades, que comprende su estructura organizativa y la correspondiente división interna de responsabilidades, los procesos para identificar, gestionar, realizar un seguimiento e informar de los riesgos a los que están o podrían estar expuestas y el marco de control interno.

8. Las directrices tratan de abarcar todas las estructuras existentes de los órganos de administración y no propugnan ninguna estructura concreta. Las directrices no interfieren en la asignación general de competencias prevista en la legislación nacional en materia de sociedades. En consecuencia, se aplicarán independientemente de la estructura de gobierno (monista, dualista u otra) utilizada en los distintos Estados miembros. Se considerará que el órgano de administración, tal como se define en el artículo 3, apartado 1, puntos 7 y 8, de la Directiva 2013/36/UE, tiene funciones de gestión (ejecutivas) y de supervisión (no ejecutivas)[4].

9. Los términos «órgano de administración en su función de dirección» y «órgano de administración en su función de supervisión» se utilizan en estas directrices sin hacer

[2] Directiva 2013/36/UE del Parlamento Europeo y del Consejo, de 26 de junio de 2013, relativa al acceso a la actividad de las entidades de crédito y a la supervisión prudencial de las entidades de crédito y las empresas de inversión, por la que se modifica la Directiva 2002/87/CE y se derogan las Directivas 2006/48/CE y 2006/49/CE (DO L 176 de 27.6.2013, p. 338).

[3] Reglamento (UE) n.° 575/2013 del Parlamento Europeo y del Consejo, de 26 de junio de 2013, sobre los requisitos prudenciales de las entidades de crédito y las empresas de inversión, y por el que se modifica el Reglamento (UE) n.° 648/2012 (DO L 176 de 27.6.2013, pp. 1-337).

[4] Véase también el considerando 56 de la Directiva 2013/36/UE.

referencia a ninguna estructura de gobierno específica, y se entenderá que las referencias a la función de dirección (ejecutiva) o de supervisión (no ejecutiva) se aplican a los órganos o a los miembros del órgano de administración responsables de dicha función de conformidad con la legislación nacional. Al aplicar estas directrices, las autoridades competentes tendrán en cuenta su legislación nacional en materia de sociedades y, cuando sea necesario, especificarán a qué órgano o miembros del órgano de administración se refieren estas funciones.

10. En los Estados miembros donde el órgano de administración delegue, parcial o totalmente, las funciones ejecutivas en una persona o en un órgano ejecutivo interno (p. ej., el primer ejecutivo (CEO), un equipo directivo o un comité ejecutivo), se considerará que las personas que desempeñan esas funciones ejecutivas sobre la base de dicha delegación constituyen la función de dirección del órgano de administración. A los efectos de las presentes directrices, cualquier referencia al órgano de administración en su función de dirección debe entenderse que incluye también a los miembros del órgano ejecutivo o al primer ejecutivo (CEO), tal como se define en estas directrices, incluso si no han sido propuestos o nombrados como miembros formales del órgano u órganos de gobierno de la entidad de conformidad con la legislación nacional.

11. En los Estados miembros donde algunas responsabilidades sean ejercidas directamente por los accionistas, los miembros o los propietarios de la entidad en lugar de por el órgano de administración, las entidades se asegurarán de que tales responsabilidades y las decisiones relacionadas con estas estén alineadas, en la medida de lo posible, con las directrices aplicables al órgano de administración.

12. Las definiciones de primer ejecutivo (CEO), director financiero (CFO) y titulares de funciones clave que se utilizan en estas directrices son puramente funcionales y no pretenden imponer el nombramiento de dichos cargos ni la creación de los mismos, a menos que así lo establezca la legislación nacional o de la UE pertinente.

13. Las entidades deberán cumplir y las autoridades competentes velarán por que las entidades de crédito cumplan estas directrices en base individual, subconsolidada y consolidada de conformidad con el nivel de aplicación previsto en el artículo 109 de la Directiva 2013/36/UE.

Definiciones

14. A menos que se indique lo contrario, los términos utilizados y definidos en la Directiva 2013/36/UE tienen idéntico significado en estas directrices. Adicionalmente, a efectos de las presentes directrices se aplicarán las definiciones siguientes:

Apetito de riesgo	El nivel agregado y los tipos de riesgo que una entidad está dispuesta a asumir dentro de su capacidad de riesgo, en línea con su modelo de negocio, con el fin de lograr sus objetivos estratégicos.

Capacidad de riesgo	El nivel máximo de riesgo que una entidad puede asumir dada su base de capital, sus capacidades de gestión y control de riesgos, y sus limitaciones regulatorias.
Cultura de riesgos	Las normas, actitudes y comportamientos de una entidad relacionados con la concienciación sobre el riesgo, la asunción de riesgos y su gestión, y los controles que determinan las decisiones sobre riesgos. La cultura de riesgos influye en las decisiones de la dirección y de los empleados durante las actividades diarias y repercute en los riesgos que asumen.
Entidades	Las entidades de crédito o empresas de inversión, tal como se definen en el artículo 4, apartado 1, puntos 1 y 2, respectivamente, del Reglamento (UE) n.º 575/2013.
Personal	Todos los empleados de una entidad y de las filiales incluidas en su ámbito de consolidación, incluidas las filiales no sujetas a la Directiva 2013/36/UE, así como todos los miembros del órgano de administración en su función de dirección y en su función de supervisión.
Primer ejecutivo (CEO)	La persona responsable de gestionar y dirigir la actividad general de una entidad.
Director financiero (CFO)	El responsable global de gestionar todas las siguientes actividades: gestión de recursos financieros, planificación financiera e información financiera.
Responsables de las funciones de control interno	Las personas de mayor nivel jerárquico que se encargan de gestionar efectivamente la operativa diaria de las funciones independientes de gestión de riesgos, cumplimiento y auditoría interna.
Titulares de funciones clave	Las personas que tienen una influencia significativa en la dirección de la entidad, pero que no son miembros del órgano de administración ni el primer ejecutivo. Se incluyen los responsables de las funciones de control interno y el director financiero, cuando no sean miembros del órgano de administración, y otros titulares de funciones clave, cuando hayan sido identificados por las entidades conforme a un enfoque basado en el riesgo. Otros titulares de funciones clave podrían ser los responsables de líneas de negocio significativas, sucursales en el Espacio Económico Europeo/Asociación Europea de Libre Comercio, filiales en terceros países y otras funciones internas.
Consolidación prudencial	La aplicación de las normas prudenciales establecidas en la Directiva 2013/36/UE y en el Reglamento (UE) n.º 575/2013 en base consolidada o subconsolidada, de conformidad con la parte

	1, título 2, capítulo 2, del Reglamento (UE) n.º 575/2013. La consolidación prudencial incluye a todas las filiales que sean entidades o entidades financieras, tal como se definen en el artículo 4, apartados 3 y 26, respectivamente, del Reglamento (UE) n.º 575/2013, y también puede incluir empresas de servicios auxiliares, tal como se definen en el artículo 4, apartado 18, de dicho Reglamento, establecidas dentro y fuera de la UE.
Entidad en base consolidada	Una entidad que debe cumplir los requisitos prudenciales sobre la base de la situación consolidada, de conformidad con la parte 1, título 2, capítulo 2, del Reglamento (UE) n.º 575/2013.
Entidades significativas	Las entidades mencionadas en el artículo 131 de la Directiva 2013/36/UE (entidades de importancia sistémica mundial o EISM y otras entidades de importancia sistémica u OEIS) y, en su caso, otras entidades que determine la autoridad competente o la legislación nacional, en función de una evaluación del tamaño de la entidad, su organización interna y la naturaleza, la escala y la complejidad de sus actividades.
Entidad DRC cotizada	Las entidades cuyos instrumentos financieros están admitidos a negociación en un mercado regulado o en un sistema multilateral de negociación, según se define en el artículo 4, apartados 21 y 22, de la Directiva 2014/65/UE, en uno o más Estados miembros[5].
Accionista	La persona que posee acciones de una entidad o, dependiendo de la forma jurídica de la entidad, otros propietarios o miembros de la misma.
Cargo	Puesto en el órgano de administración de una entidad u otra persona jurídica.

3. Aplicación

Fecha de aplicación

15. Estas directrices serán de aplicación a partir del 30 de junio de 2018.

[5] Directiva 2014/65/UE del Parlamento Europeo y del Consejo, de 15 de mayo de 2014, relativa a los mercados de instrumentos financieros y por la que se modifican la Directiva 2002/92/CE y la Directiva 2011/61/UE (DO L 173 de 12.6.2014, p. 349).

Derogación

16. Las Directrices de la ABE sobre gobierno interno (GL 44) del 27 de septiembre de 2011 quedan derogadas con efectos a partir del 30 de junio de 2018.

4. Directrices

Título I - Proporcionalidad

17. El principio de proporcionalidad previsto en el artículo 74, apartado 2, de la Directiva 2013/36/UE pretende garantizar que los sistemas de gobierno interno sean coherentes con el perfil de riesgo individual y el modelo de negocio de la entidad, de modo que se alcancen eficazmente los objetivos de los requisitos regulatorios.

18. Las entidades tendrán en cuenta su tamaño, su organización interna y la naturaleza, escala y complejidad de sus actividades al desarrollar y aplicar sus sistemas de gobierno interno. Las entidades significativas contarán con sistemas de gobierno más sofisticados, mientras que las entidades pequeñas y menos complejas pueden aplicar sistemas más sencillos.

19. A efectos de la aplicación del principio de proporcionalidad y para garantizar la aplicación adecuada de los requisitos, las entidades y las autoridades competentes tendrán en cuenta los siguientes criterios:

    a. el tamaño en términos del total del balance de la entidad y sus filiales dentro del ámbito de consolidación prudencial;

    b. la presencia geográfica de la entidad y el volumen de sus operaciones en cada jurisdicción;

    c. la forma jurídica de la entidad y si la entidad es parte de un grupo y, en caso afirmativo, la evaluación de los criterios de proporcionalidad realizada para el grupo;

    d. si la entidad está admitida a cotización;

    e. si la entidad está autorizada a utilizar modelos internos para el cálculo de los requerimientos de capital (p. ej., el método basado en calificaciones internas);

    f. el tipo de actividades y servicios autorizados realizados por la entidad (véanse también el anexo 1 de la Directiva 2013/36/UE y el anexo 1 de la Directiva 2014/65/UE);

    g. el modelo y la estrategia de negocio subyacentes; la naturaleza y la complejidad de las actividades de negocio y la estructura organizativa de la entidad;

    h. la estrategia de riesgo, el apetito de riesgo y el perfil de riesgo real de la entidad, teniendo en cuenta también el resultado de las evaluaciones de capital y liquidez del PRES;

i. la estructura de propiedad y de financiación de la entidad;

j. el tipo de clientes (p. ej., minoristas, corporativos, institucionales, pequeñas empresas, entidades públicas) y la complejidad de los productos o contratos;

k. las actividades externalizadas y los canales de distribución, y

l. los sistemas de tecnología de la información (TI) existentes, incluidos los sistemas de continuidad y las actividades externalizadas en esta área.

Título II - Funciones y composición del órgano de administración y de los comités

1 Funciones y responsabilidades del órgano de administración

20. De conformidad con el artículo 88, apartado 1, de la Directiva 2013/36/UE, el órgano de administración debe asumir la responsabilidad última y general de la entidad y definir, supervisar y responder de la aplicación de un sistema de gobierno en la entidad que garantice una gestión eficaz y prudente de la misma.

21. Las funciones del órgano de administración estarán claramente definidas, distinguiendo entre los cometidos de la función de dirección (ejecutiva) y los de la función de supervisión (no ejecutiva). Las responsabilidades y funciones del órgano de administración se describirán en un documento escrito y debidamente aprobado por dicho órgano.

22. Todos los miembros del órgano de administración conocerán bien la estructura y las responsabilidades de dicho órgano y la distribución de tareas entre las distintas funciones del propio órgano de administración y sus comités. A fin de contar con controles y contrapesos adecuados, los procesos de toma de decisiones no estarán dominados por un solo miembro o un pequeño grupo de miembros. El órgano de administración en su función de supervisión y en su función de dirección interactuarán de manera eficaz. Ambas funciones intercambiarán información suficiente para poder desempeñar sus respectivas funciones.

23. Las responsabilidades del órgano de administración incluirán el establecimiento, la aprobación y la supervisión de la aplicación de:

a. la estrategia general de negocio y las políticas clave de la entidad dentro del marco legal y reglamentario aplicable, teniendo en cuenta la solvencia y los intereses financieros a largo plazo de la entidad;

b. la estrategia general de riesgo, incluido el apetito de riesgo de la entidad y su marco de gestión de riesgos, así como las medidas para garantizar que el órgano de administración dedique tiempo suficiente a las cuestiones relacionadas con los riesgos;

c. un marco de control y de gobierno interno adecuado y eficaz que incluya una estructura organizativa clara y funciones internas de gestión de riesgos, de cumplimiento y de auditoría que sean independientes y que cuenten con la autoridad, el rango y los recursos suficientes para desempeñar sus cometidos correctamente;

d. los importes, los tipos y la distribución del capital interno y del capital regulatorio para cubrir adecuadamente los riesgos de la entidad;

e. los objetivos de gestión de la liquidez de la entidad;

f. una política de remuneración acorde con los principios de remuneración establecidos en los artículos 92 a 95 de la Directiva 2013/36/UE y las directrices de la ABE sobre políticas de remuneración adecuadas en virtud de los artículos 74, apartado 3, y 75, apartado 2, de la Directiva 2013/36/UE[6];

g. medidas que garanticen que las evaluaciones de idoneidad, individuales y en su conjunto, del órgano de administración se lleven a cabo eficazmente, que la composición y la planificación de la sucesión del órgano de administración sean adecuadas, y que el órgano de administración desempeñe sus funciones con eficacia[7];

h. un proceso de selección y de evaluación de la idoneidad para los titulares de funciones clave[8];

i. disposiciones que garanticen el funcionamiento interno de cada comité del órgano de administración, si se han constituido, detallando:

    i. las funciones, composición y cometidos de cada comité;

    ii. un flujo de información apropiado, incluida la documentación de recomendaciones y conclusiones, y canales de comunicación entre cada comité y el órgano de administración, las autoridades competentes y otras partes;

j. una cultura de riesgos en línea con la sección 9 de las presentes directrices, que aborde la concienciación sobre el riesgo y la asunción de riesgos de la entidad;

[6] Directrices de la ABE sobre políticas de remuneración adecuadas en virtud de los artículos 74, apartado 3, y 75, apartado 2, de la Directiva 2013/36/UE y la divulgación de información en virtud del artículo 450 del Reglamento (UE) n.º 575/2013 (EBA/GL/2015/22).

[7] Véanse también las directrices conjuntas de la AEMV y la ABE sobre la evaluación de la adecuación de los miembros del órgano de administración y de los titulares de funciones clave en virtud de la Directiva 2013/36/UE y la Directiva 2014/65/UE.

[8] Véanse también las directrices conjuntas de la AEMV y la ABE sobre la evaluación de la adecuación de los miembros del órgano de administración y de los titulares de funciones clave en virtud de la Directiva 2013/36/UE y la Directiva 2014/65/UE.

k. una cultura y unos valores corporativos en línea con la sección 10, que fomenten un comportamiento responsable y ético, incluido un código de conducta o un instrumento similar;

l. una política sobre conflictos de interés a nivel de la entidad en línea con la sección 11 y para el personal acorde con la sección 12, y

m. disposiciones que garanticen la integridad de los sistemas de información contable y financiera, incluidos controles financieros y operativos, y el cumplimiento de la legislación y de las normas pertinentes.

24. El órgano de administración debe supervisar el proceso de divulgación de información y las comunicaciones con terceros con intereses en la entidad y con las autoridades competentes.

25. Todos los miembros del órgano de administración deberán estar informados sobre la operativa global de la entidad, su situación financiera y su perfil de riesgo, teniendo en cuenta el entorno económico, y sobre las decisiones adoptadas que tengan un impacto significativo en el negocio de la entidad.

26. Un miembro del órgano de administración podrá ser responsable de una función de control interno como se menciona en el título V, sección 19.1, siempre que no realice otras funciones que comprometan sus actividades de control interno y la independencia de la función de control interno.

27. El órgano de administración realizará un seguimiento, revisará periódicamente y abordará cualquier deficiencia identificada en la ejecución de procesos, estrategias y políticas relacionadas con las responsabilidades enumeradas en los apartados 23 y 24. El marco de gobierno interno y su aplicación se revisarán y se actualizarán periódicamente teniendo en cuenta el principio de proporcionalidad, como se explica en el título I. En caso de producirse cambios relevantes que afecten a la entidad se llevará a cabo una revisión más detallada.

2 Función de dirección del órgano de administración

28. El órgano de administración en su función de dirección participará activamente en las actividades de la entidad y tomará decisiones sobre una base adecuada y bien fundamentada.

29. El órgano de administración en su función de dirección será responsable de la ejecución de las estrategias fijadas por dicho órgano y analizará periódicamente su aplicación e idoneidad con el órgano de administración en su función de supervisión. Los directivos de la entidad podrán encargarse de su ejecución práctica.

30. El órgano de administración en su función de dirección cuestionará de forma constructiva y analizará con espíritu crítico las propuestas, explicaciones e información que reciba para formarse un criterio y tomar decisiones. El órgano de administración en su función de dirección informará al órgano de administración en su función de supervisión de manera periódica y

exhaustiva y, cuando sea preciso, sin demoras innecesarias, de cuanto sea relevante para valorar una situación, los riesgos y los cambios que afectan o pueden afectar a la entidad, por ejemplo, decisiones importantes sobre las actividades de negocio y los riesgos asumidos, la evaluación del entorno económico y de negocio de la entidad, de su liquidez y base sólida de capital, y la evaluación de sus exposiciones a riesgos relevantes.

3 Función de supervisión del órgano de administración

31. Las funciones de los miembros del órgano de administración en su función de supervisión incluirán el seguimiento y la crítica constructiva de la estrategia de la entidad.

32. Sin perjuicio de la legislación nacional, el órgano de administración en su función de supervisión incluirá miembros independientes, como se establece en la sección 9.3 de las directrices conjuntas de la AEMV y la ABE sobre la evaluación de la adecuación de los miembros del órgano de administración y de los titulares de funciones clave en virtud de la Directiva 2013/36/UE y la Directiva 2014/65/UE.

33. Sin perjuicio de las responsabilidades asignadas en virtud de la legislación nacional en materia de sociedades, el órgano de administración en su función de supervisión deberá:

    a. vigilar y realizar un seguimiento de los procesos de toma de decisiones y de las actuaciones de la dirección, y realizar un seguimiento efectivo del órgano de administración en su función de dirección, incluyendo el seguimiento y el análisis de su desempeño a título individual y en su conjunto, así como la implementación de la estrategia y la consecución de los objetivos de la entidad;

    b. cuestionar de forma constructiva y examinar de manera crítica las propuestas y la información proporcionada por los miembros del órgano de administración en su función de dirección, así como sus decisiones;

    c. teniendo en cuenta el principio de proporcionalidad establecido en el título I, llevar a cabo adecuadamente los cometidos y las funciones del comité de riesgos, del comité de remuneraciones y del comité de nombramientos, en caso de que dichos comités no se hayan constituido;

    d. garantizar y evaluar periódicamente la efectividad del marco de gobierno interno de la entidad y tomar las medidas adecuadas para corregir cualquier deficiencia identificada;

    e. vigilar y controlar que los objetivos estratégicos, la estructura organizativa y la estrategia de riesgo de la entidad, incluidos su apetito de riesgo y el marco de gestión de riesgos, así como otras políticas (p. ej., la política de remuneración) y el marco de divulgación de la información se apliquen de manera coherente;

    f. vigilar que la cultura de riesgos de la entidad se aplique de manera coherente;

g. realizar un seguimiento de la aplicación y la actualización de un código de conducta o similar y de políticas efectivas para identificar, gestionar y mitigar conflictos de interés reales y potenciales;

h. vigilar la integridad de la información financiera y de los informes financieros que se emitan, así como el marco de control interno, incluido un marco de gestión de riesgos sólido y eficaz;

i. garantizar que los responsables de las funciones de control interno puedan actuar de manera independiente y, sin perjuicio de la obligación de informar a otros órganos, líneas o unidades de negocio internos, puedan elevar sus preocupaciones y advertir directamente al órgano de administración en su función de supervisión, en caso necesario, cuando se observe una evolución adversa de los riesgos que afecte o pueda afectar a la entidad, y

j. realizar un seguimiento de la ejecución del plan de auditoría interna, previa participación de los comités de riesgo y de auditoría, cuando dichos comités se hayan constituido.

4 Funciones del presidente del órgano de administración

34. El presidente del órgano de administración dirigirá dicho órgano, contribuirá a que haya un flujo de información eficaz en su seno y entre este órgano y sus comités, cuando se hayan constituido, y será responsable de que su funcionamiento general sea eficaz.

35. El presidente promoverá e incentivará debates abiertos y críticos y se asegurará de que las opiniones discrepantes puedan expresarse y considerarse en el proceso de toma de decisiones.

36. Como principio general, el presidente del órgano de administración será un miembro no ejecutivo de este. Cuando el presidente asuma funciones ejecutivas, la entidad deberá contar con medidas para mitigar cualquier impacto adverso sobre sus mecanismos de control y contrapeso (p. ej., designando a un miembro destacado del Consejo o a un consejero *senior* independiente, o contando con más miembros no ejecutivos en el órgano de administración en su función de supervisión). En particular, de conformidad con el artículo 88, apartado 1, letra e), de la Directiva 2013/36/UE, el presidente del órgano de administración en su función de supervisión no debe ejercer simultáneamente las funciones de primer ejecutivo (CEO) de la misma entidad, salvo que la entidad lo justifique y las autoridades competentes lo autoricen.

37. El presidente establecerá los órdenes del día de las reuniones y se asegurará de que los temas estratégicos se traten con prioridad. Se asegurará de que las decisiones del órgano de administración se tomen sobre una base adecuada y bien fundamentada, y de que los documentos y la información se reciban con suficiente antelación antes de cada reunión.

38. El presidente del órgano de administración contribuirá a que las responsabilidades entre los miembros del órgano de administración se asignen de forma clara y a que exista un flujo de

información eficiente entre ellos, a fin de permitir que los miembros de dicho órgano en su función de supervisión puedan contribuir constructivamente a los debates y emitan sus votos de manera adecuada y bien fundamentada.

5 Comités del órgano de administración en su función de supervisión

5.1 Constitución de los comités

39. De conformidad con el artículo 109, apartado 1, de la Directiva 2013/36/UE junto con el artículo 76, apartado 3, el artículo 88, apartado 2, y el artículo 95, apartado 1, de la Directiva 2013/36/UE, todas las entidades que sean significativas a nivel individual, subconsolidado y consolidado, deben constituir comités de riesgos, de nombramientos[9] y de remuneraciones[10] para asesorar al órgano de administración en su función de supervisión y facilitar las decisiones que debe tomar dicho órgano. Las entidades no significativas, incluso cuando estén incluidas en el ámbito de consolidación prudencial de una entidad que sea significativa en base subconsolidada o consolidada, no están obligadas a establecer estos comités.

40. Cuando no se constituya un comité de riesgos o de nombramientos, las referencias en estas directrices a dichos comités se interpretarán como aplicables al órgano de administración en su función de supervisión, teniendo en cuenta el principio de proporcionalidad recogido en el Título I.

41. Las entidades podrán constituir otros comités (p. ej., comités de ética, de conducta y de cumplimiento) teniendo en cuenta los criterios establecidos en el Título I de las presentes directrices.

42. Las entidades se asegurarán de asignar y distribuir claramente las funciones y los cometidos entre los comités especializados del órgano de administración.

43. Cada comité tendrá un mandato documentado (incluido su ámbito de responsabilidad) otorgado por el órgano de administración en su función de supervisión, y establecerá procedimientos de trabajo adecuados.

44. Los comités prestarán apoyo a la función de supervisión en áreas específicas y facilitarán el desarrollo y la aplicación de un marco de gobierno interno sólido. La delegación de funciones en los comités no eximirá al órgano de administración en su función de supervisión del cumplimiento colectivo de sus cometidos y responsabilidades.

[9] Véanse también las directrices conjuntas de la AEMV y la ABE sobre la evaluación de la adecuación de los miembros del órgano de administración y de los titulares de funciones clave en virtud de la Directiva 2013/36/UE y la Directiva 2014/65/UE.

[10] Con respecto al comité de remuneraciones, véanse las directrices de la ABE sobre prácticas de remuneración adecuadas.

5.2 Composición de los comités[11]

45. Todos los comités estarán presididos por un miembro no ejecutivo del órgano de administración que pueda actuar con objetividad.

46. Los miembros independientes[12] del órgano de administración en su función de supervisión participarán activamente en los comités.

47. Cuando deban establecerse comités de conformidad con la Directiva 2013/36/UE o con la legislación nacional, estarán integrados por al menos tres miembros.

48. Las entidades se asegurarán, teniendo en cuenta el tamaño del órgano de administración y el número de miembros independientes de dicho órgano en su función de supervisión, de que la composición de los comités no sea idéntica.

49. Las entidades considerarán la rotación ocasional de los presidentes y los miembros de los comités, teniendo en cuenta la experiencia concreta, los conocimientos y las competencias que se requieran individual o colectivamente para formar parte de dichos comités.

50. Los comités de riesgos y de nombramientos estarán compuestos por miembros no ejecutivos del órgano de administración en su función de supervisión de la entidad de que se trate. La composición del comité de auditoría se establecerá de conformidad con el artículo 41 de la Directiva 2006/43/CE[13], y la del comité de remuneraciones de acuerdo con la sección 2.4.1 de las directrices de la ABE sobre políticas de remuneración adecuadas[14].

51. En el caso de EISM y OEIS, el comité de nombramientos incluirá una mayoría de miembros independientes, uno de los cuales actuará como presidente. En otras entidades significativas determinadas por las autoridades competentes o la legislación nacional, el comité de nombramientos incluirá un número suficiente de miembros independientes; estas entidades también pueden considerar una buena práctica que el presidente del comité de nombramientos sea independiente.

[11] Esta sección deberá leerse junto con las directrices conjuntas de la AEMV y la ABE sobre la evaluación de la adecuación de los miembros del órgano de administración y de los titulares de funciones clave en virtud de la Directiva 2013/36/UE y la Directiva 2014/65/UE.

[12] Como se define en la sección 9.3 de las directrices conjuntas de la AEMV y la ABE sobre la evaluación de la adecuación de los miembros del órgano de administración y de los titulares de funciones clave en virtud de la Directiva 2013/36/UE y la Directiva 2014/65/UE.

[13] Directiva 2006/43/CE del Parlamento Europeo y del Consejo, de 17 de mayo de 2006, relativa a la auditoría legal de las cuentas anuales y de las cuentas consolidadas, por la que se modifican las Directivas 78/660/CEE y 83/349/CEE del Consejo y se deroga la Directiva 84/253/CEE del Consejo (DO L 157 de 9.6.2006, p. 87), en su versión modificada por la Directiva 2014/56/UE del Parlamento Europeo y del Consejo, de 16 de abril de 2014.

[14] Directrices de la ABE sobre políticas de remuneración adecuadas en virtud de los artículos 74, apartado 3, y 75, apartado 2, de la Directiva 2013/36/UE y la divulgación de información en virtud del artículo 450 del Reglamento (UE) n.º 575/2013 (EBA/GL/2015/22).

52. Los miembros del comité de nombramientos tendrán, individualmente y en su conjunto, los conocimientos, las competencias y la experiencia adecuados en relación con el proceso de selección y los requisitos de idoneidad.

53. En el caso de EISM y OEIS, el comité de riesgos incluirá una mayoría de miembros independientes. En estas entidades, el comité de riesgos estará presidido por un miembro independiente. En otras entidades significativas determinadas por las autoridades competentes o la legislación nacional, el comité de riesgos incluirá un número suficiente de miembros independientes y, en la medida de lo posible, uno de ellos actuará como presidente. En todas las entidades, el presidente del comité de riesgos no presidirá el órgano de administración ni ningún otro comité.

54. Los miembros del comité de riesgos tendrán, individualmente y en su conjunto, los conocimientos, las competencias y la experiencia adecuados en relación con las prácticas de gestión y control de riesgos.

5.3 Procedimientos de los comités

55. Los comités informarán periódicamente al órgano de administración en su función de supervisión.

56. Los comités interactuarán entre sí cuando sea preciso. Sin perjuicio de lo dispuesto en el apartado 48, dicha interacción podría revestir la forma de participación cruzada de manera que el presidente o un miembro de un comité también pueda ser miembro de otro comité.

57. Los miembros de los comités tendrán debates abiertos y críticos en los que las opiniones discrepantes se abordarán de manera constructiva.

58. Los comités documentarán los órdenes del día de sus reuniones, así como los principales acuerdos y conclusiones.

59. Los comités de riesgos y de nombramientos deberán, como mínimo:

    a. tener acceso a toda la información relevante y los datos necesarios para desempeñar su función, incluidos los provenientes de las funciones corporativas y de control pertinentes (p. ej., función financiera, servicios jurídicos, recursos humanos, TI, riesgos, cumplimiento, auditoría, etc.);

    b. recibir informes periódicos, información *ad hoc*, comunicaciones y opiniones de los responsables de las funciones de control interno sobre el perfil de riesgo actual de la entidad, su cultura de riesgos y sus límites de riesgo, así como sobre cualquier infracción relevante que pueda haberse producido, con información detallada y recomendaciones relativas a las medidas correctivas adoptadas, que se adoptarán o que se hayan propuesto para abordarla;

c. analizar periódicamente y decidir sobre el contenido, el formato y la frecuencia de la información sobre riesgos sobre los que se vaya a informar a los comités, y

d. cuando sea necesario, garantizar una participación adecuada de las funciones de control interno y otras funciones relevantes (recursos humanos, servicios jurídicos, función financiera) en sus respectivas áreas de especialización y/o solicitar asesoramiento a expertos externos.

5.4 Funciones del comité de riesgos

60. Si se ha constituido, el comité de riesgos deberá, como mínimo:

a. asesorar y apoyar al órgano de administración en su función de supervisión en relación con el seguimiento del apetito de riesgo y de la estrategia general de riesgo actuales y futuros de la entidad, teniendo en cuenta todos los tipos de riesgos, para garantizar que estén en línea con la estrategia de negocio, los objetivos, la cultura corporativa y los valores de la entidad;

b. prestar asistencia al órgano de administración en su función de supervisión en la vigilancia de la aplicación de la estrategia de riesgo de la entidad y los límites correspondientes establecidos;

c. vigilar la ejecución de las estrategias de gestión del capital y de la liquidez, así como de todos los demás riesgos relevantes de una entidad, como los riesgos de mercado, de crédito, operacionales (incluidos los legales y tecnológicos) y reputacionales, a fin de evaluar su adecuación a la estrategia y el apetito de riesgo aprobados;

d. recomendar al órgano de administración en su función de supervisión los ajustes en la estrategia de riesgo que se consideren precisos como consecuencia, entre otros, de cambios en el modelo de negocio de la entidad, de la evolución del mercado o de recomendaciones formuladas por la función de gestión de riesgos;

e. prestar asesoramiento sobre el nombramiento de consultores externos que la función de supervisión pueda decidir contratar con fines de asesoramiento o apoyo;

f. analizar una serie de escenarios posibles, incluidos escenarios de estrés, para evaluar cómo reaccionaría el perfil de riesgo de la entidad ante eventos externos e internos;

g. vigilar la coherencia entre todos los productos y servicios financieros importantes ofrecidos a clientes y el modelo de negocio y la estrategia de riesgo de la entidad[15]. El comité de riesgos evaluará los riesgos asociados a los productos y servicios financieros

[15] Véanse también las Directrices de la ABE sobre procedimientos de gobierno y vigilancia de productos de banca minorista, disponibles en: http://www.eba.europa.eu/regulation-and-policy/consumer-protection-and-financial-innovation/guidelines-on-product-oversight-and-governance-arrangements-for-retail-banking-products .

ofrecidos y tendrá en cuenta la coherencia entre los precios asignados a dichos productos y servicios y los beneficios obtenidos, y

h. valorar las recomendaciones de los auditores internos o externos y verificar la adecuada aplicación de las medidas tomadas.

61. El comité de riesgos colaborará con otros comités cuyas actividades puedan tener un impacto en la estrategia de riesgo (p. ej., los comités de auditoría y de remuneraciones) y se comunicará periódicamente con las funciones de control interno de la entidad, en particular con la función de gestión de riesgos.

62. Si ha constituido, el comité de riesgos examinará, sin perjuicio de los cometidos del comité de remuneraciones, si los incentivos incluidos en las políticas y prácticas de remuneración tienen en cuenta el riesgo, el capital y la liquidez de la entidad, así como la probabilidad y el período de generación de beneficios.

5.5 Funciones del comité de auditoría

63. De conformidad con la Directiva 2006/43/CE[16], cuando se haya constituido, el comité de auditoría deberá, entre otras cosas:

a. supervisar la eficacia de los sistemas internos de control de calidad y de gestión de riesgos de la entidad y, cuando corresponda, de su función de auditoría interna, con respecto a la información financiera de la entidad auditada, sin quebrantar su independencia;

b. supervisar el establecimiento de políticas contables por parte de la entidad;

c. supervisar el proceso de elaboración de información financiera y formular recomendaciones destinadas a garantizar su integridad;

d. examinar y supervisar la independencia de los auditores legales o las sociedades de auditoría de conformidad con los artículos 22, 22 bis, 22 ter, 24 bis y 24 ter de la Directiva 2006/43/UE y el artículo 6 del Reglamento (UE) n.º 537/2014[17] y, en particular, la adecuación de la prestación de servicios distintos de los de auditoría a la entidad auditada de conformidad con el artículo 5 de dicho Reglamento;

e. supervisar la auditoría legal de los estados financieros anuales y consolidados, en particular de su resultado, teniendo en cuenta las observaciones y las conclusiones de

[16] Directiva 2006/43/CE del Parlamento Europeo y del Consejo, de 17 de mayo de 2006, relativa a la auditoría legal de las cuentas anuales y de las cuentas consolidadas, por la que se modifican las Directivas 78/660/CEE y 83/349/CEE del Consejo y se deroga la Directiva 84/253/CEE del Consejo (DO L 157 de 9.6.2006, pp. 87), en su versión modificada por la Directiva 2014/56/UE del Parlamento Europeo y del Consejo, de 16 de abril de 2014.

[17] Reglamento (UE) n.° 537/2014 del Parlamento Europeo y del Consejo, de 16 de abril de 2014, sobre los requisitos específicos para la auditoría legal de las entidades de interés público y por el que se deroga la Decisión 2005/909/CE de la Comisión (DO L 158 de 27.5.2014, p. 77).

la autoridad competente de conformidad con el artículo 26, apartado 6, del Reglamento (UE) n.º 537/2014;

f. ser responsable del procedimiento de selección de auditores legales o sociedades de auditoría externos y recomendar la aprobación de su nombramiento por el órgano competente de la entidad (de conformidad con el artículo 16 del Reglamento (UE) n.º 537/2014, excepto cuando se aplique el artículo 16, apartado 8, de dicho Reglamento, su remuneración y destitución;

g. revisar el alcance de la auditoría y la frecuencia de la auditoría legal de las cuentas anuales o consolidadas;

h. de conformidad con el artículo 39, apartado 6, letra a), de la Directiva 2006/43/UE, informar al órgano administrativo o de supervisión de la entidad auditada del resultado de la auditoría legal y explicar cómo ha contribuido esta a la integridad de la información financiera y la función que ha desempeñado el comité de auditoría en ese proceso, y

i. recibir y tener en cuenta los informes de auditoría.

5.6 Comités conjuntos

64. De conformidad con el artículo 76, apartado 3, de la Directiva 2013/36/UE, las autoridades competentes podrán permitir que las entidades que no se consideren significativas combinen el comité de riesgos con el comité de auditoría, cuando se haya constituido, como dispone el artículo 39 de la Directiva 2006/43/CE.

65. Cuando entidades no significativas hayan constituido comités de riesgos y de nombramientos, podrán constituir un comité conjunto. En tal caso, las entidades documentarán las razones por las que han optado por combinarlos y cómo con este sistema se cumplen los objetivos de los comités.

66. Las entidades velarán en todo momento por que los miembros de un comité conjunto posean, individual y colectivamente, los conocimientos, las competencias y la experiencia necesarios para comprender plenamente las funciones que debe desempeñar el comité conjunto[18].

Título III – Marco de gobierno

6 Marco organizativo y estructura

6.1 Marco organizativo

[18] Véanse también las directrices conjuntas de la AEMV y la ABE sobre la evaluación de la adecuación de los miembros del órgano de dirección y de los titulares de funciones clave en virtud de la Directiva 2013/36/UE y la Directiva 2014/65/UE.

67. El órgano de administración de una entidad deberá asegurarse de que la estructura organizativa y operativa de dicha entidad sea adecuada y transparente, y dispondrá de una descripción escrita de la misma. Dicha estructura fomentará y acreditará la gestión prudente y eficaz de la entidad a nivel individual, subconsolidado y consolidado. El órgano de administración velará por que las funciones de control interno sean independientes de las líneas de negocio que controlan, con una segregación de funciones adecuada, y con los recursos financieros y humanos y las competencias apropiadas para desempeñar eficazmente sus funciones. Los canales de comunicación y la asignación de responsabilidades de una entidad, en particular entre los titulares de funciones clave, estarán bien definidos y serán claros, coherentes y exigibles y estarán debidamente documentados. La documentación se actualizará según corresponda.

68. La estructura de la entidad no comprometerá la capacidad del órgano de administración para supervisar y gestionar eficazmente los riesgos a los que se enfrente la entidad o el grupo o la capacidad de la autoridad competente para supervisar eficazmente la entidad.

69. El órgano de administración determinará si los cambios relevantes en la estructura del grupo (p. ej., la creación de nuevas filiales, fusiones y adquisiciones, la venta o liquidación de partes del grupo, o acontecimientos externos) afectan a la adecuación del marco organizativo de la entidad y de qué manera. En caso de que se identifican deficiencias, el órgano de administración realizará los ajustes que sean necesarios con rapidez.

6.2 Conoce tu estructura

70. El órgano de administración conocerá y entenderá plenamente la estructura jurídica, organizativa y operativa de la entidad («conoce tu estructura») y velará por que sea conforme con la estrategia de negocio y el perfil de riesgo aprobados.

71. El órgano de administración será el responsable de aprobar estrategias y políticas adecuadas para la creación de nuevas estructuras. Cuando una entidad establezca muchas entidades jurídicas dentro de su grupo, su número y, en particular, las interconexiones y transacciones entre ellas no afectarán al diseño de su gobierno interno ni a la gestión y la vigilancia eficaces de los riesgos del grupo en su conjunto. El órgano de administración se asegurará de que la estructura de la entidad y, en su caso, las estructuras dentro del grupo, teniendo en cuenta los criterios especificados en la sección 7, sean claras, eficaces y transparentes para el personal de la entidad, los accionistas y otras partes interesadas, así como para la autoridad competente.

72. El órgano de administración dirigirá la estructura de la entidad, su evolución y sus limitaciones, y velará por que esta estructura esté justificada y sea eficiente, y no entrañe una complejidad indebida o inadecuada.

73. El órgano de administración de una entidad en base consolidada deberá conocer no solo la estructura jurídica, organizativa y operativa del grupo, sino también los objetivos y las

actividades de las distintas entidades y los vínculos y relaciones entre ellas. Esto incluye conocer los riesgos operacionales específicos del grupo, los riesgos intragrupo y el modo en que la financiación, el capital, la liquidez y los perfiles de riesgo del grupo pueden verse afectados en circunstancias normales y adversas. El órgano de administración velará por que la entidad pueda generar información sobre el grupo oportunamente en relación con el tipo, las características, el organigrama, la estructura de propiedad y las actividades de cada entidad, y por que las entidades del grupo cumplan con todas las exigencias de información a efectos de supervisión a nivel individual, subconsolidado y consolidado.

74. El órgano de administración de una entidad en base consolidada velará por que las diferentes entidades del grupo (incluida la propia entidad en base consolidada) reciban información suficiente para tener una idea clara de los objetivos generales, las estrategias y el perfil de riesgo del grupo y cómo la entidad está integrada en su estructura y en su funcionamiento operativo. Dicha información y sus actualizaciones se documentarán y se pondrán a disposición de las funciones pertinentes interesadas, incluidos el órgano de administración, las líneas de negocio y las funciones de control interno. Los miembros del órgano de administración de una entidad en base consolidada se mantendrán informados de los riesgos que genera la estructura del grupo, teniendo en cuenta los criterios especificados en la sección 7 de estas directrices. Esto incluye recibir:

    a. información sobre los principales factores de riesgo;

    b. informes periódicos de evaluación de la estructura global de la entidad y del cumplimiento de las actividades de cada una de las entidades con la estrategia aprobada para todo el grupo, e

    c. informes periódicos sobre cuestiones en las que el marco regulatorio exija el cumplimiento a nivel individual, subconsolidado y consolidado.

6.3 Estructuras complejas y actividades atípicas o no transparentes

75. Las entidades evitarán establecer estructuras complejas y potencialmente no transparentes. Al tomar decisiones, tendrán en cuenta tanto los resultados de la evaluación de riesgos realizada para identificar si tales estructuras podrían utilizarse con fines relacionados con el blanqueo de capitales u otros delitos financieros, como los mecanismos de control y el marco jurídico vigente[19]. Con este fin, las entidades tendrán en cuenta, como mínimo:

[19] Para más detalles sobre la evaluación del riesgo asociado a países y del riesgo vinculado a productos y clientes individuales, las entidades deberán consultar también las directrices conjuntas finales (una vez publicadas) sobre factores de riesgo: https://www.eba.europa.eu/regulation-and-policy/anti-money-laundering-and-e-money/guidelines-on-risk-factors-and-simplified-and-enhanced-customer-due-diligence/-/regulatory-activity/consultation-paper.

a. hasta qué punto la jurisdicción en la que se establecerá la estructura cumple efectivamente con las normas internacionales y de la UE sobre transparencia fiscal, lucha contra el blanqueo de capitales y la financiación del terrorismo;

b. hasta qué punto la estructura tiene una finalidad económica y legal obvia;

c. hasta qué punto la estructura podría utilizarse para ocultar la identidad del titular real;

d. hasta qué punto la posible estructura que se cree para atender la petición del cliente sería motivo de preocupación;

e. si la estructura podría impedir una vigilancia adecuada por parte del órgano de administración de la entidad o mermar la capacidad de esta para gestionar el riesgo asociado, y

f. si la estructura plantea obstáculos para una supervisión efectiva por parte de las autoridades competentes.

76. En cualquier caso, las entidades no establecerán estructuras opacas o innecesariamente complejas sin un fundamento económico o una finalidad legal claros, y tampoco las establecerán si tienen dudas de que puedan utilizarse para un propósito relacionado con la delincuencia financiera.

77. Al establecer tales estructuras, el órgano de administración deberá entenderlas, conocer su finalidad y los riesgos concretos asociados a ellas, y asegurarse de que las funciones de control interno participen adecuadamente. Dichas estructuras únicamente se aprobarán y se mantendrán cuando su finalidad haya sido claramente definida y entendida, y cuando el órgano de administración esté convencido de que se han identificado todos los riesgos materiales, incluidos los reputacionales, de que todos los riesgos pueden gestionarse con eficacia y se ha informado adecuadamente sobre ellos, y de que se ha asegurado una supervisión eficaz. Cuanto más compleja y opaca sea la estructura organizativa y operativa y mayores sean los riesgos, más intensiva deberá ser la supervisión de la estructura.

78. Las entidades deberán documentar sus decisiones y poder justificarlas ante las autoridades competentes.

79. El órgano de administración velará por que se adopten las medidas pertinentes para evitar o mitigar los riesgos derivados de las actividades de tales estructuras. Esto incluye asegurarse de que:

a. la entidad cuenta con políticas y procedimientos adecuados, así como con procesos documentados (p. ej., límites aplicables, requisitos de información) para la consideración, el cumplimiento, la aprobación y la gestión de los riesgos derivados de dichas actividades, teniendo en cuenta las consecuencias para la estructura organizativa y operativa del grupo, su perfil de riesgo y su riesgo reputacional;

b. la entidad en base consolidada y los auditores internos y externos pueden acceder a la información sobre estas actividades y sus riesgos, y que esta se comunique al órgano de administración en su función de supervisión y a la autoridad competente que otorgó la autorización, y

c. la entidad evalúa periódicamente si persiste la necesidad de mantener tales estructuras.

80. Estas estructuras y actividades, incluido su acomodo en la legislación y las normas profesionales, estarán sujetas a revisión periódica por parte de la función de auditoría interna siguiendo un enfoque basado en el riesgo.

81. Las actividades atípicas o no transparentes que las entidades realicen para sus clientes (p. ej., ayudarles a establecer sociedades instrumentales en jurisdicciones de terceros países, desarrollar estructuras complejas, financiarles transacciones o proporcionar servicios de fideicomiso) y que generen riesgos operacionales y reputacionales significativos deberán estar sujetas a las mismas medidas de gestión de riesgos que aplican esas entidades cuando actúan en su ámbito de negocio, si en ambos casos se plantearan retos similares en materia de gobierno interno. En particular, las entidades deberán analizar la razón por la cual un cliente desea establecer una estructura concreta.

7 Marco organizativo en un contexto de grupo

82. De conformidad con el artículo 109, apartado 2, de la Directiva 2013/36/UE, las empresas matrices y las filiales sujetas a dicha Directiva se asegurarán de que los sistemas, procedimientos y mecanismos de gobierno sean coherentes y estén bien integrados en base consolidada y subconsolidada. Con este fin, las empresas matrices y filiales incluidas en el ámbito de consolidación prudencial implementarán tales sistemas, procedimientos y mecanismos en sus filiales que no estén sujetas a la Directiva 2013/36/UE para garantizar que los procedimientos de gobierno de que disponen son adecuados en base consolidada y subconsolidada. Las funciones competentes de la entidad en base consolidada y de sus filiales interactuarán e intercambiarán datos e información según sea necesario. Los sistemas, procedimientos y mecanismos de gobierno asegurarán que la entidad en base consolidada disponga de datos e información suficientes para poder evaluar el perfil de riesgo de todo el grupo, como se detalla en la sección 6.2.

83. El órgano de administración de una filial sujeta a la Directiva 2013/36/UE adoptará y aplicará a nivel individual las políticas de gobernanza del grupo establecidas a nivel consolidado o subconsolidado, de forma que cumpla con todos los requisitos específicos de la legislación de la UE y nacional.

84. La entidad en base consolidada asegurará el cumplimiento de las políticas de gobierno del grupo a nivel consolidado y subconsolidado por parte de todas las entidades y de otras instituciones incluidas en el ámbito de consolidación prudencial, comprendiendo también las

filiales que no estén sujetas a la Directiva 2013/36/UE. Al implementar políticas de gobierno, la entidad en base consolidada se asegurará de que existan sistemas de gobernanza adecuados para cada filial y considerará sistemas, procedimientos y mecanismos específicos cuando las actividades de negocio no estén organizadas en entidades jurídicas separadas, sino en una matriz de líneas de negocio que abarque múltiples entidades jurídicas.

85. Las entidades en base consolidada considerarán los intereses de todas sus filiales y cómo las estrategias y políticas contribuyen a los intereses a largo plazo de cada filial y del grupo en su conjunto.

86. Las empresas matrices y sus filiales se asegurarán de que las entidades e instituciones del grupo cumplan todos los requisitos específicos en cualquier jurisdicción pertinente.

87. Las entidades en base consolidada se asegurarán de que las filiales establecidas en terceros países y que estén incluidas en el ámbito de consolidación prudencial cuenten con sistemas, procedimientos y mecanismos de gobierno coherentes con las políticas de gobernanza de todo el grupo y cumplan los requisitos de los artículos 74 a 96 de la Directiva 2013/36/UE y de las presentes directrices, siempre que no sea ilícito con arreglo a las leyes del tercer país.

88. Los requisitos de gobernanza de la Directiva 2013/36/UE y estas directrices son de aplicación a las entidades con independencia de que sean filiales de una entidad matriz en un tercer país. Cuando una filial en la UE de una entidad matriz situada en un tercer país sea una entidad en base consolidada, el perímetro de consolidación prudencial no incluirá el nivel de la entidad matriz situada en un tercer país ni otras filiales directas de dicha entidad matriz. La entidad en base consolidada se asegurará que la política de gobernanza del grupo de la entidad matriz situada en un tercer país se tenga en cuenta en su propia política de gobernanza, siempre que no sea contraria a los requisitos establecidos en la legislación de la UE aplicable, incluidas la Directiva 2013/36/UE y estas directrices.

89. Al establecer políticas y documentar los sistemas de gobierno, las entidades tendrán en cuenta los aspectos enumerados en el anexo I de estas directrices. Aunque las políticas y la documentación se pueden incluir en documentos separados, las entidades deberán considerar su combinación en un único documento o que este documento haga referencia a ambas.

8 Política de externalización[20]

90. El órgano de administración aprobará, y revisará y actualizará periódicamente, la política de externalización de la entidad, asegurando la aplicación oportuna de los cambios apropiados.

91. La política de externalización considerará el impacto de la externalización en las actividades de la entidad y los riesgos a los que se enfrenta (como los riesgos operacionales, incluidos los riesgos legales y tecnológicos, los riesgos reputacionales y de concentración). Esta política

[20] Las presentes directrices se limitan a la política general de externalización; los aspectos específicos de la externalización se abordan en las directrices del CEBS sobre externalización, cuya revisión está pendiente. Estas directrices están disponibles en: https://www.eba.europa.eu/regulation-and-policy/internal-governance/guidelines-on-outsourcing.

recogerá los procedimientos de presentación de información y de seguimiento que deberán aplicarse desde el comienzo hasta la finalización de un acuerdo de externalización (incluida la elaboración de los argumentos que justifican la externalización, la celebración de un contrato de externalización, el cumplimiento del contrato hasta su extinción, los planes de contingencia y las estrategias de salida). La entidad seguirá siendo plenamente responsable de todos los servicios y actividades externalizados, así como de las decisiones de gestión que se deriven de ellos. En consecuencia, la política de externalización establecerá con claridad que la externalización no eximirá a la entidad del cumplimiento de sus obligaciones en materia de regulación ni de sus responsabilidades frente a sus clientes.

92. La política pondrá de manifiesto que los procedimientos de externalización no impedirán la supervisión eficaz *in situ* o a distancia de la entidad, ni contravendrán ninguna restricción sobre servicios y actividades impuesta por el supervisor. La política también abarcará la externalización intragrupo (es decir, la prestación de servicios por una entidad jurídica separada perteneciente al propio grupo) y tendrá en cuenta cualquier circunstancia específica del grupo.

93. La política exigirá que, cuando se seleccionen proveedores externos de servicios esenciales o se externalicen actividades, la entidad tenga en cuenta si el proveedor del servicio tiene establecidas normas éticas o un código de conducta apropiados.

Título IV - Cultura de riesgos y conducta profesional

9 Cultura de riesgos

94. Una cultura de riesgos sólida y coherente debe ser un elemento clave en la gestión eficaz de los riesgos de las entidades y permitir que estas tomen decisiones adecuadas y bien fundamentadas.

95. Las entidades desarrollarán una cultura de riesgos integrada y para el conjunto de la organización, basada en un conocimiento exhaustivo y en una visión global de los riesgos a los que se enfrentan y la forma en que se gestionan, teniendo en cuenta su apetito de riesgo.

96. Las entidades, teniendo en cuenta sus actividades, estrategia y perfil de riesgo, desarrollarán su cultura de riesgos a través de políticas, de la comunicación y la formación del personal, y adaptarán la comunicación y la formación del personal teniendo en cuenta las responsabilidades del personal en la asunción de riesgos y su gestión.

97. El personal será plenamente consciente de sus responsabilidades en la gestión de riesgos. Esta gestión no corresponderá únicamente a los expertos en riesgos o a las funciones de control interno. Las unidades de negocio, bajo la supervisión del órgano de administración, serán responsables, principalmente, de la gestión diaria de los riesgos, en línea con las políticas, procedimientos y controles de la entidad, y teniendo en cuenta el apetito de riesgo de la entidad y su capacidad de riesgo.

98. Una cultura de riesgos sólida deberá incluir, entre otros, los siguientes elementos:

a. Actitud de los directivos: el órgano de administración será responsable de establecer y comunicar los valores fundamentales de la entidad y sus expectativas. El comportamiento de sus miembros reflejará los valores propugnados. La dirección de la entidad, incluidos los titulares de funciones clave, participará en la comunicación interna al personal de dichos valores fundamentales y expectativas de la entidad. El personal actuará de acuerdo con todas las leyes y normativas aplicables y elevará rápidamente los casos de incumplimiento observados dentro o fuera de la entidad (p. ej., a la autoridad competente a través de un procedimiento de denuncia de irregularidades). El órgano de administración promoverá, supervisará y evaluará la cultura de riesgos de la entidad de forma continua, considerará el impacto de dicha cultura en la estabilidad financiera, en el perfil de riesgo y en la gobernanza adecuada de la entidad, y hará cambios cuando sea necesario.

b. Rendición de cuentas: los miembros del personal a todos los niveles deberán conocer y comprender los valores fundamentales de la entidad y, en la medida necesaria para su función, su apetito y su capacidad de riesgo. Este personal estará capacitado para desempeñar sus funciones y será consciente de que será responsable de sus acciones en la medida en que se relacionen con la de asunción de riesgos de la entidad.

c. Comunicación y crítica efectivas: una cultura de riesgos sólida promoverá un entorno de comunicación abierta y una actitud crítica efectiva en el que los procesos de toma de decisiones fomenten una amplia variedad de puntos de vista, permitan poner a prueba las prácticas vigentes, estimulen una actitud crítica constructiva entre el personal y promuevan un entorno de compromiso abierto y constructivo en toda la organización.

d. Incentivos: la existencia de incentivos apropiados desempeñará un papel clave a la hora de adecuar la asunción de riesgos al perfil de riesgo de la entidad y sus intereses a largo plazo[21].

10 Valores corporativos y código de conducta

99. El órgano de administración desarrollará, adoptará, observará y promoverá rigurosas normas éticas y profesionales, teniendo en cuenta las necesidades y las características específicas de la entidad, y garantizará la aplicación de dichas normas (a través de un código de conducta o un instrumento similar). También supervisará el cumplimiento de estas normas por parte del personal. Cuando corresponda, el órgano de administración podrá adoptar y aplicar las normas al grupo o las normas comunes publicadas por asociaciones u otras organizaciones relevantes.

[21] Véanse también las Directrices de la ABE sobre políticas de remuneración adecuadas en virtud de los artículos 74, apartado 3, y 75, apartado 2, de la Directiva 2013/36/UE y la divulgación de información en virtud del artículo 450 del Reglamento (UE) n.º 575/2013 (EBA/GL/2015/22), disponibles en: https://www.eba.europa.eu/regulation-and-policy/remuneration.

100. Las normas aplicadas tratarán de reducir los riesgos a los que está expuesta la entidad, en particular los riesgos operacionales y reputacionales, que pueden tener un impacto adverso considerable sobre la rentabilidad y la sostenibilidad de la entidad a través de multas, gastos judiciales, restricciones impuestas por las autoridades competentes, otras sanciones financieras o penales, y la pérdida del valor de marca y de la confianza de los consumidores.

101. El órgano de administración contará con políticas claras y documentadas sobre cómo deberán cumplirse estas normas. Estas políticas deberán:

a. recordar a los destinatarios que todas las actividades de la entidad deberán llevarse a cabo de conformidad con la legislación aplicable y con los valores corporativos de la entidad;

b. promover la concienciación sobre el riesgo a través de una cultura de riesgos sólida, de acuerdo con la sección 9 de estas directrices, transmitiendo la expectativa del órgano de administración de que las actividades no irán más allá del apetito de riesgo definido y los límites establecidos por la entidad y las responsabilidades respectivas del personal;

c. establecer principios y proporcionar ejemplos de comportamientos aceptables e inaceptables vinculados, en particular, a deficiencias en la información financiera y a conductas irregulares, y a delitos económicos y financieros (incluidos fraude, blanqueo de capitales y prácticas antimonopolio, sanciones financieras, soborno y corrupción, manipulación del mercado, ventas inadecuadas y otras infracciones de la legislación de protección del consumidor);

d. aclarar que, además de cumplir los requisitos legales y regulatorios y las políticas internas, se espera que el personal se comporte con honestidad e integridad y realice sus tareas con la competencia, el esmero y la diligencia debidos, y

e. asegurar que el personal esté al tanto de las posibles acciones disciplinarias internas y externas, de las acciones legales y sanciones que pueden derivarse de una conducta irregular y de comportamientos inaceptables.

102. Las entidades supervisarán el cumplimiento de tales normas y asegurarán la concienciación del personal, por ejemplo, mediante formación. Las entidades definirán qué función será la responsable de supervisar el cumplimiento y evaluar las infracciones del código de conducta o un instrumento similar y establecerán un procedimiento a seguir casos de incumplimiento. Las conclusiones se notificarán periódicamente al órgano de administración.

11 Política de conflictos de interés a nivel de la entidad

103. El órgano de administración será responsable de establecer, aprobar y supervisar la aplicación y el mantenimiento de políticas eficaces para identificar, evaluar, gestionar y mitigar o prevenir conflictos de intereses reales y potenciales a nivel de la entidad, por ejemplo como resultado

de las diversas actividades y funciones de la entidad, de entidades diferentes incluidas en el ámbito de consolidación prudencial o de diferentes líneas o unidades de negocio de una entidad, o con respecto a terceros con intereses en la entidad.

104. Las entidades adoptarán medidas adecuadas en el marco de sus procedimientos organizativos y administrativos para evitar que los conflictos de interés afecten negativamente a los intereses de sus clientes.

105. Las medidas de las entidades para gestionar o, en su caso, mitigar los conflictos de intereses, deberán documentarse e incluir, entre otras cosas:

    a. una segregación de funciones adecuada, por ejemplo, encargando a personas diferentes la realización de actividades que puedan entrar en conflicto en los procesos relacionados con las transacciones o en la prestación de servicios, o confiando a personas distintas las responsabilidades de supervisión y de comunicación de las actividades en conflicto;

    b. el establecimiento de barreras a la información, por ejemplo, a través de la separación física de determinadas líneas o unidades de negocio, y

    c. el establecimiento de procedimientos adecuados para las transacciones con partes vinculadas, por ejemplo, exigir que las transacciones se lleven a cabo en condiciones de mercado.

12 Política de conflictos de intereses para el personal[22]

106. El órgano de administración será responsable de establecer, aprobar y supervisar la aplicación y el mantenimiento de políticas eficaces para identificar, evaluar, gestionar y mitigar o prevenir conflictos reales y potenciales entre los intereses de la entidad y los intereses privados del personal, incluidos los miembros del órgano de administración, lo que podría influir adversamente en el desempeño de sus deberes y responsabilidades. Las entidades en base consolidada considerarán los intereses dentro de la política de conflictos de intereses del grupo a nivel consolidado o subconsolidado.

107. La política tendrá como objetivo identificar los conflictos de intereses del personal, incluidos los intereses de los familiares más cercanos. Las entidades tendrán en cuenta que estos conflictos pueden surgir no solo de las relaciones personales o profesionales actuales, sino también de relaciones anteriores. Cuando se planteen conflictos de interés, las entidades valorarán su importancia y acordarán y aplicarán medidas apropiadas para mitigarlos.

108. Con respecto a los conflictos de intereses que puedan surgir de relaciones anteriores, las entidades establecerán un plazo apropiado para que el personal informe de tales conflictos,

[22] Esta sección deberá leerse junto con las directrices conjuntas de la AEMV y la ABE sobre la evaluación de la adecuación de los miembros del órgano de administración y de los titulares de funciones clave en virtud de la Directiva 2013/36/UE y la Directiva 2014/65/UE.

por considerar que aún pueden tener un impacto sobre el comportamiento del personal y su participación en la toma de decisiones.

109. La política abarcará al menos las siguientes situaciones o relaciones en las que puedan surgir conflictos de intereses:

    a. intereses económicos (p. ej., acciones, otros derechos de propiedad y pertenencia a asociaciones, participaciones financieras y otros intereses económicos en clientes comerciales, derechos de propiedad intelectual, préstamos otorgados por la entidad a una empresa propiedad del personal, pertenencia a un órgano o propiedad de un órgano o una entidad con intereses enfrentados);

    b. relaciones personales o profesionales con los propietarios de participaciones significativas en la entidad;

    c. relaciones personales o profesionales con personal de la entidad o de entidades incluidas en el ámbito de consolidación prudencial (p. ej., relaciones familiares);

    d. otros empleos y empleos anteriores en el pasado reciente (p. ej., los últimos cinco años);

    e. relaciones personales o profesionales con terceros relevantes con intereses en la entidad (p. ej., asociaciones con proveedores , consultores u otros proveedores de servicios esenciales), e

    f. influencia política o relaciones políticas.

110. No obstante lo anterior, las entidades tendrán en cuenta que ser accionista de una entidad, tener cuentas privadas o préstamos, o utilizar otros servicios de la misma no debería llevar a una situación en la que se considere que el personal tiene un conflicto de intereses si permanecen dentro de un umbral mínimo adecuado.

111. La política establecerá los procesos de notificación y comunicación a la función responsable pertinente. El personal tendrá la obligación de informar internamente de manera inmediata de cualquier asunto que pueda generar o haya generado un conflicto de interés.

112. La política diferenciará entre los conflictos de intereses que persisten y necesitan ser gestionados de modo permanente y los que se producen inesperadamente debido a un solo evento (p. ej., una transacción, la selección de un proveedor de servicios, etc.) y que, por lo general, se pueden gestionar con una medida puntual. En todas las circunstancias, el interés de la entidad será primordial en la toma de decisiones.

113. La política establecerá procedimientos, medidas, requisitos de documentación y responsabilidades para la identificación y prevención de conflictos de intereses, para la

evaluación de su materialidad y para tomar medidas de mitigación. Tales procedimientos, requisitos, responsabilidades y medidas incluirán:

a. encomendar a personas diferentes la realización de actividades o transacciones conflictivas;

b. evitar que el personal que también lleva a cabo actividades fuera de la entidad ejerza una influencia indebida en esta como consecuencia de dichas actividades;

c. establecer que los miembros del órgano de administración se abstengan de votar en cualquier asunto en el que un miembro tenga o pueda tener un conflicto de interés o en el que la objetividad o la capacidad del miembro para cumplir adecuadamente sus obligaciones con la entidad pueda verse comprometida;

d. establecer procedimientos adecuados para las transacciones con partes vinculadas (las entidades podrán considerar, entre otras cosas, exigir que las transacciones se realicen en condiciones de mercado, requerir que todos los procedimientos de control interno pertinentes se apliquen íntegramente a tales transacciones, solicitar asesoramiento vinculante a miembros independientes del órgano de administración, solicitar la aprobación de las transacciones más relevantes por parte de los accionistas y limitar la exposición a tales transacciones), e

e. impedir que los miembros del órgano de administración ocupen cargos en entidades competidoras, a menos que formen parte de entidades que pertenezcan al mismo sistema institucional de protección, según se establece en el artículo 113, apartado 7, del Reglamento (UE) n.º 575/2013, entidades de crédito afiliadas de forma permanente a un organismo central, tal como se menciona en el artículo 10 del Reglamento (UE) n.º 575/2013, o entidades incluidas en el ámbito de consolidación prudencial.

114. La política cubrirá específicamente el riesgo de conflictos de intereses a nivel del órgano de administración y proporcionará orientaciones suficientes sobre la identificación y la gestión de conflictos de intereses que puedan comprometer la capacidad de los miembros del órgano de administración para tomar decisiones objetivas e imparciales que persigan salvaguardar los intereses de la entidad. Las entidades tendrán en cuenta que los conflictos de intereses pueden tener un impacto en la independencia de ideas de los miembros del órgano de administración[23].

115. Los conflictos de intereses reales o potenciales que se hayan notificado a la función responsable de la entidad se evaluarán y se gestionarán adecuadamente. Si se identifica un conflicto de intereses del personal, la entidad documentará la decisión tomada, en particular

[23] Véanse también las directrices conjuntas de la AEMV y la ABE sobre la evaluación de la adecuación de los miembros del órgano de administración y de los titulares de funciones clave en virtud de la Directiva 2013/36/UE y la Directiva 2014/65/UE.

si el conflicto de intereses y los riesgos relacionados se han reconocido y en tal caso, cómo se ha mitigado o solventado.

116. Todos los conflictos de intereses reales y potenciales a nivel del órgano de administración, tanto individuales como colectivos, se documentarán adecuadamente, serán notificados al órgano de administración y este será quien los valore, tome una decisión al respecto y los gestione apropiadamente.

13 Procedimientos internos de alerta

117. Las entidades establecerán y mantendrán políticas y procedimientos internos de alerta adecuados para que el personal informe, a través de un canal específico, independiente y autónomo, sobre incumplimientos potenciales o reales de requisitos regulatorios o internos, incluidos, entre otros, los del Reglamento (UE) n.º 575/2013 y las disposiciones nacionales que transponen la Directiva 2013/36/UE, o de los sistemas de gobierno interno. No será necesario que el personal que informe disponga de pruebas del incumplimiento, aunque deberá tener un nivel de certeza que proporcione razones suficientes para iniciar una investigación.

118. Con el fin de evitar conflictos de interés, deberá brindarse al personal la posibilidad de denunciar infracciones sin seguir los canales de comunicación ordinarios (p. ej., a través de la función de cumplimiento o de auditoría interna, o mediante un procedimiento de denuncia interno independiente). Los procedimientos de alerta garantizarán la protección de los datos personales, tanto de la persona que denuncia la infracción como de la persona física presuntamente responsable de la misma, de conformidad con la Directiva 95/46/CE.

119. Los procedimientos de alerta se pondrán a disposición de todo el personal de la entidad.

120. La información proporcionada por el personal mediante los procedimientos de alerta deberá ponerse a disposición, si corresponde, del órgano de administración y de otras funciones responsables establecidas en la política interna de alertas. Cuando el empleado que denuncie una infracción lo solicite, se deberá facilitar la información al órgano de administración y a otras funciones responsables de forma anónima. Las entidades también podrán establecer un procedimiento de denuncia de irregularidades que permita que la información se presente de forma anónima.

121. Las entidades velarán por que la persona que denuncie la infracción esté debidamente protegida de cualquier efecto negativo, como represalias, discriminación u otros tipos de trato injusto. La entidad se asegurará de que ninguna persona bajo control de la entidad victimice a una persona que haya denunciado una infracción y tomará las medidas apropiadas contra los responsables de dicha victimización.

122. Las entidades también protegerán a las personas a quienes se haya denunciado de cualquier efecto negativo en el caso de que en la investigación no se encuentren pruebas que justifiquen la adopción de medidas contra ellas. Si se toman medidas, la entidad las adoptará con el

objetivo de proteger a la persona afectada de efectos negativos no deseados que vayan más allá del objetivo de la medida adoptada.

123. En particular, los procedimientos internos de alerta deberán:

a. estar documentados (p. ej., manuales para el personal);

b. establecer normas claras que garanticen que la información sobre los denunciantes y los denunciados y la infracción se traten de forma confidencial, de conformidad con la Directiva 95/46/CE, a menos que se exija su divulgación en virtud de la legislación nacional en el contexto de nuevas investigaciones o procedimientos judiciales posteriores;

c. proteger al personal que eleva su preocupación de ser victimizado por haber revelado infracciones susceptibles de ser comunicadas;

d. asegurar que las infracciones potenciales o reales denunciadas se analicen y se eleven, incluyendo, según sea el caso, a la autoridad competente o a las fuerzas y cuerpos de seguridad;

e. en la medida de lo posible, asegurar que el personal que haya denunciado infracciones potenciales o reales reciba una confirmación de que la información ha sido recibida;

f. garantizar el seguimiento del resultado de una investigación sobre una infracción denunciada, y

g. asegurar que se llevan los registros apropiados.

14 Notificación de infracciones a las autoridades competentes

124. Las autoridades competentes establecerán mecanismos efectivos y fiables para que el personal de las entidades pueda notificar a las autoridades competentes incumplimientos importantes, potenciales o reales, de los requerimientos o disposiciones legales, incluidos, entre otros, los del Reglamento (UE) n.º 575/2013 y las disposiciones nacionales que transponen la Directiva 2013/36/UE. Estos mecanismos incluirán al menos:

a. procedimientos específicos para la recepción de denuncias de infracciones y su seguimiento, por ejemplo, un departamento, unidad o función específica de denuncia de irregularidades;

b. protección apropiada según se establece en la sección 13;

c. protección de los datos personales tanto de la persona física que denuncia la infracción como de la persona física presuntamente responsable de la infracción, de conformidad con la Directiva 95/46/CE, y

d. procedimientos claros según se establece en el apartado 123.

125. Sin perjuicio de la posibilidad de denunciar infracciones a través de los mecanismos establecidos por las autoridades competentes, estas podrán recomendar al personal que utilice primero los procedimientos internos de alerta de su entidad.

Título V - Marco y mecanismos de control interno

15 Marco de control interno

126. Las entidades desarrollarán y mantendrán una cultura que fomente una actitud positiva hacia el control de riesgos y el cumplimiento interno por parte de la entidad, así como un marco de control interno sólido y exhaustivo. En este marco, las líneas de negocio de las entidades serán responsables de gestionar los riesgos en los que incurran al llevar a cabo sus actividades y tendrán establecidos controles que garanticen el cumplimiento de los requisitos internos y externos. Como parte de este marco, las entidades contarán con funciones de control interno con autoridad, rango y acceso adecuados y suficientes al órgano de administración para cumplir su misión, y un marco de gestión de riesgos.

127. El marco de control interno de la entidad en cuestión se adaptará de forma individual a las características específicas de su negocio, su complejidad y los riesgos asociados, teniendo en cuenta el contexto de grupo. Las entidades deben organizar el intercambio de la información necesaria de manera que se garantice que cada órgano de administración, línea de negocio y unidad interna, incluidas todas las funciones de control interno, pueden llevar a cabo sus funciones. Esto implica, por ejemplo, que haya un intercambio necesario de la información adecuada entre las líneas de negocio y la función de cumplimiento a nivel de grupo y entre los responsables de las funciones de control interno a nivel de grupo y el órgano de administración de la entidad.

128. El marco de control interno abarcará toda la organización, incluidas las responsabilidades y tareas del órgano de administración y las actividades de todas las líneas de negocio y unidades internas, incluidas las funciones de control interno, las actividades externalizadas y los canales de distribución.

129. El marco de control interno de una entidad garantizará:

a. una operativa eficaz y eficiente;

b. una gestión prudente del negocio;

c. una identificación, medición y mitigación adecuadas de los riesgos;

d. la fiabilidad de la información financiera y no financiera publicada interna y externamente;

e. unos procedimientos administrativos y contables sólidos, y

f. el cumplimiento de las leyes, normativas, requisitos en materia de supervisión y políticas, procesos, normas y decisiones internos de la entidad.

16 Aplicación del marco de control interno

130. El órgano de administración será responsable de establecer y controlar la adecuación y la eficacia del marco, los procedimientos y los mecanismos de control interno, y de supervisar todas las líneas de negocio y unidades internas, incluidas las funciones de control interno (como las funciones de gestión de riesgos, de cumplimiento y de auditoría interna). Las entidades establecerán, mantendrán y actualizarán periódicamente por escrito políticas, mecanismos y procedimientos de control interno adecuados, que deberán ser aprobados por el órgano de administración.

131. Las entidades contarán con un proceso de toma de decisiones claro, transparente y documentado, y una asignación clara de responsabilidades y competencias en su marco de control interno, incluidas sus líneas de negocio, unidades internas y funciones de control interno.

132. Las entidades comunicarán esas políticas, mecanismos y procedimientos a todo el personal y siempre que se realicen cambios relevantes.

133. Al implementar el marco de control interno, las entidades establecerán una segregación de funciones adecuada, por ejemplo, encomendando a personas diferentes la realización de actividades conflictivas en los procesos relacionados con transacciones o en la prestación de servicios, o confiando a personas distintas responsabilidades de supervisión e información relacionadas con actividades conflictivas, y establecerán barreras a la información, por ejemplo, a través de la separación física de determinados departamentos.

134. Las funciones de control interno verificarán que las políticas, mecanismos y procedimientos establecidos en el marco de control interno se apliquen correctamente en sus respectivas áreas de competencia.

135. Las funciones de control interno presentarán periódicamente al órgano de administración informes por escrito sobre las principales deficiencias identificadas. Estos informes incluirán, para cada nueva deficiencia importante identificada, los riesgos relevantes asociados, una evaluación del impacto, y las recomendaciones y medidas correctivas que se vayan a tomar. El órgano de administración realizará un seguimiento oportuno y eficaz de las conclusiones de

los informes de las funciones de control interno y exigirá que se tomen las medidas correctivas adecuadas. Se establecerá un procedimiento de seguimiento formal de las conclusiones y de las medidas correctivas tomadas.

17 Marco de gestión de riesgos

136. Como parte del marco de control interno general, las entidades contarán con un marco integral de gestión de riesgos que abarque todas sus líneas de negocio y unidades internas, incluidas las funciones de control interno, que reconozca plenamente el contenido económico de todas sus exposiciones al riesgo. El marco de gestión de riesgos permitirá que la entidad tome decisiones bien fundamentadas sobre la asunción de riesgos. El marco de gestión de riesgos incluirá los riesgos dentro y fuera de balance, así como los riesgos reales y los riesgos futuros a los que la entidad podría estar expuesta. Los riesgos se evaluarán siguiendo un enfoque ascendente (*bottom up*) y descendente (*top down*) en todas las líneas de negocio, utilizando una terminología coherente y metodologías compatibles en toda la entidad y a nivel consolidado o subconsolidado. Todos los riesgos relevantes deberán incluirse en el marco de gestión de riesgos tomando debidamente en consideración los riesgos financieros y no financieros, incluidos los riesgos de crédito, de mercado, de liquidez, de concentración, operacionales, tecnológicos, reputacionales, legales, de conducta, de cumplimiento y estratégicos.

137. El marco de gestión de riesgos de una entidad incluirá políticas, procedimientos, límites de riesgo y controles de riesgos que aseguren una identificación, medición o evaluación, vigilancia, gestión, mitigación y notificación de los riesgos adecuadas, oportunas y continuas a nivel de líneas de negocio y de la entidad, y a nivel consolidado o subconsolidado.

138. El marco de gestión de riesgos de una entidad facilitará orientaciones específicas sobre la implantación de sus estrategias. Cuando proceda, estas orientaciones establecerán y mantendrán límites internos coherentes con el apetito de riesgo de la entidad y acordes con su buen funcionamiento, su solidez financiera, su base de capital y sus objetivos estratégicos. El perfil de riesgo de una entidad deberá mantenerse dentro de estos límites. El marco de gestión de riesgos garantizará que cuando se produzcan incumplimientos de los límites de riesgo exista un proceso establecido para elevarlos y abordarlos con un procedimiento de seguimiento adecuado.

139. El marco de gestión de riesgos será objeto de revisión interna independiente, por ejemplo, realizada por la función de auditoría interna, y se volverá a evaluar periódicamente en función del apetito de riesgo de la entidad, teniendo en cuenta la información procedente de la función de gestión de riesgos y, si se ha constituido, del comité de riesgos. Entre los factores que deberán considerarse figuran la evolución interna y externa, incluidas variaciones del balance y de los ingresos, cualquier aumento de la complejidad del negocio de la entidad, de su perfil de riesgo o de su estructura operativa, la expansión geográfica, las fusiones y adquisiciones y la introducción de nuevos productos o líneas de negocio.

140. Al identificar y medir o evaluar los riesgos, las entidades desarrollarán metodologías apropiadas que incluyan herramientas prospectivas y retrospectivas. Estas metodologías permitirán agregar las exposiciones al riesgo de las distintas líneas de negocio y facilitarán la identificación de concentraciones de riesgos. Las herramientas incluirán la evaluación del perfil de riesgo real considerando el apetito de riesgo de la entidad, así como la identificación y evaluación de exposiciones al riesgo potenciales y en situaciones de estrés en una serie de supuestos adversos teniendo en cuenta la capacidad de riesgo de la entidad. Las herramientas proporcionarán información sobre cualquier ajuste al perfil de riesgo que pueda requerirse. Las entidades utilizarán supuestos suficientemente conservadores al construir escenarios de estrés.

141. Las entidades tendrán en cuenta que los resultados de las metodologías de evaluación cuantitativa, incluidas las pruebas de resistencia, dependen en gran medida de las limitaciones y los supuestos de los modelos (incluidas la gravedad y la duración de la perturbación y los riesgos subyacentes). Por ejemplo, si un modelo presenta una rentabilidad muy elevada del capital económico, ello podría deberse a una deficiencia del modelo (p. ej., la exclusión de algunos riesgos relevantes), más que a una buena estrategia o a una buena ejecución de una estrategia por parte de la entidad. Por lo tanto, la determinación del nivel de riesgo asumido no deberá basarse únicamente en información cuantitativa o en los resultados de modelos, sino que también deberá incluir un enfoque cualitativo (incluido el criterio de expertos y el análisis crítico). Las tendencias y los datos relevantes del entorno macroeconómico deberán considerarse explícitamente para identificar su posible impacto en las exposiciones y en las carteras.

142. La responsabilidad de la evaluación de riesgos recae, en última instancia, exclusivamente en la entidad que, en consecuencia, deberá evaluar sus riesgos de forma crítica y no basarse únicamente en evaluaciones externas. Por ejemplo, las entidades deberán validar los modelos de riesgo que adquieran y calibrarlos en función de sus circunstancias individuales, con el fin de garantizar que el modelo recoja y analice los riesgos con precisión y exhaustividad.

143. Las entidades conocerán adecuadamente las limitaciones de los modelos y las métricas, y utilizarán herramientas de evaluación de riesgos no solo cuantitativas sino también cualitativas (incluido el criterio de expertos y el análisis crítico).

144. Además de las evaluaciones realizadas por las propias entidades, estas podrán usar evaluaciones de riesgo externas (incluidas calificaciones crediticias externas o modelos de riesgo adquiridos externamente). Las entidades conocerán adecuadamente el alcance exacto de tales evaluaciones y de sus limitaciones.

145. Se establecerán mecanismos de información periódica y transparente para que el órgano de administración, su comité de riesgos, si se ha constituido, y todas las unidades pertinentes de una entidad, reciban informes oportunos, precisos, concisos, comprensibles y coherentes, y puedan compartir información relevante sobre la identificación, medición o evaluación, vigilancia y gestión de riesgos. El marco de información estará bien definido y documentado.

146. Una comunicación eficaz y la concienciación sobre los riesgos, así como una estrategia de riesgos, son fundamentales para todo el proceso de gestión de riesgos, incluidos los procesos de revisión y de toma de decisiones, y contribuyen a evitar decisiones que podrían aumentar los riesgos involuntariamente. Una comunicación eficaz de los riesgos requiere una adecuada consideración y comunicación internas de la estrategia de riesgos y de los datos relevantes sobre riesgos (p. ej., exposiciones a riesgos e indicadores clave de riesgos), tanto horizontalmente en toda la entidad, como verticalmente entre los diferentes niveles de la cadena de dirección.

18 Nuevos productos y cambios significativos[24]

147. Las entidades contarán con una política de aprobación de nuevos productos adecuadamente documentada y aprobada por el órgano de administración en la que se aborden el desarrollo de nuevos mercados, productos y servicios, y los cambios significativos en los ya existentes, así como las transacciones excepcionales. Dicha política también abarcará los cambios relevantes en procesos (p. ej., nuevos acuerdos de externalización) y sistemas (p. ej., procesos de cambio de TI) relacionados. Asimismo, esta política garantizará que los productos y los cambios aprobados sean coherentes con la estrategia y el apetito de riesgo de la entidad y los límites correspondientes, o que se realicen las revisiones necesarias.

148. Los cambios relevantes o las transacciones excepcionales podrán referirse a fusiones y adquisiciones, incluyendo las posibles consecuencias de realizar insuficientes procesos de diligencia debida en los que no se identifiquen los riesgos y pasivos posteriores a la fusión; la creación de estructuras (p. ej., nuevas filiales o vehículos de propósito único), nuevos productos, cambios en los sistemas o en el marco o los procedimientos de gestión de riesgos y cambios en la organización de la entidad.

149. Las entidades contarán con procedimientos específicos para evaluar el cumplimiento de estas políticas, teniendo en cuenta las aportaciones de la función de gestión de riesgos, que incluirán una evaluación sistemática previa y una opinión documentada de la función de cumplimiento sobre nuevos productos o cambios significativos en productos ya existentes.

150. La política de aprobación de nuevos productos de una entidad cubrirá todos los aspectos que deban tenerse en cuenta antes de decidir penetrar en nuevos mercados, operar con nuevos productos, lanzar un nuevo servicio o realizar cambios significativos en productos o servicios ya existentes. Dicha política también incluirá las definiciones de «nuevo producto/mercado/negocio» y de «cambios significativos» que se utilizarán en la organización y las funciones internas que intervendrán en el proceso de toma de decisiones.

151. Esta política establecerá las principales cuestiones que se deberán abordar antes de tomar una decisión, entre las que se incluyen el cumplimiento de la regulación, la contabilidad, los

[24] Véanse también las Directrices de la ABE sobre procedimientos de gobernanza y vigilancia para fabricantes y distribuidores de productos de banca minorista, disponibles en: http://www.eba.europa.eu/regulation-and-policy/consumer-protection-and-financial-innovation/guidelines-on-product-oversight-and-governance-arrangements-for-retail-banking-products.

modelos de fijación de precios, el impacto en el perfil de riesgo, la adecuación del capital y la rentabilidad, la disponibilidad de recursos adecuados de *front office* (operadores), *back office* (servicios administrativos) y *middle office* (gestión de riesgos, sistemas de TI, etc.), y la disponibilidad de herramientas internas y experiencia adecuadas para comprender y controlar los riesgos asociados. En la decisión de poner en marcha una nueva actividad se indicará claramente la unidad de negocio y las personas responsables de dicha actividad. No deberá emprenderse una nueva actividad hasta que se disponga de los recursos adecuados para entender y gestionar los riesgos asociados.

152. La función de gestión de riesgos y la función de cumplimiento participarán en la aprobación de nuevos productos o de cambios significativos en productos, procesos y sistemas existentes. Su aportación incluirá una evaluación completa y objetiva de los riesgos derivados de las nuevas actividades en diversos escenarios, de posibles deficiencias en los marcos de gestión de riesgos y de control interno de la entidad, y de la capacidad de esta para gestionar los nuevos riesgos con eficacia. La función de control de riesgos deberá tener asimismo una visión general clara del proceso de implantación de nuevos productos (o de los cambios significativos en los productos, procesos y sistemas existentes) en las diferentes líneas de negocio y carteras, así como la facultad de exigir que los cambios en productos existentes se sometan al proceso formal de aprobación de nuevos productos.

19 Funciones de control interno

153. Las funciones de control interno incluirán una función de gestión de riesgos (véase la sección 20), una función de cumplimiento (véase la sección 21) y una función de auditoría interna (véase la sección 22). Las funciones de gestión de riesgos y de cumplimiento estarán sujetas a revisión por parte de la función de auditoría interna.

154. Las tareas operativas de las funciones de control interno podrán externalizarse, teniendo en cuenta los criterios de proporcionalidad enumerados en el título I, a la entidad en base consolidada o a otra entidad dentro o fuera del grupo con el consentimiento de los órganos de administración de las entidades afectadas. Incluso cuando las tareas operativas de control interno se externalicen total o parcialmente, el responsable de la función de control interno correspondiente y el órgano de administración seguirán siendo responsables de estas actividades y de mantener la función de control interno dentro de la entidad.

19.1 Responsables de las funciones de control interno

155. Los responsables de las funciones de control interno se establecerán a un nivel jerárquico adecuado que proporcione al responsable de dicha función la autoridad y el rango adecuados para cumplir sus responsabilidades. Sin perjuicio de la responsabilidad general del órgano de administración, los responsables de las funciones de control interno serán independientes de las líneas de negocio o de las unidades que controlan. Con este fin, los responsables de las funciones de gestión de riesgos, de cumplimiento y de auditoría interna informarán y rendirán cuentas directamente al órgano de administración, y este evaluará su desempeño.

156. Cuando sea necesario, los responsables de las funciones de control interno podrán acceder e informar directamente al órgano de administración en su función de supervisión para plantear inquietudes y advertir, si procede, cuando sucesos específicos afecten o puedan afectar a la entidad. Esto no impedirá que los responsables de las funciones de control interno informen también dentro de los canales de comunicación ordinarios.

157. Las entidades tendrán establecidos procesos documentados para nombrar y cesar al responsable de una función de control interno. En cualquier caso, los responsables de las funciones de control interno no deberán ser destituidos sin la aprobación previa del órgano de administración en su función de supervisión, y en virtud del artículo 76, apartado 5, de la Directiva 2013/36/UE, el responsable de la función de gestión de riesgos no podrá ser cesado sin dicha aprobación. En las entidades significativas, las autoridades competentes serán informadas con prontitud de esta aprobación y de las principales razones para la destitución del responsable de una función de control interno.

19.2 Independencia de las funciones de control interno

158. Para que las funciones de control interno sean consideradas independientes, deberán cumplirse las siguientes condiciones:

a. su personal no realizará ninguna tarea operativa de cuyo seguimiento y control se ocupe la propia función de control;

b. estarán separadas, a nivel organizativo, de las actividades cuyo seguimiento y control le han sido encomendados;

c. sin perjuicio de la responsabilidad general de los miembros del órgano de administración de la entidad, el responsable de una función de control interno no dependerá de una persona que tenga la responsabilidad de gestionar las actividades que la función de control interno supervisa y controla, y

d. la remuneración del personal de las funciones de control interno no estará vinculada a los resultados de las actividades de cuyo seguimiento y control se ocupa la propia función de control interno, ni a otras circunstancias que puedan comprometer su objetividad[25].

19.3 Combinación de funciones de control interno

159. Teniendo en cuenta los criterios de proporcionalidad establecidos en el título I, la función de gestión de riesgos y la función de cumplimiento podrán combinarse. La función de auditoría interna no se combinará con ninguna otra función de control interno.

[25] Véanse también las directrices de la ABE sobre políticas de remuneración adecuadas, disponibles en: https://www.eba.europa.eu/regulation-and-policy/remuneration/guidelines-on-sound-remuneration-policies.

19.4 Recursos de las funciones de control interno

160. Las funciones de control interno dispondrán de recursos suficientes. Contarán con un número adecuado de empleados cualificados (tanto a nivel de la empresa matriz como de filial). El personal deberá estar cualificado en todo momento y recibirá la formación necesaria.

161. Las funciones de control interno tendrán a su disposición sistemas de TI y apoyo apropiados, con acceso a la información interna y externa necesaria para cumplir sus responsabilidades. Tendrán acceso a toda la información necesaria relativa a todas las líneas de negocio y a las filiales relevantes en la asunción de riesgos, en particular aquellas que potencialmente puedan generar riesgos importantes para las entidades.

20 Función de gestión de riesgos

162. Las entidades establecerá una función de gestión de riesgos (FGR) que abarque toda la entidad. La FGR tendrá autoridad, rango y recursos adecuados, teniendo en cuenta los criterios de proporcionalidad enumerados en el título I, para implementar políticas de riesgo y el marco de gestión de riesgos descrito en la sección 17.

163. Cuando sea necesario, la FGR tendrá acceso directo al órgano de administración en su función de supervisión y a sus comités, si se han constituido, incluido, en particular, el comité de riesgos.

164. La FGR tendrá acceso a todas las líneas de negocio y a otras unidades internas con potencial para generar riesgos, así como a las filiales y asociadas relevantes.

165. El personal de la FGR poseerá conocimientos, competencias y experiencia adecuados en relación con las técnicas y procedimientos de gestión de riesgos, así como con mercados y productos, y tendrá acceso a formación periódica.

166. La FGR será independiente de las líneas y unidades de negocio cuyos riesgos controle, pero no se impedirá que interactúe con ellas. La interacción entre las funciones operativas y la FGR deberá facilitar el objetivo de que todo el personal de la entidad asuma la responsabilidad de gestionar los riesgos.

167. La FGR será un elemento central de la organización de la entidad, y se estructurará de modo que pueda implementar las políticas de riesgos y controlar el marco de gestión de riesgos. La FGR desempeñará un papel esencial en la tarea de garantizar que la entidad tenga implantados procesos eficaces de gestión de riesgos. La FGR participará activamente en todas las decisiones importantes en materia de gestión de riesgos.

168. Las entidades significativas podrán establecer FGR específicas para cada línea de negocio importante. Sin embargo, deberá contar con una FGR central, que incluya una FGR de grupo a nivel de la entidad en base consolidada, para ofrecer una visión integral de todos los riesgos a nivel de la entidad y del grupo y garantizar el cumplimiento de la estrategia de riesgos.

169. La FGR proporcionará información, análisis y criterios expertos independientes y pertinentes sobre las exposiciones al riesgo y facilitará asesoramiento sobre las propuestas y las decisiones en materia de riesgos adoptadas por las líneas de negocio o las unidades internas, e informará al órgano de administración sobre si son coherentes con el apetito y la estrategia de riesgo de la entidad. La FGR podrá recomendar mejoras del marco de gestión de riesgos y medidas correctivas ante cualquier incumplimiento de las políticas, los procedimientos y los límites de riesgo.

20.1 Papel de la FGR en la estrategia y las decisiones en materia de riesgos

170. La FGR participará activamente, y en una fase inicial, en la elaboración de la estrategia de riesgo de una entidad y en asegurar que la entidad tenga implantados procedimientos eficaces de gestión de riesgos. La FGR proporcionará al órgano de dirección toda la información relevante relacionada con los riesgos a fin de permitirle establecer el nivel de apetito de riesgo de la entidad. La FGR evaluará la solidez y la sostenibilidad de la estrategia y el apetito de riesgo, y velará por que el dicho apetito se traduzca adecuadamente en límites de riesgo específicos. La FGR también evaluará las estrategias de riesgo de las unidades de negocio, incluidos los objetivos propuestos por estas, y participará antes de que el órgano de administración tome una decisión sobre tales estrategias. Los objetivos serán razonables y coherentes con la estrategia de riesgo de la entidad.

171. La participación de la FGR en los procesos de toma de decisiones garantizará que se tengan en cuenta debidamente los aspectos relacionados con los riesgos. Sin embargo, la responsabilidad de las decisiones adoptadas seguirá recayendo en las unidades de negocio e internas y, en última instancia, en el órgano de administración.

20.2 Papel de la FGR en los cambios significativos

172. En línea con la sección 18, antes de tomar decisiones sobre cambios significativos o transacciones excepcionales, la FGR participará en la evaluación del impacto de tales cambios y transacciones excepcionales en el riesgo global de la entidad y del grupo, e informará de sus conclusiones directamente al órgano de administración antes de que este tome una decisión.

173. La FGR evaluará cómo los riesgos identificados podrían afectar a la capacidad de la entidad o del grupo para gestionar su perfil de riesgo, su liquidez y su base sólida de capital en circunstancias normales y adversas.

20.3 Papel de la FGR en la identificación, medición, evaluación, gestión, mitigación, control y comunicación de los riesgos

174. La FGR se asegurará de que todas las unidades de la entidad identifiquen, evalúen, midan, controlen, gestionen y comuniquen adecuadamente todos los riesgos.

175. La FGR se asegurará de que la identificación y la evaluación no se basen únicamente en información cuantitativa o en resultados de modelos, sino que también tengan en cuenta enfoques cualitativos. La FGR mantendrá informado al órgano de administración sobre los supuestos utilizados y las posibles deficiencias de los modelos y del análisis de riesgos.

176. La FGR se asegurará de que se revisen las transacciones con partes vinculadas y de que se identifiquen y evalúen debidamente los riesgos que dichas transacciones planteen para la entidad.

177. La FGR se asegurará de que todos los riesgos identificados sean controlados de manera eficaz por las unidades de negocio.

178. La FGR hará un seguimiento periódico del perfil de riesgo real de la entidad, comparándolo cuidadosamente con sus objetivos estratégicos y con su apetito de riesgo, para que la función de dirección del órgano de administración pueda tomar decisiones y la función de supervisión pueda cuestionarlas.

179. La FGR analizará tendencias e identificará los riesgos nuevos o emergentes, así como el incremento de los riesgos derivados de cambios en las circunstancias y las condiciones. Asimismo, revisará periódicamente los resultados reales de los riesgos comparándolos con estimaciones previas (es decir, pruebas retrospectivas), con el fin de evaluar y mejorar la precisión y la eficacia del proceso de gestión de riesgos.

180. La FGR evaluará posibles formas de mitigar los riesgos. La información que se presente al órgano de administración incluirá propuestas de medidas de mitigación de riesgos apropiadas .

20.4 Papel de la FGR en exposiciones a riesgos no aprobadas

181. La FGR evaluará de forma independiente los incumplimientos del apetito o de los límites de riesgo (incluyendo la determinación de su causa y la realización de un análisis jurídico y económico del coste real de cerrar, reducir o cubrir la exposición al riesgo frente al coste potencial de mantenerla). La FGR informará a las unidades de negocio pertinentes y al órgano de administración, y recomendará posibles soluciones. La FGR informará directamente al órgano de administración en su función de supervisión cuando el incumplimiento sea significativo, sin perjuicio de que la FGR informe a otras funciones internas y comités.

182. La FGR desempeñará un papel fundamental a la hora de garantizar que se adopte una decisión sobre su recomendación al nivel adecuado, que las unidades de negocio correspondientes la cumplan y que se comunique debidamente al órgano de administración y, si se ha constituido, al comité de riesgos.

20.5 Responsable de la función de gestión de riesgos

183. El responsable de la FGR tendrá la responsabilidad de facilitar información exhaustiva y comprensible sobre los riesgos y de asesorar al órgano de administración para que este pueda entender el perfil global de riesgo de la entidad. Lo mismo es aplicable al responsable de la FGR de una entidad matriz con respecto a la situación consolidada.

184. El responsable de la FGR tendrá suficiente experiencia, independencia y categoría para cuestionar las decisiones que afecten a la exposición al riesgo de la entidad. Cuando el responsable de la FGR no sea miembro del órgano de administración, las entidades significativas nombrarán un responsable de la FGR independiente que no tenga responsabilidades en otras funciones y que informe directamente al órgano de administración. Cuando no resulte proporcionado nombrar una persona con dedicación exclusiva como responsable de la FGR, teniendo en cuenta el principio de proporcionalidad establecido en el título I, esta función se podrá combinar con la de responsable de la función de cumplimiento o podrá encomendarse a otro directivo, siempre que no haya un conflicto de intereses entre las funciones combinadas. En cualquier caso, esta persona deberá tener autoridad, rango e independencia suficientes (p. ej., responsable de los servicios jurídicos).

185. El responsable de la FGR podrá cuestionar las decisiones adoptadas por la dirección de la entidad y por su órgano de administración, y los motivos de objeción deberán documentarse formalmente. Si una entidad desea conceder al responsable de la FGR el derecho de veto de las decisiones (p. ej. sobre un crédito, una decisión de inversión o la fijación de un límite) adoptadas a niveles inferiores al órgano de administración, especificarán el alcance de ese derecho de veto y los procedimientos para elevar los asuntos o para apelar, y el papel que desempeñará el órgano de administración.

186. Las entidades establecerán procedimientos reforzados para la aprobación de decisiones sobre las que el responsable de la FGR haya expresado una opinión negativa. El órgano de administración en su función de supervisión deberá poder comunicarse directamente con el responsable de la FGR sobre cuestiones clave relativas a los riesgos, incluidos acontecimientos que puedan ser incompatibles con el apetito de riesgo y la estrategia de la entidad.

21 Función de cumplimiento

187. Las entidades establecerán una función de cumplimiento permanente y eficaz para gestionar el riesgo de cumplimiento y nombrarán a una persona responsable de esta función en toda la entidad (el director o responsable de cumplimiento).

188. Cuando no resulte proporcionado nombrar a una persona que únicamente desempeñe la función de responsable de cumplimiento, teniendo en cuenta el principio de proporcionalidad establecido en el título I, esta función se podrá combinar con la de responsable de la FGR o podrá encomendarse a otro directivo (p. ej., al responsable de los servicios jurídicos), siempre que no exista conflicto de intereses entre las funciones combinadas.

189. La función de cumplimiento, incluido su responsable, será independiente de las líneas de negocio y de las unidades internas que controla, y tendrá la autoridad, el rango y los recursos adecuados. Teniendo en cuenta los criterios de proporcionalidad establecidos en el título I, esta función podrá recibir asistencia de la FGR o combinarse con dicha función u otras funciones apropiadas, por ejemplo, los servicios jurídicos o recursos humanos.

190. El personal de la función de cumplimiento poseerá los conocimientos, las competencias y la experiencia adecuados en relación con los procedimientos de cumplimiento y otros procedimientos pertinentes, y tendrá acceso a formación periódica.

191. El órgano de administración en su función de supervisión vigilará la aplicación de una política de cumplimiento bien documentada, que se comunicará a todo el personal. Las entidades establecerán un proceso para evaluar periódicamente las modificaciones de las leyes y normativas aplicables a sus actividades.

192. La función de cumplimiento asesorará al órgano de administración sobre las medidas que se vayan a tomar para garantizar el cumplimiento de las leyes, normas, regulación y estándares aplicables, y evaluará el posible impacto de cualquier cambio en el entorno jurídico o regulatorio sobre las actividades de la entidad y el marco de cumplimiento.

193. La función de cumplimiento velará por que la supervisión del cumplimiento se lleve a cabo mediante un programa de supervisión del cumplimiento estructurado y bien definido y que se respete la política de cumplimiento. Dicha función informará al órgano de administración y se comunicará, según corresponda, con la FGR sobre el riesgo de cumplimiento de la entidad y su gestión. La función de cumplimiento y la FGR cooperarán e intercambiarán información, si procede, para realizar sus tareas respectivas. El órgano de administración y la FGR tendrán en cuenta las conclusiones de la función de cumplimiento en el proceso de toma de decisiones.

194. De conformidad con la sección 18 de estas directrices, la función de cumplimiento también verificará, en estrecha cooperación con la FGR y el departamento jurídico, que los nuevos productos y procedimientos cumplan con el marco jurídico vigente y, cuando proceda, con cualquier modificación conocida inminente de la legislación, la normativa y los requisitos de supervisión.

195. Las entidades adoptarán las medidas adecuadas frente a conductas fraudulentas internas o externas y frente a infracciones disciplinarias (p. ej., incumplimiento de procedimientos internos o de límites).

196. Las entidades se asegurarán de que sus filiales y sucursales tomen medidas para garantizar que sus operaciones cumplan las leyes y normativas locales. Si dichas leyes y normativas dificultan la aplicación de procedimientos y de sistemas de cumplimiento más estrictos implantados por el grupo, especialmente si impiden la divulgación y el intercambio de información necesaria entre entidades del grupo, las filiales y sucursales informarán al director o al responsable de cumplimiento de la entidad en base consolidada.

22 Función de auditoría interna

197. Las entidades establecerán una función de auditoría interna (FAI) independiente y eficaz, teniendo en cuenta los criterios de proporcionalidad establecidos en el título I, y nombrarán a una persona responsable de esta función en toda la entidad. La FAI será independiente y tendrá la autoridad, el rango y los recursos adecuados. En concreto, la entidad se asegurará de que la cualificación del personal de la FAI y los recursos de esta función, en particular sus herramientas de auditoría y métodos de análisis de los riesgos, sean adecuados al tamaño y el emplazamiento de la entidad, así como a la naturaleza, escala y complejidad de los riesgos asociados al modelo de negocio, las actividades, la cultura de riesgos y el apetito de riesgo de la entidad.

198. La FAI será independiente de las actividades auditadas. Por tanto, la FAI no deberá combinarse con ninguna otra función.

199. Utilizando un enfoque basado en el riesgo, la FAI verificará de forma independiente y asegurará 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 los requisitos externos. Todas las entidades del grupo estarán incluidas en el ámbito de competencias de la FAI.

200. La FAI no participará en el diseño, selección, establecimiento y aplicación de políticas, mecanismos y procedimientos específicos de control interno y límites de riesgo. Sin embargo, esto no impedirá que el órgano de administración en su función de gestión solicite información a la función de auditoría interna sobre cuestiones relacionadas con el riesgo, los controles internos y el cumplimiento de las normas aplicables.

201. La FAI evaluará si el marco de control interno de la entidad, como se establece en la sección 15, es eficaz y eficiente. En particular, la FAI evaluará:

a. la adecuación del marco de gobierno de la entidad;

b. si las políticas y procedimientos existentes siguen siendo apropiados y se adecúan a los requisitos legales y regulatorios y al apetito de riesgo y a la estrategia de la entidad;

c. la adecuación de los procedimientos a las leyes y normativas aplicables y a las decisiones del órgano de administración;

d. si los procedimientos se aplican de manera correcta y eficaz (p. ej., conformidad de las operaciones, el nivel de riesgo efectivamente incurrido, etc.), y

e. la idoneidad, calidad y efectividad de los controles realizados y de la información presentada por las unidades de negocio y por las funciones de gestión de riesgos y de cumplimiento.

202. La FAI verificará, en particular, la integridad de los procesos que garantizan la fiabilidad de los métodos y técnicas de la entidad, así como los supuestos y las fuentes de información utilizados en sus modelos internos (p. ej., la modelización de riesgos y la valoración contable). Deberá evaluar asimismo la calidad y la utilización de herramientas cualitativas de identificación y evaluación de los riesgos y las medidas de mitigación de riesgos adoptadas.

203. La FAI tendrá libre acceso a todos los registros, documentos, información y edificios de la entidad. Esto incluirá el acceso a los sistemas de información de gestión y a las actas de todos los comités y los órganos de decisión.

204. La FAI cumplirá las normas profesionales nacionales e internacionales. Un ejemplo de normas profesionales a las que se hace referencia en este apartado son las normas establecidas por el Instituto de Auditores Internos.

205. Los trabajos de auditoría interna se llevarán a cabo con arreglo a un plan de auditoría y a programas de auditoría detallados siguiendo un enfoque basado en el riesgo.

206. Se elaborará un plan de auditoría interna al menos una vez al año basándose en los objetivos anuales de control de la auditoría interna. El plan de auditoría interna deberá ser aprobado por el órgano de administración.

207. Todas las recomendaciones de auditoría se someterán a un procedimiento formal de seguimiento por parte de los niveles directivos adecuados, con el fin de garantizar e informar de su resolución eficaz y oportuna.

Título VI – Gestión de la continuidad del negocio

208. Las entidades establecerán un plan adecuado de gestión de la continuidad del negocio, con el fin de garantizar su capacidad para operar de forma continuada y limitar las pérdidas en caso de perturbaciones graves en el negocio.

209. Las entidades podrán establecer una función de continuidad del negocio independiente específica, por ejemplo, como parte de la FGR[26].

210. El negocio de una entidad depende de diversos recursos críticos (p. ej., sistemas de TI, incluidos servicios en la nube, sistemas de comunicación y edificios). La gestión de la continuidad del negocio tiene por objeto atenuar las consecuencias operativas, financieras, jurídicas,

[26] Véase también el artículo 312 del Reglamento (UE) n° 575/2013.

reputacionales y cualesquiera otras de importancia resultantes de una catástrofe o de una interrupción prolongada de estos recursos, y la consiguiente perturbación en los procedimientos de negocio ordinarios de la entidad. El objetivo de otras medidas de gestión de riesgos podría ser reducir la probabilidad de tales incidentes o en transferir su impacto financiero a terceros (p. ej., mediante seguros).

211. Para establecer un plan de continuidad del negocio adecuado, las entidades deberán analizar con detenimiento su exposición a perturbaciones graves y evaluar (cuantitativa y cualitativamente) su posible impacto, sirviéndose de datos internos y/o externos y de análisis de escenarios. Este análisis abarcará todas las líneas de negocio y unidades internas, incluida la FGR, y tendrá en cuenta su interdependencia. Los resultados del análisis contribuirán a definir las prioridades y los objetivos de recuperación de la entidad.

212. En función del análisis anterior, las entidades deberán elaborar:

a. planes de contingencia y de continuidad del negocio, con el fin de garantizar que la entidad reaccione adecuadamente ante situaciones de emergencia y pueda mantener sus actividades más importantes en caso de perturbación en sus procedimientos de negocio ordinarios, y

b. planes de recuperación de los recursos críticos que permitan a la entidad restablecer los procedimientos de negocio ordinarios en un plazo de tiempo apropiado. Cualquier riesgo residual derivado de posibles perturbaciones en el negocio será acorde con el apetito de riesgo de la entidad.

213. Los planes de contingencia, de continuidad del negocio y de recuperación deberán documentarse e implantarse con meticulosidad. La documentación deberá estar a disposición de las líneas de negocio, las unidades internas y la FGR, y se almacenará en sistemas físicamente separados y de fácil acceso en caso de contingencia. Se impartirá la formación apropiada. Los planes se someterán a prueba y se actualizarán periódicamente. Las dificultades o fallos detectados en las pruebas deberán documentarse y analizarse, y los planes se revisarán en consecuencia.

Título VII – Transparencia

214. Las estrategias, políticas y procedimientos se comunicarán a todo el personal pertinente de la entidad. El personal deberá conocer y cumplir las políticas y los procedimientos correspondientes a sus obligaciones y responsabilidades.

215. En consecuencia, el órgano de administración informará a toda la plantilla y la mantendrá al tanto de las estrategias y políticas de la entidad de manera clara y coherente, al menos en la medida necesaria para desempeñar sus obligaciones específicas. Esta información podrá facilitarse mediante guías escritas, manuales u otros medios.

216. Cuando las autoridades competentes exijan a las empresas matrices, de conformidad con el artículo 106, apartado 2, de la Directiva 2013/36/UE, publicar anualmente una descripción de su estructura jurídica y de gobierno y de la estructura organizativa del grupo de entidades, la información incluirá a todas las entidades de la estructura del grupo tal como se define en la Directiva 2013/34/UE[27], por país.

217. La información publicada deberá incluir al menos:

a. una descripción general de la organización interna de las entidades y de la estructura del grupo tal como se definen en la Directiva 2013/34/UE y en sus modificaciones, incluidos los principales canales de comunicación y responsabilidades;

b. cualquier cambio relevante desde la publicación anterior y la fecha de dicho cambio;

c. nuevas estructuras jurídicas, de gobernanza u organizativas;

d. información sobre la estructura, la organización y los miembros del órgano de administración, incluido el número de miembros y de los calificados como independientes, y especificando el género y la duración del mandato de cada miembro del órgano de administración;

e. las principales responsabilidades del órgano de administración;

f. una lista de los comités del órgano de administración en su función de supervisión y su composición;

g. una descripción general de la política de conflictos de intereses aplicable a las entidades y al órgano de administración;

h. una descripción general del marco de control interno; y

i. una descripción general del marco de gestión de la continuidad del negocio.

Anexo I – Aspectos que se deben tener en cuenta al establecer una política de gobierno interno

[27] Directiva 2013/34/UE del Parlamento Europeo y del Consejo, de 26 de junio de 2013, sobre los estados financieros anuales, los estados financieros consolidados y otros informes afines de ciertos tipos de empresas, por la que se modifica la Directiva 2006/43/CE del Parlamento Europeo y del Consejo y se derogan las Directivas 78/660/CEE y 83/349/CEE del Consejo (DO L 182 de 29.6.2013, p. 19).

En línea con el título III, las entidades considerarán los siguientes aspectos al documentar las políticas y los sistemas de gobierno interno:

1. Estructura del accionariado
2. Estructura del grupo, si corresponde (estructura jurídica y funcional)
3. Composición y funcionamiento del órgano de administración
   a) criterios de selección
   b) número, duración del mandato, rotación, edad
   c) miembros independientes del órgano de administración
   d) miembros ejecutivos del órgano de administración
   e) miembros no ejecutivos del órgano de administración
   f) división interna de funciones, si corresponde
4. Estructura de gobierno y organigrama (incluyendo, en su caso, el impacto en el grupo)
   a) comités especializados
      i. composición
      ii. funcionamiento
   b) comité ejecutivo, si existe
      i. composición
      ii. funcionamiento
5. Titulares de funciones clave
   a) responsable de la función de gestión de riesgos
   b) responsable de la función de cumplimiento
   c) responsable de la función de auditoria interna
   d) director financiero
   e) otros titulares de funciones clave
6. Marco de control interno
   a) descripción de cada función, incluida su organización, recursos, rango y autoridad
   b) descripción del marco de gestión de riesgos, incluida la estrategia de riesgo
7. Estructura organizativa (incluyendo, en su caso, el impacto en el grupo)
   a) estructura operativa, líneas de negocio y asignación de competencias y responsabilidades
   b) actividades externalizadas
   c) gama de productos y servicios
   d) expansión geográfica del negocio
   e) libre prestación de servicios

f) sucursales

g) filiales, agrupaciones temporales de empresas, etc.

h) uso de centros financieros extraterritoriales

8. Código de conducta y comportamiento (incluyendo, en su caso, el impacto en el grupo)
   a) objetivos estratégicos y valores corporativos
   b) códigos y reglamentos internos, política de prevención
   c) política en materia de conflictos de intereses
   d) denuncia de irregularidades
9. Situación de la política de gobierno interno, con fecha
   a) desarrollo
   b) última modificación
   c) última evaluación
   d) aprobación por el órgano de administración.