EBA/GL/2021/05

2 de julio de 2021

Borrador de 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) n.º 1093/2010[1]. De conformidad con el artículo 16, apartado 3, del Reglamento (UE) n.º 1093/2010, las autoridades competentes y las entidades financieras, incluidas las entidades, harán todo lo posible para atenerse a ellas.

2. En las directrices 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) n.º 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) n.º 1093/2010, las autoridades competentes deberán notificar a la Autoridad Bancaria Europea (ABE), a más tardar el (05.12.2021), 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/2021/05». 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, del Reglamento (UE) n.º 1093/2010.

[1] Reglamento (UE) n.º 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 n.º 716/2009/CE y se deroga la Decisión 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 con mayor detalle los sistemas, procedimientos y mecanismos de gobierno interno que las entidades sujetas a la Directiva 2013/36/UE[2] y las empresas de inversión sujetas al título VII de la Directiva 2013/36/UE en aplicación del artículo 1, apartados 2 y 5, del Reglamento 2019/2033/UE, deberían implementar de conformidad con el artículo 74, apartado 1, de la Directiva 2013/36/UE para garantizar su gestión eficaz y prudente.

Destinatarios

Estas directrices están dirigidas a las autoridades competentes según se definen en el artículo 4, apartado 2, inciso i), del Reglamento (UE) 1093/2010, así como a las entidades financieras definidas en el artículo 4, apartado 1, del mismo Reglamento, y que sean entidades a efectos de la aplicación de la Directiva 2013/36/UE según se definen en el artículo 3, apartado 1, punto 3, de la citada Directiva, teniendo en cuenta también el artículo 3, apartado 3, de dicha Directiva, o a las empresas de inversión sujetas al título VII de la Directiva 2013/36/UE en aplicación del artículo 1, apartados 2 y 5, del Reglamento 2019/2033/UE («entidades»).

Ámbito de aplicación

6. Las presentes directrices se aplican en relación con los sistemas de gobierno interno 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 todos los riesgos[3] a los que están o podrían estar expuestas, y el marco de control interno.

7. 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, deberían aplicarse independientemente de la estructura de gobierno (monista, dualista u otra) utilizada en los distintos Estados miembros. Se considerará que el órgano de dirección, tal como se define en el artículo 3, apartado 1, puntos 7 y 8, de la

[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] Cualquier referencia a los riesgos en estas directrices debería incluir los riesgos de blanqueo de capitales y financiación del terrorismo.

Directiva 2013/36/UE, tiene funciones de gestión (ejecutivas) y de supervisión (no ejecutivas)[4].

8. Los términos «órgano de dirección en su función de dirección» y «órgano de dirección en su función de supervisión» se utilizan en estas directrices sin hacer referencia a ninguna estructura de gobierno específica, y debería entenderse 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 dirección responsables de dicha función de conformidad con la legislación nacional. Al aplicar estas directrices, las autoridades competentes deberían tener en cuenta su legislación nacional en materia de sociedades y, cuando sea necesario, especificar a qué órgano o miembros del órgano de dirección se deberían referir estas funciones.

9. En los Estados miembros donde el órgano de dirección 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 dirección. A los efectos de las presentes directrices, cualquier referencia al órgano de dirección en su función de dirección debe entenderse que incluye también a los miembros del órgano ejecutivo o al primer ejecutivo (CEO), tal como se definen en estas directrices, incluso si no han sido propuestos o designados como miembros formales del órgano u órganos de gobierno de la entidad, de conformidad con la legislación nacional.

10. 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 dirección, las entidades deberían asegurase de que tales responsabilidades y las decisiones relacionadas con aquellas estén alineadas, en la medida de lo posible, con las directrices aplicables al órgano de dirección.

11. 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.

12. Las entidades deberían cumplir y las autoridades competentes deberían velar por que las entidades 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

13. A menos que se indique lo contrario, los términos utilizados y definidos en la Directiva 2013/36/UE y en el Reglamento (UE) n.º 575/2013 tienen idéntico significado en estas

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

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 los 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.
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 dirección 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 actividades siguientes: gestión de recursos financieros, planificación financiera e información financiera.
Brecha salarial de género	La diferencia entre el salario bruto medio por hora de hombres y mujeres, expresada como porcentaje del salario bruto medio por hora de los hombres.
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 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 dirección de una entidad u otra persona jurídica.
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[6].
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 dirección 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 dirección, 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.

3. Aplicación

Fecha de aplicación

14. Estas directrices actualizadas serán de aplicación a partir del 31 de diciembre de 2021.

[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).

[6] Véase también la norma técnica de regulación sobre consolidación prudencial, disponible (en inglés) en: https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Draft%20Technical%20Standards/2021/973355/Final%20Report%20Draft%20RTS%20methods%20of%20consolidation.pdf.

Derogación

15. Las Directrices de la ABE sobre gobierno interno (EBA/GL/2017/11) del 26 de septiembre de 2017 quedarán derogadas con efectos a partir del 31 de diciembre de 2021.

4. Directrices

Título I - Proporcionalidad

16. 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 las disposiciones y los requisitos regulatorios.

17. Las entidades deberían tener en cuenta su tamaño y organización interna, así como la naturaleza, escala y complejidad de sus actividades, al desarrollar y aplicar sus sistemas de gobierno interno. Las entidades significativas deberían contar con sistemas de gobierno más sofisticados, mientras que las entidades pequeñas y menos complejas pueden aplicar sistemas de gobierno más sencillos. No obstante, las entidades deberían tener en cuenta que el tamaño o la importancia sistémica de una entidad pueden no ser, por sí mismos, indicativos del grado de exposición de una entidad a los riesgos.

18. A efectos de la aplicación del principio de proporcionalidad y para garantizar la aplicación adecuada de los requisitos regulatorios y de las presentes directrices, las entidades y las autoridades competentes deberían tener 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 forma 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 proceso de revisión y evaluación supervisora (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;

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

m. si la entidad encaja en la definición de «entidad pequeña y no compleja» o de «entidad grande» recogidas en el artículo 4, apartado 1, puntos 145 y 146, del Reglamento (UE) n.º 575/2013.

Título II – Funciones y composición del órgano de dirección y de los comités

1 Funciones y responsabilidades del órgano de dirección

19. De conformidad con el artículo 88, apartado 1, de la Directiva 2013/36/UE, el órgano de dirección 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.

20. Las funciones del órgano de dirección deberían estar 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 dirección deberían describirse en un documento escrito y debidamente aprobado por dicho órgano. Todos los miembros del órgano de dirección deberían conocer bien la estructura y las responsabilidades de dicho órgano y la distribución de tareas entre las distintas funciones del órgano de dirección y sus comités.

21. El órgano de dirección en su función de supervisión y en su función de dirección deberían interactuar de manera eficaz. Ambas funciones deberían intercambiar información suficiente para permitirles desempeñar sus respectivas funciones. A fin de contar con controles y contrapesos adecuados, los procesos de toma de decisiones del órgano de dirección no deberían estar dominados por un solo miembro o un pequeño grupo de miembros.

22. Las responsabilidades del órgano de dirección deberían incluir 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, el apetito de riesgo de la entidad y su marco de gestión de riesgos, así como las medidas para garantizar que el órgano de dirección dedique tiempo suficiente a las cuestiones relacionadas con los riesgos y a la gestión de riesgos;

c. un marco de gobierno interno y de control interno adecuado y eficaz, según se define en el título V, que:

i. incluya una estructura organizativa clara y funciones internas de gestión de riesgos, de cumplimiento y de auditoría independientes, que funcionen adecuadamente y que cuenten con la autoridad, el rango y los recursos suficientes para desempeñar sus cometidos correctamente;

ii. garantice el cumplimiento de los requisitos regulatorios aplicables en el contexto de prevención del blanqueo de capitales y la financiación del terrorismo;

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 del artículo 74, apartado 3, y el artículo 75, apartado 2, de la Directiva 2013/36/UE[7];

g. medidas que garanticen que las evaluaciones de idoneidad, individuales y en su conjunto, del órgano de dirección se lleven a cabo eficazmente, que la composición y la planificación de la sucesión del órgano de dirección sean adecuadas, y que el órgano de dirección desempeñe sus funciones con eficacia[8];

h. un proceso de selección y de evaluación de la idoneidad para los titulares de funciones clave[9];

[7] Directrices de la ABE sobre políticas de remuneración adecuadas.

[8] Véanse también las directrices conjuntas de la Autoridad Europea de Valores y Mercados (AEVM) y la ABE sobre la evaluación de la idoneidad de los miembros del órgano de administración y de los titulares de funciones clave.

[9] Véanse también las directrices conjuntas de la AEMV y la ABE sobre la evaluación de la idoneidad de los miembros del órgano de dirección y los titulares de funciones clave.

i. disposiciones que garanticen el funcionamiento interno de cada comité del órgano de dirección, si se ha 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 dirección, 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;

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.

23. Al establecer, aprobar y supervisar la aplicación de los aspectos enumerados en el apartado 22, el órgano de dirección debería tratar de garantizar un modelo de negocio y un sistema de gobierno, incluyendo un marco de gestión de riesgos, que tengan en cuenta todos los riesgos. Al tener en cuenta todos los riesgos a los que están expuestos las entidades, estas deberían considerar todos los factores de riesgo relevantes, incluidos los riesgos ambientales, sociales y de gobernanza (ASG). Las entidades deberían tener en cuenta que estos últimos pueden orientar sus riesgos prudenciales, incluidos los riesgos de crédito, por ejemplo a través de factores de riesgo relacionados con la transición hacia una economía sostenible o con eventos climáticos externos que pueden afectar a los deudores, al mercado, a la liquidez, a los riesgos operativos y a los reputacionales, por ejemplo a través de factores de riesgo sociales y de gobernanza, en particular en el contexto de los acuerdos de externalización[10]. Estos riesgos incluyen, por ejemplo, riesgos legales en el ámbito del Derecho contractual o laboral, riesgos relacionados con posibles violaciones de los derechos humanos u otros factores de riesgo ambientales, sociales y de gobernanza que puedan afectar al país en el que esté ubicado un prestador de servicios y a su capacidad para prestar los niveles de servicio acordados.

[10] Véase el informe de la ABE sobre gestión y supervisión de riesgos ASG, publicado en virtud del artículo 98, apartado 8, de la Directiva sobre Requisitos de Capital (DRC), en el que se describe cómo entiende la ABE los riesgos ASG, los canales de transmisión y las recomendaciones acerca de los sistemas, procesos, mecanismos y estrategias que deben establecer las entidades para identificar, evaluar y gestionar los riesgos ASG.

24. El órgano de dirección 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 dirección deberían 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 dirección puede 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 dirección debería realizar un seguimiento, revisar periódicamente y abordar cualquier deficiencia identificada en la ejecución de procesos, estrategias y políticas relacionadas con las responsabilidades enumeradas en los apartados 22 y 23. El marco de gobierno interno y su aplicación deberían revisarse y actualizarse 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 debería llevar a cabo una revisión más detallada.

2 Función de dirección del órgano de dirección

28. El órgano de dirección en su función de dirección debería participar activamente en las actividades de la entidad y tomar decisiones sobre una base adecuada y bien fundamentada.

29. El órgano de dirección en su función de dirección debería ser responsable de la ejecución de las estrategias fijadas por dicho órgano y analizar periódicamente la aplicación e idoneidad de esas estrategias con el órgano de dirección en su función de supervisión. Los directivos de la entidad pueden encargarse de su ejecución práctica.

30. El órgano de dirección en su función de dirección debería cuestionar de forma constructiva y analizar con espíritu crítico las propuestas, explicaciones e información que reciba para formarse un criterio y tomar decisiones. El órgano de dirección en su función de dirección debería informar al órgano de dirección 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.

31. Sin perjuicio de la transposición de las disposiciones de la Directiva 2015/849/UE a la legislación nacional, el órgano de dirección debería designar a uno de sus miembros, en línea con los requisitos del artículo 46, apartado 4, de la Directiva 2015/849/UE («Directiva antiblanqueo»), para que sea responsable de la aplicación de las disposiciones legislativas,

reglamentarias y administrativas necesarias para cumplir con lo dispuesto en dicha directiva, incluidas las correspondientes políticas y procedimientos de prevención del blanqueo de capitales y la financiación del terrorismo de la entidad a nivel del órgano de dirección[11].

3 Función de supervisión del órgano de dirección

32. Las funciones de los miembros del órgano de dirección en su función de supervisión deberían incluir el seguimiento y la crítica constructiva de la estrategia de la entidad.

33. Sin perjuicio de la legislación nacional, el órgano de dirección en su función de supervisión debería incluir a 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 idoneidad 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.

34. Sin perjuicio de las responsabilidades asignadas en virtud de la legislación nacional en materia de sociedades, el órgano de dirección en su función de supervisión debería:

    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 dirección 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 proporcionadas por los miembros del órgano de dirección 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, 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;

[11] Dada su condición de órgano colegiado, el órgano de dirección sigue asumiendo la responsabilidad de forma solidaria o colectiva.

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 dirección 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 auditoría, cuando dichos comités se hayan constituido.

4 Funciones del presidente del órgano de dirección

35. El presidente del órgano de dirección debería dirigir dicho órgano, contribuir a que haya un flujo de información eficaz en su seno y entre este órgano y sus comités, cuando se hayan constituido, y ser responsable de que su funcionamiento general sea eficaz.

36. El presidente debería promover e incentivar debates abiertos y críticos y asegurarse de que las opiniones discrepantes puedan expresarse y considerarse en el proceso de toma de decisiones.

37. Como principio general, el presidente del órgano de dirección debería ser un miembro no ejecutivo de este. Cuando el presidente tenga permitido asumir funciones ejecutivas, la entidad debería 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 dirección 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 dirección en su función de supervisión de una entidad 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.

38. El presidente debería establecer los órdenes del día de las reuniones y asegurarse de que los temas estratégicos se traten con prioridad. Debería asegurarse de que las decisiones del órgano de dirección 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.

39. El presidente del órgano de dirección debería contribuir a que las responsabilidades entre los miembros de dicho órgano de dirección 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 una manera adecuada y bien fundamentada.

5 Comités del órgano de dirección en su función de supervisión

5.1 Constitución de los comités

40. 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[12] y de remuneraciones[13] para asesorar al órgano de dirección 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.

41. Cuando no se constituya un comité de riesgos o de nombramientos, las referencias en estas directrices a dichos comités deberían interpretarse como aplicables al órgano de dirección en su función de supervisión, teniendo en cuenta el principio de proporcionalidad recogido en el título I.

42. Las entidades pueden constituir otros comités (p. ej., de prevención del blanqueo de capitales y de la financiación del terrorismo, de ética, de conducta y de cumplimiento) teniendo en cuenta los criterios establecidos en el título I de las presentes directrices.

43. Las entidades deberían asegurarse de asignar y distribuir claramente las funciones y los cometidos entre los comités especializados del órgano de dirección.

44. Cada comité debería tener un mandato documentado, incluido su ámbito de responsabilidad, otorgado por el órgano de dirección en su función de supervisión, y establecer procedimientos de trabajo adecuados.

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

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

[13] Con respecto al comité de remuneraciones, consúltense las Directrices de la ABE sobre prácticas de remuneración adecuadas.

5.2 Composición de los comités[14]

46. Todos los comités deberían estar presididos por un miembro no ejecutivo del órgano de dirección que pueda actuar con objetividad.

47. Los miembros independientes [15] del órgano de dirección en su función de supervisión participarán activamente en los comités.

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

49. Las entidades deberían asegurarse, teniendo en cuenta el tamaño del órgano de dirección y el número de miembros independientes de dicho órgano en su función de supervisión, de que la composición de los comités no sea idéntica.

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

51. Los comités de riesgos y de nombramientos deberían estar compuestos por miembros no ejecutivos del órgano de dirección en su función de supervisión de la entidad de que se trate. La composición del comité de auditoría debería establecerse de conformidad con el artículo 41 de la Directiva 2006/43/CE[16], y la del comité de remuneración de acuerdo con la sección 2.4.1 de las Directrices de la ABE sobre políticas de remuneración adecuadas[17].

52. En el caso de EISM y OEIS, el comité de nombramientos debería incluir 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 debería incluir un número suficiente de miembros independientes; estas entidades también pueden considerar una buena práctica que el presidente del comité de nombramientos sea independiente.

53. Los miembros del comité de nombramientos deberían tener, 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 establecidos en la Directiva 2013/36/UE.

[14] Esta sección debería leerse junto con las directrices conjuntas de la AEMV y la ABE sobre la evaluación de la idoneidad 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.

[15] Como se definen en la sección 9.3 de las directrices conjuntas de la AEMV y la ABE sobre la evaluación de la idoneidad 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.

[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, p. 87), en su versión modificada por la Directiva 2014/56/UE del Parlamento Europeo y del Consejo, de 16 de abril de 2014.

[17] Directrices de la ABE sobre políticas de remuneración adecuadas en virtud del artículo 74, apartado 3, y el artículo 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).

54. En el caso de EISM y OEIS, el comité de riesgos debería incluir 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 debería incluir 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 debería presidir el órgano de dirección ni ningún otro comité.

55. Los miembros del comité de riesgos deberían tener, 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

56. Los comités deberían informar periódicamente al órgano de dirección en su función de supervisión.

57. Los comités deberían interactuar entre sí cuando sea preciso. Sin perjuicio de lo dispuesto en el apartado 49, 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.

58. Los miembros de los comités deberían entablar debates abiertos y críticos en los que las opiniones discrepantes se aborden de manera constructiva.

59. Los comités deberían documentar los órdenes del día de sus reuniones, así como los principales acuerdos y conclusiones.

60. Los comités de riesgos y de nombramientos deberían, como mínimo:

    a. tener acceso a toda la información relevante y a los datos necesarios para desempeñar su función, incluidos los provenientes de las funciones corporativas y de control pertinentes (por ejemplo, servicios jurídicos, función financiera, recursos humanos, TI, auditoría interna, riesgos, cumplimiento, incluida la información sobre el cumplimiento de la normativa de prevención del blanqueo de capitales y de la financiación del terrorismo e información agregada acerca de las comunicaciones de operaciones sospechosas, así como acerca de los factores de riesgo de blanqueo de capitales y de financiación del terrorismo);

    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[18] que pueda haberse producido, con información detallada y

[18] En relación con infracciones graves en el ámbito de la prevención del blanqueo de capitales y de la financiación del terrorismo. Consúltense también las directrices que deben elaborarse en virtud del artículo 117, apartado 6, de la Directiva 2013/36/UE, en las que se especificará la forma de cooperación e intercambio de información entre las

recomendaciones relativas a las medidas correctivas adoptadas, que se adoptarán o que se hayan propuesto para abordarla; analizar periódicamente y decidir el contenido, el formato y la frecuencia de la información sobre riesgos sobre los que se vaya a informar a los comités, y

c. 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

61. Si se ha constituido, el comité de riesgos debería, como mínimo:

a. asesorar y apoyar al órgano de dirección en su función de supervisión en relación con el seguimiento de la estrategia general de riesgo y del apetito 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 dirección 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, operativos (incluidos los legales y tecnológicos) y reputacionales, a fin de evaluar su adecuación a la estrategia de riesgo y al apetito de riesgo aprobados;

d. recomendar al órgano de dirección en su función de supervisión los ajustes de 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 las 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 para recibir 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;

autoridades a las que hace referencia el apartado 5 de dicho artículo, particularmente en relación con grupos transfronterizos y en el contexto de la identificación de infracciones graves de las normas de prevención del blanqueo de capitales.

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[19]. El comité de riesgos debería evaluar los riesgos asociados a los productos y servicios financieros ofrecidos y tener 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.

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

63. Si se ha constituido, el comité de riesgos debe examinar, 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 periodo de generación de beneficios.

5.5 Funciones del comité de auditoría

64. De conformidad con la Directiva 2006/43/CE[20], cuando se haya constituido, el comité de auditoría debería, 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

[19] Véanse también las Directrices de la ABE sobre procedimientos de gobierno y vigilancia de productos de banca minorista, disponibles en https://www.eba.europa.eu/sites/default/documents/files/documents/10180/1412678/0defef0f-3f21-4e96-9175-73b1884e906a/EBA-GL-2015-18%20Guidelines%20on%20product%20oversight%20and%20Governance_ES.pdf?retry=1.

[20] 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 última vez por la Directiva 2014/56/UE del Parlamento Europeo y del Consejo, de 16 de abril de 2014.

Directiva 2006/43/UE y el artículo 6 del Reglamento (UE) n.º 537/2014 [21] 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 su resultado, teniendo en cuenta las observaciones y las conclusiones de 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, del Reglamento (UE) n.º 537/2014], 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

65. De conformidad con el artículo 76, apartado 3, de la Directiva 2013/36/UE, las autoridades competentes pueden 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.

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

67. Las entidades deberían velar en todo momento por que los miembros de un comité conjunto posean, individual y colectivamente, los conocimientos, las competencias y la experiencia

[21] Reglamento (UE) n.º 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).

necesarios para comprender plenamente las funciones que debe desempeñar el comité conjunto[22].

Título III – Marco de gobierno

6 Marco organizativo y estructura

6.1 Marco organizativo

68. El órgano de dirección de una entidad debería asegurarse de que la estructura organizativa y operativa de dicha entidad sea adecuada y transparente, y debería disponer de una descripción escrita de la misma. Dicha estructura debería fomentar y acreditar la gestión prudente y eficaz de la entidad a nivel individual, subconsolidado y consolidado. El órgano de dirección debería velar 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 apropiados 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, deberían estar bien definidos, ser claros, coherentes y exigibles, y estar debidamente documentados. La documentación debería actualizarse según corresponda.

69. La estructura de la entidad no debería comprometer la capacidad del órgano de dirección 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.

70. El órgano de dirección debería determinar 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 identifiquen deficiencias, el órgano de dirección debería realizar los ajustes que sean necesarios con rapidez.

6.2 Conoce tu estructura

71. El órgano de dirección debería conocer y entender plenamente la estructura jurídica, organizativa y operativa de la entidad («conoce tu estructura»), y debería velar por que sea conforme con la estrategia de negocio y el perfil de riesgo aprobados y por que esté cubierta por su marco de gestión de riesgos.

72. El órgano de dirección debería ser 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 deberían afectar al diseño de su gobierno interno, ni a la gestión y la vigilancia

[22] Véanse también las directrices conjuntas de la AEMV y la ABE sobre la evaluación de la idoneidad 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.

eficaces de los riesgos del grupo en su conjunto. El órgano de dirección debería asegurarse 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.

73. El órgano de dirección debería dirigir la estructura de la entidad, su evolución y sus limitaciones, y velar por que esta estructura esté justificada y sea eficiente, y no entrañe una complejidad indebida o inadecuada.

74. El órgano de dirección de una entidad en base consolidada debería 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 operativos 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 dirección debería velar 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 todas las exigencias de información a efectos de supervisión a nivel individual, subconsolidado y consolidado.

75. El órgano de dirección de una entidad en base consolidada debería velar 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 deberían documentarse y ponerse a disposición de las funciones pertinentes interesadas, incluidos el órgano de dirección, las líneas de negocio y las funciones de control interno. Se debería mantener informados a los miembros del órgano de dirección de una entidad en base consolidada 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 las entidades individuales 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

76. Las entidades deberían evitar establecer estructuras complejas y potencialmente no transparentes. Al tomar decisiones, deberían tener en cuenta los resultados de la evaluación de riesgos realizada para identificar si tales estructuras podrían utilizarse con fines relacionados con el blanqueo de capitales, la financiación del terrorismo u otros delitos financieros, así como los mecanismos de control correspondientes y el marco jurídico vigente[23]. Con este fin, las entidades deberían tener en cuenta, como mínimo:

    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[24];

    b. hasta qué punto la estructura tiene una finalidad económica y lícita aparente;

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

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

    e. si la estructura podría impedir una vigilancia adecuada por parte del órgano de dirección 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.

77. En cualquier caso, las entidades no deberían establecer 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.

78. Al establecer tales estructuras, el órgano de dirección debería 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 deberían aprobarse y mantenerse cuando su finalidad haya sido claramente definida y entendida, y cuando el órgano de dirección 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

[23] Para más detalles sobre la evaluación del riesgo asociado a países y del riesgo vinculado a productos y clientes individuales, las entidades deberían consultar también las directrices conjuntas sobre los factores de riesgo de blanqueo de capitales y de financiación del terrorismo (EBA GL JC/2017/37), actualmente en revisión.

[24] Véase también: https://eba.europa.eu/regulation-and-policy/anti-money-laundering-and-e-money/rts-on-the-implementation-of-group-wide-aml/cft-policies-in-third-countries.

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 debería ser la supervisión de la estructura.

79. Las entidades deberían documentar sus decisiones y poder justificarlas ante las autoridades competentes.

80. El órgano de dirección debería velar 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, flujos 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 dirección 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.

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

82. Las actividades atípicas o no transparentes que las entidades realicen para sus clientes (p. ej., ayudarles a establecer sociedades instrumentales en centros financieros extraterritoriales, desarrollar estructuras complejas, financiarles transacciones o proporcionar servicios de fideicomiso) y que generen riesgos operativos y reputacionales significativos deberían 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 riesgos similares en materia de gobierno interno. En particular, las entidades deberían analizar la razón por la cual un cliente desea establecer una estructura concreta.

7 Marco organizativo en un contexto de grupo

83. De conformidad con el artículo 109, apartado 2, de la Directiva 2013/36/UE, las empresas matrices y las filiales sujetas a dicha Directiva deberían asegurarse de que los sistemas, procedimientos y mecanismos de gobierno sean coherentes y estén bien integrados en base consolidada o subconsolidada. Con este fin, las empresas matrices y las filiales incluidas en el ámbito de consolidación prudencial deberían implementar tales sistemas, procedimientos y

mecanismos en sus filiales que no estén sujetas a la Directiva 2013/36/UE, incluidas las establecidas en terceros países, también en centros financieros extraterritoriales, para garantizar que los procedimientos de gobierno de que disponen son adecuados en base consolidada y subconsolidada. En relación con los requisitos de remuneración, son aplicables determinadas excepciones en línea con el artículo 109, apartados 4 y 5[25]. Las funciones competentes de la entidad en base consolidada y de sus filiales deberían interactuar e intercambiar datos e información según sea necesario. Los sistemas, procedimientos y mecanismos de gobierno deberían asegurar que la entidad en base consolidada disponga de datos e información suficientes y para poder evaluar el perfil de riesgo de todo el grupo, como se detalla en la sección 6.2.

84. El órgano de dirección de una filial sujeta a la Directiva 2013/36/UE debería adoptar y aplicar a nivel individual las políticas de gobierno 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.

85. La entidad en base consolidada debería asegurarse del cumplimiento a nivel consolidado y subconsolidado de las políticas de gobierno del grupo y del marco de control interno a que se hace referencia en el título V por parte de todas las entidades y de otras instituciones incluidas en el ámbito de consolidación prudencial, incluidas también las filiales que no estén sujetas a la Directiva 2013/36/UE. Al implementar políticas de gobierno, la entidad en base consolidada debería asegurarse de que existan sistemas de gobierno adecuados para cada filial y considerar 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.

86. Las entidades en base consolidada deberían considerar 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.

87. Las empresas matrices y sus filiales deberían asegurarse de que las entidades e instituciones del grupo cumplen todos los requisitos regulatorios específicos en cualquier jurisdicción pertinente.

88. Las entidades en base consolidada deberían asegurarse 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 gobierno 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 esto no sea ilícito conforme al ordenamiento jurídico del tercer país.

89. Los requerimientos sobre gobernanza de la Directiva 2013/36/UE y las disposiciones de estas directrices se aplican a las entidades con independencia de que sean filiales de una entidad

[25] Consúltense también las Directrices de la ABE sobre políticas de remuneración adecuadas.

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 debería asegurarse de 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 las especificaciones adicionales de estas directrices.

90. Al establecer políticas y documentar los sistemas de gobierno, las entidades deberían tener 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 deberían considerar su combinación en un único documento o que este documento haga referencia a ambas.

8 Política de externalización[26]

91. El órgano de dirección debería aprobar, y revisar y actualizar periódicamente, la política de externalización de la entidad, asegurando la aplicación oportuna de los cambios apropiados.

92. La política de externalización debería considerar el impacto de la externalización en las actividades de la entidad y los riesgos a los que se enfrenta (como los riesgos operativos, incluidos los riesgos legales y tecnológicos, los riesgos reputacionales y de concentración). Esta política debería recoger 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.

93. La política debería poner de manifiesto que los procedimientos de externalización no deberían impedir la supervisión eficaz *in situ* o a distancia de la entidad ni contravenir ninguna restricción sobre servicios y actividades impuesta por el supervisor. La política también debería abarcar la externalización intragrupo (es decir, la prestación de servicios por una entidad jurídica separada perteneciente al propio grupo) y tener en cuenta cualquier circunstancia específica del grupo.

[26] Véase también: Directrices de la ABE sobre externalización, disponibles en: https://www.eba.europa.eu/sites/default/documents/files/documents/10180/2761380/9ce29347-20e1-41d0-a8d7-6019bc6b1bf8/EBA%20revised%20Guidelines%20on%20outsourcing_ES.pdf?retry=1.

Título IV - Cultura de riesgos y conducta profesional

9 Cultura de riesgos

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

95. Las entidades deberían desarrollar 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, deberían desarrollar su cultura de riesgos a través de políticas, de la comunicación y la formación del personal, y deberían adaptar 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 debería ser 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 dirección, deberían ser 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 debería incluir, entre otros, los siguientes elementos:

    a. Actitud de los directivos: el órgano de dirección debería ser responsable de establecer y comunicar los valores fundamentales de la entidad y sus expectativas. El comportamiento de sus miembros debería reflejar 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 comunicación de infracciones). El órgano de dirección debería promover, supervisar y evaluar la cultura de riesgos de la entidad de forma continua, considerar 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 deberían 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 debería estar capacitado para desempeñar sus funciones y ser 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 debería promover un entorno de comunicación abierta y de 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 debería desempeñar 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[27].

10 Valores corporativos y código de conducta

99. El órgano de dirección debería desarrollar, adoptar, observar y promover rigurosas normas éticas y profesionales, teniendo en cuenta las necesidades y las características específicas de la entidad, y debería garantizar la aplicación de dichas normas (a través de un código de conducta o un instrumento similar). También debería supervisar el cumplimiento de estas normas por parte del personal. Cuando corresponda, el órgano de dirección podrá adoptar y aplicar las normas al grupo o las normas comunes publicadas por asociaciones u otras organizaciones relevantes.

100. Las entidades deberían asegurarse de que ningún miembro del personal sea objeto de discriminación por su género, raza, color de piel, origen étnico o social, características genéticas, lengua, religión o creencia, opinión política o de otro tipo, pertenencia a una minoría nacional, patrimonio, nacimiento, discapacidad, edad u orientación sexual.

101. Las políticas de la entidad deberían ser no discriminatorias en cuanto al género. Esto incluye, con carácter no limitativo, la remuneración, las políticas de contratación, los planes de desarrollo profesional y de sucesión, el acceso a formación y la posibilidad de optar a vacantes internas. Las entidades deberían garantizar la igualdad de oportunidades[28] para todo el personal con independencia de su género, incluido en lo que respecta a las perspectivas de desarrollo profesional, y deberían tener como objetivo mejorar la representación del género menos representado en el órgano de dirección y en el grupo del personal con responsabilidades de dirección, según se define en el Reglamento Delegado de la Comisión (normas técnicas de regulación para la determinación del colectivo identificado)[29]. Las entidades deberían realizar un seguimiento de la evolución de la brecha salarial de género de forma diferenciada para el colectivo identificado (excluyendo a los miembros del órgano de dirección), los miembros del órgano de dirección en su función de

[27] Véanse también las Directrices de la ABE sobre políticas de remuneración adecuadas en virtud del artículo 74, apartado 3, y el artículo 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.

[28] Véase también la Directiva 2006/54/CE del Parlamento Europeo y del Consejo, de 5 de julio de 2006, relativa a la aplicación del principio de igualdad de oportunidades e igualdad de trato entre hombres y mujeres en asuntos de empleo y ocupación.

[29] Véanse también las Directrices de la ABE sobre políticas de remuneración no discriminatorias en cuanto al género.

dirección, los miembros del órgano de dirección en su función de supervisión y el resto del personal. Las entidades deberían contar con políticas que faciliten la reincorporación del personal tras el permiso de maternidad, paternidad o parental.

102. Las normas aplicadas deberían tratar de mejorar los sólidos sistemas de gobierno de la entidad y de reducir los riesgos a los que está expuesta, en particular los riesgos operativos 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 y penales, y la pérdida del valor de marca y la confianza de los consumidores.

103. El órgano de dirección debería contar con políticas claras y documentadas sobre cómo deberían cumplirse estas normas. Estas políticas deberían:

a. recordar al personal que todas las actividades de la entidad deberían 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 dirección de que las actividades no irán más allá del apetito de riesgo definido y de 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, con carácter no limitativo, fraude, blanqueo de capitales y financiación del terrorismo, prácticas antimonopolio, sanciones financieras, soborno y corrupción, manipulación del mercado, ventas inadecuadas y otras infracciones de la legislación de protección del consumidor, así como delitos fiscales cometidos de forma directa o indirecta, también a través de estrategias de arbitraje fiscal ilícitas o prohibidas;

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, y de las acciones legales y sanciones que pueden derivarse de una conducta irregular y de comportamientos inaceptables.

104. Las entidades deberían supervisar el cumplimiento de tales normas y asegurarse de la concienciación del personal, por ejemplo, mediante formación. Las entidades deberían definir qué función será la responsable de supervisar el cumplimiento y evaluar las infracciones del código de conducta o un instrumento similar y establecer un procedimiento a seguir en casos

de incumplimiento. Las conclusiones deberían notificarse periódicamente al órgano de dirección.

11 Política de conflictos de interés a nivel de la entidad

105. El órgano de dirección debería ser responsable de establecer, aprobar y supervisar la aplicación y el mantenimiento de políticas eficaces para identificar, evaluar, gestionar y mitigar o prevenir conflictos de interés 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.

106. Las entidades deberían adoptar medidas adecuadas en el marco de sus procedimientos organizativos y administrativas para evitar que los conflictos de interés afecten negativamente a los intereses de sus clientes.

107. Las medidas de las entidades para gestionar o, en su caso, mitigar los conflictos de interés, deberían 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 ciertas líneas o unidades de negocio.

12 Política de conflictos de interés para el personal[30]

108. El órgano de dirección debería ser 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 dirección, lo que podría influir adversamente en el desempeño de sus deberes y responsabilidades. Las entidades en base consolidada deberían considerar los intereses dentro de la política de conflictos de interés del grupo a nivel consolidado o subconsolidado.

109. La política debería tener como objetivo identificar los conflictos de interés del personal, incluidos los intereses de los familiares más cercanos. Las entidades deberían tener 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

[30] Esta sección debe leerse junto con las directrices conjuntas de la AEMV y la ABE sobre la evaluación de la idoneidad 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.

entidades deberían valorar su importancia y acordar y aplicar medidas apropiadas para mitigarlos.

110. Con respecto a los conflictos de interés que puedan surgir de relaciones anteriores, las entidades deberían establecer un plazo apropiado para que el personal informe de tales conflictos, por considerar que aún pueden tener un impacto sobre el comportamiento del personal y su participación en la toma de decisiones.

111. La política debería abarcar al menos las siguientes situaciones o relaciones en las que pueden surgir conflictos de interés:

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 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.

112. No obstante lo anterior, las entidades deberían tener en cuenta que ser accionista de una entidad o 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 interés si permanecen dentro de un umbral mínimo adecuado.

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

114. La política debería diferenciar entre los conflictos de interés 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 del 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 debería ser primordial en la toma de decisiones.

115. La política debería establecer procedimientos, medidas, requisitos de documentación y responsabilidades para la identificación y prevención de conflictos de interés, para la evaluación de su materialidad y para tomar medidas de mitigación. Tales procedimientos, requisitos, responsabilidades y medidas deberían incluir:

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 tales actividades;

c. establecer que los miembros del órgano de dirección 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 puedan verse comprometidas, e

d. impedir que los miembros del órgano de dirección 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.

116. La política debería cubrir específicamente el riesgo de conflictos de interés a nivel del órgano de dirección y proporcionar orientaciones suficientes sobre la identificación y la gestión de conflictos de interés que puedan comprometer la capacidad de los miembros del órgano de dirección para tomar decisiones objetivas e imparciales que persigan salvaguardar los intereses de la entidad. Las entidades deberían tener en cuenta que los conflictos de interés pueden tener un impacto en la independencia de ideas de los miembros del órgano de dirección[31].

117. Al mitigar los conflictos de interés identificados de miembros del órgano de dirección, las entidades deberían documentar las medidas adoptadas, indicando las razones por las que se consideran eficaces para garantizar una toma de decisiones objetiva.

118. Los conflictos de interés reales o potenciales que se hayan notificado a la función responsable de la entidad deberían evaluarse y gestionarse adecuadamente. Si se identifica un conflicto de interés del personal, la entidad debería documentar la decisión tomada, en

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

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

119. Todos los conflictos de interés reales y potenciales a nivel del órgano de dirección, tanto individuales como colectivos, deberían documentarse adecuadamente y notificarse al órgano de dirección, y este será quien los valore, tome una decisión al respecto y los gestione apropiadamente.

12.1 Política de conflictos de interés en el contexto de préstamos y otras operaciones con miembros del órgano de dirección y las partes vinculadas a estos

120. Como parte de sus políticas de conflictos de interés del personal (sección 12) y de la gestión de conflictos de interés de miembros del órgano de dirección según lo dispuesto en el apartado 117, el órgano de dirección debería establecer un marco para la identificación y gestión de conflictos de interés en relación con la concesión de préstamos y la concertación de otras operaciones (por ejemplo, *factoring*, *leasing*, operaciones inmobiliarias, etc.) con miembros del órgano de dirección y las partes vinculadas a estos.

121. Sin perjuicio de la transposición de la Directiva 2013/36/UE[32] a la legislación nacional, las entidades pueden considerar categorías adicionales de partes vinculadas a las que apliquen, en parte o en su integridad, su marco de conflictos de interés en relación con los préstamos y otras operaciones.

122. El marco de conflictos de interés debería garantizar que las decisiones relativas a la concesión de préstamos y la concertación de otras operaciones con miembros del órgano de dirección y las partes vinculadas a estos se adopten de manera objetiva, sin influencia indebida por conflictos de interés, y se tomen, como principio general, en condiciones habituales del curso ordinario del negocio.

123. El órgano de dirección debería establecer los procesos de toma de decisiones aplicables a la concesión de préstamos y la concertación de otras operaciones con miembros del órgano de dirección y las partes vinculadas a estos. Dicho marco podría diferenciar entre operaciones de negocio ordinarias[33], suscritas en el curso ordinario del negocio y concertadas en condiciones habituales del curso ordinario del negocio, y los préstamos y operaciones suscritos con el personal, otorgados en condiciones disponibles para todo el personal. Además, el marco de conflictos de interés y los procesos de toma de decisiones podrían diferenciar entre préstamos significativos y no significativos y otras operaciones, diferentes tipos de préstamos y otras operaciones, y el nivel de conflictos de interés reales o potenciales que pueden crear.

[32] Consúltese también el Principio básico de Basilea n.º 20.

[33] Las operaciones de negocio ordinarias incluyen préstamos y otras operaciones [por ejemplo, *leasing*, *factoring*, servicios relacionados con ofertas públicas iniciales (OPI), fusiones y adquisiciones o compraventa de inmuebles].

124. Como parte del marco de conflictos de interés, el órgano de dirección debería establecer umbrales adecuados (por ejemplo, por tipo de producto o dependiendo de las condiciones) por encima de los cuales el préstamo u otra operación con un miembro del órgano de dirección o con partes vinculadas a este siempre requiera la aprobación del órgano de dirección. Las decisiones relativas a los préstamos significativos u otras operaciones significativas con miembros del órgano de dirección que no se concierten en condiciones habituales del curso ordinario del negocio, pero se otorguen en condiciones disponibles para todo el personal, deberían ser adoptadas siempre por el órgano de dirección.

125. El miembro del órgano de dirección que se beneficie de un préstamo significativo o de otra operación significativa, o el miembro del órgano de dirección que esté vinculado con la contraparte, no debería involucrarse en el proceso de toma de decisiones.

126. Antes de tomar una decisión sobre un préstamo u otra operación con un miembro del órgano de dirección o con las partes vinculadas a este, las entidades deberían evaluar el riesgo al que podrían verse expuestas como consecuencia de la operación.

127. Cuando los préstamos se otorguen mediante la apertura de líneas de crédito (por ejemplo, descubiertos en cuenta), la decisión inicial y sus posteriores modificaciones deberían documentarse. Cualquier disposición de este tipo de líneas de crédito dentro de los límites acordados no debería ser considerada como una nueva decisión sobre la concesión de un préstamo a un miembro del órgano de dirección o a una parte vinculada a este. Cuando se realice una modificación significativa en una línea de crédito de acuerdo con la política de la entidad, se debería realizar una nueva evaluación y adoptar una nueva decisión.

128. Para garantizar el cumplimiento de sus políticas de conflictos de interés, las entidades deberían asegurarse de que todos los procedimientos de control interno relevantes sean de aplicación a los préstamos y otras operaciones con los miembros del órgano de dirección o con las partes vinculadas a estos y de que existe un marco de supervisión adecuado a nivel del órgano de dirección en su función de supervisión.

12.2 Documentación de préstamos a miembros del órgano de dirección y las partes vinculadas a estos e información adicional

129. A efectos de lo dispuesto en el artículo 88, apartado 1, de la Directiva 2013/36/UE, las entidades deberían documentar de manera adecuada los datos sobre los préstamos [34] concedidos a los miembros del órgano de dirección y a las partes vinculadas a estos, incluyendo, como mínimo, lo siguiente:

[34] Véanse también las Directrices de la ABE sobre concesión de préstamos, disponibles en: https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Guidelines/2020/Guidelines%20on%20loan%20origination%20and%20monitoring/Translations/886679/Final%20Report%20on%20GL%20on%20loan%20origination%20and%20monitoring_COR_ES.pdf.

a. el nombre del deudor y su condición (es decir, si es miembro del órgano de dirección o una parte vinculada) y, en relación con los préstamos concedidos a una parte vinculada, el miembro del órgano de dirección con el que está vinculada dicha parte y la naturaleza de su relación con él;

b. el tipo o naturaleza del préstamo, así como su importe;

c. los términos y condiciones contractuales aplicables al préstamo;

d. la fecha de aprobación del préstamo;

e. el nombre del individuo u órgano, y su composición, encargado de tomar la decisión de aprobar el préstamo y las condiciones aplicables;

f. si el préstamo se concedió o no (sí/no) en condiciones habituales del curso ordinario del negocio, y

g. si el préstamo se otorgó o no (sí/no) en condiciones disponibles para todo el personal.

130. Las entidades deberían asegurarse de que la documentación de todos los préstamos a miembros del órgano de dirección y a las partes vinculadas a estos esté completa y actualizada, y que la entidad pueda poner a disposición de las autoridades competentes la documentación completa en un formato adecuado y sin demoras injustificadas si así lo solicitan.

131. En el caso de un préstamo concedido a un miembro del órgano de dirección o a partes vinculadas a este por un importe superior a 200 000 EUR, las entidades deberían poder proporcionar a la autoridad competente, si esta lo solicita, la información adicional siguiente:

a. el porcentaje del préstamo y el porcentaje de la suma de todas las cantidades pendientes de pago de los préstamos otorgados al mismo deudor, en relación con:

i. la suma de su capital de nivel 1 y su capital de nivel 2, y

ii. el capital de nivel 1 ordinario de la entidad;

b. si el préstamo es parte de una gran exposición[35], y

c. la ponderación relativa de la suma agregada de todas las cantidades pendientes de pago de los préstamos concedidos al mismo deudor, calculada como un porcentaje mediante la división de la cantidad total pendiente de pago entre el importe total de todos los préstamos pendientes de pago concedidos a miembros del órgano de dirección y a las partes vinculadas a estos.

[35] Véase también la parte IV del Reglamento (UE) n.º 575/2013 y, en particular, el artículo 392.

13 Procedimientos de alerta interna

132. Las entidades deberían establecer y mantener políticas y procedimientos de alerta interna adecuados para que el personal informe, a través de un canal específico, independiente y autónomo, sobre infracciones 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 debería ser necesario que el personal que informe disponga de pruebas de una infracción, aunque debería tener un nivel de certeza que proporcione razones suficientes para iniciar una investigación. Las entidades deberían implementar asimismo sistemas y procedimientos adecuados que aseguren el cumplimiento de sus obligaciones derivadas de la transposición a la legislación nacional de la Directiva (UE) 2019/1937 del Parlamento Europeo y del Consejo, de 23 de octubre de 2019, relativa a la protección de las personas que informen sobre infracciones del Derecho de la Unión.

133. Con el fin de evitar conflictos de interés, debería 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 deberían garantizar la protección de los datos personales, tanto de la persona que denuncie la infracción como de la persona física presuntamente responsable de la infracción, de conformidad con el Reglamento (UE) 2016/679[36] (RGPD).

134. Los procedimientos de alerta deberían ponerse a disposición de todo el personal de la entidad.

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

136. Las entidades deberían velar 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 debería asegurarse de que ninguna persona bajo control de la entidad victimice a una persona que haya denunciado una infracción y tomar las medidas apropiadas contra los responsables de dicha victimización.

137. Las entidades también deberían proteger a las personas a quienes se haya denunciado de cualquier efecto negativo en caso de que en la investigación no se encuentren pruebas que

[36] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).

justifiquen la adopción de medidas contra ellas. Si se toman medidas, la entidad debería adoptarlas con el objetivo de proteger a la persona afectada de efectos negativos no deseados que vayan más allá del objetivo de la medida adoptada.

138. En particular, los procedimientos de alerta interna deberían:

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 el Reglamento (UE) 2016/679, 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. asegurarse de que las infracciones potenciales o reales denunciadas se analizan y se elevan, 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

139. Las autoridades competentes establecerán mecanismos efectivos y fiables para permitir que el personal de las entidades pueda notificar a las autoridades competentes incumplimientos importantes, potenciales o reales, de los requisitos regulatorios aplicables, incluyendo, entre otros, los establecidos en el Reglamento (UE) n.º 575/2013 y en las disposiciones nacionales que transponen la Directiva 2013/36/UE. Estos mecanismos deberían incluir al menos:

a. procedimientos específicos para la recepción de denuncias de infracciones y su seguimiento, por ejemplo, un departamento, unidad o función específicos 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 el Reglamento (UE) 2016/679 (RGPD), y

d. procedimientos claros según se establece en la sección 13.

140. 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 de alerta interna de su entidad.

Título V - Marco y mecanismos de control interno

15 Marco de control interno

141. Las entidades deberían desarrollar y mantener una cultura que fomente una actitud positiva hacia el control de riesgos y el cumplimiento 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 deberían ser responsables de gestionar los riesgos en los que incurran al llevar a cabo sus actividades y tendrán establecidos controles encaminados a asegurar el cumplimiento de los requisitos internos y externos. Como parte de este marco, las entidades deberían contar con funciones de control interno con autoridad, rango y acceso adecuados y suficientes al órgano de dirección para cumplir su misión, y un marco de gestión de riesgos.

142. El marco de control interno de la entidad en cuestión debería adaptarse 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 deberían organizar el intercambio de la información necesaria de manera que garantice que el órgano de dirección, cada 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, la función de cumplimiento y la función de cumplimiento normativo en materia de prevención del blanqueo de capitales y de la financiación del terrorismo, cuando exista como una función de control separada a nivel de grupo, y entre los responsables de las funciones de control interno a nivel de grupo y el órgano de dirección de la entidad.

143. Las entidades deberían implementar sistemas y procedimientos adecuados que garanticen el cumplimiento de sus obligaciones de prevención del blanqueo de capitales y de la financiación del terrorismo. Las entidades deberían evaluar su exposición al riesgo de ser utilizadas con fines de blanqueo de capitales y de financiación del terrorismo y, en caso necesario, adoptar medidas para mitigar dichos riesgos y los riesgos operativos y reputacionales que conllevan. Las entidades deberían adoptar medidas para asegurarse de que su personal conozca los riesgos de blanqueo de capitales y de financiación del terrorismo y sea consciente del impacto de dichas actividades en la entidad y en la integridad del sistema financiero.

144. El marco de control interno debería abarcar toda la organización, incluidas las responsabilidades y tareas del órgano de dirección 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.

145. El marco de control interno de una entidad debería garantizar:

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

146. El órgano de dirección debería ser 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, cumplimiento, cumplimiento de la normativa de prevención del blanqueo de capitales y de la financiación del terrorismo, si está separada de la de cumplimiento, y de auditoría interna). Las entidades deberían establecer, mantener y actualizar periódicamente por escrito políticas, mecanismos y procedimientos de control interno adecuados, que deberían ser aprobados por el órgano de dirección.

147. Las entidades deberían contar 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.

148. Las entidades deberían comunicar esas políticas, mecanismos y procedimientos a todo el personal y siempre que se realicen cambios relevantes.

149. Al implementar el marco de control interno, las entidades deberían establecer 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 establecer barreras a la información, por ejemplo, a través de la separación física de determinados departamentos.

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

151. Las funciones de control interno deberían presentar periódicamente al órgano de dirección informes por escrito sobre las principales deficiencias identificadas. Estos informes deberían incluir, 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 dirección debería realizar un seguimiento oportuno y eficaz de las conclusiones de los informes de las funciones de control interno y exigir que se tomen las medidas correctivas adecuadas. Se debería establecer un procedimiento de seguimiento formal de las conclusiones y de las medidas correctivas tomadas.

17 Marco de gestión de riesgos

152. Como parte del marco de control interno general, las entidades deberían contar 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 debería permitir 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 deberían evaluarse 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 deberían 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, operativos, tecnológicos, reputacionales, legales, de conducta, y de cumplimiento de la normativa de prevención del blanqueo de capitales y de la financiación del terrorismo y otros delitos económicos, así como los riesgos ASG y estratégicos.

153. El marco de gestión de riesgos de una entidad debería incluir 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.

154. El marco de gestión de riesgos de una entidad debería facilitar orientaciones específicas sobre la implantación de sus estrategias. Cuando proceda, estas orientaciones deberían establecer y mantener 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 debería mantenerse dentro de estos límites. El marco de gestión de riesgos debería garantizar que cuando se produzcan incumplimientos de los límites de riesgo exista un proceso establecido para elevarlos y abordarlos con un procedimiento de seguimiento adecuado.

155. El marco de gestión de riesgos debería ser objeto de una revisión interna independiente, por ejemplo, realizada por la función de auditoría interna, y debería volver a evaluarse 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. Los factores que deberían considerarse abarcan la evolución interna y externa, incluidas las 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.

156. Al identificar y medir o evaluar los riesgos, las entidades deberían desarrollar metodologías apropiadas que incluyan herramientas prospectivas y retrospectivas. Estas metodologías deberían permitir agregar las exposiciones al riesgo de las distintas líneas de negocio y facilitar la identificación de concentraciones de riesgos. Las herramientas deberían incluir la evaluación del perfil de riesgo real considerando el apetito de riesgo de la entidad, así como la identificación y evaluación de exposiciones de 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 deberían proporcionar información sobre cualquier ajuste al perfil de riesgo que pueda requerirse. Las entidades deberían utilizar supuestos suficientemente conservadores al construir escenarios de estrés.

157. Las entidades deberían tener 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 debería basarse únicamente en información cuantitativa o en los resultados de modelos, sino que también debería incluir un enfoque cualitativo (incluido el criterio de expertos y el análisis crítico). Las tendencias y los datos relevantes del entorno macroeconómico deberían considerase explícitamente para identificar su posible impacto en las exposiciones y en las carteras.

158. La responsabilidad de la evaluación de riesgos recae, en última instancia, exclusivamente en la entidad que, en consecuencia, debería evaluar sus riesgos de forma crítica y no basarse únicamente en evaluaciones externas. Por ejemplo, una entidad debería validar los modelos de riesgo que adquiera 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.

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

160. 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 deberían conocer adecuadamente el alcance exacto de tales evaluaciones y sus limitaciones.

161. Deberían establecerse mecanismos de información periódica y transparente para que el órgano de dirección, 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 los riesgos. El marco de información debería estar bien definido y documentado.

162. Una comunicación eficaz y la concienciación sobre los riesgos y la 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[37]

163. Las entidades deberían contar con una política de aprobación de nuevos productos adecuadamente documentada y aprobada por el órgano de dirección 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 debería abarcar los cambios relevantes en los procesos (p. ej., nuevos acuerdos de externalización) y sistemas (p. ej., procesos de cambio de TI) relacionados. Asimismo, esta política debería garantizar que los productos y los cambios aprobados sean coherentes con la estrategia de riesgo y el apetito de riesgo de la entidad y los límites correspondientes, o que se realicen las revisiones necesarias.

164. Los cambios relevantes o las transacciones excepcionales podrían incluir 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

[37] Véanse también las Directrices de la ABE sobre procedimientos de gobernanza y vigilancia para fabricantes y distribuidores de productos de banca minorista, disponibles en: https://www.eba.europa.eu/-/eba-publishes-final-product-oversight-and-governance-requirements-for-manufactures-and-distributors-of-retail-banking-products.

productos, cambios en los sistemas o el marco o los procedimientos de gestión de riesgos, y cambios en la organización de la entidad.

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

166. La política de aprobación de nuevos productos de una entidad debería cubrir 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 debería incluir 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.

167. La política de aprobación de nuevos productos debería establecer las principales cuestiones a abordar antes de tomar una decisión, entre las que se incluyen el cumplimiento de la regulación, la contabilidad, los 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. Asimismo, para cumplir las obligaciones que se derivan de la Directiva (UE) 2015/849, las entidades deberían identificar y evaluar el riesgo de blanqueo de capitales y de financiación del terrorismo asociado al nuevo producto o práctica comercial, y establecer las medidas que deban adoptarse para mitigar dichos riesgos. 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 debería emprenderse una nueva actividad hasta que se disponga de los recursos adecuados para entender y gestionar los riesgos asociados.

168. La función de gestión de riesgos y la función de cumplimiento deberían involucrarse en la aprobación de nuevos productos o de cambios significativos en productos, procesos y sistemas existentes. Su aportación debería incluir 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 la entidad para gestionar los nuevos riesgos con eficacia. La función de control de riesgos debería 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

169. Las funciones de control interno deberían incluir 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 deberían estar sujetas a revisión por parte de la función de auditoría interna. Las responsabilidades de las funciones de control incluyen también la de garantizar el cumplimiento de los requisitos de prevención del blanqueo de capitales y de la financiación del terrorismo.

170. Las tareas operativas de las funciones de control interno pueden 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 dirección 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 dirección seguirán siendo responsables de estas actividades y de mantener una función de control interno dentro de la entidad.

171. Sin perjuicio de lo dispuesto en la legislación nacional de transposición de la Directiva 2015/849/UE, las entidades deberían asignar a un miembro del personal (por ejemplo, el responsable de cumplimiento) la responsabilidad de asegurar el cumplimiento de los requisitos de la citada directiva por parte de la entidad y de sus políticas y procedimientos. Las entidades pueden establecer una función separada de cumplimiento de la normativa sobre prevención del blanqueo de capitales y de la financiación del terrorismo como una función de control independiente [38]. En caso necesario, la persona responsable de la prevención del blanqueo de capitales y de la financiación del terrorismo debería poder informar directamente al órgano de dirección en sus funciones de dirección y de supervisión.

19.1 Responsables de las funciones de control interno

172. Los responsables de las funciones de control interno deberían establecerse 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 dirección, 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 deberían informar y rendir cuentas directamente al órgano de dirección, y este evaluará su desempeño.

173. Cuando sea necesario, los responsables de las funciones de control interno deberían poder acceder e informar directamente al órgano de dirección en su función de supervisión para plantear inquietudes y advertir a dicha función, si procede, cuando sucesos específicos afecten o puedan afectar a la entidad. Esto no debería impedir que los responsables de las

[38] Véanse también las Directrices de la ABE sobre la función de cumplimiento de la normativa sobre prevención del blanqueo de capitales y de la financiación del terrorismo (actualmente en elaboración).

funciones de control interno informen también dentro de los canales de comunicación ordinarios.

174. Las entidades deberían tener 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 deberían ser destituidos sin la aprobación previa del órgano de dirección 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 deberían ser 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

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

a. su personal no realizará ninguna tarea operativa incluida en el ámbito de las actividades de cuyo seguimiento y control se ocupen las propias funciones de control interno;

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 dirección de la entidad, el responsable de una función de control interno no debería depender 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 debería estar 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[39].

19.3 Combinación de funciones de control interno

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

[39] Véanse también las Directrices de la ABE sobre políticas de remuneración adecuadas, disponibles en: https://www.eba.europa.eu/sites/default/documents/files/documents/10180/1504751/5db4e2ef-7e07-4d7f-a8a9-7f09da5fa86a/EBA-GL-2015-22%20GLs%20on%20Sound%20Remuneration%20Policies_ES.pdf?retry=1.

19.4 Recursos de las funciones de control interno

177. Las funciones de control interno deberían disponer de recursos suficientes. Deberían contar con un número adecuado de empleados cualificados (tanto a nivel de la empresa matriz como de filial). El personal debería estar cualificado en todo momento y recibir la formación necesaria.

178. Las funciones de control interno deberían tener a su disposición sistemas de TI y de 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 riesgos, en particular aquellas que potencialmente pueden generar riesgos importantes para las entidades.

20 Función de gestión de riesgos

179. Las entidades deberían establecer una función de gestión de riesgos (FGR) que abarque toda la entidad. La FGR debería tener 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.

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

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

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

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

184. La FGR debería ser un elemento central de la organización de la entidad, y estructurarse de modo que pueda implementar las políticas de riesgos y controlar el marco de gestión de riesgos. La FGR debería desempeñar un papel esencial en la tarea de garantizar que la entidad tenga implantados procesos eficaces de gestión de riesgos. La FGR debería participar activamente en todas las decisiones importantes en materia de gestión de riesgos.

185. Las entidades significativas pueden considerar establecer FGR específicas para cada línea de negocio importante. Sin embargo, deberían contar con una FGR central, que incluya una FGR a nivel de grupo en 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.

186. La FGR debería proporcionar información independiente, análisis y criterios expertos y pertinentes sobre las exposiciones al riesgo, y asesorar sobre las propuestas y las decisiones en materia de riesgos adoptadas por las líneas de negocio o las unidades internas, y debería informar al órgano de dirección sobre si son coherentes con la estrategia de riesgo y el apetito de riesgo de la entidad. La FGR puede 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

187. La FGR debería involucrarse 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 debería proporcionar 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 debería evaluar la solidez y la sostenibilidad de la estrategia y el apetito de riesgo, y velar por que dicho apetito se traduzca adecuadamente en límites de riesgo específicos. La FGR también debería evaluar las estrategias y el apetito de riesgo de las unidades de negocio, incluidos los objetivos propuestos por las unidades de negocio, y debería involucrarse antes de que el órgano de dirección tome una decisión sobre tales estrategias y el apetito de riesgo. Los objetivos deberían ser razonables y coherentes con la estrategia de riesgo de la entidad.

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

20.2 Papel de la FGR en los cambios significativos

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

190. La FGR debería evaluar 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

191. La FGR debería asegurarse de que exista un marco de gestión de riesgos adecuado y de que todos los riesgos sean identificados, evaluados, medidos, controlados, gestionados y comunicados adecuadamente por todas las unidades relevantes de la entidad.

192. La FGR debería asegurarse 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 debería mantener informado al órgano de dirección sobre los supuestos utilizados y las posibles deficiencias de los modelos y del análisis de riesgos.

193. La FGR debería asegurarse 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.

194. La FGR debería asegurarse de que todos los riesgos identificados sean controlados de manera eficaz por las unidades de negocio.

195. La FGR debería hacer 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 dirección pueda tomar decisiones y la función de supervisión pueda cuestionarlas.

196. La FGR debería analizar tendencias e identificar los riesgos nuevos o emergentes, así como incrementos de los riesgos derivados de cambios en las circunstancias y las condiciones. Asimismo, debería revisar 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.

197. La FGR debería evaluar posibles formas de mitigar los riesgos. La información que se presente al órgano de dirección debería incluir propuestas de medidas de mitigación de riesgos apropiadas.

20.4 Papel de la FGR en exposiciones a riesgos no aprobadas

198. La FGR debería evaluar de forma independiente los incumplimientos del apetito de riesgo 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 debería informar a las unidades de negocio pertinentes y al órgano de dirección, y recomendar posibles soluciones. La FGR debería informar directamente al órgano de dirección en su función de supervisión cuando el

incumplimiento sea significativo, sin perjuicio de que la FGR informe a otras funciones internas y comités.

199. La FGR debería desempeñar 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 dirección y, si se ha constituido, al comité de riesgos.

20.5 Responsable de la función de gestión de riesgos

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

201. El responsable de la FGR debería tener 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 dirección, las entidades significativas nombrarán un responsable de la FGR independiente que no tenga responsabilidades en otras funciones y que informe directamente al órgano de dirección. 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 *senior*, siempre que no haya un conflicto de interés entre las funciones combinadas. En cualquier caso, esta persona debería tener autoridad, rango e independencia suficientes (p. ej., el responsable de los servicios jurídicos).

202. El responsable de la FGR podrá cuestionar las decisiones adoptadas por la dirección de la entidad y por su órgano de dirección, y los motivos de objeción deberían documentarse formalmente. Si una entidad desea conceder al responsable de la FGR el derecho de veto de determinadas decisiones (p. ej., sobre un crédito, una decisión de inversión o la fijación de un límite) adoptadas a niveles inferiores al órgano de dirección, debería especificar el alcance de ese derecho de veto, los procedimientos para elevar los asuntos o para apelar, y cómo se involucrará al órgano de dirección.

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

21 Función de cumplimiento

204. Las entidades deberían establecer una función de cumplimiento permanente y eficaz para gestionar el riesgo de cumplimiento normativo y nombrar a una persona responsable de esta función en toda la entidad (el director o responsable de cumplimiento).

205. 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 *senior* (p. ej., el responsable de los servicios jurídicos), siempre que no exista conflicto de interés entre las funciones combinadas.

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

207. El personal de la función de cumplimiento debería poseer los conocimientos, las competencias y la experiencia adecuados en relación con los procedimientos de cumplimiento y otros procedimientos pertinentes, y debería tener acceso a formación periódica.

208. El órgano de dirección en su función de supervisión debería supervisar la aplicación de una política de cumplimiento bien documentada, que se comunicará a todo el personal. Las entidades deberían establecer un proceso para evaluar periódicamente las modificaciones de las leyes y normativas aplicables a sus actividades.

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

210. La función de cumplimiento debería asegurarse de que la supervisión del cumplimiento se lleve a cabo mediante un programa de supervisión del cumplimiento estructurado y bien definido y de que se respete la política de cumplimiento. Dicha función debería informar al órgano de dirección y comunicarse, según corresponda, con la FGR sobre el riesgo de cumplimiento de la entidad y su gestión. La función de cumplimiento y la FGR deberían cooperar e intercambiar información, si procede, para realizar sus tareas respectivas. El órgano de dirección y la FGR deberían tener en cuenta las conclusiones de la función de cumplimiento en los procesos de toma de decisiones.

211. De conformidad con la sección 18 de estas directrices, la función de cumplimiento también debería verificar, 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.

212. Las entidades deberían adoptar las medidas adecuadas frente a conductas internas o externas que puedan facilitar o permitir el fraude, el blanqueo de capitales, la financiación del terrorismo u otros delitos económicos y frente a infracciones disciplinarias (por ejemplo, incumplimiento de procedimientos internos o de límites).

213. Las entidades deberían asegurarse 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 deberían informar al director o al responsable de cumplimiento de la entidad en base consolidada.

22 Función de auditoría interna

214. Las entidades deberían establecer una función de auditoría interna (FAI) independiente y eficaz, teniendo en cuenta los criterios de proporcionalidad establecidos en el título I, y nombrar a una persona responsable de esta función en toda la entidad. La FAI debería ser independiente y tener la autoridad, el rango y los recursos adecuados. En concreto, la entidad debería asegurarse 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.

215. La FAI debería ser independiente de las actividades auditadas. Por tanto, la FAI no debería combinarse con ninguna otra función.

216. Utilizando un enfoque basado en el riesgo, la FAI debería verificar de forma independiente y proporcionar una certeza objetiva de que todas las actividades y unidades de una entidad, incluidas las actividades externalizadas, cumplen con las políticas y los procedimientos de la entidad y con los requisitos regulatorios. Todas las entidades del grupo estarán incluidas en el ámbito de competencias de la FAI.

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

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

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 a la estrategia de riesgo y el apetito de riesgo de la entidad;

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

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 adecuación, 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.

219. La FAI debería verificar, 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). Debería 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.

220. La FAI debería tener acceso sin restricciones a todos los registros, documentos, información y edificios de la entidad. Esto debería incluirá el acceso a los sistemas de información de gestión y a las actas de todos los comités y los órganos de decisión.

221. La FAI debería adherirse a los estándares profesionales nacionales e internacionales. Un ejemplo de estándares profesionales a los que se hace referencia en este apartado son las normas establecidas por el Instituto de Auditores Internos.

222. Los trabajos de auditoría interna deberían llevarse a cabo con arreglo a un plan de auditoría y a programas de auditoría detallados siguiendo un enfoque basado en el riesgo.

223. Debería elaborase 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 debería ser aprobado por el órgano de dirección.

224. Todas las recomendaciones de auditoría deberían someterse a un procedimiento formal de seguimiento por parte de los niveles de dirección adecuados, con el fin de garantizar e informar de su resolución eficaz y oportuna.

Título VI - Gestión de la continuidad del negocio[40]

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

226. Las entidades pueden establecer una función de continuidad del negocio independiente específica, por ejemplo, como parte de la FGR[41].

227. El negocio de una entidad depende de diversos recursos críticos (p. ej., sistemas de TI, incluidos servicios en la nube, sistemas de comunicación, personal esencial y edificios). La gestión de la continuidad del negocio tiene por objeto atenuar las consecuencias operativas, financieras, jurídicas, 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 transferir su impacto financiero a terceros (p. ej., mediante seguros).

228. Para establecer un plan de gestión de la continuidad del negocio adecuado, las entidades deberían analizar con detenimiento sus factores de riesgo y su exposición a perturbaciones graves en el negocio y evaluar (cuantitativa y cualitativamente) su posible impacto, sirviéndose de datos internos y/o externos y de análisis de escenarios. Este análisis debería abarcar todas las líneas de negocio y unidades internas, incluida la FGR, y tener en cuenta su interdependencia. Los resultados del análisis deberían contribuir a definir las prioridades y los objetivos de recuperación de la entidad.

229. En función del análisis anterior, las entidades deberían 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 debería ser acorde con el apetito de riesgo de la entidad.

230. Los planes de contingencia, de continuidad del negocio y de recuperación deberían documentarse e implantarse con meticulosidad. La documentación debería estar a

[40] Las entidades deberían consultar también las Directrices de la ABE sobre gestión de riesgos de TIC, disponibles en: https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Guidelines/2020/GLs%20on%20ICT%20and%20security%20risk%20management/Updated%20Translations/880812/Final%20draft%20Guidelines%20on%20ICT%20and%20security%20risk%20management_COR_ES.pdf.

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

disposición de las líneas de negocio, las unidades internas y la FGR, y almacenarse en sistemas físicamente separados y de fácil acceso en caso de contingencia. Debería impartirse la formación apropiada. Los planes deberían someterse a prueba y actualizarse periódicamente. Las dificultades o fallos detectados en las pruebas deberían documentarse y analizarse, y los planes revisarse en consecuencia.

Título VII - Transparencia

231. Las estrategias, políticas y procedimientos deberían comunicarse a todo el personal pertinente de la entidad. El personal debería conocer y cumplir las políticas y los procedimientos correspondientes a sus obligaciones y responsabilidades.

232. En consecuencia, el órgano de dirección debería informar a todo el personal pertinente y mantenerle 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 puede facilitarse mediante guías escritas, manuales u otros medios.

233. 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 debería incluir a todas las entidades de la estructura de grupo tal como se define en la Directiva 2013/34/UE[42], por país.

234. La información publicada debería 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 gobierno u organizativas;

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

e. las principales responsabilidades del órgano de dirección;

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

[42] 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).

g. una descripción general de la política de conflictos de interés aplicable a la entidad y al órgano de dirección;

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

En línea con el título III, las entidades deberían considerar 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 dirección
   a) criterios de selección, incluyendo cómo se tiene en cuenta la diversidad
   b) número, duración del mandato, rotación, edad
   c) miembros independientes del órgano de dirección
   d) miembros ejecutivos del órgano de dirección
   e) miembros no ejecutivos del órgano de dirección
   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 auditoría 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
7. Descripción de la estrategia de riesgo y del marco de gestión de riesgos
8. 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) prestación de servicios bajo el régimen de libre de prestación de servicios

f) sucursales

g) filiales, agrupaciones temporales de empresas, etc.

h) uso de centros financieros extraterritoriales

9. 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 interés

d) denuncia de irregularidades

10. Situación de la política de gobierno interno, con fecha

a) desarrollo

b) última modificación

c) última evaluación

d) aprobación por el órgano de dirección.