

Guía de la EBA sobre gobierno interno (GL 44) (27 de septiembre de 2011)
[1]

[1] *Traducción al español de la Guía de la EBA. En caso de discrepancia prevalece la versión en inglés.*

El 27 de septiembre de 2011, EBA aprobó la EBA Guidelines on Internal Governance (GL44), cuyo objetivo es la implantación por las entidades de mejores prácticas de gobierno interno y la armonización de las expectativas supervisoras en la revisión de esta área en el seno del Proceso de Revisión y Evaluación Supervisora (SREP, en inglés).

Su contenido agrupa directrices relativas al gobierno interno de las entidades en seis secciones, que en conjunto recogen disposiciones sobre treinta aspectos distintos. Tales secciones corresponden a las facetas del gobierno interno siguientes: Estructura y organización, órgano de administración, gestión del riesgo, control del riesgo, sistemas de información y continuidad del negocio, y transparencia.

Esta Guía, en cuyo nivel de aplicación ha de tenerse en cuenta el principio de proporcionalidad referido en ella, ha supuesto la revocación expresa, de la sección 2.1 de la CEBS Guidelines on the Application of the Supervisory Review Process (25.01.06) y total de otras dos guías de CEBS: High Level Principles for Remuneration Policies (20.04.09) y High Level Principles for Risk Management (16.02.10).

La Comisión Ejecutiva del Banco de España, con fecha 27 de junio de 2012, ha acordado hacer suya esta Guía. Esta adhesión lo es sin perjuicio del contenido de nuestro derecho positivo y sin menoscabo de que en un futuro el Banco de España pueda concretar algún criterio supervisor adicional sobre el seguimiento de las directrices contenidas en aquella Guía.

El Banco de España entiende que, por tratarse de principios paralelos a los de la Guía adoptada, con la mera adopción anterior está igualmente cumpliendo con todos los principios recogidos en el documento elaborado por el Comité de Supervisores Bancarios de Basilea "Enhancing corporate governance for banking organisations", salvo:

- El referido al papel de la alta dirección de las aludidas entidades, aspecto no específicamente tratado en el documento de EBA.
- Aquellas referencias a las relaciones con accionistas y otros interesados así como al papel del supervisor que, por referirse a cuestiones relativas al ámbito del "gobierno corporativo", más amplio que el de "gobierno interno" de la Guía adoptada, no son tampoco objeto de esta.

Índice

I. Resumen ejecutivo	3
II. Contexto y justificación	7
1. Importancia del gobierno interno	7
2. Finalidad y ámbito de aplicación de la guía sobre gobierno interno	8
3. Conceptos utilizados en la guía	9
III. Guía de la EBA sobre gobierno interno	12
Título I – Objeto, ámbito de aplicación y definiciones	16
Título II – Requisitos sobre el gobierno interno de las entidades	16
Título III – Disposiciones finales e implantación	48

I.

Resumen ejecutivo

1. El **gobierno interno** de las entidades [2] de la Comunidad Europea se trata en el **artículo 22 de la Directiva 2006/48/CE**, que exige que «cada entidad de crédito disponga de sólidos procedimientos de gobierno corporativo, incluida una estructura organizativa clara, con líneas de responsabilidad bien definidas, transparentes y coherentes, así como procedimientos eficaces para la identificación, gestión, control y comunicación de los riesgos a los que esté o pueda estar expuesta, junto con mecanismos adecuados de control interno, incluidos procedimientos administrativos y contables adecuados», además de prácticas y políticas de remuneración que promuevan y sean coherentes con una gestión de riesgos sólida y eficaz. El artículo 73(3) de la Directiva 2006/48/CE exige que el artículo 22 se aplique también a las empresas matrices y filiales de manera consolidada o subconsolidada.

2. La confianza en la fiabilidad del sistema bancario es crucial para su buen funcionamiento y constituye un requisito previo para que contribuya a la economía en conjunto. En consecuencia, los procedimientos de gobierno interno eficaces son fundamentales para que las entidades, individualmente, y el sistema bancario funcionen correctamente. Sobre esta base y en el contexto del marco mencionado anteriormente, el Comité Europeo de Supervisores Bancarios (CEBS, en sus siglas en inglés) publicó guías que tratan aspectos completos o parciales relativos al gobierno interno: la guía sobre externalización de 2006 (*Guidelines on Outsourcing*) ; la guía sobre el proceso de revisión supervisora de 2006 (*Guidelines on the Application of the Supervisory Review Process under Pillar 2*); los principios de alto nivel para la política de remuneración de 2009 (*High-Level principles for Remuneration Policies*), y los principios de alto nivel para la gestión de riesgos de 2010 (*High level principles for risk management*).

3. A raíz de la crisis financiera que estalló en 2008, el CEBS realizó una encuesta sobre la implantación del gobierno interno en las entidades y las autoridades competentes. No se determinó que los problemas provocados por un gobierno interno deficiente fueran el desencadenante directo de la crisis pero sí un factor subyacente crucial. Los fallos eran con frecuencia el resultado de no implantar las guías existentes de forma adecuada.

4. Con el fin de tener en cuenta estos fallos identificados en la crisis financiera y los avances observados desde la publicación de las guías del CEBS anteriores (como la actualización de las orientaciones del Comité de Supervisión Bancaria de Basilea [BCBS, en sus siglas en inglés] sobre *La mejora del gobierno corporativo en las organizaciones bancarias*), la EBA actualizó la anterior guía del CEBS sobre gobierno interno y procuró consolidar las directrices en esta guía sobre gobierno interno, con referencias, en caso necesario, a otras guías que tratan aspectos más específicos de cuestiones relativas al gobierno interno (como externalización o remuneración). Más concretamente, las secciones de la Guía sobre el proceso de revisión supervisora [3] que hacen referencia al gobierno interno han sido revisadas y fusionadas con los Principios de alto nivel para la política de remuneración y para la gestión de riesgos. Se han añadido nuevos capítulos sobre «gestión de riesgos» y «sistemas y continuidad».

5. En el primer capítulo sobre «organización y estructura corporativa», se analiza con más detalle el concepto de controles y contrapesos en estructuras de grupo, y se introduce el principio de «conozca su estructura» para corregir los fallos identificados en la encuesta con respecto a estructuras complejas que no se han entendido y contrarrestado lo suficiente. El objetivo de esta parte de la guía es restringir las actividades opacas por medio de estructuras no supervisadas.

6. El segundo capítulo sobre «órgano de dirección» se ha mejorado al añadir directrices sobre la composición, el nombramiento y la sucesión y cualificaciones del órgano de dirección, que se centra más en el uso de comités y la identificación y gestión de conflictos de interés. Como la falta de supervisión fue uno de los fallos más significativos identificados en la crisis financiera, el objetivo de esta parte de la guía es garantizar que los miembros del órgano de dirección (en especial, cuando ejercen su función de supervisión) dedican el tiempo suficiente a sus funciones. Por último, para ofrecer una perspectiva completa de las funciones del órgano de dirección, también se ha añadido a la guía su responsabilidad con respecto a la externalización y al establecimiento de la política de remuneración. Sin embargo, dado que existen guías separadas del CEBS sobre estos aspectos de gobierno interno, que siguen vigentes, se han añadido referencias, cuando ha sido necesario [4].

7. En el tercer capítulo sobre «gestión de riesgos» se han incluido partes extensas de los principios de alto nivel para la gestión de riesgos (como los principios de alto nivel sobre gobierno corporativo y cultura de riesgos, sobre modelos de riesgo e integración de áreas de gestión de riesgos, y sobre proceso y política de aprobación de nuevos productos). Partes de los anteriores principios de alto nivel sobre apetito al riesgo y tolerancia al riesgo se han asignado a la nueva guía sobre el marco de gestión de riesgos.

8. El cuarto capítulo sobre «control interno» incluye la sección titulada «La función del director responsable del control de riesgos y de la función de gestión de riesgos», procedente de los Principios de alto nivel para la gestión de riesgos, cuyo objetivo es garantizar la composición adecuada del personal de la función de control, ya que uno de los fallos identificados en la encuesta del CEBS mencionada anteriormente fue que las funciones de control no contaban con los recursos suficientes para cumplir con sus obligaciones. Los principios también tratan la cuestión de exposiciones a riesgos no aprobadas, con el objetivo de implantar procesos adecuados para vigilar los límites establecidos y adoptar las medidas apropiadas cuando sea necesario.

9. El quinto capítulo sobre «sistemas y continuidad» contiene nuevas directrices sobre sistemas de información y comunicación, así como sobre la gestión de la continuidad del negocio. En lugar de formular amplios requisitos con respecto a los sistemas de tecnología de la información (TI), la guía hace referencia a normas generalmente aceptadas a este respecto. Los principios sobre la continuidad del negocio son coherentes con los principios de alto nivel para la continuidad del negocio del BCBS (*High-level principles for business continuity*).

10. El sexto capítulo sobre «transparencia» contiene el capítulo titulado «*Public Disclosure and Transparency*» («Divulgación pública y transparencia») en la anterior guía del CEBS sobre gobierno interno. En este caso, solo se han realizado pequeñas modificaciones a la versión anterior de la guía, ya que en la encuesta del CEBS no se identificaron fallos importantes en esta área.

11. Cuando se elaboró la presente guía, la EBA tuvo en cuenta las respuestas recibidas de las partes interesadas durante la consulta pública. La EBA también evaluó los costes y beneficios de sus propuestas.

12. En general, los consultados respaldaron la guía propuesta y agradecieron el hecho de que la EBA haya elaborado un conjunto completo de directrices sobre gobierno interno acordes con las normas internacionales. También estuvieron de acuerdo con la aplicación del principio de proporcionalidad. Los consultados señalaron que la cuestión clave durante la crisis financiera no fue la ausencia de normas sobre gobierno corporativo sino la implantación ineficaz de dichas normas. Un componente clave en toda economía moderna consiste en contar con un sistema bancario de confianza y que funcione bien, respaldado por marcos de buen gobierno corporativo en las entidades.

13. El 27 de mayo de 2011, se presentó el borrador de la guía sobre gobierno interno al Grupo de partes interesadas del sector bancario (BSG, en sus siglas en inglés) de la EBA. No se consideró necesaria una opinión formal del BSG, dado el hecho de que el trabajo había comenzado bajo el mandato del CEBS y la guía ya había sido objeto de una consulta pública.

14. También se efectuó un análisis de costes y beneficios, que utiliza como referencia la legislación vigente, concretamente, las Directivas 2006/48/CE y

2006/49/CE, en el que se comparan los cambios realizados por esta guía con la guía anterior del CEBS. Al hacerlo, también se utilizan los resultados de la consulta pública.

15. En el análisis de costes y beneficios se concluyó, con relación a los costes, que la implantación de la guía generará costes excepcionales moderados para las entidades y las autoridades competentes, mientras que los costes fijos de mantener y supervisar un marco de gobierno corporativo mejorado deberían ser relativamente bajos. En lo que respecta a los beneficios, el análisis sugiere que las entidades se beneficiarán de un marco de gobierno corporativo mejorado gracias a una mayor adecuación de su perfil de riesgo a su estrategia/apetito de riesgo y una mejor gestión de riesgos, algo que podría conllevar la reducción de las pérdidas. Se espera que la implantación de la guía dé lugar a un sistema bancario más resistente. Por lo tanto, se considera que los beneficios de introducir esta guía revisada compensan con creces los costes en los que se pueda incurrir.

[2] *Las entidades a las que se hace referencia en esta guía son las entidades de crédito y las empresas de inversión según el artículo 22 de la Directiva 2006/48/CE del Parlamento Europeo y del Consejo, de 14 de junio de 2006, relativa al acceso a la actividad de las entidades de crédito y a su ejercicio (refundición); en el caso de las empresas de inversión, véase también el artículo 34 de la Directiva 2006/49/CE del Parlamento Europeo y del Consejo, de 14 de junio de 2006, sobre la adecuación del capital de las empresas de inversión y las entidades de crédito (refundición), en lo sucesivo, ambas directivas se denominarán «la Directiva sobre la adecuación del capital» (DAC).*

[3] *La guía (Guidelines on the Application of the Supervisory Review Process under Pillar 2) está disponible, en inglés, en el sitio web de la EBA.*

[4] *Las guías del CEBS están publicadas, en inglés, en el sitio web de la EBA.*

II. Contexto y justificación

1. Importancia del gobierno interno

16. La confianza en la fiabilidad del sistema bancario es crucial para su buen funcionamiento y constituye un requisito previo para que contribuya a la economía en conjunto. En consecuencia, los procedimientos de gobierno interno eficaces son fundamentales para que las entidades, individualmente, y el sistema bancario funcionen correctamente.

17. En los últimos años, el gobierno interno ha recibido una atención cada vez mayor por parte de varios organismos internacionales [5]. Su principal esfuerzo ha

consistido en corregir las prácticas de gobierno interno superficiales o con fallos identificadas en la crisis financiera. Estas prácticas defectuosas, aunque no constituyeron un desencadenante directo de la crisis financiera, estuvieron estrechamente relacionadas con ella y, por tanto, representaron un factor fundamental que contribuyó a dicha crisis.

18. La Autoridad Bancaria Europea (EBA) se constituyó oficialmente el 1 de enero de 2011 y ha asumido todas las tareas y responsabilidades existentes y en curso del Comité Europeo de Supervisores Bancarios (CEBS, en sus siglas en inglés). A finales de 2009, el CEBS llevó a cabo una **encuesta sobre la implantación** por parte de las autoridades de supervisión y las entidades **de su guía sobre gobierno interno** publicada en enero de 2006 [6]. Los principales resultados [7] indicaron que, aunque los marcos nacionales reguladores y de supervisión para el gobierno interno en general se podían considerar, en gran medida, completos, su cobertura estaba, en cierto modo, fragmentada y se identificaron una serie de deficiencias. La encuesta también reveló que muchas entidades deben mejorar su implantación de la guía y los supervisores deben mejorar sus procedimientos a este respecto.

19. Con respecto a la organización y estructura corporativa, el principal fallo identificado fue que la **complejidad** de las entidades no se contrarrestaba lo suficiente con procedimientos de gobierno interno adecuados. La complejidad y los riesgos de los productos y servicios ofrecidos por las entidades, así como las diferentes características de los mercados locales en los que operan grupos transfronterizos, aumentaban el nivel de complejidad de las entidades. La estructura corporativa ni era siempre transparente ni estaba organizada para demostrar y promover una gestión prudente y eficaz, debido, a menudo, a unas líneas de comunicación ineficaces.

20. También se identificó un **control** deficiente por parte de la función de supervisión del órgano de dirección. Es posible que el órgano de dirección, tanto en el ejercicio de su función de dirección, como especialmente en el ejercicio de su función de supervisión, no entendiese la complejidad del negocio y los riesgos que entrañaba; por consiguiente, no lograba identificar y limitar los excesivos riesgos asumidos. Las limitaciones de tiempo contribuían a impedir que los miembros del órgano de dirección cumplieren sus obligaciones en el ejercicio de su función de supervisión.

21. Con frecuencia los **marcos de gestión de riesgos y de control interno** no estaban lo suficientemente integrados en las entidades o grupos. Faltaba una metodología y una terminología uniformes; por lo tanto, no existía una perspectiva holística de todos los riesgos. Las funciones de control carecían a menudo de los recursos, el estatus o los conocimientos especializados adecuados.

22. A la inversa, las buenas prácticas de gobierno interno ayudaron a algunas entidades a gestionar la crisis financiera significativamente mejor que otras. Entre estas prácticas se incluyen el establecimiento de una estrategia adecuada y de

niveles de tolerancia/apetito al riesgo, un planteamiento holístico en la gestión de riesgos y líneas de comunicación eficaces hacia el órgano de dirección en el ejercicio de sus funciones de dirección y supervisión.

[5] Véase en particular: *BCBS Principles for enhancing corporate governance*, de 4 de octubre de 2010, disponible en: <http://www.bis.org/publ/bcbs176.htm>; *Corporate governance and the financial crisis -Conclusions and emerging good practices to enhance implementation of the Principles (Gobierno Corporativo y la Crisis Financiera: Conclusiones y Buenas Prácticas Emergentes para Mejorar la Implementación de los Principios)* de la OCDE, de febrero de 2010, disponible en <http://www.oecd.org/dataoecd/53/62/44679170.pdf>; el Libro Verde sobre El gobierno corporativo en las entidades financieras y las políticas de remuneración de la Comisión Europea, de junio de 2010, disponible en <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0284:FIN:ES:PDF>.

[6] La guía (*Guidelines on the Application of the Supervisory Review Process under Pillar 2*) está disponible, en inglés, en el sitio web de la EBA.

[7] Se puede consultar un resumen de los resultados en inglés en el sitio web de la EBA en el siguiente enlace: http://www.eba.europa.eu/documents/About-us/Key-dates/Summary-of-survey-results_Workshop

2. Finalidad y ámbito de aplicación de la guía sobre gobierno interno

23. El organismo predecesor de la EBA, el CEBS, había abordado ya algunas de las cuestiones más significativas derivadas de la crisis financiera en los **Principios de alto nivel para la política de remuneración** publicados en abril de 2009 y en los **Principios de alto nivel para la gestión de riesgos** [8] publicados en febrero de 2010. Sin embargo, teniendo en cuenta los resultados de la encuesta de 2009 y la labor reciente efectuada por otros organismos europeos e internacionales sobre gobierno corporativo (especialmente los Principios para la mejora del gobierno corporativo del Comité de Basilea), la EBA consideró acertado mejorar esos principios de alto nivel. Consecuentemente, se añadieron a la guía directrices sobre el funcionamiento y la composición del órgano de dirección, las cualificaciones, el nombramiento y la sucesión de sus miembros, así como principios mejorados sobre la función de control de riesgos.

24. La Asociación Bancaria Europea ha consolidado la mayoría de sus directrices sobre cuestiones de gobierno interno generales en la presente Guía sobre gobierno interno, mientras que, cuando resulta adecuado, se hacen referencias a otras guías que tratan aspectos más específicos del gobierno interno. La guía del CEBS sobre gobierno interno se ha revisado y fusionado con los principios de alto nivel para la política de remuneración y para la gestión de riesgos. La guía unifica los conceptos utilizados, integra los principios de alto nivel mencionados anteriormente en el contexto del gobierno interno y tiene en cuenta los fallos identificados en la

encuesta mencionada previamente, así como los avances observados desde la publicación de la Guía sobre el proceso de revisión supervisora de 2006 (por ejemplo, el contexto del grupo, sistemas y continuidad).

25. La presente guía se centra en el gobierno interno y excluye otros aspectos del gobierno corporativo (véase más adelante la sección 3 «Conceptos utilizados en la guía»). Por lo tanto, no abarca las funciones de los auditores externos, los accionistas u otras partes interesadas externas.

26. Existen otras guías del CEBS (por ejemplo, guías sobre validación, pruebas de resistencia y riesgo de concentración) que tratan aspectos detallados del gobierno interno en sus respectivas áreas. No se han fusionado con la presente guía, que se limita a los principios dirigidos directamente a la correcta implantación del gobierno interno en las entidades [9] . Todas las guías publicadas por el CEBS se pueden consultar, en inglés, en el sitio web de la EBA.

27. Al mejorar la implantación del marco de gobierno interno, se espera que las entidades sean más resistentes frente a condiciones de mercado adversas y que se contribuya de este modo a la estabilidad del sector financiero.

[8] *Ambas publicaciones (High-Level principles for Remuneration Policies y High level principles for risk management) están disponibles en inglés en el sitio web de la EBA.*

[9] *Esta guía tampoco trata las disposiciones internas que se aplican a los servicios de inversión que se incluyen en la Directiva 2004/39, conocida como la Directiva relativa a los mercados de instrumentos financieros (MiFID, en sus siglas en inglés).*

3. Conceptos utilizados en la guía

28. **Gobierno corporativo** es un concepto amplio que puede describirse como el conjunto de relaciones entre una entidad, su dirección, sus accionistas y otras partes interesadas. El gobierno interno es un componente limitado pero crucial del gobierno corporativo que se centra en la organización y la estructura interna de una entidad.

29. El **gobierno interno** de las entidades [10] de la Comunidad Europea se trata en el **artículo 22 de la Directiva 2006/48/CE**, que exige que «cada entidad de crédito disponga de sólidos procedimientos de gobierno corporativo, incluida una estructura organizativa clara, con líneas de responsabilidad bien definidas, transparentes y coherentes, así como procedimientos eficaces de identificación, gestión, control y comunicación de los riesgos a los que esté o pueda estar expuesta, junto con mecanismos adecuados de control interno, incluidos procedimientos administrativos y contables adecuados», además de prácticas y políticas de

remuneración que promuevan y sean coherentes con una gestión de riesgos sólida y eficaz. El artículo 73(3) de la Directiva 2006/48/CE exige que el artículo 22 se aplique también a las empresas matrices y filiales de manera consolidada o subconsolidada.

30. El gobierno interno incluye todas las pautas y principios relativos al establecimiento de los objetivos, estrategias y tolerancia/apetito al riesgo de una entidad, la forma en la que se organiza el negocio, la distribución de autoridad y de responsabilidades, el modo de establecer las líneas de comunicación y el tipo de información que se transmite, así como la forma de organizar el control interno. El gobierno interno abarca también la solidez de los sistemas de TI, los acuerdos de externalización y la gestión de la continuidad del negocio.

31. La EBA es consciente de que en los Estados miembros suelen utilizarse una o dos **estructuras de gobierno corporativo**: una estructura unitaria o dual. En una estructura unitaria, un órgano (por ejemplo, el consejo de administración) ejerce las funciones de supervisión y de dirección, mientras que, en una estructura dual, estas funciones son desempeñadas por un consejo de supervisión y un comité de dirección, respectivamente. Estas funciones se describen con más detalle en el capítulo B del título II.

32. La guía no aboga por ninguna estructura particular. El término «**órgano de dirección**» se utiliza en la guía para referirse a todas las estructuras de gobierno corporativo posibles. Se trata de un concepto puramente funcional, a efectos de establecer orientaciones y principios dirigidos a un resultado concreto independientemente de la estructura jurídica específica aplicable a una entidad en su Estado miembro. En consecuencia, la guía no indica si una tarea o responsabilidad particular corresponde a la función de supervisión o de dirección del órgano de dirección, puesto que variará de acuerdo con la legislación nacional de cada Estado miembro. Lo fundamental es garantizar que se lleva a cabo esa tarea o responsabilidad particular.

33. La guía es coherente con el modelo de las tres líneas defensivas. La primera «línea defensiva» establece que una entidad debe contar con procesos eficaces para la identificación, medición o evaluación, control, mitigación y comunicación de los riesgos. Estos procesos se conocen como **gestión de riesgos**.

34. Como «segunda línea defensiva», una entidad debe disponer de un marco adecuado de **control interno** para desarrollar y mantener sistemas que garanticen: operaciones eficaces y eficientes, un control adecuado de los riesgos, una conducta empresarial prudente, la fiabilidad de la información financiera y no financiera comunicada o divulgada (interna y externamente), así como el cumplimiento de las leyes, normativas, requisitos de los supervisores y las políticas y procedimientos internos de la entidad. El marco de control interno debe abarcar toda la organización, incluidas las actividades de todas las unidades de negocio, de apoyo y de control. La tercera «línea defensiva» consiste en la función de auditoría interna, que se encarga de realizar una revisión independiente de las dos primeras «líneas defensivas».

35. Al evaluar la eficacia del control interno de una entidad, el órgano de dirección debe ser capaz de confiar en la labor de las **funciones de control**, incluida la **función de control de riesgos**, la **función de cumplimiento** y la **función de auditoría interna**. Estas funciones de control deberían ser organizativamente independientes de las unidades que controlan.

36. «**Tolerancia/apetito al riesgo**» es un término que abarca todas las definiciones correspondientes utilizadas por las distintas entidades y autoridades de supervisión. Estos dos términos se utilizan indistintamente en la presente guía para describir tanto los riesgos absolutos que una entidad está dispuesta a asumir a priori (que algunos llaman «apetito al riesgo») como los límites reales dentro de ese apetito al riesgo que las entidades procuran mantener (que algunos llaman «tolerancia al riesgo»).

37. Por último, cabe destacar que, aparte del trasfondo proporcionado aquí, entre los textos correspondientes a las directrices que se exponen a continuación se intercalan a veces explicaciones adicionales sobre aspectos específicos de las directrices, que, o bien ofrecen ejemplos, o bien exponen los motivos que justifican una disposición. Cuando se da este caso, el texto explicativo aparece en un recuadro.

[10] *Las entidades a las que se hace referencia en esta guía son las entidades de crédito y las empresas de inversión según el artículo 22 de la Directiva 2006/48/CE del Parlamento Europeo y del Consejo, de 14 de junio de 2006, relativa al acceso a la actividad de las entidades de crédito y a su ejercicio (refundición); en el caso de las empresas de inversión, véase también el artículo 34 de la Directiva 2006/49/CE del Parlamento Europeo y del Consejo, de 14 de junio de 2006, sobre la adecuación del capital de las empresas de inversión y las entidades de crédito (refundición), en lo sucesivo, ambas directivas se denominarán «la Directiva sobre la adecuación del capital» (DAC).*

III. Guía de la EBA sobre gobierno interno

Estatus de la Guía

1. El presente documento contiene directrices publicadas en el artículo 16 del Reglamento (UE) n° 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° 716/2009/CE y se deroga

la Decisión 2009/78/CE de la Comisión («Reglamento de la EBA»). De conformidad con el artículo 16(3) del Reglamento de la EBA, las autoridades competentes y las entidades financieras harán todo lo posible para atenerse a la guía.

2. La guía establece el modo de ver de la EBA en lo que respecta a las prácticas de supervisión adecuadas en el Sistema Europeo de Supervisión Financiera o la manera en la que debe aplicarse el Derecho de la Unión a un área en particular. Por lo tanto, la EBA espera que todas las autoridades competentes y los participantes en los mercados financieros a los que se aplica la presente guía la cumplan a menos que se indique lo contrario. Las autoridades competentes a las que se aplica la guía deben cumplirla incorporándola a sus prácticas de supervisión (por ejemplo, modificando su marco jurídico, sus normas y/o recomendaciones de supervisión, o procesos de supervisión), incluidos los casos en los que directrices particulares de este documento vayan dirigidas principalmente a las entidades.

Requisitos de información

3. Las autoridades competentes deben notificar a la EBA si cumplen o si se proponen cumplir esta guía, o los motivos para no cumplirla, el 28 de noviembre de 2011 a más tardar. Las notificaciones deberán ser enviadas por personas autorizadas para notificar a la EBA en nombre de sus autoridades competentes a compliance@eba.europa.eu.

4. La notificación de las autoridades competentes mencionada en el apartado anterior se publicará en el sitio web de la EBA, tal como establece el artículo 16 del Reglamento de la EBA.

Entre los textos correspondientes a las directrices que se exponen a continuación se intercalan a veces explicaciones adicionales sobre aspectos específicos de las directrices, que, o bien ofrecen ejemplos, o bien exponen los motivos que justifican una disposición. Cuando se da este caso, el texto explicativo aparece en un recuadro.

Índice

I. Resumen ejecutivo	3
II. Contexto y justificación.....	7
1. Importancia del gobierno interno	7
2. Finalidad y ámbito de aplicación de la guía sobre gobierno interno	8
3. Conceptos utilizados en la guía	9
III. Guía de la EBA sobre gobierno interno	12
Título I –Objeto, ámbito de aplicación y definiciones	16
1. Objeto	16
2. Ámbito y nivel de aplicación	16
3. Definiciones.....	16
Título II – Requisitos sobre el gobierno interno de las entidades	16
A. Organización y estructura corporativa	16
4. Marco organizativo	16
5. Controles y contrapesos en una estructura de grupo	17
6. Conozca su estructura	18
7. Actividades atípicas o no transparentes	19
B. Órgano de dirección	21
B.1 Obligaciones y responsabilidades del órgano de dirección	21
8. Responsabilidades del órgano de dirección.....	21
9. Evaluación del marco de gobierno interno	22
10. Funciones de dirección y supervisión del órgano de dirección	22
B.2 Composición y funcionamiento del órgano de dirección	23
11. Composición, nombramiento y sucesión del órgano de dirección	23
12. Compromiso, independencia y gestión de conflictos de interés en el órgano de dirección	24
13. Cualificaciones del órgano de dirección	25
14. Funcionamiento organizativo del órgano de dirección	26
Evaluación del funcionamiento del órgano de dirección	26
Papel del presidente del órgano de dirección	27
Comités especializados del órgano de dirección	27
Comité de auditoría	28
Comité de riesgos	29
B.3 Marco para la conducta empresarial	29
15. Valores corporativos y código de conducta	29
16. Conflictos de interés en la entidad	29
17. Procedimientos de alerta interna	30

B.4 Políticas de externalización y remuneración	31
18. Externalización	31
19. Gestión de la política de remuneración	32
C. Gestión de riesgos	32
20. Cultura de riesgos	32
21. Adecuación de la remuneración al perfil de riesgo	33
22. Marco de gestión de riesgos	34
23. Nuevos productos	36
D. Control interno	37
24. Marco de control interno	37
25. La Función de Control de Riesgos (FCR)	38
26. El papel de la Función de Control de Riesgos (FCR)	39
Papel de la FCR en la estrategia y en las decisiones	39
Papel de la FCR en las transacciones con partes vinculadas	40
Papel de la FCR en la complejidad de la estructura jurídica	40
Papel de la FCR en los cambios importantes	40
Papel de la FCR en la medición y evaluación	40
Papel de la FCR en la supervisión	41
Papel de la FCR en las exposiciones a riesgos no aprobadas	41
27. El Director responsable del control de riesgos	42
28. La Función de cumplimiento	43
29. La Función de auditoría interna	43
E. Sistemas de información y continuidad del negocio	44
30. Sistema de información y comunicación	44
31. Gestión de la continuidad del negocio	45
F. Transparencia	46
32. Potenciación (<i>empowerment</i>)	46
33. Transparencia del gobierno interno	46
Título III – Disposiciones finales e implantación	48
34. Derogación	48
35. Fecha de aplicación	48

Título I

Objeto, ámbito de aplicación y definiciones

1. Objeto

El objetivo de la guía es armonizar las expectativas de los supervisores y mejorar la correcta implantación de los procedimientos de gobierno interno en consonancia con el artículo 22 y el anexo V de la Directiva 2006/48/CE y los Derechos de sociedades de los países.

2. Ámbito y nivel de aplicación

1. Las autoridades competentes exigirán a las entidades cumplir con las disposiciones establecidas en esta guía sobre gobierno interno.

2. La aplicación de esta guía será revisada por las autoridades competentes como parte de su proceso de evaluación y revisión supervisora.

Nota explicativa

CEBS/EBA ha elaborado una guía sobre el proceso de revisión supervisora que puede consultarse en el sitio web de la EBA en inglés.

3. La guía se aplica a las entidades a título individual y a las empresas matrices y filiales de manera consolidada o subconsolidada, a menos que se indique lo contrario.

4. La proporcionalidad, como estipulan las Directivas 2006/48 y 2006/49 (modificada), se aplica a todas las disposiciones incluidas en la guía. Una entidad demostrará cómo el enfoque que adopta, que refleja la naturaleza, la magnitud y la complejidad de sus actividades, cumple el resultado exigido por la guía.

3. Definiciones

1. En esta guía, el término órgano de dirección tendrá el siguiente significado: el órgano (u órganos) de gobierno de una entidad, compuesto por la función de supervisión y de dirección, que ostenta la máxima autoridad en la toma de decisiones finales y que está facultado para establecer la estrategia, los objetivos y la dirección global de la entidad. El órgano de dirección incluirá a las personas que dirigen de forma eficaz las actividades de una entidad.

2. En esta guía, el término entidad tendrá el siguiente significado: entidades de crédito y empresas de inversión de acuerdo con las Directivas 2006/48/CE y 2006/49/CE.

Título II

Requisitos sobre el gobierno interno de las entidades

A. Organización y estructura corporativa

4. Marco organizativo

1. El órgano de dirección de una entidad garantizará una estructura corporativa adecuada y transparente para la entidad en cuestión. La estructura fomentará y demostrará la gestión eficaz y prudente de la entidad tanto a título individual como en todo el grupo. Las líneas de comunicación y la distribución de autoridad y de responsabilidades de una entidad serán claras, estarán bien definidas, serán coherentes y deberán hacerse cumplir.

2. El órgano de dirección deberá garantizar que la estructura de la entidad y, cuando proceda, las estructuras del grupo sean claras y transparentes, tanto para el personal de la propia entidad como para los supervisores.

3. El órgano de dirección evaluará cómo se complementan e interactúan los diversos elementos de la estructura corporativa. La estructura no deberá menoscabar la capacidad del órgano de dirección de supervisar y gestionar de forma eficaz los riesgos a los que se enfrenta la entidad o el grupo.

4. El órgano de dirección deberá evaluar cómo afectan los cambios de la estructura del grupo a su solidez. Asimismo, deberá efectuar los ajustes necesarios rápidamente.

Nota explicativa

Los cambios pueden derivarse de, por ejemplo, la constitución de nuevas filiales, fusiones y adquisiciones, la venta o disolución de partes del grupo, o pueden proceder de factores externos.

5. Controles y contrapesos en una estructura de grupo

1. En la estructura de un grupo, el órgano de dirección de la empresa matriz de una entidad tendrá la responsabilidad global de lograr un gobierno interno adecuado en todo el grupo y de garantizar que exista un marco de gobierno corporativo adecuado para la estructura, el negocio y los riesgos del grupo y de las entidades que lo componen.

2. El órgano de dirección de cada filial regulada de un grupo deberá cumplir, en calidad de entidad jurídica, los mismos valores y políticas de gobierno interno que su empresa matriz, a menos que existan consideraciones en cuanto a proporcionalidad o requisitos legales o de supervisión que determinen lo contrario. En consecuencia, el órgano de dirección de una filial regulada deberá, dentro de sus

propias responsabilidades en materia de gobierno interno, establecer sus políticas y deberá evaluar las decisiones o prácticas adoptadas por el grupo para velar por que no contribuyan a que la filial regulada incumpla normas prudenciales o disposiciones legales o normativas aplicables. El órgano de dirección de la filial regulada deberá velar también para que tales decisiones o prácticas no vayan en detrimento de:

- a. la gestión sólida y prudente de la filial;
- b. la solidez económica de la filial; o
- c. los intereses jurídicos de las partes interesadas de la filial.

3. Los órganos de dirección de la empresa matriz y de sus filiales deberán aplicar y tener en cuenta los apartados que figuran a continuación, considerando los efectos de la dimensión del grupo en su gobierno interno.

4. En el cumplimiento de sus responsabilidades en materia de gobierno interno, el órgano de dirección de la empresa matriz de una entidad deberá ser consciente de todos los riesgos y cuestiones importantes que podrían afectar al grupo, a la propia empresa matriz y a sus filiales. Por lo tanto, deberá vigilar a sus filiales de forma adecuada y respetar a la vez las responsabilidades independientes jurídicas y de gobierno corporativo que se aplican a los órganos de dirección de las filiales reguladas.

5. Para cumplir sus responsabilidades en materia de gobierno interno, el órgano de dirección de la empresa matriz de la entidad deberá:

a. establecer una estructura de gobierno corporativo que contribuya a la supervisión eficaz de sus filiales y que tenga en cuenta la naturaleza, la magnitud y la complejidad de los diferentes riesgos a los que están expuestos el grupo y sus filiales;

b. aprobar una política de gobierno interno de todo el grupo para sus filiales, que incluya el compromiso de cumplir todos los requisitos de gobierno corporativo aplicables;

c. garantizar que se dispone de los recursos suficientes para que cada filial cumpla tanto las normas del grupo como las normas de gobierno corporativo locales;

d. contar con los medios adecuados para vigilar que cada filial cumpla todos los requisitos de gobierno interno aplicables; y

e. garantizar que las líneas de comunicación del grupo sean claras y transparentes, especialmente en los casos en los que las líneas de negocio no coinciden con la estructura jurídica del grupo.

6. Una filial regulada deberá contar, como elemento de un gobierno corporativo

sólido, con un número suficiente de miembros independientes en el órgano de dirección. Los miembros independientes del órgano de dirección son consejeros no ejecutivos que son independientes de la filial y de su grupo, así como de su accionista mayoritario.

6. Conozca su estructura

1. El órgano de dirección deberá conocer y comprender totalmente la estructura operativa de una entidad («conozca su estructura») y velar por que sea acorde con la estrategia de negocio aprobada y su perfil de riesgo.

Nota explicativa

Resulta crucial que el órgano de dirección conozca y comprenda totalmente la estructura operativa de una entidad. En los casos en los que una entidad crea muchas entidades jurídicas dentro de su grupo, su número y, particularmente, las interconexiones y transacciones entre ellas pueden plantear retos para el diseño de su gobierno interno y para la gestión y supervisión de los riesgos del grupo en conjunto, algo que representa un riesgo por sí solo.

2. El órgano de dirección deberá guiar y comprender la estructura de la entidad, su evolución y sus limitaciones, y deberá garantizar que la estructura esté justificada y no dé lugar a una complejidad indebida o inadecuada. También es responsable de aprobar políticas y estrategias sólidas para establecer nuevas estructuras. Del mismo modo, el órgano de dirección deberá reconocer los riesgos que plantea la complejidad de la estructura jurídica de la entidad por sí sola y deberá garantizar que la entidad sea capaz de elaborar información de manera oportuna sobre el tipo, los estatutos, la estructura de propiedad y las actividades de cada entidad jurídica.

3. El órgano de dirección de la empresa matriz de una entidad deberá comprender no solo la organización corporativa del grupo sino también la finalidad de sus distintas entidades y los vínculos y relaciones entre ellas. Aquí se incluye comprender los riesgos operacionales específicos del grupo, las exposiciones a riesgos intragrupo y la forma en la que la financiación del grupo, su capital y perfiles de riesgo podrían verse afectados en circunstancias habituales y adversas.

4. El órgano de dirección de la empresa matriz de una entidad deberá garantizar que las diferentes entidades del grupo (incluida la propia entidad) reciban la información suficiente para que todas obtengan una percepción clara de los objetivos generales y los riesgos del grupo. Todo flujo de información significativa entre las entidades que sea pertinente al funcionamiento operativo del grupo deberá estar documentado y, cuando se solicite, deberá ser puesto rápidamente a disposición del órgano de dirección, las funciones de control y los supervisores, según proceda.

5. El órgano de dirección de la empresa matriz de una entidad deberá mantenerse informado sobre los riesgos que causa la estructura del grupo. La información que necesita incluye:

a. información sobre los principales factores de riesgo, e

b. informes periódicos donde se evalúa la estructura global de la entidad y se evalúa si en las actividades de las entidades individuales se cumple la estrategia aprobada.

7 . Actividades atípicas o no transparentes

1. En los casos en los que una entidad opera mediante estructuras de entidades vinculadas o con cometido especial o en jurisdicciones que menoscaban la transparencia o que no cumplen las normas bancarias internacionales, el órgano de dirección comprenderá su finalidad y estructura y los riesgos particulares asociados. El órgano de dirección solo aceptará esas actividades cuando se haya cerciorado de que los riesgos se gestionarán de forma adecuada.

Nota explicativa

Además de ese principio, las autoridades competentes aplicarán también los *Principios Básicos para una supervisión bancaria eficaz*, elaborados por el Comité de Supervisión Bancaria de Basilea, cuando evalúen actividades empresariales en jurisdicciones que no son totalmente transparentes o que no cumplen las normas bancarias internacionales.

Es posible que la entidad tenga razones legítimas para operar en determinadas jurisdicciones (o con entidades o contrapartes que operan en dichas jurisdicciones) o establezcan estructuras particulares (por ejemplo, entidades con cometido especial o fideicomisos de sociedad anónima). No obstante, operar en jurisdicciones que no son totalmente transparentes o que no cumplen las normas bancarias internacionales (por ejemplo, en las áreas de supervisión prudencial, tributación, la lucha contra el blanqueo de dinero y la financiación del terrorismo) o mediante estructuras complejas o no transparentes puede plantear riesgos específicos financieros, jurídicos o de reputación. También puede menoscabar la capacidad del órgano de dirección para supervisar las actividades debidamente y puede impedir una supervisión bancaria eficaz. Por lo tanto, estas estructuras solo deberán aprobarse y mantenerse cuando su finalidad haya sido definida y comprendida, cuando se haya garantizado la supervisión y cuando todos los riesgos asociados importantes que podrían generar estas estructuras puedan gestionarse debidamente.

En consecuencia, el órgano de dirección deberá prestar especial atención a todas estas situaciones ya que plantean retos significativos para la comprensión de la estructura del grupo.

2. El órgano de dirección deberá establecer, mantener y revisar, de forma constante, estrategias, políticas y procedimientos adecuados que regulen la aprobación y el mantenimiento de tales estructuras y actividades con el fin de garantizar que sigan siendo coherentes con el objetivo deseado.

3. El órgano de dirección deberá garantizar que se adopten las medidas apropiadas para evitar o reducir los riesgos de tales actividades. Dichas medidas

implicarán que:

a. la entidad ha establecido políticas y procedimientos adecuados, así como procesos documentados (por ejemplo, límites aplicables, requisitos de información) para la consideración, aprobación y gestión de los riesgos de esas actividades, teniendo en cuenta las consecuencias para la estructura operativa del grupo;

b. la información relativa a esas actividades y a sus riesgos está a disposición de la administración central de la entidad y de los auditores, y se comunica al órgano de dirección y a los supervisores;

c. la entidad evalúa periódicamente la necesidad constante de realizar actividades que menoscaban la transparencia.

4. Se deberán tomar las mismas medidas cuando una entidad realice actividades atípicas o no transparentes para clientes.

Nota explicativa

Las actividades atípicas o no transparentes realizadas para clientes (por ejemplo, ayudar a los clientes a constituir entidades en jurisdicciones extraterritoriales; desarrollar estructuras complejas y financiar transacciones para esas estructuras o prestar servicios de fideicomiso) plantean retos similares para el gobierno interno y pueden crear riesgos operacionales y de reputación significativos. Por lo tanto, deben adoptarse las mismas medidas de gestión de riesgos que en el caso de las actividades empresariales de la propia entidad.

5. Todas estas estructuras y actividades deberán ser objeto de revisiones periódicas por las auditorías interna y externa.

B. Órgano de dirección

B.1 Obligaciones y responsabilidades del órgano de dirección

8. Responsabilidades del órgano de dirección

1. El órgano de dirección asumirá la responsabilidad global de la entidad y establecerá la estrategia de la entidad. Las responsabilidades del órgano de dirección estarán claramente definidas en un documento escrito y serán debidamente aprobadas.

Nota explicativa

La correcta ejecución de las responsabilidades del órgano de dirección constituye la base para la gestión sólida y prudente de la entidad. Las responsabilidades documentadas también deberán ser acordes con el derecho de sociedades del país en cuestión.

2. Las principales responsabilidades del órgano de dirección deberán incluir el establecimiento y la supervisión de:

a. la estrategia empresarial global de la entidad dentro del marco jurídico y regulador aplicable, que tendrá en cuenta la solvencia y los intereses financieros a largo plazo de la entidad;

b. la política y estrategia de riesgos global de la entidad, que incluirá su tolerancia/apetito al riesgo y su marco de gestión de riesgos;

c. las cantidades, tipos y distribución del capital interno y de los fondos propios adecuados para cubrir los riesgos de la entidad;

d. una estructura organizativa sólida y transparente con canales de información y comunicación eficaces;

e. una política de nombramiento y sucesión de los responsables de funciones clave en la entidad;

f. un marco de remuneración acorde con las estrategias de riesgo de la entidad;

g. los principios de gobierno corporativo y los valores corporativos de la entidad, incluido un código de conducta o documento comparable; y

h. un marco de control interno adecuado y eficaz, que incluya funciones de control de riesgos, cumplimiento y auditoría interna que funcionen debidamente, así como un marco contable y de información financiera adecuado.

3. El órgano de dirección deberá también revisar y ajustar periódicamente esas políticas y estrategias. El órgano de dirección es responsable de una adecuada comunicación con las autoridades de supervisión y otras partes interesadas.

9. Evaluación del marco de gobierno interno

1. El órgano de dirección supervisará y evaluará periódicamente la eficacia del marco de gobierno interno de la entidad.

2. Se llevará a cabo una revisión del marco de gobierno interno y de su implantación al menos una vez al año. Deberá centrarse en los cambios de factores internos y externos que afectan a la entidad.

10. Funciones de dirección y supervisión del órgano de dirección

1. Las funciones de dirección y de supervisión del órgano de dirección de una entidad deberán interactuar de manera eficaz.

Nota explicativa

Los Estados miembros suelen utilizar una de las dos **estructuras de gobierno corporativo**: una estructura unitaria o dual. En ambas estructuras el órgano de dirección en el ejercicio de su función de dirección y el órgano de supervisión desempeñan su propio papel en la gestión de la entidad, directamente o a través de comités.

La función de dirección propone la dirección de la entidad; garantiza la implantación eficaz de la estrategia y es la responsable de la gestión diaria de la entidad.

La función de supervisión controla la función de dirección y le ofrece asesoramiento. Su papel de supervisión consiste en cuestionar la función de dirección de forma constructiva cuando se elabora la estrategia de la entidad; vigilar su desempeño y la consecución de las metas y objetivos acordados; además de garantizar la integridad de la información financiera y la gestión eficaz de los riesgos y los controles internos.

Para lograr un buen gobierno corporativo, las funciones de dirección y de supervisión de la entidad deberán interactuar de manera eficaz para poner en práctica la estrategia acordada de la entidad y, en especial, para gestionar los riesgos a los que se enfrenta la entidad. Aunque pueden existir diferencias significativas entre los marcos legislativos y reguladores de los distintos países, no deberán impedir la interacción eficaz entre estas dos funciones, independientemente de si el órgano de dirección está compuesto por un órgano o más.

2. El órgano de dirección, en el ejercicio de su función de supervisión, deberá:

a. estar preparado y ser capaz de cuestionar y revisar de forma crítica y constructiva las propuestas, explicaciones e información proporcionadas por los miembros del órgano de dirección en el ejercicio de su función de dirección;

b. vigilar que la estrategia, la tolerancia/apetito al riesgo y las políticas de la entidad se implanten de manera uniforme y que se mantengan pautas de desempeño acordes con sus intereses financieros a largo plazo y su solvencia; y

c. vigilar el desempeño de los miembros del órgano de dirección en el ejercicio de su función de dirección en comparación con esas pautas.

3. El órgano de dirección, en el ejercicio de su función de dirección, deberá coordinar la estrategia empresarial y la estrategia de riesgos de la entidad con su función de supervisión, así como debatir periódicamente la implantación de esas estrategias con dicha función.

4. Cada función deberá proporcionar a la otra la información suficiente. La función de dirección del órgano de dirección deberá informar a la función de supervisión periódicamente de manera exhaustiva, y sin demora cuando sea necesario, de los elementos pertinentes para la evaluación de la situación, la gestión de la entidad y el mantenimiento de su seguridad financiera.

B.2 Composición y funcionamiento del órgano de dirección

11. Composición, nombramiento y sucesión del órgano de dirección

1. El órgano de dirección contará con un número adecuado de miembros y una composición apropiada. El órgano de dirección dispondrá de políticas para la selección, supervisión y planificación de la sucesión de sus miembros.

2. Una entidad deberá establecer el tamaño y la composición de su órgano de dirección, teniendo en cuenta el tamaño y la complejidad de la entidad además de la naturaleza y ámbito de aplicación de sus actividades. En la selección de los miembros del órgano de dirección se deberá velar por reunir conocimientos especializados suficientes.

3. El órgano de dirección deberá identificar y seleccionar a candidatos cualificados y experimentados, además de garantizar una planificación adecuada de la sucesión del órgano de dirección, considerando debidamente cualesquiera otros requisitos legales con respecto a la composición, nombramiento o sucesión.

4. El órgano de dirección deberá garantizar que una entidad cuente con políticas para seleccionar nuevos miembros y para volver a nombrar a los miembros actuales. Estas políticas deberán incluir la elaboración de una descripción de las habilidades y competencias necesarias para garantizar suficientes conocimientos especializados.

5. Los miembros del órgano de dirección deberán ser nombrados por un periodo adecuado. Las candidaturas presentadas para volver a nombrar a miembros actuales deberán basarse en el perfil indicado anteriormente y solo deberán presentarse después de considerar detenidamente el desempeño del candidato en cuestión durante su último mandato.

6. Cuando establezca un plan de sucesión de sus miembros, el órgano de dirección deberá considerar la fecha de vencimiento del mandato o contrato de cada miembro para evitar, siempre que sea posible, tener que sustituir a muchos miembros a la vez.

12. Compromiso, independencia y gestión de conflictos de interés en el órgano de dirección

1. Los miembros del órgano de dirección participarán activamente en las actividades de una entidad y serán capaces de tomar sus decisiones y emitir sus opiniones con objetividad, independencia y buen criterio.

2. La selección de los miembros del órgano de dirección deberá garantizar la independencia y conocimientos especializados suficientes en el seno del órgano de dirección. La entidad deberá velar por que los miembros del órgano de dirección puedan dedicar el tiempo y el esfuerzo suficientes para cumplir sus responsabilidades de forma eficaz.

3. Los miembros del órgano de dirección solo deberán tener un número limitado

de mandatos u otras actividades profesionales que exigen mucho tiempo. Es más, los miembros deberán informar a la entidad sobre sus actividades profesionales secundarias (por ejemplo, mandatos en otras empresas). Como el presidente asume más responsabilidades y obligaciones, se espera que dedique mucho más tiempo que los demás.

4. El tiempo que se espera que dediquen como mínimo todos los miembros del órgano de dirección deberá especificarse en un documento escrito. Cuando estén estudiando el nombramiento de un nuevo miembro, o cuando sean informados sobre un nuevo mandato de un miembro actual, los miembros del órgano de dirección deberán cuestionar cómo va a dedicar esa persona el tiempo suficiente a sus responsabilidades para con la entidad. Deberá divulgarse la asistencia de los miembros de la función de supervisión del órgano de dirección. Una entidad deberá estudiar también divulgar las ausencias prolongadas de los miembros de la función de dirección del órgano de dirección.

5. Los miembros del órgano de dirección deberán ser capaces de actuar de forma objetiva, crítica e independiente. Las medidas para mejorar la capacidad de utilizar su buen criterio de forma objetiva e independiente deberán incluir la selección de miembros de un grupo lo suficientemente amplio y garantizar un número suficiente de miembros no ejecutivos.

Nota explicativa

En los casos en los que existe una separación formal entre la función de supervisión del órgano de dirección y su función de dirección, la objetividad e independencia de la función de supervisión debe garantizarse mediante la selección adecuada de miembros independientes.

6. El órgano de dirección deberá contar con una política escrita sobre cómo gestionar los conflictos de interés de sus miembros. En esa política se deberá especificar lo siguiente:

a. la obligación de todo miembro de evitar conflictos de interés que no hayan sido comunicados al órgano de dirección y aprobados por este, pero, de darse, en todo caso, habrá que garantizar que los conflictos se gestionan debidamente;

b. un proceso de revisión o aprobación que los miembros deberán seguir antes de participar en determinadas actividades (como formar parte de otro órgano de dirección) para garantizar que ese nuevo cometido no crea un conflicto de interés;

c. la obligación de los miembros de informar a la entidad sobre cualquier asunto que podría dar lugar, o que ya haya dado lugar, a un conflicto de interés;

d. la responsabilidad de los miembros de abstenerse de participar en la toma de decisiones o en la votación de cualquier asunto donde podría existir un conflicto de interés o en los casos en los que podrían verse comprometidas la objetividad o capacidad de esos miembros para cumplir debidamente sus obligaciones para con la entidad;

e. procedimientos adecuados para que las transacciones con partes vinculadas se lleven a cabo en condiciones equitativas; y

f. la forma en la que el órgano de dirección abordará el incumplimiento de la política.

13. Cualificaciones del órgano de dirección

1. Los miembros del órgano de dirección estarán cualificados en todo momento para sus cargos, por ejemplo, mediante formación. Deberán comprender claramente los procedimientos de gobierno corporativo de la entidad y el papel que desempeñan en los mismos.

2. Los miembros del órgano de dirección, tanto individualmente como colectivamente, deberán tener los conocimientos especializados, la experiencia, las competencias, el entendimiento y las cualidades personales necesarios, incluyendo la profesionalidad y la integridad personal, para cumplir debidamente con sus obligaciones.

3. Los miembros del órgano de dirección deberán tener un conocimiento actualizado de las actividades de la entidad, en una medida proporcional a sus responsabilidades. Aquí se incluye el comprender debidamente las áreas de las que no son directamente responsables pero sobre las que deben rendir cuentas como colectivo.

4. Colectivamente, deberán comprender plenamente la naturaleza del negocio y sus riesgos asociados, y deberán contar con experiencia y conocimientos especializados adecuados pertinentes en cada una de las actividades importantes que la entidad se propone llevar a cabo, para permitir una supervisión y un gobierno corporativo eficaces.

5. Una entidad deberá contar con un proceso sólido que garantice que los miembros del órgano de dirección, individual y colectivamente, estén debidamente cualificados.

6. Los miembros del órgano de dirección deberán adquirir, mantener y profundizar en sus conocimientos y habilidades para cumplir con sus responsabilidades. Las entidades deberán garantizar que los miembros tengan acceso a programas de formación personalizados que deben tener en cuenta las diferencias entre el perfil de conocimientos que necesita la entidad y los conocimientos reales que poseen los miembros. Entre las áreas que se podrían tratar se incluyen las herramientas y modelos de gestión de riesgos de la entidad, nuevos avances, cambios en la organización, productos complejos, nuevos productos o mercados y fusiones. La formación también deberá abarcar áreas de negocio en las que los miembros individuales no tienen una responsabilidad directa. El órgano de dirección deberá dedicar a su formación tiempo, presupuesto y demás recursos suficientes.

14. Funcionamiento organizativo del órgano de dirección

1. El órgano de dirección definirá las prácticas y procedimientos de gobierno interno adecuados para su propia organización y funcionamiento y contará con los medios para garantizar que se lleve a cabo un seguimiento y una revisión periódica de dichas prácticas para mejorarlas.

Nota explicativa

Demostrar unas buenas prácticas y procedimientos de gobierno interno en el órgano de dirección proyecta una imagen positiva interna y externamente sobre las políticas de gobierno corporativo y los objetivos de la entidad. Las prácticas y procedimientos incluyen la frecuencia, los procedimientos de trabajo y las actas de las reuniones; el papel del presidente y el uso de los comités.

2. El órgano de dirección deberá reunirse periódicamente para llevar a cabo sus responsabilidades de forma adecuada y eficaz. Los miembros del órgano de dirección deberán dedicar el tiempo suficiente a la preparación de las reuniones. En esta preparación se incluye establecer un orden del día. Las actas de la reunión deberán indicar los puntos del orden del día y deberán señalar claramente las decisiones tomadas y las acciones acordadas. Estas prácticas y procedimientos, junto con los derechos, responsabilidades y actividades principales del órgano de dirección, deberán estar documentadas y deberán ser revisadas periódicamente por el órgano de dirección.

Evaluación del funcionamiento del órgano de dirección

3. El órgano de dirección deberá evaluar periódicamente la eficiencia y la eficacia individual y colectiva de sus actividades, prácticas y procedimientos de gobierno corporativo, así como el funcionamiento de los comités. Se podrá recurrir a personas externas que faciliten esa evaluación.

Papel del presidente del órgano de dirección

4. El presidente debe garantizar la correcta y bien fundada toma de decisiones del órgano de dirección. Deberá fomentar y promover un debate abierto y crítico y velar por que puedan expresarse y debatirse opiniones divergentes en el proceso de toma de decisiones.

Nota explicativa

El presidente del órgano de dirección desempeña un papel crucial en el buen funcionamiento del órgano de dirección. Es el responsable del liderazgo del órgano de dirección y de la eficacia de su funcionamiento global.

5. En las estructuras de gobierno corporativo con un único órgano, el presidente del órgano de dirección y el director ejecutivo de la entidad no deberán ser la misma

persona. En los casos en los que el presidente del órgano de dirección es también el director ejecutivo de la entidad, esta última deberá contar con medidas para minimizar el posible perjuicio para sus controles y contrapesos.

Nota explicativa

Los controles y contrapesos podrían consistir, por ejemplo, en nombrar, de entre los miembros independientes y experimentados del órgano de dirección, un consejero principal o cargo similar que conduzca o articule la función supervisora de aquel órgano.

Comités especializados del órgano de dirección

6. El órgano de dirección, en el ejercicio de su función de supervisión, deberá considerar, teniendo en cuenta el tamaño y la complejidad de la entidad, la creación de comités especializados formados por miembros del órgano de dirección (también pueden ser invitadas a asistir otras personas por sus conocimientos especializados pertinentes para una cuestión en particular o para que presten asesoramiento al respecto). Los comités especializados podrían ser, por ejemplo, un comité de auditoría, un comité de riesgos, un comité de remuneración, un comité de nombramientos o recursos humanos y un comité de gobierno corporativo o de ética o de cumplimiento.

Nota explicativa

Delegar en tales comités no exime de ningún modo al órgano de dirección, en el ejercicio de su función de supervisión, de cumplir colectivamente con sus obligaciones y responsabilidades, pero puede servir de apoyo en áreas específicas ya que se facilita el desarrollo y la implantación de buenas prácticas y decisiones en materia de gobierno corporativo.

7. Un comité especializado deberá tener una combinación óptima de conocimientos especializados, competencias y experiencia que, conjuntamente, permita comprender plenamente y evaluar objetivamente las cuestiones correspondientes, además de aportar ideas nuevas. Deberá contar con un número suficiente de miembros independientes. Cada comité deberá disponer de un mandato documentado (incluido su ámbito de aplicación) procedente del órgano de dirección en el ejercicio de su función de supervisión, así como de procedimientos de trabajo establecidos. Los miembros y la presidencia de los comités podrían rotar de vez en cuando.

Nota explicativa

La rotación de los miembros y de la presidencia contribuye a evitar una concentración indebida de poder y a promover nuevas perspectivas.

8. Los presidentes respectivos de cada comité deberán informar periódicamente

al órgano de dirección. Los comités especializados deberán interactuar unos con otros según proceda para garantizar la coherencia y evitar lagunas. Una manera de interactuar podría ser la participación conjunta: el presidente o un miembro de un comité especializado podría ser miembro también de otro comité especializado.

Comité de auditoría

9. Un comité de auditoría (o equivalente) deberá, entre otras funciones, supervisar la eficacia del control interno de la empresa, la auditoría interna y los sistemas de gestión de riesgos; supervisar a los auditores externos de la entidad; recomendar, para que se aprueben en el órgano de dirección, el nombramiento, retribución y despido de los auditores externos; revisar y aprobar el ámbito de aplicación y la frecuencia de las auditorías; revisar los informes de auditoría, y comprobar que el órgano de dirección, en el ejercicio de su función de dirección, adopta las medidas correctoras necesarias de forma oportuna para abordar los fallos de los controles, el incumplimiento de las leyes, normativas y políticas, además de otros problemas identificados por los auditores. Asimismo, el comité de auditoría deberá supervisar el establecimiento de políticas contables por parte de la entidad.

Nota explicativa

Véase también el artículo 41 de la Directiva 2006/43/CE relativa a la auditoría legal de las cuentas anuales y de las cuentas consolidadas.

10. El presidente del comité deberá ser independiente. Si el presidente es un antiguo miembro de la función de dirección de la entidad, deberá transcurrir un periodo de tiempo adecuado antes de que ocupe el puesto de presidente del comité.

11. Los miembros del comité de auditoría en conjunto deberán tener experiencia práctica reciente y pertinente en el área de mercados financieros o deberán haber obtenido, a través de las actividades empresariales realizadas previamente, experiencia profesional suficiente vinculada directamente con la actividad de los mercados financieros. En todo caso, el presidente del comité de auditoría deberá contar con experiencia y conocimientos especializados en aplicación de principios contables y procesos de control interno.

Comité de riesgos

12. Un comité de riesgos (o equivalente) deberá ser responsable de asesorar al órgano de dirección sobre la tolerancia/apetito y la estrategia de riesgo global actual y futura de la entidad, y se encargará de vigilar la implantación de esa estrategia. Para aumentar la eficacia del comité de riesgos, deberá comunicarse periódicamente con la función de control de riesgos de la entidad y con el director responsable del control de riesgos y deberá, cuando proceda, tener acceso al asesoramiento de expertos externos, especialmente con relación a transacciones estratégicas propuestas, como fusiones y adquisiciones.

B.3 Marco para la conducta empresarial

15. Valores corporativos y código de conducta

1. El órgano de dirección elaborará y promoverá estrictas pautas profesionales y éticas.

Nota explicativa

Cuando la reputación de una entidad se pone en entredicho, la pérdida de confianza puede ser difícil de restablecer y las repercusiones pueden trascender a todo el mercado.

La implantación de pautas adecuadas (por ejemplo, de un código de conducta) para lograr una conducta profesional y responsable en toda la entidad deberá contribuir a reducir los riesgos a los que está expuesta. Concretamente, los riesgos operacional y de reputación pueden reducirse si se concede una alta prioridad a esas pautas y se asientan profundamente.

2. El órgano de dirección deberá contar con políticas claras sobre cómo deben cumplirse esas pautas.

3. La implantación y el cumplimiento de esas pautas deberán revisarse constantemente. Los resultados deberán comunicarse al órgano de dirección periódicamente.

16. Conflictos de interés en la entidad

1. El órgano de dirección establecerá, implantará y mantendrá políticas eficaces para identificar conflictos de interés reales o posibles. Los conflictos de interés que se han comunicado al órgano de dirección y que han sido aprobados por este deberán gestionarse debidamente.

2. Deberá existir una política escrita en la que se identifiquen las relaciones, los servicios, las actividades o las transacciones de una entidad donde pueden surgir conflictos de interés y que deberá indicar cómo deben gestionarse tales conflictos. Esta política deberá tratar las relaciones y transacciones entre diferentes clientes de la entidad y entre la entidad y:

a. sus clientes (como resultado del modelo comercial o de los diversos servicios y actividades que realiza la entidad);

b. sus accionistas;

c. los miembros de su órgano de dirección;

d. su personal;

e. proveedores o socios comerciales significativos; y

f. otras partes vinculadas (por ejemplo, su empresa matriz o filiales).

3. Una empresa matriz debe considerar y equilibrar los intereses de todas sus filiales, y analizar cómo estos intereses contribuyen a la finalidad y a los intereses comunes del grupo en su conjunto a largo plazo.

4. En la política sobre conflictos de interés deberán establecerse las medidas que deben adoptarse para evitar o gestionar los conflictos de interés. Esos procedimientos y políticas podrían incluir, por ejemplo:

a. dividir correctamente las obligaciones, por ejemplo, confiar actividades conflictivas dentro de la cadena de transacciones o de servicios a personas diferentes, o confiar las responsabilidades de supervisión y comunicación de actividades conflictivas a personas diferentes;

b. establecer barreras de información como separación física de determinados departamentos; y

c. evitar que personas que llevan a cabo actividades fuera de la entidad ejerzan una influencia indebida en la entidad con respecto a dichas actividades.

17. Procedimientos de alerta interna

1. El órgano de dirección establecerá procedimientos de alerta interna adecuados para la comunicación de las preocupaciones del personal relativas al gobierno interno.

2. Una entidad deberá adoptar procedimientos de alerta interna adecuados que el personal pueda utilizar para llamar la atención sobre preocupaciones significativas y legítimas con respecto a cuestiones relacionadas con el gobierno interno. Estos procedimientos deberán respetar la confidencialidad del personal que plantea tales preocupaciones. Para evitar conflictos de interés, deberá brindarse la oportunidad de informar sobre este tipo de preocupaciones a través de canales distintos a las líneas de comunicación habituales (por ejemplo, a través de la función de cumplimiento, la función de auditoría interna o un procedimiento de denuncia interno). Los procedimientos de alerta deberán estar a disposición de todo el personal dentro de la entidad. La información facilitada por el personal a través del procedimiento de alerta deberá, de ser relevante, ponerse a disposición del órgano de dirección.

Nota explicativa

En algunos Estados miembros, además de los procedimientos de alerta interna en el seno de las entidades, puede existir también la posibilidad de que el personal informe a la autoridad de supervisión sobre preocupaciones de este tipo.

B.4 Políticas de externalización y remuneración

18. Externalización

1. El órgano de dirección aprobará y revisará periódicamente la política de

externalización de la entidad.

Nota explicativa

La presente guía se limita a la política de externalización; los aspectos específicos sobre externalización se tratan en la guía del CEBS sobre externalización, disponible en inglés en el sitio web de la EBA.

Se espera que las entidades cumplan ambas guías. En el caso de discrepancias, prevalecerá la guía (del CEBS) sobre externalización, ya que es más específica. En el caso de que no se trate de una cuestión abarcada en la guía del CEBS, se aplicará el principio general de la presente guía.

2. La política de externalización deberá considerar el impacto de la externalización en el negocio de la entidad y los riesgos a los que se enfrenta (como el riesgo operacional, de reputación y de concentración). La política deberá incluir los procedimientos de comunicación y supervisión que deberán aplicarse desde el comienzo hasta el vencimiento de un acuerdo de externalización (incluida la elaboración del argumento empresarial para justificar una externalización, la suscripción de un contrato de externalización, la implantación del contrato hasta su vencimiento, planes de contingencias y estrategias de salida). La política deberá ser revisada y actualizada periódicamente y los cambios deberán aplicarse de manera oportuna.

3. La entidad sigue siendo plenamente responsable de todos los servicios y actividades externalizados, así como de las decisiones de gestión derivadas de los mismos. En consecuencia, la política de externalización deberá dejar claro que una externalización no exime a la entidad de sus obligaciones normativas y de sus responsabilidades para con sus clientes.

4. La política deberá indicar que los acuerdos de externalización no deberán impedir la supervisión eficaz in situ o a distancia de la entidad y no deberán contravenir ninguna restricción impuesta por los supervisores sobre servicios y actividades. La política deberá tratar también la externalización interna (por ejemplo, mediante una entidad jurídica separada perteneciente al grupo de la entidad) y las circunstancias específicas del grupo que deben tenerse en cuenta.

19. Gestión de la política de remuneración

1. La responsabilidad de la supervisión de la política de remuneración recae, en última instancia, en el órgano de dirección de la entidad.

Nota explicativa

La presente guía ofrece el marco *general* aplicable a la gestión de la política de remuneración. Los aspectos *específicos* sobre remuneración se tratan en la guía del CEBS sobre remuneración de diciembre de 2010. Se espera que las entidades cumplan con ambas guías.

2. El órgano de dirección, en el ejercicio de su función de supervisión, deberá

mantener, aprobar y supervisar los principios de la política global de remuneración de la entidad. Los procedimientos de la entidad para determinar la remuneración deberán ser claros, estar bien documentados y ser internamente transparentes.

3. Además de la responsabilidad general del órgano de dirección con respecto a la política global de remuneración y su revisión, también es necesaria la correcta participación de las funciones de control. Los miembros del órgano de dirección, los miembros del comité de remuneraciones y otros miembros del personal que intervienen en el diseño e implantación de la política de remuneración deberán tener los conocimientos especializados pertinentes y ser capaces de emitir opiniones independientes con buen criterio sobre la idoneidad de la política de remuneración, incluidas sus implicaciones para la gestión de riesgos.

4. La política de remuneración también deberá estar orientada a evitar conflictos de interés. El órgano de dirección, en el ejercicio de su función de dirección, no deberá determinar su propia remuneración; para evitarlo, podría considerarse, por ejemplo, el uso de un comité de remuneración independiente. Una unidad de negocio no deberá determinar la remuneración de sus funciones de control.

5. El órgano de dirección deberá supervisar la aplicación de la política de remuneración para garantizar que funciona según lo previsto. La implantación de la política de remuneración también deberá ser objeto de una revisión central e independiente.

C. Gestión de riesgos

20. Cultura de riesgos

1. Una entidad desarrollará una cultura de riesgos integrada para toda la entidad, basada en una total comprensión de los riesgos a los que se enfrenta y la forma en la que se gestionan, teniendo en cuenta su tolerancia/apetito al riesgo.

Nota explicativa

Dado que las actividades de una entidad básicamente implican la asunción de riesgos, es fundamental que se gestionen los riesgos correctamente. Un elemento clave para la gestión eficaz de los riesgos es la existencia de una cultura de riesgos sólida y coherente en toda la entidad.

2. Una entidad deberá desarrollar su cultura de riesgos mediante políticas, ejemplos, comunicaciones y formación del personal con respecto a sus responsabilidades en materia de riesgos.

3. Todo miembro de la organización deberá ser plenamente consciente de sus responsabilidades en la gestión de riesgos. La gestión de riesgos no deberá confinarse a los profesionales especializados en riesgos o a las funciones de control. Las unidades de negocio, supervisadas por el órgano de dirección, deberán ser

principalmente responsables de la gestión diaria de los riesgos; deberán tener en cuenta la tolerancia/apetito al riesgo de la entidad y respetar sus políticas, procedimientos y controles.

4. Una entidad deberá contar con un marco de gestión de riesgos holístico que se aplique a todas sus unidades de negocio, de apoyo y de control, en el que se reconozca totalmente el fondo económico de sus exposiciones a riesgos y que abarque todos los riesgos pertinentes (por ejemplo, financieros y no financieros, dentro y fuera de balance, y tanto si son contingentes o contractuales como si no). Su ámbito de aplicación no deberá limitarse a los riesgos de crédito, de mercado, de liquidez y operacional, sino que también deberá incluir los riesgos de concentración, de reputación, de cumplimiento y estratégico.

5. El marco de gestión de riesgos deberá permitir a la entidad tomar decisiones bien fundadas. Deberá basarse en la información derivada de la identificación, medición o evaluación y control de los riesgos. Los riesgos deberán evaluarse de abajo arriba y de arriba abajo, en toda la cadena de dirección, así como en todas las líneas de negocio. Se deberán emplear una terminología coherente y metodologías compatibles en toda la entidad y su grupo.

6. El marco de gestión de riesgos deberá ser objeto de una revisión independiente interna o externa y deberá volver a evaluarse periódicamente en comparación con la tolerancia/apetito al riesgo de la entidad, teniendo en cuenta la información procedente de la función de control de riesgos y, cuando proceda, del comité de riesgos. Los factores que deberán considerarse son, por ejemplo, los avances internos y externos, como el balance y el incremento de ingresos, el aumento de la complejidad del negocio de la entidad, el perfil de riesgo y la estructura operativa, la expansión geográfica, las fusiones y adquisiciones y la introducción de nuevos productos o líneas de negocio.

21. Adecuación de la remuneración al perfil de riesgo

1. Las prácticas y la política de remuneración de la entidad deberán ser coherentes con su perfil de riesgo y promover una gestión de riesgos sólida y eficaz.

Nota explicativa

La presente guía ofrece el marco *general* aplicable a la adecuación de la política de remuneración al perfil de riesgo de las entidades. Los aspectos *específicos* de la política de remuneración se tratan en la guía del CEBS sobre remuneración de diciembre de 2010. Se espera que las entidades cumplan ambas guías.

2. La política global de remuneración de una entidad deberá ser acorde con sus valores, estrategia de negocio, tolerancia/apetito al riesgo e intereses a largo plazo. No deberá fomentar la asunción de riesgos excesivos. La remuneración variable garantizada o las indemnizaciones por despido que recompensan el fracaso no son coherentes con una buena gestión de riesgos ni con el principio de remuneración basada en el desempeño y, por norma general, deberán estar prohibidas.

3. En el caso del personal cuyas actividades profesionales tienen un impacto sustancial en el perfil de riesgo de una entidad (por ejemplo, miembros del órgano de dirección, alta dirección, profesionales que asumen riesgos en las unidades de negocio, personal encargado del control interno y cualquier empleado cuya remuneración total lo sitúe en el mismo tramo de remuneración que la alta dirección y los profesionales que asumen riesgos), la política de remuneración deberá establecer procedimientos específicos para garantizar que su remuneración sea acorde con una gestión de riesgos sólida y eficaz.

4. El personal de las funciones de control deberá ser debidamente retribuido de acuerdo con sus objetivos y desempeño y no con relación al desempeño de las unidades de negocio que controlan.

5. En los casos en los que la retribución está vinculada al desempeño, la remuneración deberá basarse en una combinación de desempeño individual y colectivo. Cuando se defina el desempeño individual, deberán considerarse otros factores distintos al rendimiento financiero. La medición del desempeño para la concesión de primas deberá incluir ajustes para todos los tipos de riesgo y el coste del capital y de liquidez.

6. Deberá existir una relación proporcional entre retribución básica y primas. Una prima significativa no deberá ser simplemente un pago inicial al contado, sino que deberá contener un componente flexible y diferido ajustado al riesgo. El horizonte temporal del pago de las primas deberá tener en cuenta los resultados de los riesgos subyacentes.

22. Marco de gestión de riesgos

1. El marco de gestión de riesgos de una entidad deberá incluir políticas, procedimientos, límites y controles que establezcan procesos eficaces, oportunos y constantes para la identificación, medición o evaluación, control, mitigación y comunicación de los riesgos que plantean sus actividades en las líneas de negocio y en todos los niveles de la entidad.

2. El marco de gestión de riesgos de una entidad deberá proporcionar orientaciones específicas sobre la implantación de sus estrategias. Deberá, cuando proceda, establecer y mantener límites internos coherentes con su tolerancia/apetito al riesgo y acordes con su buen funcionamiento, solidez financiera y objetivos estratégicos. El perfil de riesgo de la entidad (es decir, la suma de sus exposiciones a los riesgos reales y posibles) deberá mantenerse dentro de esos límites. El marco de gestión de riesgos deberá garantizar que el incumplimiento de esos límites se notifique de forma escalonada a los niveles adecuados y se aborde con un seguimiento adecuado.

3. Cuando se identifican y se miden los riesgos, una entidad deberá desarrollar herramientas prospectivas y retrospectivas para complementar la labor realizada en las exposiciones a riesgos actuales. Las herramientas deberán permitir la agregación de las exposiciones a riesgos de todas las líneas de negocio y deberán contribuir a la identificación de concentraciones de riesgos.

4. Las herramientas prospectivas (como el análisis de escenarios y las pruebas de resistencia) deberán identificar las posibles exposiciones a riesgos en una variedad de circunstancias adversas; las herramientas retrospectivas deberán contribuir a revisar el perfil de riesgo real frente a la tolerancia/apetito al riesgo de la entidad y su marco de gestión de riesgos, además de proporcionar información para efectuar ajustes.

Nota explicativa

La guía del CEBS sobre pruebas de resistencia puede consultarse en inglés en el sitio web de la EBA.

5. La responsabilidad de la evaluación de riesgos recae, en última instancia, exclusivamente en la entidad que, por consiguiente, deberá evaluar sus riesgos de forma crítica y no deberá confiar exclusivamente en las evaluaciones externas.

Nota explicativa

Por ejemplo, una entidad deberá validar los modelos de riesgo que adquiera y calibrarlos con sus circunstancias individuales para garantizar que se reflejan y se analizan los riesgos de manera completa y precisa. Las evaluaciones de riesgos externas (incluidas las calificaciones crediticias externas o los modelos de riesgos adquiridos externamente) pueden contribuir a disponer de una estimación más completa de los riesgos. Las entidades deberán ser conscientes del ámbito de aplicación de esas evaluaciones.

6. Las decisiones que determinan el nivel de riesgos asumidos no deberán basarse solo en información cuantitativa o en los resultados de los modelos, sino que también deberán tener en cuenta las limitaciones prácticas y conceptuales de métricas y modelos, y emplear un enfoque cualitativo (incluidas opiniones expertas y análisis críticos). Las tendencias y datos del entorno macroeconómico pertinente deberán tratarse de forma explícita para identificar su posible impacto en las exposiciones y carteras. Esas evaluaciones deberán integrarse formalmente en las decisiones importantes sobre riesgos.

Nota explicativa

Una entidad deberá considerar que los resultados de las evaluaciones cuantitativas prospectivas y de los ejercicios de pruebas de resistencia dependen, en gran medida, de las limitaciones y supuestos de los modelos (incluida la gravedad y la duración de la perturbación y los riesgos subyacentes). Por ejemplo, los modelos que muestran una rentabilidad muy alta sobre el capital económico podrían ser el resultado de un fallo de los modelos (por ejemplo, la exclusión de algunos riesgos pertinentes) en lugar de ser la consecuencia de una buena estrategia o ejecución por parte de la entidad.

7. Deberán establecerse mecanismos de transferencia de información periódica y transparente para que el órgano de dirección y todas las unidades pertinentes de la entidad reciban informes de manera oportuna, precisa, concisa, comprensible y significativa, y para que puedan intercambiar información pertinente sobre la identificación, medición o evaluación y control de los riesgos. El marco de transferencia de información deberá estar bien definido, estar documentado y ser aprobado por el órgano de dirección.

8. Si se ha establecido un comité de riesgos, deberá recibir periódicamente informes formales y comunicaciones informales, cuando proceda, de la función de control de riesgos y del director responsable del control de riesgos.

Nota explicativa

La comunicación eficaz de la información sobre riesgos es crucial para todo el proceso de gestión de riesgos, facilita los procesos de revisión y de toma de decisiones y contribuye a evitar decisiones que podrían aumentar los riesgos involuntariamente. La comunicación eficaz de los riesgos implica una consideración y una comunicación internas eficaces de la estrategia de riesgos y de los datos de riesgos pertinentes (por ejemplo, exposiciones a riesgos e indicadores clave de riesgos) tanto horizontalmente en toda la entidad como entre los diferentes niveles de la cadena de dirección.

23. Nuevos productos

1. Una entidad contará con una política de aprobación de nuevos productos bien documentada, aprobada por el órgano de dirección, que aborde el desarrollo de nuevos mercados, productos y servicios, así como cambios significativos a los ya existentes.

2. La política de aprobación de nuevos productos de una entidad deberá tratar todos los aspectos que deben tenerse en cuenta antes de decidir entrar en nuevos mercados, negociar nuevos productos, lanzar un nuevo servicio o cambiar de forma significativa productos o servicios ya existentes. Esta política deberá incluir también la definición de «nuevo producto/mercado/negocio» que se utilizará en la organización y las funciones internas que participarán en el proceso de toma de decisiones.

3. La política de aprobación de nuevos productos deberá establecer las cuestiones principales que deben abordarse antes de tomar una decisión. Dichas cuestiones deberán incluir el cumplimiento normativo, los modelos de precios, los efectos en el perfil de riesgo, la adecuación del capital y la rentabilidad, la disponibilidad de recursos adecuados de front office (operadores), back office (personal administrativo) y middle office (gestión de riesgos, sistemas de TI, etc.), así como las herramientas y los conocimientos especializados adecuados para comprender y controlar los riesgos asociados. La decisión de lanzar una nueva actividad deberá indicar claramente la unidad de negocio y las personas que se responsabilizarán de ella. No deberá llevarse a cabo una nueva actividad hasta que estén disponibles los recursos adecuados para comprender y gestionar sus riesgos asociados.

4. La función de control de riesgos deberá participar en la aprobación de nuevos productos o de cambios significativos en los productos existentes. Su aportación deberá incluir una evaluación completa y objetiva de los riesgos derivados de las nuevas actividades de acuerdo con una variedad de escenarios, una evaluación de posibles deficiencias en los marcos de control interno y de gestión de riesgos de la entidad, así como una evaluación de la capacidad de la entidad para gestionar los nuevos riesgos de manera eficaz. La función de control de riesgos deberá tener una perspectiva general clara de la implantación progresiva de los nuevos productos (o de los cambios significativos en los productos existentes) en todas las líneas de negocio y carteras, así como autoridad para exigir que los cambios en los productos existentes pasen por el proceso formal de la política de aprobación de nuevos productos.

D. Control interno

24. Marco del control interno

1. Una entidad desarrollará y mantendrá un marco de control interno sólido y completo, incluidas funciones de control independientes específicas con la debida autoridad para cumplir su misión.

2. El marco de control interno de una entidad deberá garantizar operaciones eficientes y eficaces, un control adecuado de los riesgos, una conducta empresarial prudente, la fiabilidad de la información financiera y no financiera comunicada interna y externamente, así como el cumplimiento de las leyes, normativas, requisitos de los supervisores y decisiones y normas internas de la entidad. El marco de control interno deberá abarcar toda la organización, incluidas las actividades de todas las unidades de negocio, apoyo y control. El marco de control interno deberá ser apropiado para el negocio de la entidad y deberá incluir procedimientos administrativos y contables sólidos.

3. Al elaborar su marco de control interno, una entidad deberá garantizar que existe un proceso de toma de decisiones claro, transparente y documentado y una distribución clara de autoridad y de responsabilidades para garantizar el cumplimiento de las decisiones y normas internas. Con vistas a implantar un marco de control interno sólido en todas las áreas de la entidad, las unidades de negocio y de apoyo deberán ser responsables, en primera instancia, del establecimiento y mantenimiento de políticas y procedimientos de control interno adecuados.

4. Un marco de control interno adecuado también exige la verificación por parte de funciones de control independientes de que se cumplen esas políticas y procedimientos. Entre las funciones de control deberán incluirse una función de control de riesgos, una función de cumplimiento y una función de auditoría interna.

5. Las funciones de control deberán establecerse en un nivel jerárquico adecuado y deberán rendir cuentas directamente al órgano de dirección. Deberán ser independientes de las unidades de negocio y de apoyo que vigilan y controlan, y deberán ser organizativamente independientes unas de otras (puesto que llevan a

cabo funciones diferentes). Sin embargo, en entidades menos complejas o de menor tamaño, las tareas de las funciones de control de riesgos y de cumplimiento pueden combinarse. Las funciones de control del grupo deberán vigilar las funciones de control de las filiales.

6. Para que la función de control sea considerada independiente, deben cumplirse las condiciones siguientes:

a. su personal no realiza tareas que se incluyen en el ámbito de aplicación de las actividades que la función de control se propone vigilar y controlar;

b. la función de control está organizativamente separada de las actividades que le han asignado vigilar y controlar;

c. el jefe de la función de control está subordinado a una persona que no es responsable de gestionar las actividades que la función de control vigila y controla. El jefe de la función de control deberá rendir cuentas, por lo general, directamente al órgano de dirección y a los comités pertinentes, y deberá asistir periódicamente a sus reuniones; y

d. la remuneración del personal de la función de control no deberá estar vinculada al desempeño de las actividades que la función de control vigila y controla, ni ser susceptible de otro modo de comprometer su objetividad.

7. Las funciones de control deberán contar con un número adecuado de empleados (tanto en la empresa matriz como en las filiales de los grupos). El personal deberá estar cualificado en todo momento y deberá recibir la formación debida. También deberán disponer de sistemas de datos y de apoyos adecuados, así como de acceso a la información interna y externa necesaria para cumplir sus responsabilidades.

8. Las funciones de control deberán presentar periódicamente al órgano de dirección informes formales sobre las deficiencias importantes identificadas. Estos informes deberán incluir un seguimiento sobre los resultados de los anteriores y, para cada nueva deficiencia importante identificada, los riesgos pertinentes asociados, una evaluación del impacto y recomendaciones. El órgano de dirección deberá actuar con respecto a los resultados obtenidos por las funciones de control de manera oportuna y eficaz, además de exigir las medidas correctoras adecuadas.

25. La Función de Control de Riesgos (FCR)

1. Una entidad establecerá una función de control de riesgos completa e independiente.

2. La FCR garantizará que cada riesgo clave al que se enfrenta la entidad es identificado y debidamente gestionado por las unidades correspondientes de la entidad y se asegurará de que el órgano de dirección reciba una perspectiva holística de todos los riesgos relevantes. La FCR deberá facilitar información independiente relevante, análisis y opiniones expertas sobre las exposiciones a riesgos, así como

asesoramiento sobre propuestas y decisiones de riesgos tomadas por el órgano de dirección y por las unidades de negocio o de apoyo con respecto a si son coherentes con la tolerancia/apetito al riesgo de la entidad. La FCR puede recomendar mejoras del marco de gestión de riesgos y opciones para corregir el incumplimiento de las políticas, procedimientos y límites en materia de riesgos.

3. La FCR deberá ser un componente de la organización central de la entidad y deberá estar estructurada de modo que pueda implantar las políticas de riesgos y controlar el marco de gestión de riesgos. Las entidades de gran tamaño, complejas y sofisticadas pueden considerar la posibilidad de crear FCR especializadas para cada línea de negocio importante. Sin embargo, deberá existir en la entidad una FCR central (incluida, cuando proceda, una FCR del grupo en la empresa matriz) para ofrecer una perspectiva holística de todos los riesgos.

4. La FCR deberá ser independiente de las unidades de negocio y de apoyo cuyos riesgos controla pero no deberá estar aislada de esas unidades. Deberá poseer los conocimientos suficientes sobre procedimientos y técnicas de gestión de riesgos y sobre mercados y productos. La interacción entre las funciones operativas y la FCR deberá facilitar el objetivo de que todo el personal de la entidad asuma la responsabilidad de gestionar los riesgos.

26. El papel de la Función de Control de Riesgos (FCR)

1. La FCR deberá participar activamente en una etapa inicial en la elaboración de la estrategia de riesgo de la entidad y en todas las decisiones importantes sobre gestión de riesgos. La FCR desempeñará un papel fundamental para asegurar que la entidad tenga implantados procesos de gestión eficaz de los riesgos.

Papel de la FCR en la estrategia y en las decisiones

2. La FCR deberá facilitar al órgano de dirección toda la información relacionada con los riesgos relevantes (por ejemplo, mediante un análisis técnico sobre la exposición a riesgos) para permitirle que establezca el nivel de tolerancia/apetito al riesgo de la entidad.

3. La FCR deberá evaluar también la estrategia de riesgos, incluidas las metas propuestas por las unidades de negocio, y asesorar al órgano de dirección antes de que tome una decisión. Las metas, que incluyen calificaciones crediticias y tasas de rentabilidad sobre recursos propios, deberán ser plausibles y coherentes.

4. La FCR deberá compartir con todas las unidades de negocio la responsabilidad de implantar la estrategia y política de riesgos de la entidad. Las unidades de negocio deberán implantar los límites de riesgos pertinentes, mientras que la FCR deberá hacerse cargo de velar por que los límites sean acordes con la tolerancia/apetito al riesgo global de la entidad y de vigilar constantemente que la entidad no asuma riesgos excesivos.

5. La participación de la FCR en los procesos de toma de decisiones deberá garantizar que se tienen en cuenta de forma adecuada las consideraciones

concernientes a los riesgos. Sin embargo, la responsabilidad de las decisiones tomadas deberá recaer en las unidades de negocio y de apoyo y, en última instancia, en el órgano de dirección.

Papel de la FCR en las transacciones con partes vinculadas

6. La FCR deberá garantizar que se revisen las transacciones con partes vinculadas, y que se identifiquen y evalúen debidamente los riesgos, reales o posibles, que plantean para la entidad.

Papel de la FCR en la complejidad de la estructura jurídica

7. La FCR deberá procurar identificar los riesgos importantes derivados de la complejidad de la estructura jurídica de la entidad.

Nota explicativa

Los riesgos pueden consistir en una falta de transparencia, riesgos operacionales causados por estructuras de financiación complejas e interconectadas, exposiciones a riesgos intragrupo, garantías inmovilizadas y riesgo de contraparte.

Papel de la FCR en los cambios importantes

8. La FCR deberá evaluar cómo podrían afectar los riesgos importantes a la capacidad de la entidad o del grupo para gestionar su perfil de riesgo y para movilizar financiación y capital en circunstancias normales y adversas.

9. Antes de que se tomen decisiones sobre cambios importantes o transacciones excepcionales, la FCR deberá participar en la evaluación del impacto de tales cambios y transacciones excepcionales sobre el riesgo global del grupo y de la entidad.

Nota explicativa

Entre los cambios importantes o las transacciones excepcionales se podrían incluir fusiones y adquisiciones, creación o venta de filiales o entidades con cometido especial, nuevos productos, cambios en sistemas, el marco de gestión de riesgos o procedimientos y cambios en la organización de la entidad.

Véase la guía publicada conjuntamente por los tres anteriores comités supervisores financieros europeos de nivel tres (CEBS, CESR y CEIOPS) de 2008 sobre la evaluación prudencial de las adquisiciones y de los incrementos de participación en el sector financiero (*Guidelines for the prudential assessment of acquisitions and increases in holdings in the financial sector*), que está publicada, en inglés, en el sitio web de la EBA. La FCR deberá participar activamente en una etapa inicial en la identificación de los riesgos relevantes (incluidas las posibles consecuencias de realizar insuficientes procesos de diligencia debida en los que no se logran identificar los riesgos posteriores a la fusión) relacionados con cambios de la estructura del grupo (incluidas fusiones y adquisiciones), y deberá comunicar sus conclusiones directamente al órgano de dirección.

Papel de la FCR en la medición y evaluación

10. La FCR deberá garantizar que las mediciones y evaluaciones de riesgos internos de la entidad abarcan una variedad adecuada de escenarios y se basan en supuestos lo suficientemente conservadores con respecto a dependencias y correlaciones. Aquí deberán incluirse perspectivas cualitativas de toda la empresa (incluidas opiniones expertas) sobre las relaciones entre los riesgos y la rentabilidad de la entidad y el marco exterior en el que opera.

Papel de la FCR en la supervisión

11. La FCR deberá garantizar que todos los riesgos identificados puedan ser supervisados de forma eficaz por las unidades de negocio. La FCR deberá vigilar periódicamente el perfil de riesgo real de la entidad y examinarlo cuidadosamente en comparación con los objetivos estratégicos de la entidad, y su tolerancia/apetito al riesgo, para permitir que el órgano de dirección tome decisiones, en el ejercicio de su función de dirección, y para permitir que las decisiones sean cuestionadas por el órgano de dirección, en el ejercicio de su función de supervisión.

12. La FCR deberá analizar tendencias y reconocer los riesgos nuevos o emergentes derivados del cambio de circunstancias y condiciones. También deberá revisar periódicamente los resultados reales de los riesgos frente a las estimaciones previas (es decir, pruebas retrospectivas) para evaluar y mejorar la precisión y eficacia del proceso de gestión de riesgos.

13. La FCR del grupo deberá vigilar los riesgos asumidos por las filiales. Las incoherencias con la estrategia aprobada del grupo deberán comunicarse al órgano de dirección correspondiente.

Papel de la FCR en las exposiciones a riesgos no aprobadas

14. La FCR deberá participar debidamente en los cambios de la estrategia de la entidad, su tolerancia/apetito al riesgo aprobados y los límites.

15. La FCR deberá evaluar de forma independiente los incumplimientos o infracciones (incluyendo su causa y un análisis jurídico y económico del coste real de eliminar, reducir o cubrir la exposición al riesgo frente al posible coste de mantenerla). La FCR deberá informar, según proceda, a las unidades de negocio afectadas y recomendar posibles soluciones.

Nota explicativa

El incumplimiento o la infracción de las estrategias, la tolerancia/apetito al riesgo o los límites pueden ser consecuencia de nuevas transacciones, de cambios en las circunstancias del mercado o de una evolución en la estrategia, políticas o procedimientos de la entidad, cuando no se cambian los límites o la tolerancia/apetito al riesgo en consecuencia.

16. La FCR deberá desempeñar un papel fundamental para garantizar que se toma una decisión sobre su recomendación en el nivel pertinente, que se cumple en las unidades de negocio correspondientes y que se comunica debidamente al órgano de dirección, al comité de riesgos y a la unidad de negocio o de apoyo.

17. Una entidad deberá adoptar las medidas adecuadas frente a conductas fraudulentas internas o externas y frente a infracciones disciplinarias (por ejemplo, la vulneración de procedimientos internos o la contravención de límites).

Nota explicativa

En el ámbito de aplicación de la presente guía, «fraude» abarca el fraude interno y externo tal como se definen en la parte 5 del anexo X de la Directiva 2006/48/CE. Por lo tanto, este término incluye, tanto las pérdidas derivadas de algún tipo de actuación encaminada a cometer fraude, apropiarse de bienes indebidamente o soslayar regulaciones, leyes o políticas empresariales, excluidos los eventos de diversidad/discriminación, en las que se encuentra implicada, al menos, una parte interna de la empresa (fraude interno), como las pérdidas derivadas de algún tipo de actuación encaminada a cometer fraude, apropiarse de bienes indebidamente o soslayar la legislación, por parte de un tercero (fraude externo).

27. El Director responsable del control de riesgos

1. Las entidades nombrarán a una persona, el director responsable del control de riesgos (en adelante, «responsable de riesgos»), que será el responsable exclusivo de la FCR y de la supervisión del marco de gestión de riesgos de la entidad en toda la organización.

2. El responsable de riesgos (o cargo equivalente) será responsable de facilitar información completa y comprensible sobre los riesgos para permitir al órgano de dirección comprender el perfil global de riesgo de la entidad. Lo mismo se aplica al responsable de riesgos de una empresa matriz con respecto a todo el grupo.

3. El responsable de riesgos deberá tener suficientes conocimientos especializados, experiencia práctica, independencia y antigüedad para cuestionar las decisiones que afectan a la exposición al riesgo de una entidad. Las entidades deberán considerar otorgar derecho de veto al responsable de riesgos. El responsable de riesgos y el órgano de dirección o los comités pertinentes deberán ser capaces de comunicarse directamente entre ellos sobre cuestiones que afectan a riesgos clave, incluidos los avances que pueden ser incoherentes con la tolerancia/apetito al riesgo y la estrategia de la entidad.

4. Si una entidad desea otorgar al responsable de riesgos el derecho de vetar decisiones, en sus políticas de riesgos se deberán establecer las circunstancias en las que el responsable de riesgos podrá ejercerlo y en qué tipo de propuestas (por ejemplo, una decisión sobre un crédito o una inversión o el establecimiento de un límite). En las políticas se deberán describir los procedimientos de notificación escalonada o de recurso y la forma en la que se informará al órgano de dirección.

5. Cuando las características de la entidad, en particular su tamaño, organización y la naturaleza de sus actividades, no justifiquen confiar tal responsabilidad a una persona nombrada especialmente para ello, la función puede ser desempeñada por otra persona de rango superior de la entidad, siempre que no haya conflicto de intereses.

6. La entidad deberá disponer de procesos documentados en vigor para asignar el puesto de responsable de riesgos y para destituirlo de sus responsabilidades. Si el responsable de riesgos es sustituido, deberá hacerse con la aprobación previa del órgano de dirección en el ejercicio de su función de supervisión. En general, la destitución o el nombramiento del responsable de riesgos deberá comunicarse y deberán indicarse las razones a la autoridad de supervisión.

28. La Función de cumplimiento

1. Una entidad establecerá una función de cumplimiento para gestionar su riesgo de cumplimiento.

2. Una entidad aprobará y aplicará una política de cumplimiento que deberá ser comunicada a todo el personal.

Nota explicativa

El riesgo de cumplimiento (definido como el riesgo actual o futuro para las ganancias y el capital derivado de infracciones o incumplimiento de leyes, reglas, normativas, acuerdos, prácticas prescritas o pautas éticas) puede dar lugar a sanciones, daños o anulación de contratos y puede perjudicar la reputación de la entidad.

3. Una entidad deberá establecer una función de cumplimiento eficaz y permanente y nombrar a una persona responsable de esta función en toda la entidad y el grupo (el responsable de cumplimiento o el jefe de cumplimiento). En las entidades más pequeñas y menos complejas esta función puede combinarse con funciones de apoyo (por ejemplo, recursos humanos, área jurídica, etc.) o de control de riesgos o puede recibir el apoyo de dichas funciones.

4. La función de cumplimiento deberá velar por que se respete la política de cumplimiento y deberá informar al órgano de dirección y, según proceda, a la FCR sobre la gestión del riesgo de cumplimiento de la entidad. El órgano de dirección y la FCR deberán tener en cuenta las conclusiones de la función de cumplimiento en el proceso de toma de decisiones.

5. La función de cumplimiento deberá asesorar al órgano de dirección sobre leyes, reglas, normativas y pautas que la entidad debe cumplir y evaluar el impacto de los cambios en el entorno jurídico o normativo sobre las actividades de la entidad.

6. La función de cumplimiento deberá verificar también que los nuevos productos y los nuevos procedimientos cumplen con el entorno jurídico actual y con los cambios conocidos próximos a entrar en vigor de la legislación, la normativa y los requisitos de los supervisores.

Nota explicativa

Debe prestarse especial atención cuando la entidad presta determinados servicios o establece estructuras en nombre de clientes (por ejemplo, en calidad de intermediario en la constitución de una asociación o empresa, en los servicios fiduciarios o en el desarrollo de transacciones financieras de estructura compleja para los clientes) que pueden dar lugar a particulares dificultades en materia de gobierno interno y consideraciones prudenciales.

29. La Función de auditoría interna

1. La función de auditoría interna («FAI») evaluará si la calidad del marco de control interno de la entidad es eficaz y eficiente.

2. La FAI deberá tener acceso ilimitado a la información y los documentos pertinentes en todas las unidades operativas y de control.

3. La FAI deberá evaluar el cumplimiento de todas las actividades y unidades de la entidad (incluidas la función de control de riesgos y la función de cumplimiento) con sus políticas y procedimientos. Por lo tanto, la FAI no deberá combinarse con ninguna otra función. La FAI deberá evaluar también si las políticas y procedimientos existentes siguen siendo adecuadas y cumplen con los requisitos legales y normativos.

4. La FAI deberá verificar, en particular, la integridad de los procesos para

garantizar la fiabilidad de los métodos y técnicas de la entidad, los supuestos y fuentes de información utilizados en sus modelos internos (por ejemplo, la modelización de los riesgos y las mediciones contables). También deberá evaluar la calidad y el uso de la identificación de riesgos cualitativos y las herramientas de evaluación. Sin embargo, la FAI no deberá participar directamente en el diseño o selección de modelos u otras herramientas de gestión de riesgos.

5. El órgano de dirección deberá animar a los auditores internos a adherirse a las normas profesionales nacionales e internacionales. La labor de auditoría interna deberá efectuarse de conformidad con un plan de auditoría y programas de auditoría detallados que sigan un método «basado en riesgos». El plan de auditoría deberá ser aprobado por el comité de auditoría, por el órgano de dirección, o por ambos.

Nota explicativa

Un ejemplo de las normas profesionales a las que se hace referencia en el presente documento son las pautas establecidas por el Instituto de Auditores Internos.

6. La FAI deberá comunicar directamente al órgano de dirección y a su comité de auditoría (si procede) sus conclusiones y sugerencias sobre mejoras importantes de los controles internos. Todas las recomendaciones de auditoría deberán ser objeto de un procedimiento de seguimiento por parte de los niveles de dirección respectivos para asegurar y comunicar su resolución.

E. Sistemas de información y continuidad del negocio

30. Sistema de información y comunicación

1. Las entidades dispondrán de sistemas de información y comunicación eficaces y fiables que abarquen todas las actividades significativas.

Nota explicativa

La toma de decisiones por parte de la dirección podría verse perjudicada por información no fiable o confusa facilitada por sistemas mal diseñados y controlados. Por lo tanto, un componente fundamental para las actividades de una entidad es el establecimiento y mantenimiento de sistemas de información y comunicación que abarquen toda la variedad de sus actividades. Esta información suele ser facilitada mediante medios electrónicos y no electrónicos.

Las entidades deberán ser especialmente conscientes tanto de los requisitos organizativos y de control interno relativos al procesamiento de información en formato electrónico como de la necesidad de contar con una adecuada traza de seguimiento de la auditoría. Lo mismo se aplica a los sistemas de TI externalizados a un proveedor de servicios de TI.

2. Los sistemas de información, incluidos los que almacenan y emplean datos en formato electrónico, deberán ser seguros, estar supervisados de manera independiente y estar respaldados por procedimientos adecuados frente a contingencias. Una entidad deberá cumplir con las normas de TI generalmente aceptadas cuando implanta sistemas de TI.

31. Gestión de la continuidad del negocio

1. Las entidades deberán establecer una sólida gestión de la continuidad del negocio para garantizar su capacidad de operar constantemente y limitar las pérdidas en caso de incidencias graves en el negocio.

Nota explicativa

El negocio de una entidad se basa en varios recursos fundamentales (por ejemplo, sistemas de TI, sistemas de comunicación, edificios). La finalidad de la gestión de la continuidad del negocio es reducir las consecuencias operativas, financieras, jurídicas, de reputación y cualesquiera otras de importancia derivadas de un desastre o de incidencias prolongadas en esos recursos y la consecuente perturbación en los procedimientos de negocio ordinarios de la entidad. Otras medidas de gestión de riesgos podrían consistir en reducir la probabilidad de tales incidencias o en transferir su impacto financiero (por ejemplo, mediante seguros) a terceros.

2. Para establecer una buena gestión de la continuidad del negocio, una entidad deberá analizar definitivamente su exposición a incidencias graves en el negocio y evaluar (de forma cualitativa y cuantitativa) su posible impacto, mediante el uso de datos internos o externos y análisis de escenarios. Este análisis deberá abarcar todas las unidades de negocio y de apoyo, así como la función de control de riesgos, y deberá tener en cuenta su interdependencia. Asimismo, deberá participar activamente una función de continuidad del negocio independiente específica, la función de control de riesgos o la función de gestión del riesgo operacional. Los resultados del análisis deberán contribuir a definir las prioridades y objetivos de recuperación de la entidad.

Nota explicativa

Con respecto a la función de gestión del riesgo operacional, véase también el apartado 3 de la parte 3 del anexo X de la Directiva 2006/48/CE que exige una función independiente de ese tipo para las entidades que utilizan métodos de medición avanzada; las tareas de esta función se describen en la guía sobre validación, en los apartados 615-620 (publicada en 2006), disponible en inglés en el sitio web de la EBA.

3. Con base en el análisis anterior, una entidad deberá contar con:

a. planes de contingencias y de continuidad del negocio para garantizar que la

entidad responde debidamente a situaciones de emergencia y es capaz de mantener sus actividades empresariales más importantes en caso de perturbación en sus procedimientos de negocio ordinarios.

b. planes de recuperación para sus recursos fundamentales con el fin de permitirle volver a los procedimientos de negocio ordinarios en un plazo de tiempo adecuado. Cualquier riesgo residual procedente de posibles incidencias en el negocio deberá ser coherente con la tolerancia/apetito al riesgo de la entidad.

4. Los planes de contingencias, continuidad del negocio y recuperación deberán estar documentados e implantarse cuidadosamente. La documentación deberá estar a disposición de las unidades de negocio y de apoyo, y de la función de control de riesgos. Además, deberá ser almacenada en sistemas que estén físicamente separados y sean fáciles de acceder en caso de contingencias. Deberá proporcionarse la formación adecuada. Los planes deberán comprobarse y actualizarse periódicamente. Las dificultades o fallos producidos en las pruebas deberán ser documentados y analizados, y los planes deberán ser revisados en consecuencia.

F. Transparencia

32. Potenciación (empowerment)

1. Las estrategias y políticas se comunicarán a todo el personal pertinente en toda la entidad.

2. El personal de una entidad deberá comprender y cumplir las políticas y procedimientos correspondientes a sus obligaciones y responsabilidades.

3. En consecuencia, el órgano de dirección deberá informar al personal pertinente y mantenerlo al tanto de las estrategias y políticas de la entidad de manera clara y coherente, al menos en la medida necesaria para cumplir sus obligaciones particulares. Esta comunicación puede realizarse mediante guías escritas, manuales u otros medios.

33. Transparencia del gobierno interno

1. El marco de gobierno interno de las entidades será transparente. Una entidad presentará su situación actual y sus perspectivas de futuro de manera clara, equilibrada, precisa y oportuna.

Nota explicativa

El objetivo de la transparencia en el área de gobierno interno consiste en ofrecer a todas las partes interesadas en la entidad relevantes (incluidos accionistas, empleados, clientes y el público en general) la información clave necesaria para permitirles valorar la eficacia del órgano de dirección en la gestión de la entidad.

Según el artículo 72 de la Directiva 2006/48/CE y el artículo 2 de la Directiva 2006/49/CE, las empresas matrices de la UE y las entidades controladas por una sociedad financiera de cartera matriz de la UE deberán publicar información completa y significativa que describa su gobierno interno con carácter consolidado. Una buena práctica consiste en que toda entidad publique, de manera proporcional, información sobre su gobierno interno con carácter individual.

2. Una entidad deberá divulgar públicamente al menos lo siguiente:

a. sus estructuras y políticas de gobierno corporativo, incluidos sus objetivos, estructura organizativa, procedimientos de gobierno interno, estructura y organización de su órgano de dirección, incluida la asistencia, y la estructura de incentivos y de remuneración de la entidad;

b. la naturaleza, magnitud, finalidad y fondo económico de las transacciones con sus filiales y partes vinculadas, si tienen un impacto significativo en la entidad;

c. la forma de establecer la estrategia de negocio y de riesgos (incluida la participación del órgano de dirección), así como los factores de riesgo previsibles;

d. sus comisiones y comités constituidos, sus mandatos y composiciones;

e. su marco de control interno y la forma en la que se organizan sus funciones de control, las tareas principales que llevan a cabo, la manera en que el órgano de dirección vigila su desempeño y los cambios importantes previstos en esas funciones; e

f. información importante sobre sus resultados financieros y operativos.

3. La información sobre la situación actual de la entidad deberá cumplir con los requisitos legales de divulgación. La información deberá ser clara, precisa, pertinente, oportuna y accesible.

4. En los casos en los que garantizar un alto grado de precisión retrasaría la publicación oportuna de información, la entidad deberá tomar una decisión para lograr el equilibrio adecuado entre presentar información de manera oportuna y presentar información precisa, teniendo en cuenta la obligación de ofrecer una imagen verdadera y fiel de su situación y explicar de forma satisfactoria cualquier retraso. Esta explicación no deberá utilizarse para retrasar los requisitos de información habitual.

Título III

Disposiciones finales e implantación

34. Derogación

Con la adopción y publicación de esta guía sobre gobierno interno, quedan derogadas las siguientes guías: la sección 2.1, titulada «Directrices sobre gobierno interno» (*Guidelines on Internal Governance*), de la guía del CEBS sobre la aplicación del proceso de revisión supervisora (*Guidelines on the Application of the Supervisory Review Process under Pillar 2*), de 25 de enero de 2006; los principios de alto nivel para las políticas de remuneración (*High-Level principles for Remuneration Policies*), de 20 de abril de 2009, y los principios de alto nivel para la gestión de riesgos (*High level principles for risk management*), de 16 de febrero de 2010.

35. Fecha de aplicación

Las autoridades competentes implantarán la guía sobre gobierno interno incorporándola a sus procedimientos de supervisión el 31 de marzo de 2012 a más tardar. Después de esa fecha, las autoridades competentes deberán garantizar que las entidades cumplan con la guía de forma satisfactoria.