Documento consultivo de Directrices sobre gobierno interno

Autoridad Bancaria Europea (EBA)

Índice

Introducción

En octubre de 2016 la EBA publicó Directrices (GL) consultivas sobre gobierno interno, para actualizar las GL 44 actuales, introduciendo aspectos adicionales que pretenden fomentar una cultura de riesgo sólida

Introducción

Durante los últimos años, el gobierno interno ha recibido una mayor atención por parte de diversos organismos internacionales. Su principal esfuerzo en este sentido ha sido para corregir las deficiencias en las prácticas de gobierno interno, dado que estas prácticas inadecuadas, aunque no hayan sido un desencadenante de la crisis financiera, estaban relacionadas con la misma y eran cuestionables.

En este sentido, en septiembre de 2011 la EBA publicó Directrices sobre gobierno interno (GL 44) con el objetivo de mejorar y consolidar expectativas supervisoras, así como fortalecer el marco de gobierno interno. No obstante, para tratar el potencial efecto adverso de mecanismos de gobierno corporativo inadecuados en lo relativo a gestión de riesgos y para considerar los nuevos requerimientos introducidos por la CRD IV, la EBA pretende actualizar las GL 44.

- En este contexto, la EBA publicó en octubre 2016 un **Documento Consultivo de Directrices sobre gobierno interno**, por el cual se actualizarán las GL 44. Este documento consultivo pone mayor énfasis en las tareas y responsabilidades del órgano de dirección en su función supervisora de control de riesgo. En concreto, este documento trata los siguientes aspectos:
  - El **rol del órgano de dirección** en relación a gobierno interno.
  - La **política de gobierno interno**, **cultura de riesgo** y **conducta de negocio**.
  - El **marco de control interno**.
  - Los principios de **proporcionalidad** y **transparencia** que serán aplicados en el marco de gobierno interno.

Este documento incluye un **análisis de los requerimientos** de las Directrices consultivas sobre gobierno interno.

Índice

Resumen ejecutivo

Estas GL sobre gobierno interno incluyen disposiciones sobre los siguientes aspectos: i) órgano de dirección; ii) política de gobierno interno, cultura de riesgo y conducta de negocio; iii) marco de control interno; y iv) principios aplicados al marco de gobierno interno

Resumen ejecutivo

Ámbito de aplicación

- Estas directrices están dirigidas a **entidades de crédito** y **empresas de servicios de inversión**, según los define el CRR.

Contexto regulatorio

- **Directrices sobre gobierno interno** (GL 44), publicadas por la EBA en septiembre de 2011.

Próximos pasos

- Los comentarios a este documento deberán enviarse antes del **28 de enero de 2017**.
- Se espera que las CA implementen estas GL antes de **mediados de 2017**.

Contenido principal

Órgano de dirección

- Deberes y responsabilidades del órgano de dirección, función supervisora y función de gestión, presidente del órgano de dirección, marco organizativo y estructura, y comités.

Política de gobierno interno, cultura de riesgo y conducta de negocio

- Política de gobierno interna (incluida política a nivel de grupo), cultura de riesgo, valores corporativos y código de conducta, conflictos de interés, procedimientos de alerta temprana, reporting de incumplimientos, y política de externalización.

Marco de control interno

- Marco de control interno, funciones de control interno (función de gestión del riesgo, función de cumplimiento y función de auditoría interna), marco de gestión de riesgo, nuevos productos y cambios significativos, y gestión de la continuidad de negocio.

Principios aplicados al marco de gobierno interno

- Principios de proporcionalidad y transparencia aplicados por las entidades al definir su marco de gobierno interno.

Índice

GL consultivas sobre gobierno interno

Rol del órgano de dirección en relación a gobierno interno

Estas GL ofrecen orientaciones sobre los deberes y responsabilidades del órgano de dirección, los cuales deberían definirse distinguiendo entre la función supervisora…

Órgano de dirección (1/4)

Deberes y responsabilidades

- El órgano de dirección debe ser el **máximo responsable** de la entidad y definir, supervisar y ser responsable de la implementación de los mecanismos de gobierno. Sus responsabilidades deberían definirse distinguiendo entre su **función de gestión**, compuesta por los miembros ejecutivos; y la **función supervisora**, formada por los miembros del órgano de dirección no ejecutivos (a continuación se detallan las funciones de cada una).
- Los deberes y responsabilidades del órgano de dirección deberían describirse en un **documento escrito y aprobado por el órgano de dirección en su función supervisora**. En concreto, deberían incluir el establecimiento, aprobación y control de la implementación de, entre otros:
  - La **estrategia global** y la **estrategia de riesgo global** (ej. apetito al riesgo).
  - Un **marco de control interno** adecuado, efectivo e independiente.
  - Los importes, tipos y distribución del **capital interno** y del **capital regulatorio**.
  - Una **política de remuneración** en línea con la CRD IV y con las GL de la EBA sobre remuneración.
  - Mecanismos que garanticen una eficaz **evaluación de la idoneidad** de sus miembros.
  - Una **cultura de riesgo**, **valores** y **cultura corporativa** adecuados.
- El órgano de dirección debe supervisar el proceso de **divulgación y comunicación** de modo que sus miembros estén informados sobre la actividad global y sobre la situación financiera y de riesgo de la entidad. Además, debería monitorizar y **revisar periódicamente** cualquier debilidad identificada en la implementación de procesos, estrategias, etc. en relación a las responsabilidades mencionadas anteriormente.

Función supervisora

- El órgano de dirección en su función supervisora debería, entre otros aspectos:
  - Monitorizar y **cuestionar la estrategia** de la entidad de forma constructiva, **supervisar al órgano de dirección en su función de gestión** y garantizar la **integridad** de la información financiera y de reporting, así como del marco de control interno, lo que incluye una gestión del riesgo sólida y efectiva.
  - Contar con miembros adecuados que no realicen ninguna **función ejecutiva**.
  - Supervisar la implementación de la **cultura de riesgo** y de los **objetivos estratégicos**.
  - Garantizar que los responsables de las funciones de control interno actúan de manera **independiente**.
  - Evaluar periódicamente la eficiencia del **marco de gobierno interno** de la entidad.
  - Implementar políticas para identificar, gestionar y mitigar **conflictos de interés** actuales o potenciales.

GL consultivas sobre gobierno interno

Rol del órgano de dirección en relación a gobierno interno

…y la función de gestión. Además, las GL también ofrecen orientaciones sobre el rol del presidente del órgano de dirección como principal responsable de su funcionamiento efectivo

Órgano de dirección (2/4)

Función de gestión

- El órgano de dirección en su función de gestión debería:
  - **Participar activamente en el negocio** de una entidad y **tomar decisiones** formadas y fundamentadas.
  - Ser el responsable de la **implementación de estrategias** establecidas por el órgano de dirección y discutir periódicamente la implementación y adecuación de dichas estrategias.
  - **Cuestionar** de forma constructiva y **revisar** de manera crítica las propuestas, explicaciones e información recibida para la toma de decisiones.
  - **Reportar e informar** periódicamente y sin demora al **órgano de dirección en su función supervisora** sobre los elementos relevantes para la evaluación de los riesgos que afecten o que puedan afectar a la entidad (ej. decisiones materiales sobre actividades de negocio y riesgos asumidos, evaluación del entorno económico y de negocio de la entidad, etc.).

Presidente del órgano de dirección

- El presidente debería liderar el órgano de dirección y ser el **responsable de su funcionamiento efectivo** así como fomentar y **promover debates abiertos y críticos** para garantizar que se pueden manifestar opiniones divergentes.
- Como principio general, el presidente debería ser un miembro **independiente o no ejecutivo**. El presidente en su función supervisora y el CEO de un entidad no deben ser la misma persona, a menos que esté justificado por la entidad y autorizado por la CA.
- El presidente debería, entre otras funciones:
  - Fijar la **agenda de reuniones** y garantizar que los problemas estratégicos se discuten con prioridad.
  - Garantizar una **clara asignación de responsabilidades** entre miembros ejecutivos y no ejecutivos del órgano de dirección, así como la existencia de un flujo eficiente de información entre los mismos.

GL consultivas sobre gobierno interno

Rol del órgano de dirección en relación a gobierno interno

Además, las GL también incluyen disposiciones relacionadas con los comités del órgano de dirección, en concreto relativas a su establecimiento, composición, procesos y tipos. Las GL también especifican las funciones de los comités de riesgos y auditoría

Órgano de dirección (3/4)

Comités

- Todas las entidades que son **sistémicas**[1] deben establecer un **comité de riesgos y un comité de nombramientos** para asesorar al órgano de dirección en su función supervisora[2]. Además, cualquier entidad puede establecer **otros comités especializados** (ej. de ética, de conducta, de cumplimiento, etc.).
- En relación a la **composición de los comités**:
  - Los miembros del comité de riesgos y de nombramientos no deberían realizar **funciones ejecutivas**.
  - El comité de riesgos debería incluir una **mayoría** de miembros **independientes** y todos sus miembros deberían contar con **adecuados conocimientos, capacidades** y **experiencia** individuales/colectivos.
  - Los comités especializados deberían estar compuestos por **suficientes miembros independientes**.
  - Cada comité debería tener un presidente que sea **miembro independiente** del órgano de dirección en su función supervisora.
- En cuanto a **procesos**, los comités deberían tener acceso a toda la **información relevante** y **revisar** regularmente el contenido, formato y frecuencia de la información sobre riesgos que se les reporta.

Comité de riesgos

- Entre otras funciones, el comité debería:
  - Asesorar y apoyar al órgano de dirección en su función supervisora respecto a la monitorización del **apetito al riesgo** global de la entidad y la **estrategia**, considerando todos los tipos de riesgo.
  - Asistir al órgano de dirección en su función supervisora respecto a la implementación de la **estrategia de riesgo** de la entidad y de sus correspondientes **límites** fijados.
  - Supervisar la implementación de las estrategias para la **gestión de capital y liquidez** y para todos los riesgos relevantes restantes de una institución (ej. mercado, crédito, operacional, IT, etc.).
  - Proporcionar **recomendaciones** sobre los ajustes necesarios en la estrategia de riesgo.

Comité de auditoria

- Entre otras funciones, el comité debería:
  - Monitorizar la efectividad del **control de calidad interno** de la entidad, de los **sistemas de gestión del riesgo**, y cuando corresponda, de su **auditoría interna**.
  - Supervisar el establecimiento de **políticas contables** por parte de la entidad
  - Monitorizar el **proceso de reporting financiero** y dar recomendaciones para garantizar su integridad.

(1) Entidades de importancia sistémica global o 'G-SII', otras entidades de importancia sistémica u 'O-SII', y otras entidades identificadas como tal por las CA.
(2) Las entidades no sistémicas podrían establecer un único comité con ambas funciones.

GL consultivas sobre gobierno interno

Rol del órgano de dirección en relación a gobierno interno

De acuerdo a estas GL, el órgano de dirección debería garantizar un marco organizativo y una estructura adecuados y transparentes. En este sentido, debería evitar el establecimiento de estructuras complejas y se deberían considerar la aplicación de medidas de mitigación

Órgano de dirección (4/4)

Marco organizativo y estructura

- En relación al **marco organizativo**, el órgano de dirección debería:
  - Garantizar una **estructura operativa y organizativa adecuada y transparente**, respecto a la cual debería tener una descripción escrita, clara y detallada.
  - Garantizar el **mayor nivel de independencia posible de las funciones de control interno**, considerando los recursos financieros y humanos necesarios para realizar sus funciones de manera efectiva. La asignación de responsabilidades debería ser coherente, vinculante, y estar documentada.
  - Ser plenamente consciente de la **estructura del órgano de dirección**, de la división de tareas y responsabilidades dentro del órgano de dirección, de sus comités y dentro de la propia entidad.
  - Evaluar los **elementos** de la estructura organizativa y operativa y el **impacto de los cambios** a la estructura de grupos sobre la solidez del marco organizativo.
- Con respecto a la **estructura**, el órgano de dirección debería:
  - Conocer y entender plenamente la estructura organizativa y operativa (**know-your-structure**) y garantizar que está en línea con el negocio, estrategia de riesgo y apetito al riesgo.
  - Ser responsable de la **aprobación de estrategias y políticas sólidas**.
- Las entidades deberían **evitar el establecimiento de estructuras complejas y potencialmente no transparentes**, considerando varios aspectos (ej. en qué medida la jurisdicción en la que se aplica una estructura cumple con los estándares internacionales de transparencia fiscal, blanqueo de capitales, etc.; en qué medida esa estructura cumple con un propósito económico y legal; etc.). El órgano de dirección debería garantizar la adopción de **medidas de mitigación adecuadas** para evitar los riesgos derivados de actividades en dichas estructuras, lo que incluye que:
  - La entidad cuente con **políticas y procedimientos adecuados** y procesos documentados para la consideración, cumplimiento, aprobación y gestión del riesgo de estas actividades.
  - La información derivada de estas actividades y riesgos sea **accesible** para la entidad, auditores internos y externos, y sea reportada al órgano de dirección en su función supervisora y a la CA.
  - La entidad **revise periódicamente** la necesidad de mantener estas estructuras.

GL consultivas sobre gobierno interno

Política de gobierno interno, cultura del riesgo y conducta de negocio

Las GL establecen que las entidades deberían contar con una política de gobierno interno con líneas de responsabilidad bien definidas y transparentes, así como con una cultura del riesgo integrada a nivel grupo basada en los riesgos a los que están expuestas

Política de gobierno interno, cultura del riesgo y conducta de negocio (1/3)

Política de gobierno interno[1]

- El órgano de dirección debería **definir, adoptar y mantener una política de gobierno** para implementar una estructura organizativa y operativa clara, con líneas de responsabilidad bien definidas y transparentes.
- El **órgano de dirección en su función de gestión** es responsable de la implementación de la política, mientras que el órgano de dirección en su **función de supervisión** es responsable de supervisar la implementación, de monitorizar los efectos de la política y de revisar su diseño y efectividad.
  - Esta política debería ser **clara y transparente**, y estar **bien documentada**. Las funciones de control interno deberían **proporcionar input efectivo** en línea con sus responsabilidades, considerando cómo la política afecta al cumplimiento por parte de la entidad de las normas legales y de las políticas internas.
  - Cualquier **modificación** sobre esta política debería ser **aprobada por el órgano de dirección** y comunicada a la CA.

Política de gobierno para grupos

- A nivel consolidado o sub-consolidado, la entidad de consolidación y las CA deberían asegurar que todas las entidades dentro del perímetro de consolidación prudencial, incluyendo también las filiales no sujetas a la CRD IV, implementan una **política de gobierno interno a nivel grupo** que describe todos los mecanismos y procesos de gobierno.

Cultura del riesgo

- Una cultura del riesgo sólida debería ser un **elemento clave de la gestión de riesgos**, y debería permitir a la entidad tomar decisiones sólidas y fundadas. Así, la entidad debería desarrollar una **cultura del riesgo integrada a nivel grupo**, que deberá basarse, entre otros aspectos, en los riesgos a los que está expuesta.
- Los **empleados** deberían ser **conscientes de sus responsabilidades** relacionadas con gestión del riesgo. Así, las unidades de negocio bajo supervisión del órgano de dirección, son **responsables de gestionar los riesgo en el día a día**, considerando la capacidad/apetito al riesgo de la entidad.
- La cultura del riesgo debería mostrar las siguientes características: i) '**tone from the top'** (el órgano de dirección es el responsable de fijar y comunicar los valores/expectativas de la entidad), ii) **responsabilidad**, de manera que todos los empleados relevantes a todos los niveles deben conocer los valores de la entidad, y el apetito y capacidad al riesgo, iii) **comunicación efectiva y challenge**, y iv) **incentivos** para alinear el comportamiento de asunción de riesgos al perfil de riesgo y los intereses a largo plazo.

(1) En el anexo se incluye un listado de los aspectos que deben considerarse a la hora de desarrollar y documentar la política de gobierno interno escrita.

GL consultivas sobre gobierno interno

Política de gobierno interno, cultura del riesgo y conducta de negocio

El órgano de dirección debería desarrollar altos estándares éticos y profesionales. Además, la entidad debería contar con una política para identificar, gestionar y mitigar conflictos de interés actuales y potenciales de sus empleados

Política de gobierno interno, cultura del riesgo y conducta de negocio (2/3)

Valores y Código de Conducta

- El **órgano de dirección** debería desarrollar, adoptar, seguir y promover **altos estándares éticos y profesionales**, considerando las necesidades y características específicas de la entidad, con el objetivo de reducir los riesgos a los que la entidad está expuesta. El órgano de dirección debería contar con **políticas claras y documentadas** sobre cómo se deben cumplir estos estándares. En concreto, estas políticas deberían:
  - Recordar que las actividades deben realizarse cumpliendo las **leyes y los valores corporativos**.
  - Promover la **conciencia del riesgo** a través de una sólida cultura del riesgo.
  - Definir **comportamientos inaceptables** (ej. conducta indebida, fraude, blanqueo de capitales, etc.).
  - Aclarar que se espera de los empleados que se comporten con **honestidad** e **integridad**.
  - Asegurar que los empleados son conscientes de las **medidas disciplinarias internas y externas**.

Conflictos de interés

- El **órgano de dirección** debería establecer y supervisar la implementación y mantenimiento de políticas **efectivas** para identificar, gestionar y mitigar conflictos de interés actuales y potenciales de los empleados. Los **conflictos de interés materiales** a nivel órgano de dirección, individuales y colectivos, deberían ser documentados de manera adecuada, comunicados al órgano de dirección, y ser gestionados por éste.
- Una **política escrita** debidamente aprobada debería identificar las relaciones, servicios, actividades u operaciones de una entidad respecto a las cuales podrían surgir conflictos de interés[1] (ej. relaciones entre entidades y miembros del órgano de dirección), y definir cómo se deberían gestionar estos conflictos.
- La política de conflictos de interés debería definir los **procedimientos y medidas** (ej. adecuada segregación de responsabilidades, barreras de información, etc.) que deberían adoptarse para prevenir, identificar conflictos de interés actuales o potenciales, evaluar su materialidad, decidir sobre medidas de mitigación, y para que los empleados los comuniquen al órgano de dirección[2].
- Si se identifica cualquier conflicto de interés, la entidad debería emitir una **declaración** sobre cómo este conflicto ha sido mitigado o remediado de manera satisfactoria.

(1) También debe cubrir el riesgo de conflicto de interés específico del órgano de dirección en su función de supervisión.
(2) La entidad de consolidación debería considerar los intereses de todas sus filiales.

GL consultivas sobre gobierno interno

Política de gobierno interno, cultura del riesgo y conducta de negocio

Las GL proporcionan también orientaciones en lo relativo a los procedimientos de alerta interna, a los mecanismos para el reporting de incumplimientos a las CA, y a la política de externalización de las entidades

Política de gobierno interno, cultura del riesgo y conducta de negocio (3/3)

Procedimientos de alerta interna

- Se debería contar con procedimientos para que los **empleados reporten incumplimientos** actuales o potenciales de los **requerimientos regulatorios**[1], que deberían reportarse **fuera de las líneas de reporting normales** (ej. función de cumplimiento o de auditoría, o procedimiento de 'whistleblowing').
- Los procedimientos de alerta deberían estar **disponibles para todos los empleados**.
- Cuando sea apropiado, la información proporcionada por el empleado que reporta el incidente debería ponerse a disposición del **órgano de dirección y de otras funciones responsables** (de manera anónima).
- Las entidades deberían asegurar la **protección de datos personales** de la persona que reporta el incidente y de la persona que presuntamente es responsable del incumplimiento.
- Los **procedimientos de alerta interna** deberían estar documentados, y entre otros aspectos deberían:
  - Proporcionar reglas claras para garantizar la confidencialidad en todos los casos.
  - Garantizar que los incumplimientos actuales y potenciales son evaluados.
  - Garantizar que se proporciona confirmación de recibo al empleado que reporta el incumplimiento.
  - Permitir el seguimiento del resultado de los incumplimientos, y un apropiado record-keeping.

Reporting de incumplimientos a las CA

- Las CA deberían establecer **mecanismos efectivos** que **incentiven a los empleados a reportar a las CA** los incumplimientos de los requerimientos regulatorios actuales o potenciales. Dichos mecanismos también pueden incentivar a los empleados a, en primer lugar, usar los procedimientos de alerta interna.

Política de externalización

- El órgano de dirección debería **aprobar y revisar y actualizar regularmente la política de externalización**, considerando el **impacto de la externalización** sobre el negocio de la entidad y los riesgos a los que está expuesta (ej. operacional, reputacional, riesgo de concentración, etc.). La política debería incluir los mecanismos de reporting y monitorización que deberían implementarse.
- La política debería establecer que los mecanismos de externalización **no deben obstaculizar la supervisión**, y no deben contravenir ninguna restricción supervisora sobre los servicios y actividades.
- La entidad se mantiene como **responsable** de todos los servicios externalizados.

(1) No debería ser necesario que el empleado tenga prueba de ello, sino un nivel inicial de certidumbre suficiente para iniciar una investigación.
(2) Procedimiento para reportar incumplimientos de manera anónima.

GL consultivas sobre gobierno interno

Marco de control interno

Estas GL ofrecen orientaciones sobre cómo deberían organizarse las funciones de control interno, sobre los recursos de las funciones de control interno, la externalización, y sobre cómo se implementa el marco de control interno

Marco de control interno (1/5)

Control interno

- Las entidades deberían desarrollar y mantener un marco de control interno sólido y global que abarque toda la organización, incluyendo las **responsabilidades y tareas del órgano de dirección** así como las **actividades de todas las líneas de negocio y de las unidades internas**, incluidas las funciones de control interno, actividades externalizadas y los canales de distribución.
- También debería incluir las **funciones de gestión del riesgo, de cumplimiento y de auditoría interna**. En este sentido, las funciones de gestión del riesgo y de cumplimiento podrían combinarse, pero no así la función de auditoría.

Responsables de las funciones de control interno

- Un **miembro del órgano de dirección en su función de gestión** puede ser responsable de una función de control interno siempre que no ostente otros cargos que comprometan las actividades de control interno de otros miembros, así como la independencia de la función de control interno.
- Cuando un **responsable no forme parte del órgano de dirección en su función de gestión**, el cargo debería establecerse a un nivel jerárquico adecuado e independiente de las áreas bajo su control.

Recursos

- Las funciones de control interno deberían contar con **suficientes recursos** y con **acceso a la formación necesaria** para llevar a cabo sus tareas. Así, deberían contar con un **número adecuado de empleados cualificados** (a nivel matriz y filial).

Externalización

- Las **tareas operativas** de las funciones de control interno **pueden externalizarse** de acuerdo con el principio de proporcionalidad, tanto en la entidad consolidada como en cualquier otra entidad dentro o fuera del grupo, con el **consentimiento de los órganos de dirección** de las entidades involucradas.

Implementación

- Las entidades deberían establecer, mantener y actualizar periódicamente **políticas de control interno adecuadas**, que deberían ser aprobadas por el órgano de dirección.
- Las entidades deberían **informar** sobre dichas políticas, mecanismos y procedimientos a **todos los empleados**, así como sobre cualquier cambio material que se haya producido al respecto.
- Las funciones de control interno deberían verificar que las políticas, mecanismos y procedimientos son **implementados correctamente**.

GL consultivas sobre gobierno interno

Marco de control interno

El marco de control interno debería incluir una función de gestión del riesgo, establecida para implementar las políticas de riesgo y el marco de gestión del riesgo de la entidad…

Marco de control interno (2/5)

Control interno: funciones

- Las funciones de control interno deberían incluir una **función de gestión del riesgo**, una **función de cumplimiento** y una **función de auditoría interna**.

Función de gestión del riesgo (RMF)

- Las entidades deberían establecer una RMF con **suficiente autoridad y recursos** para implementar las políticas de riesgo y el marco de gestión del riesgo.
- Consecuentemente, debería ser una **función central de la entidad**[1], y debería tener **acceso directo** al órgano de dirección en su función de supervisión y a los comités, a todas las líneas de negocio y otras unidades internas con potencial para generar riesgos, así como a las filiales relevantes.
- Los empleados de la RMF deberían tener **conocimientos, habilidades y experiencia suficiente** sobre técnicas de gestión del riesgo, mercados y productos; y deberían tener acceso a formación periódica.
- La RMF debería ser **independiente de las líneas y unidades de negocio cuyos riesgos controla**, aunque no se le debería prohibir interactuar con ellas.
- La RMF debería proporcionar **información relevante e independiente**, análisis y juicio experto sobre exposiciones de riesgo, así como asesoramiento sobre las propuestas y decisiones de riesgo planteadas por las líneas de negocio o unidades internas, o por el órgano de dirección, en relación a si dichas propuestas son consistentes con el apetito al riesgo y la estrategia de la entidad.
- La RMF podría recomendar **mejoras** sobre el marco de gestión del riesgo, así como **medidas correctivas** para solventar incumplimientos en las políticas, procedimientos y límites de riesgos.
- En relación al **rol de la RMF**, ésta debe involucrarse activamente en, entre otros, la estrategia de riesgo; en la identificación, medición, evaluación, gestión, monitorización y reporting de los riesgos; etc.
- El **responsable de la RMF** debería proporcionar información global y comprensible sobre riesgos. En el caso de que no esté justificado nombrar a una persona dedicada solo a este cargo, puede realizarse **conjuntamente con la función de cumplimiento**.

(1) Las entidades sistémicas podrían considerar establecer una RMF para cada línea de negocio material. No obstante, debería existir una RMF central, incluyendo una RMF en la entidad consolidada a nivel grupo.

GL consultivas sobre gobierno interno

Marco de control interno

…así como una función de cumplimiento para gestionar el riesgo de cumplimiento de la entidad, y una función de auditoría interna que debería evaluar, entre otros aspectos, la calidad del marco de control interno

Marco de control interno (3/5)

Función de cumplimiento

- La entidad debería establecer una función de cumplimento permanente y efectiva para gestionar su **riesgo de cumplimiento**, y nombrar una persona responsable de esta función en la entidad (‘Compliance Officer’ o responsable de cumplimiento).
- El **responsable de la función de cumplimiento** debería ser capaz de **reportar directamente**, cuando sea necesario y por iniciativa propia, al **órgano de dirección en su función de supervisión**.
- La función de cumplimiento debería ser **independiente** de las líneas de negocio y de las unidades internas bajo su control, y debería tener **suficiente autoridad y recursos**.
- Los empleados de la función de cumplimiento deberían tener **conocimientos, habilidades y experiencia suficiente** sobre cumplimiento, y deberían tener acceso a formación periódica.
- Además, debería **asesorar al órgano de dirección** sobre las leyes, normas y estándares que las entidades tienen que cumplir, así como evaluar el posible impacto de los cambios en el marco regulatorio.

Función de auditoría interna (IAF)

- La entidad debería establecer una **función de auditoría interna independiente**, considerando el criterio de proporcionalidad, y nombrar una persona responsable de esta función en toda la entidad. En este sentido, la IAF debería:
  - Ser **independiente** y tener suficiente autoridad y recursos.
  - Realizar una **revisión independiente** sobre el cumplimiento de todas las actividades y unidades de la entidad.
  - Evaluar la **calidad del marco de control interno** considerando, entre otros, la idoneidad de dicho marco, si las políticas y procedimientos son adecuados y cumplen con los requerimientos legales, con el apetito al riesgo y la estrategia, etc.
- El **responsable de la IAF** debería ser capaz de **reportar directamente** y por iniciativa propia al **órgano de dirección en su función de supervisión** la no-implementación de las medidas correctivas propuestas.
- La función de auditoría interna debería realizarse de acuerdo con el **plan de auditoría**, el cual debería elaborarse **al menos anualmente** conforme a los objetivos de control anuales y en línea con las directrices del órgano de dirección en su función de supervisión.

GL consultivas sobre gobierno interno

Marco de control interno

Las entidades deberían contar con un marco de gestión del riesgo para todas las líneas de negocio y funciones de control interno. Las GL establecen directrices sobre cómo debería establecerse dicho marco

Marco de control interno (4/5)

Control interno: gestión del riesgo

- Como parte del marco de control interno, la entidad debería contar con un **marco de gestión del riesgo integral** aplicable a todas las líneas de negocio y funciones de control interno. Este marco debería:
  - Comprender los **riesgos en balance** y **fuera de balance**, así como los riesgos **actuales y futuros** a los que la entidad podría estar expuesta (i.e. riesgos financieros y no financieros).
  - Incluir las **políticas**, **procedimientos**, **límites al riesgo** y **controles** que garanticen una adecuada y oportuna identificación, medición, evaluación, monitorización, gestión y reporting de los riesgos a nivel de línea de negocio, entidad y grupo.
  - Evaluar los riesgos a través de evaluaciones bottom up y top down.
  - Proporcionar **directrices específicas** sobre la **implementación de las estrategias** que deberían establecer y mantener límites internos en línea con el apetito al riesgo, capital y objetivos estratégicos.
  - Garantizar que en el caso de que se produzca un **incumplimiento de los límites de riesgo**, existe un **proceso para solucionarlo** con un seguimiento adecuado.
  - Estar sujeto a una **revisión interna independiente**, y ser re-evaluado de manera periódica frente al apetito al riesgo, considerando la información de la RMF, y cuando sea adecuado, del comité de riesgos.
  - Desarrollar metodologías apropiadas para la identificación y medición de los riesgos, incluyendo tanto herramientas **forward-looking** (ej. análisis de escenarios y stress test) como **backward-looking** (que consisten en evaluar el perfil de riesgo real y compararlo con el apetito al riesgo).
- La **responsabilidad última** de la evaluación del riesgo corresponde a la **entidad**, de tal manera que no debe depender exclusivamente de evaluaciones externas (ej. calificaciones de agencias de rating).
- Las decisiones que determinan el nivel de riesgos asumidos no solo deben basarse en **información cuantitativa**, sino también emplear un **enfoque cualitativo** (lo que incluye juicio experto y análisis crítico).
- Se deben establecer **mecanismos de reporting** de tal manera que se les proporcione al **órgano de dirección**, a su **comité de riesgos** y a **todas las unidades relevantes** información de manera oportuna, fiable, concisa, entendible y coherente. El marco de reporting debe estar bien definido, documentado, y aprobado de manera debida por el órgano de dirección.

(1) Lo que incluye crédito, mercado, liquidez, concentración, operacional, IT, reputacional, legal, de conducta, de cumplimiento, y estratégico.

GL consultivas sobre gobierno interno

Marco de control interno

Además, las entidades deberían contar con una política de aprobación de nuevos productos (NPAP) para tratar el desarrollo de nuevos mercados, productos y servicios, así como con una sólida gestión de continuidad del negocio (Business Continuity Management)

Marco de control interno (5/5)

Control interno: nuevos productos

- Se debería contar con una **política de aprobación de nuevos productos (NPAP)** documentada, aprobada por el órgano de dirección, que trate el desarrollo de nuevos mercados, productos y servicios, y los cambios significativos sobre los actuales; así como con **políticas para cambios materiales** sobre los procesos (ej. nuevos mecanismos de externalización) y los sistemas (ej. cambios sobre los procesos IT)[1].
- En este sentido, la **NPAP** debería:
  - **Cubrir todas las consideraciones** que deban tenerse en cuenta antes de decidir entrar en nuevos mercados, productos, o servicios, y antes de realizar cambios significativos sobre los existentes.
  - Incluir la **definición de 'cambios significativos'** sobre productos/mercados/negocio que deba utilizarse en la organización, así como las funciones internas que están involucradas en la toma de decisiones.
  - Exponer los **principales problemas** que deben tratarse antes de tomar una decisión (ej. cumplimiento de regulación, contabilidad, modelos de pricing, impactos en el perfil de riesgo, etc.). La decisión de lanzar una nueva actividad debería establecer la unidad del negocio y las personas responsables.
- La **RMF** debería estar también involucrada en la **aprobación de nuevos productos** o **cambios significativos** a los ya existentes y debería tener una visión general del **roll-out de nuevos productos**.

Business Continuity Management

- Las entidades deberían establecer una sólida gestión de continuidad del negocio para reducir las **consecuencias operacionales, financieras, legales, reputacionales**, etc. derivadas de un fallo o una interrupción extendida sobre recursos críticos (ej. sistemas IT).
- Deberían analizar su **exposición a graves interrupciones del negocio** y evaluar (cuantitativamente y cualitativamente) su impacto potencial, usando datos externos e internos y un análisis de escenarios.
- Sobre la base de dicho análisis, las entidades deberían poner en marcha **planes de continuidad del negocio y de contingencia**, así como **planes de recuperación**, que deberían estar documentados.
- Además, una función de continuidad del negocio de operativo (la '**Función de Gestión del Riesgo Operacional**'), parte de la RMF, debería estar involucrada activamente para aquellas entidades que usan AMA.

(1) La función de cumplimiento, en colaboración con la RMF, debería ser responsable de garantizar el cumplimiento interno de estas políticas.

GL consultivas sobre gobierno interno

Principios aplicados al marco de gobierno interno

La EBA especifica que las entidades deberían aplicar los principios de proporcionalidad y transparencia para establecer mecanismos de gobierno interno alineados con el perfil de riesgo y el modelo de negocio de la entidad y para que los empleados estén informados

Principios aplicados al marco de gobierno interno

Proporcionalidad

- Las entidades deberían considerar su **tamaño**, **organización interna** y la **naturaleza** y **complejidad** de sus actividades a la hora de desarrollar e implementar mecanismos de gobierno interno.
- Entre otros, las **entidades** y **CAs deberían considerar** la presencia geográfica de la entidad y el volumen de las operaciones en cada jurisdicción, la forma legal, si la entidad es parte de un grupo, etc.
- De acuerdo con el principio de proporcionalidad:
  - Las entidades sistémicas y las entidades y grupos más complejos deberían tener **mecanismos de gobierno más sofisticados**.
  - Las entidades y grupos menores y no complejos pueden implementar **mecanismos de gobierno más sencillos**.

Transparencia

- El órgano de dirección debería **informar a los empleados** sobre las estrategias y políticas de la entidad de manera clara y consistente, al menos al nivel necesario para llevar a cabo sus tareas particulares (ej. mediante políticas escritas, manuales, etc.).
- Cuando la matriz esté requerida por la CA a publicar anualmente una descripción de su estructura legal y de gobierno y de la estructura organizativa del grupo de entidades, la información debería incluir a **todas las entidades** que se encuentran **dentro de la estructura de grupo** y debería presentarse por país.
- La **publicación debería incluir**, entre otros:
  - Un resumen de la **organización interna** de la entidad y de la estructura de grupo, incluyendo las principales líneas de reporting y las responsabilidades.
  - Cualquier **cambio material**, en comparación con la publicación anterior.
  - **Nuevas estructuras** legales, de gobierno u organizativas.
  - Una visión general de la **externalización material** de actividades, procesos y sistemas.
  - Información sobre la estructura, organización, responsabilidades y miembros del **órgano de dirección**.
  - Una lista de los **comités del órgano de dirección** en su función supervisora y su composición.

Índice

Próximos pasos

Los comentarios a este documento consultivo deberán ser enviados antes del 28 de enero de 2017. Se espera que las CA implementen estas GL a mediados de 2017

Próximos pasos

- Los comentarios a este documento consultivo deberán ser enviados antes del **28 de enero de 2017.**
- Se espera que las CA implementen estas GL para **mediados de 2017**. Las directrices existentes sobre gobierno interno (GL 44) serán derogadas cuando las GL revisadas sean aplicables.

Índice

Anexo
Política de gobierno interno

Las entidades deberían considerar cierto aspectos (ej. estructura de accionistas, estructura de grupo, etc.) a la hora de desarrollar y documentar la política de gobierno interno

Política de gobierno interno (documento escrito)

1. Estructura de accionistas

2. Estructura de grupo, si aplica (estructura legal y funcional)

3. Composición y funcionamiento del órgano de dirección (con impacto sobre el grupo, si aplica)

a) criterios de selección
b) número, duración del mandato, rotación, edad
c) miembros independientes del órgano de dirección
d) miembros ejecutivos del órgano de dirección
e) miembros no ejecutivos del órgano de dirección
f) división interna de tareas, si aplica

4. Estructura de gobierno y organigrama (con impacto sobre el grupo, si aplica)

a) comités especializados
  i. composición
  ii. funcionamiento

b) comité de gestión, si existe
  i. composición
  ii. funcionamiento (regulación interna)

5. Titulares de funciones clave

a) Responsable de la función de gestión de riesgo
b) Responsable de la función de cumplimiento
c) Responsable de la función de auditoría
d) Chief Financial Officer (CFO)
e) Otros titulares de funciones clave

6. Marco de control interno

a) descripción de cada función (recursos, categoría, autoridad)
b) descripción del marco de gestión de riesgo incluyendo estrategia de riesgo
c) debilidades identificadas para cada función de control interna y medidas tomadas
d) recomendaciones de la función de auditoría y medidas tomadas

7. Estructura organizativa (con impacto sobre grupo, si aplica)

a) estructura operacional, líneas de negocio y asignación de competencias y responsabilidades
b) externalización
c) rango de productos y servicios
d) ámbito geográfico del negocio
e) prestación libre de servicios
f) sucursales
g) filiales, joint ventures, ...
h) uso de centros off-shore

8. Código de conducta y comportamiento (con impacto sobre grupo, si aplica)

a) objetivos estratégicos y valores empresariales
b) códigos internos y reglamentos, política de prevención
c) política de conflictos de interés
d) whistleblowing

9. Status de la política interna con fecha

a) desarrollo
b) última modificación
c) última evaluación
d) aprobación por el órgano de dirección