

## **MECANISMOS DE CONTROL INTERNO DE LA ENTIDAD, INCLUYENDO LOS PROCEDIMIENTOS ADMINISTRATIVOS Y CONTABLES**

El gobierno interno de las entidades de crédito 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 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.

Las **Directrices sobre gobierno interno EBA/GL/2017/11 de la Autoridad Bancaria Europea** (EBA por sus siglas en inglés) publicadas en su versión en inglés el 26 de septiembre de 2017 (versión en español el 21 de marzo de 2018) y de aplicación desde el 30 de junio de 2018 (en adelante, las "Directrices sobre gobierno interno"), conscientes de que la confianza en la fiabilidad del sistema bancario es crucial para su buen funcionamiento, señalan que **los procedimientos de gobierno interno eficaces son fundamentales para que las entidades, individualmente, y el sistema bancario funcionen correctamente**.

El **gobierno interno**, según se define en las Directrices sobre 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**.

El Grupo Kutxabank cuenta con un Marco de Control Interno dirigido a garantizar, entre otros aspectos, i) una operativa eficaz y eficiente, ii) una gestión prudente del negocio, iii) una identificación, medición y mitigación del negocio, iv) una identificación, medición y mitigación adecuada de los riesgos, v) la fiabilidad de la información financiera y no financiera publicada interna y externamente, vi) unos procedimientos contables sólidos y vii) el cumplimiento de la normativa de aplicación, de los requisitos en materia de supervisión y de las políticas, procesos, normas y decisiones internas del Grupo Kutxabank.

Al elaborar su marco de control interno, el Grupo Kutxabank ha tratado de 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.

A la hora de identificar dentro de su organización las unidades responsables del control y gestión de los riesgos, el Grupo Kutxabank ha adoptado el **modelo de líneas de defensa descrito en el capítulo introductorio de las Directrices sobre gobierno interno** antes referidas.

Según dicho modelo cabe distinguir tres líneas de defensa:

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. En consecuencia, la primera línea de defensa en el Grupo Kutxabank se sitúa al nivel de las líneas de negocio del Grupo, donde se asumen y gestionan los riesgos de manera directa. Para ello, las líneas de negocio deben contar con los mecanismos adecuados para la identificación, análisis, medición, monitorización, seguimiento y reporting de los diferentes tipos de riesgo, para lo que deben disponer de áreas y/o recursos especializados en la gestión de los mismos.

Como **«segunda línea defensiva»**, señalan las Directrices de gobierno interno, 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.

En atención a lo anterior, la segunda línea de defensa del Grupo Kutxabank está formada por la Función de Gestión de Riesgos y la Función de Cumplimiento Normativo:

- La Función de Gestión de Riesgos debe asegurarse de que el Grupo cuenta con una sólida gobernanza del riesgo, y abordar la identificación, análisis, medición, monitorización, seguimiento y reporting del riesgo desde una perspectiva global, monitorizando la evolución del perfil global del riesgo del Grupo e informando sobre ello a los principales órganos directivos y de gobierno. Para ello revisará las medidas de gestión del riesgo implantadas por la primera línea de defensa, y se asegurará de que los mecanismos en vigor estén adecuadamente diseñados y de que sean efectivos.
- La Función de Cumplimiento Normativo por su parte supervisará el cumplimiento del marco regulatorio, la normativa interna y los códigos de conducta aplicables a la actividad bancaria, que puedan derivar en sanciones administrativas o daños reputacionales, proporcionando asesoramiento sobre el particular al Consejo de Administración y al personal clave. Asimismo, establecerá y/o impulsará políticas y procedimientos sobre sus

ámbitos de actuación, supervisará los controles y actividades de la primera línea de defensa e informará de los riesgos de incumplimiento a los órganos de gobierno y de dirección.

Cuando lo estimen necesario, ambas funciones podrán intervenir para solicitar la introducción de modificaciones en los sistemas de gestión de riesgos y control interno implantados en la primera línea de defensa.

La **tercera «línea defensiva»** contemplada por las Directrices de gobierno interno consiste en la función de auditoría interna, que se encarga de realizar una revisión independiente de las dos primeras «líneas defensivas». En el Grupo Kutxabank la tercera línea de defensa está formada por la Función de Auditoría Interna. La Función de Auditoría Interna llevará a cabo auditorías y revisiones sobre los mecanismos de identificación, análisis, medición, monitorización, seguimiento y reporting de los diferentes tipos de riesgos para asegurarse de que están implantados de forma sólida y efectiva y de que se aplican de manera consistente. Realizando sus tareas de forma independiente de las otras dos líneas de defensa.

**En el Grupo Kutxabank las Funciones de Control Interno** de una entidad de crédito definidas por las Directrices de Control Interno (Función de Gestión de Riesgos, Función de Cumplimiento Normativo y Función de Auditoría Interna) **han sido asignadas**, respectivamente, **a las siguientes áreas** (sin perjuicio de que dichas áreas puedan desempeñar otras responsabilidades no relacionadas con las Funciones de Control Interno):

- **Control Global del Riesgo;**
- **Cumplimiento Normativo y Control de Grupo;**
- **Auditoría Interna;**

El siguiente cuadro resume la estructura del Marco de Control Interno del Grupo Kutxabank:

MODELO DE LÍNEAS DE DEFENSA EN MATERIA DE GESTIÓN DEL RIESGO		
Líneas de defensa	Funciones (tal y como se definen en las Directrices de Gobierno Interno)	Áreas Kutxabank
1ª	Líneas de negocio	D.G. Corporativa Financiera y de Grupo D. G. Corporativa de Medios D.G. Negocio Minorista D.G. Negocio Mayorista D.G. Participadas

2ª	Función de Gestión de Riesgos* Función de Cumplimiento*	Control Global del Riesgo Cumplimiento Normativo y Control de Grupo
3ª	Función de Auditoría Interna*	Auditoría Interna

\*Funciones de Control Interno.

Adicionalmente, el Consejo de Administración de Kutxabank, SA, aprobó en su sesión de 30 de mayo de 2019, la Política de Gobierno Interno de Kutxabank que recoge, en un único documento, las políticas y los sistemas de gobierno interno del Grupo Bancario (tal y como se define a continuación), contando de esta forma con un documento matriz que enmarca y del que toman razón cuantas políticas y procedimientos se establezcan al respecto y que, en ocasiones, vienen expresamente referenciados en dicho documento. Dicha política es de aplicación al grupo de entidades que, dentro del Grupo Kutxabank, llevan a cabo actividades bancarias sin perjuicio del que el resto de entes del sector financiero del grupo prudencial apliquen políticas que sean coherentes y cumplan con las líneas generales de la mencionada política, considerando en todo caso el principio de proporcionalidad al que se refieren las Directrices de gobierno interno.

El control interno es un proceso dinámico, iterativo e integrado, llevado a cabo por el Consejo de Administración, la Dirección y el resto del personal de la organización, diseñado con el objeto de proporcionar un grado de aseguramiento razonable para la consecución de los objetivos relativos a las operaciones, a la información y al cumplimiento.

El control interno forma parte íntegra de la gestión de riesgos corporativos y sus cinco componentes básicos, que deben estar relacionados a través de un proceso integrado, son los siguientes: (i) entorno de control; (ii) evaluación de riesgos; (iii) actividades de control; (iv) información y comunicación; y (v) supervisión. Éstos deben estar coordinados y operar de forma conjunta para prevenir, detectar, compensar, mitigar o corregir errores, con impacto material, o fraudes en la información financiera.

El Sistema de Control Interno de la Información Financiera (en adelante, SCIIF) es una parte del control interno y se configura como el conjunto de procesos que el Consejo de Administración, la Comisión de Auditoría y Cumplimiento, la Alta Dirección y el personal involucrado de la Entidad llevan a cabo para proporcionar seguridad razonable respecto a la fiabilidad de la información financiera que se publica en los mercados.

En este contexto, los aspectos clave del sistema en Kutxabank son:

- ✓ Establecer las responsabilidades en el Banco con respecto a la información financiera.
- ✓ Identificar los riesgos críticos de error para que puedan ser gestionados.
- ✓ Proporcionar garantías al Consejo de Administración y la Alta Dirección con respecto a la fiabilidad de la información financiera contenida en las cuentas anuales.

La determinación de responsabilidades sobre el SCIIF y los procedimientos y criterios para

asegurar un correcto mecanismo de supervisión han sido difundidos a la organización mediante una Política de carácter interno, aprobada por el Consejo de Administración.

El Consejo de Administración tiene entre sus funciones el garantizar la integridad de los sistemas de información contable y financiero, incluidos el control financiero y operativo, y el cumplimiento de la legislación aplicable; supervisar el proceso de divulgación de información y las comunicaciones relativas al Banco; así como en materia de control y gestión de riesgos, establecer los principios y políticas que marquen las líneas generales de actuación de la Sociedad, y del Grupo, en materia de gestión de riesgos.

La Dirección Financiera, como primera línea de defensa, participa en el diseño e implementación de los sistemas de gestión y control de riesgos, en especial en lo que respecta al proceso de elaboración, presentación e integridad de la información financiera que se difunde a los mercados. La Dirección financiera y el resto de áreas y líneas de negocio de Kutxabank son responsables del diseño, implantación y funcionamiento del control interno de la información financiera bajo su responsabilidad. Asimismo, la Dirección Financiera es responsable junto con la Unidad CIF, CINF y CNE de la ejecución y actualización periódica del procedimiento de identificación y evaluación de áreas/procesos y riesgos materiales de la información financiera en el ámbito del SCIIF.

El Consejo de Administración tiene delegada la función de supervisión de los sistemas de control interno a la Comisión de Auditoría y Cumplimiento, la cual, encarga la ejecución de los trabajos de supervisión y evaluación del SCIIF a las funciones de apoyo de segunda y tercera línea de defensa que se ubican en el Departamento de Cumplimiento Normativo y Control de Grupo, en concreto a la Unidad de Control de la Información Financiera, Información No Financiera y Controles no Especializados (Unidad CIF, CINF y CNE,) y en Auditoría Interna.

La Unidad CIF, CINF y CNE del Departamento de Cumplimiento Normativo y Control de Grupo evalúa, dentro de sus actividades de supervisión del SCIIF:

- ✓ **El Diseño del SCIIF**, que contempla todo el proceso de Identificación de Riesgos y de Controles. Se identifican las Áreas materiales, los Procesos asociados y los Riesgos en cada uno de ellos. Posteriormente se verifica la existencia y suficiencia de controles para mitigar estos riesgos.

La Entidad dispone de un Proceso de identificación y evaluación de riesgos de la información financiera que incluye los de error o fraude. El proceso de identificación de los riesgos, cuyo impacto potencial en los estados financieros es significativo, se focaliza en la identificación de los procesos críticos de gestión afectos a la generación de información financiera y de las áreas o epígrafes de los estados financieros donde se materializan los referidos riesgos. En el análisis de procesos y áreas se están considerando tanto factores cuantitativos (saldo y granularidad) como cualitativos (grado de automatización de los

procesos, estandarización de las operaciones, nivel de complejidad contable, cambios con respecto al ejercicio precedente, debilidades de control identificadas, etc.). Este proceso de evaluación de riesgos cubre la totalidad de objetivos de la información financiera: existencia y ocurrencia, integridad, valoración, presentación, desglose y comparabilidad y derechos y obligaciones.

En lo relativo a las actividades y controles relacionados directamente con transacciones que puedan afectar de modo material a los estados financieros, la Entidad dispone de Procedimientos y Matrices de riesgos y controles de los procesos y áreas significativos, que afectan a la generación, elaboración y preparación de la información financiera.

La documentación descriptiva comentada anteriormente contempla:

- La descripción de las actividades relacionadas con el proceso desde su inicio, indicando las particularidades que puede contener un determinado producto u operativa.
- La identificación de los riesgos relevantes con impacto material en los estados financieros de la Entidad.
- La identificación de los controles y su descripción, así como su asociación con los riesgos identificados previamente.

Las actividades y controles se diseñan con el fin de garantizar el adecuado registro, valoración, presentación y desglose de las transacciones acaecidas.

- ✓ **El Funcionamiento del SCIIF en cuanto su ejecución**, mediante la monitorización de los controles y del proceso de certificación interna, implantado para garantizar la fiabilidad de la información financiera, certificando cada uno de los responsables de los controles la ejecución eficaz de los mismos en el período de referencia.
- ✓ **Las debilidades detectadas**, identificado un conjunto de incidencias o aspectos de mejora para los que se proponen los correspondientes Planes de Acción.

Por su parte, Auditoría Interna dispone de un plan plurianual de supervisión sobre las actividades desarrolladas por la Unidad CIF, CINF y CNE en el ámbito del Sistema de Control Interno de la Información Financiera (SCIIF) del Grupo Kutxabank, según el cual, emite un informe en el que evalúa dichas actividades, identificando en su caso, los hallazgos que considera relevantes, así como las correspondientes recomendaciones de cara a mitigar los riesgos puestos de manifiesto en su revisión.



Para mayor información respecto al sistema interno de control y gestión de riesgos en relación con el proceso de emisión de la información financiera (SCIIF), véase el IAGC de la Entidad, a disposición en la página web de la Entidad.