Política de control y gestión de riesgos de Indexa Capital Group SA

Versión 19/10/2026

Emisor: Cumplimiento Normativo

Cumplimiento Normativo: Director de Cumplimiento Normativo

Órgano de aprobación: Consejo de Administración

Contenido

0. Registro de actualizaciones 2
1. Introducción 2
   1.1. Objeto 2
   1.2. Normativa de referencia 2
2. Ámbito de aplicación 3
3. Principios básicos 3
4. Tipos de riesgo 3
5. Modelo de control y gestión de riesgos 4
   5.1. Órganos de gobierno 4
   5.2. Tres líneas de control 5
6. Nivel de riesgo aceptable 5
7. Medidas de mitigación 6
8. Sistemas de información y control interno 6
9. Supervisión, revisión y aprobación 7
10. Anexo: Responsabilidades 7

0. Registro de actualizaciones

Versión	Fecha de elaboración	Fecha de aprobación	Descripción de la revisión
0	28/09/2026		Primera versión

1. Introducción

El artículo 529 ter de la Ley de Sociedades de Capital atribuye al Consejo de Administración de las sociedades cotizadas, con carácter indelegable, la determinación de la política de control y gestión de riesgos, incluidos los fiscales, y la supervisión de los sistemas internos de información y control. En la misma línea, la Recomendación 45 del Código de Buen Gobierno de las Sociedades Cotizadas de la CNMV establece el contenido mínimo que debe recoger dicha política.

Indexa Capital Group SA (en adelante, "Indexa" o "la Entidad") es la sociedad matriz de un grupo que presta servicios financieros a través de sociedades dependientes debidamente autorizadas y supervisadas (en adelante, el "Grupo"). La gestión de los riesgos es un elemento inherente a su modelo de negocio, basado en la gestión automatizada, la eficiencia y la protección de los intereses de sus clientes y accionistas.

1.1. Objeto

La presente política (en adelante, la "Política") tiene por objeto establecer los principios básicos y el marco general de actuación para la identificación, evaluación, control, gestión y seguimiento de los riesgos de toda naturaleza a los que se enfrenta el Grupo. En particular, la Política identifica:

a) Los distintos tipos de riesgo, financieros y no financieros, a los que se enfrenta el Grupo (apartado 4).
b) El modelo de control y gestión de riesgos basado en diferentes niveles (apartado 5).
c) El nivel de riesgo que el Grupo considera aceptable (apartado 6).
d) Las medidas previstas para mitigar el impacto de los riesgos, en caso de que llegaran a materializarse (apartado 7).
e) Los sistemas de información y control interno utilizados para controlar y gestionar los riesgos (apartado 8).

La Política se desarrolla y complementa con las políticas, manuales y procedimientos específicos aprobados por la Entidad y por las sociedades del Grupo, entre otros, el Código de Conducta, el Reglamento Interno de Conducta, el Manual de prevención de riesgos penales, la Política y el Procedimiento de gestión del sistema interno de información y los procedimientos de cumplimiento normativo y gestión de riesgos de las sociedades dependientes.

1.2. Normativa de referencia

- Real Decreto Legislativo 1/2010, de 2 de julio, por el que se aprueba el texto refundido de la Ley de Sociedades de Capital (artículos 249 bis, 529 ter y 529 quaterdecies).
- Código de Buen Gobierno de las Sociedades Cotizadas de la CNMV, revisado en junio de 2020 (Recomendaciones 42, 45 y 46).
- Guía Técnica 1/2024, de la CNMV, sobre comisiones de auditoría de entidades de interés público.
- Ley 6/2023, de 17 de marzo, de los Mercados de Valores y de los Servicios de Inversión.
- Real Decreto 813/2023, de 8 de noviembre, sobre el régimen jurídico de las empresas de servicios de inversión y de las demás entidades que prestan servicios de inversión.

- Reglamento (UE) 2019/2033 y Directiva (UE) 2019/2034, relativos a los requisitos y la supervisión prudencial de las empresas de servicios de inversión.
- Reglamento (UE) 2022/2554, sobre la resiliencia operativa digital del sector financiero (DORA).
- Reglamento (UE) 596/2014, sobre el abuso de mercado.
- Circular 1/2014, de 26 de febrero, de la CNMV, sobre los requisitos de organización interna y de las funciones de control de las entidades que prestan servicios de inversión.
- Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal (artículo 31 bis).
- Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo.

Adicionalmente, se toman como referencia los estándares internacionales en materia de gestión de riesgos, en particular el marco COSO ERM, la norma ISO 31000 y el Modelo de las Tres Líneas del Instituto de Auditores Internos.

2. Ámbito de aplicación

La presente Política tiene carácter corporativo y se aplica a Indexa y a todas las sociedades del Grupo sobre las que Indexa ejerza, directa o indirectamente, el control, en los términos del artículo 42 del Código de Comercio. Es de obligado cumplimiento para todos los consejeros, directivos y empleados del Grupo.

Las sociedades del Grupo sujetas a regulación y supervisión sectorial aplicarán la Política respetando la normativa específica que les resulte de aplicación y las competencias de sus propios órganos de administración. A tal efecto, podrán aprobar políticas, procedimientos y límites de riesgo propios, que deberán ser coherentes con los principios establecidos en esta Política. En las sociedades participadas en las que no se ejerza el control, la Entidad promoverá, en la medida de lo posible, principios de gestión de riesgos coherentes con los aquí establecidos.

3. Principios básicos

El control y la gestión de los riesgos del Grupo se rigen por los siguientes principios:

- **Integración en la gestión:** el riesgo se tiene en cuenta en la definición de la estrategia, en la planificación y en la toma de decisiones del día a día.
- **Responsabilidad compartida:** cada profesional es responsable de conocer y gestionar los riesgos de su ámbito de actuación, dentro de los límites establecidos.
- **Segregación de funciones e independencia:** existe una adecuada separación entre las áreas que asumen y gestionan los riesgos y las funciones responsables de su control y supervisión.
- **Prudencia y proporcionalidad:** el Grupo no desarrolla actividad de negociación por cuenta propia distinta de la gestión de sus recursos propios, y el sistema de control y gestión de riesgos se adecúa a la naturaleza, escala y complejidad de sus actividades.
- **Tolerancia cero:** el Grupo rechaza cualquier conducta ilícita, fraudulenta o contraria a su Código de Conducta, con independencia del beneficio que pudiera derivarse de ella.
- **Transparencia y mejora continua:** se informa con transparencia a los órganos de gobierno, a los supervisores y al mercado sobre los riesgos del Grupo y el funcionamiento de sus sistemas de control, que se revisan periódicamente para su mejora.

4. Tipos de riesgo

Se entiende por riesgo cualquier amenaza de que un evento, acción u omisión, de origen interno o externo, pueda impedir al Grupo alcanzar sus objetivos o afectar negativamente a sus clientes, a

sus resultados, a su solvencia o a su reputación. El Grupo clasifica sus riesgos en las siguientes categorías:

- **Riesgos estratégicos y de negocio:** derivados del entorno macroeconómico y de la evolución de los mercados financieros, de los que dependen el patrimonio gestionado y los ingresos, así como de la competencia, la dependencia de proveedores clave, los cambios tecnológicos y las decisiones de crecimiento u operaciones corporativas.
- **Riesgos financieros y de solvencia:** riesgo de mercado sobre los recursos propios, riesgo de crédito y contraparte, riesgo de liquidez y riesgo de incumplimiento de los requisitos de fondos propios y de liquidez exigibles a las sociedades reguladas del Grupo, incluidos los pasivos contingentes y otros riesgos fuera de balance.
- **Riesgos operacionales:** pérdidas derivadas de errores o fallos en los procesos, las personas o los sistemas, o de acontecimientos externos, incluido el riesgo de no ejecutar la operativa pactada con los clientes, el derivado de la externalización de funciones y el de interrupción del negocio. Se presta especial atención a que, en procesos automatizados, un error puede tener un efecto multiplicador.
- **Riesgos tecnológicos y de ciberseguridad:** relacionados con la disponibilidad, integridad y confidencialidad de los sistemas y de la información, los ciberataques, la protección de los datos personales y la resiliencia operativa digital.
- **Riesgos de cumplimiento normativo y regulatorio:** derivados del incumplimiento de la normativa aplicable, en particular la relativa a normas de conducta y protección del cliente, prevención del blanqueo de capitales, abuso de mercado y protección de datos, así como de los cambios regulatorios. Incluyen los riesgos fiscales.
- **Riesgos penales:** relativos a la posible comisión, en el seno del Grupo, de delitos que puedan generar responsabilidad penal para las personas jurídicas, que se gestionan conforme al Manual de prevención de riesgos penales.
- **Riesgos de gobierno corporativo y de la condición de sociedad cotizada:** derivados del incumplimiento del sistema de gobierno corporativo y de las obligaciones como emisor, incluidas la fiabilidad de la información financiera y no financiera, la gestión de la información privilegiada, los conflictos de interés y las operaciones vinculadas.
- **Riesgos sociales y medioambientales:** derivados de factores ambientales, sociales y de gobernanza que puedan afectar a la actividad del Grupo o a la de los productos que gestiona o comercializa.

Todos estos riesgos pueden derivar, además, en un riesgo reputacional, que se considera de forma transversal por su potencial impacto en la confianza de clientes, accionistas y supervisores. El Grupo presta también atención a los riesgos emergentes, entendidos como nuevas amenazas de impacto incierto que podrían llegar a ser significativas.

5. Modelo de control y gestión de riesgos

El Grupo cuenta con un sistema de control y gestión de riesgos basado en el Modelo de las Tres Líneas, bajo la supervisión del Consejo de Administración y de la Comisión de Auditoría y Cuentas. Las responsabilidades de cada órgano y función se resumen en el Anexo de esta Política.

5.1. Órganos de gobierno

El **Consejo de Administración** es el responsable último del sistema: aprueba esta Política, determina el nivel de riesgo aceptable y supervisa los sistemas internos de información y control.

La **Comisión de Auditoría y Cuentas** supervisa y evalúa la eficacia de los sistemas de control y gestión de los riesgos financieros y no financieros, incluidos los fiscales; revisa periódicamente

esta Política y propone al Consejo sus modificaciones, y supervisa la función interna de control y gestión de riesgos y la función de auditoría interna.

5.2. Tres líneas de control

- **Primera línea:** las áreas de negocio y de soporte de cada sociedad del Grupo son responsables de identificar, gestionar y controlar los riesgos de su ámbito, aplicar los controles establecidos en los procedimientos y comunicar de inmediato cualquier incidencia.
- **Segunda línea:** las funciones de cumplimiento normativo y gestión de riesgos supervisan la actividad de la primera línea, elaboran y mantienen el mapa de riesgos, proponen el nivel de riesgo aceptable y los límites, realizan el seguimiento de los riesgos e informan a los órganos de gobierno. A nivel de Grupo, la función interna de control y gestión de riesgos se ejerce por la unidad de cumplimiento normativo y gestión de riesgos de Indexa Capital AV, SA, sociedad con mayor actividad del Grupo, con la independencia y los medios necesarios, sin perjuicio de las funciones propias de las demás sociedades reguladas. El Comité de Defensa Corporativa supervisa el modelo de prevención de riesgos penales.
- **Tercera línea:** la función de auditoría interna, que podrá estar externalizada en un proveedor especializado, revisa de forma independiente la eficacia del sistema de control y gestión de riesgos e informa a la Comisión de Auditoría y Cuentas. En aquellas sociedades del Grupo en las que la normativa aplicable no exija una función de auditoría interna, el Grupo realizará esta actividad de supervisión conforme al principio de proporcionalidad, pudiendo llevarla a cabo con sus propios recursos internos, siempre que estos no participen en las actividades supervisadas.

6. Nivel de riesgo aceptable

El Grupo define su nivel de riesgo aceptable (apetito al riesgo) como el nivel de riesgo que está dispuesto a asumir para alcanzar sus objetivos estratégicos. La tolerancia es la desviación admisible respecto de dicho nivel, y la capacidad, el máximo nivel de riesgo que el Grupo puede soportar sin comprometer su solvencia, su liquidez o el cumplimiento de sus obligaciones regulatorias.

Con carácter general, el Grupo mantiene un perfil de riesgo bajo, coherente con su modelo de negocio: no asume riesgos por cuenta propia distintos de los derivados de la gestión de sus recursos propios, y sus principales exposiciones son de naturaleza operacional, tecnológica y regulatoria. Por categorías, el nivel de riesgo aceptable es el siguiente:

- **Tolerancia cero:** riesgos penales, corrupción, fraude, blanqueo de capitales y cualquier conducta contraria al Código de Conducta.
- **Muy bajo:** riesgos de cumplimiento normativo y regulatorio (incluidos los fiscales), de protección de los clientes y salvaguarda de sus activos, de solvencia y liquidez, de gobierno corporativo e información al mercado, y reputacional.
- **Bajo:** riesgos operacionales, tecnológicos y de ciberseguridad, que no pueden eliminarse por completo, pero se mantienen dentro de límites reducidos mediante controles, automatización supervisada y planes de continuidad.
- **Moderado:** riesgos estratégicos y de negocio, inherentes a la actividad y al crecimiento del Grupo, siempre que sean compatibles con sus objetivos estratégicos y con el resto de niveles aquí fijados.

Los riesgos se evalúan con una metodología común, que combina probabilidad e impacto para obtener el riesgo inherente y lo corrige en función del grado de mitigación de los controles para obtener el riesgo residual. Los riesgos cuyo riesgo residual supere el nivel aceptable para su

categoría serán objeto de un plan de acción y de seguimiento específico por la Comisión de Auditoría y Cuentas. Las sociedades reguladas del Grupo fijarán, además, los indicadores y límites cuantitativos que exija su normativa prudencial, manteniendo en todo momento sus recursos propios y su liquidez por encima de los mínimos regulatorios.

7. Medidas de mitigación

Ante los riesgos identificados, el Grupo adopta la respuesta más adecuada en cada caso: evitar la actividad que genera el riesgo, reducirlo mediante controles, transferirlo a terceros (por ejemplo, mediante seguros o cláusulas contractuales) o aceptarlo de forma informada cuando se encuentre dentro del nivel aceptable. Entre las principales medidas de mitigación se encuentran:

- Políticas, manuales y procedimientos que definen responsabilidades y controles preventivos, de detección y de reacción.
- Segregación de funciones, régimen de poderes y autorizaciones, y automatización de procesos con controles de supervisión.
- Planes de continuidad de negocio y de respuesta ante incidentes, incluidos los de ciberseguridad.
- Formación y concienciación de los profesionales, canal de denuncias y régimen disciplinario.

Cuando un riesgo llegue a materializarse, el responsable del área afectada lo comunicará sin demora a la función de cumplimiento normativo y gestión de riesgos, que evaluará su impacto, clasificará la incidencia en función de su gravedad (alta, media o baja), propondrá las medidas correctoras y realizará su seguimiento hasta su resolución. Las incidencias de especial relevancia se comunicarán de forma inmediata a la Comisión de Auditoría y Cuentas y al Consejo de Administración.

8. Sistemas de información y control interno

El Grupo dispone de los siguientes sistemas de información y control interno para controlar y gestionar sus riesgos:

- **Mapa de riesgos del Grupo,** incluido el de riesgos penales, que se revisa al menos anualmente y recoge, para cada riesgo, su evaluación inherente y residual y los controles asociados.
- **Supervisión permanente,** a través de un plan anual de controles y revisiones ejecutado por las funciones de cumplimiento normativo y gestión de riesgos, con registro de incidencias y reclamaciones.
- **Información periódica** a la Comisión de Auditoría y Cuentas y al Consejo de Administración, mediante informes trimestrales y anuales de las funciones de control, el informe anual del Comité de Defensa Corporativa y los informes de auditoría interna.
- **Sistema de control interno sobre la información financiera,** bajo la supervisión de la Comisión de Auditoría y Cuentas, que garantiza la fiabilidad de la información financiera que se publica.
- **Sistema interno de información (canal de denuncias),** que permite a profesionales y terceros comunicar, incluso de forma anónima, posibles irregularidades.

La información sobre los principales riesgos del Grupo y el funcionamiento de sus sistemas de control se publica en el Informe Anual de Gobierno Corporativo y en el informe de gestión.

9. Supervisión, revisión y aprobación

Corresponde a la Comisión de Auditoría y Cuentas velar por el cumplimiento de esta Política. La Política será revisada por el Consejo de Administración, al menos, cada tres años. No obstante, la función de cumplimiento normativo y gestión de riesgos revisará su contenido anualmente y, si lo considera oportuno, propondrá modificaciones que, previo informe de la Comisión de Auditoría y Cuentas, se someterán a la aprobación del Consejo de Administración.

La presente Política entrará en vigor en la fecha de su aprobación por el Consejo de Administración y se publicará en la página web corporativa de la Entidad.

10. Anexo: Responsabilidades

Órgano o función	Responsabilidades
Consejo de Administración	Aprobar la Política y el nivel de riesgo aceptable. Supervisar los sistemas internos de información y control. Responsable último de la gestión de riesgos del Grupo.
Comisión de Auditoría y Cuentas	Supervisar la eficacia del sistema de control y gestión de riesgos, incluidos los fiscales. Revisar la Política y proponer modificaciones. Supervisar la función de control y gestión de riesgos y la auditoría interna.
Consejeros delegados y equipo directivo	Implantar la Política en su ámbito, dotar de los medios necesarios y aprobar y seguir los planes de acción sobre los riesgos identificados.
Áreas de negocio y soporte (primera línea)	Identificar, gestionar y controlar los riesgos de su ámbito, aplicar los controles y comunicar las incidencias.
Cumplimiento normativo y gestión de riesgos (segunda línea)	Mantener el mapa de riesgos, proponer el nivel de riesgo aceptable y los límites, ejecutar la supervisión permanente e informar a los órganos de gobierno.
Comité de Defensa Corporativa	Supervisar el funcionamiento y cumplimiento del modelo de prevención de riesgos penales y gestionar el sistema interno de información.
Auditoría interna (tercera línea)	Revisar de forma independiente la eficacia del sistema de control y gestión de riesgos e informar a la Comisión de Auditoría y Cuentas.