# POLÍTICA DE CONTROL Y GESTIÓN DE RIESGOS DE MERLIN PROPERTIES, SOCIMI, S.A.

**Junio 2026**

El Consejo de Administración de MERLIN Properties, SOCIMI, S.A. (en adelante, "**MERLIN**", "**el Grupo**" o "**la Sociedad**"), tiene la responsabilidad general de la supervisión del riesgo y de la existencia de un sistema eficaz sobre la gestión del riesgo y del control interno de la compañía. Así, el Reglamento del Consejo establece, en el artículo 4 "Función General del Consejo", aquellas funciones legal o estatutariamente reservadas al propio Consejo de Administración de MERLIN, entre las que se encuentra la aprobación de la política de control y gestión de riesgos y el seguimiento periódico de los sistemas de información y control. El Consejo de Administración, consciente de la importancia de este aspecto, establece, a través de la presente **Política de Control y Gestión de Riesgos** (en adelante, "**la Política**"), a propuesta de la Comisión de Auditoría y Control, los mecanismos y principios básicos para una adecuada gestión de los riesgos clave a los que se enfrenta la Sociedad.

Esta Política ayudará a la organización a alcanzar los objetivos estratégicos marcados e identificar las oportunidades de mejora, así como dar respuesta a los retos y desafíos en el desarrollo de su actividad en un entorno cada vez más cambiante.

Por su parte, la **Comisión de Auditoría y Control**, de acuerdo con las competencias establecidas en su propio Reglamento es la encargada de supervisar todo lo relativo a los distintos tipos de riesgo a los que se enfrenta la Sociedad, incluyendo riesgos financieros o económicos, pasivos contingentes, otros riesgos (a) fuera de balance, (b) operativos, (c) sociales, medioambientales y tecnológicos, (d) riesgos de gobernanza y gestión del talento, (e) legales, y (f) políticos y reputacionales, lo anterior en colaboración con la **Comisión de Sostenibilidad e Innovación** y la **Comisión de Nombramientos y Retribuciones**, en materias de competencia.

El **Sistema de Gestión de Riesgos** de MERLIN está alineado con los estándares internacionales de referencia en materia de gestión de riesgos (**COSO ERM 2017** ***Marco de gestión de riesgos empresariales – integrado con la estrategia y el desempeño***) y se basa en un modelo que identifica los eventos de Riesgo clave de la Compañía, los evalúa en función del Impacto y la Probabilidad de ocurrencia considerando los Controles en funcionamiento y monitoriza y reporta su evolución de forma periódica.

La Dirección de MERLIN es responsable de liderar, implantar, transmitir y gestionar la estrategia y recursos que constituyen el Sistema de Gestión de Riesgos y asume como compromiso fundamental garantizar un nivel de independencia adecuado, basado en los siguientes principios:

- Considerar el Riesgo como cualquier amenaza que un evento, acción u omisión, pueda impedir a MERLIN lograr sus objetivos, ejecutar sus estrategias con éxito, la realización correcta de sus operaciones o la pérdida de oportunidades.
- Establecer los mecanismos para una adecuada Gestión del Riesgo, considerando su identificación, evaluación, respuesta, seguimiento y reporting.
- Promover e implantar la estrategia, cultura, recursos y procesos que constituyan la Gestión Integral de Riesgos, que será revisada periódicamente para su adecuación a la situación de MERLIN y su entorno.
- Atribuir, entre los diferentes niveles de la Organización, la responsabilidad de identificar, analizar, valorar, evaluar y supervisar el Sistema de Gestión de Riesgos.
- Favorecer el establecimiento e implantación de directrices, límites y mecanismos que contribuyan a que la Gestión de Riesgos se realice de acuerdo con el Apetito al Riesgo aceptado por la Compañía.
- Impulsar, fomentar y difundir, mediante formación y comunicación, el Sistema de Gestión Riesgos, garantizando la difusión de la presente Política, junto con la documentación que la desarrolle.

## 1. Principios para la Gestión de los Riesgos en MERLIN

La gestión y control de los riesgos se plantea como un proceso continuo compuesto por una serie de etapas dentro de las cuales deben realizarse determinadas actividades. El sistema centra su acción en 10 principios o pasos básicos:

1. Conocer los objetivos estratégicos y de negocio de MERLIN.
2. Conocer el entorno de control de MERLIN (lo que implica valorar factores como los procesos, procedimientos, recursos humanos involucrados, infraestructura tecnológica, normativa vigente aplicable a las actividades de la Compañía, etc.).
3. Realizar un análisis de los riesgos potenciales, esto es, identificar las actividades, procesos, lugares, etc. (por ejemplo: identificar todas las actividades de un mismo proceso).
4. Determinar los puntos críticos de respuesta y control de los riesgos clave, esto es, identificar los peligros presentes en cada actividad, proceso, lugar, etc., evaluar los controles existentes, en su caso, y definir qué aspectos del proceso son críticos y deben ser

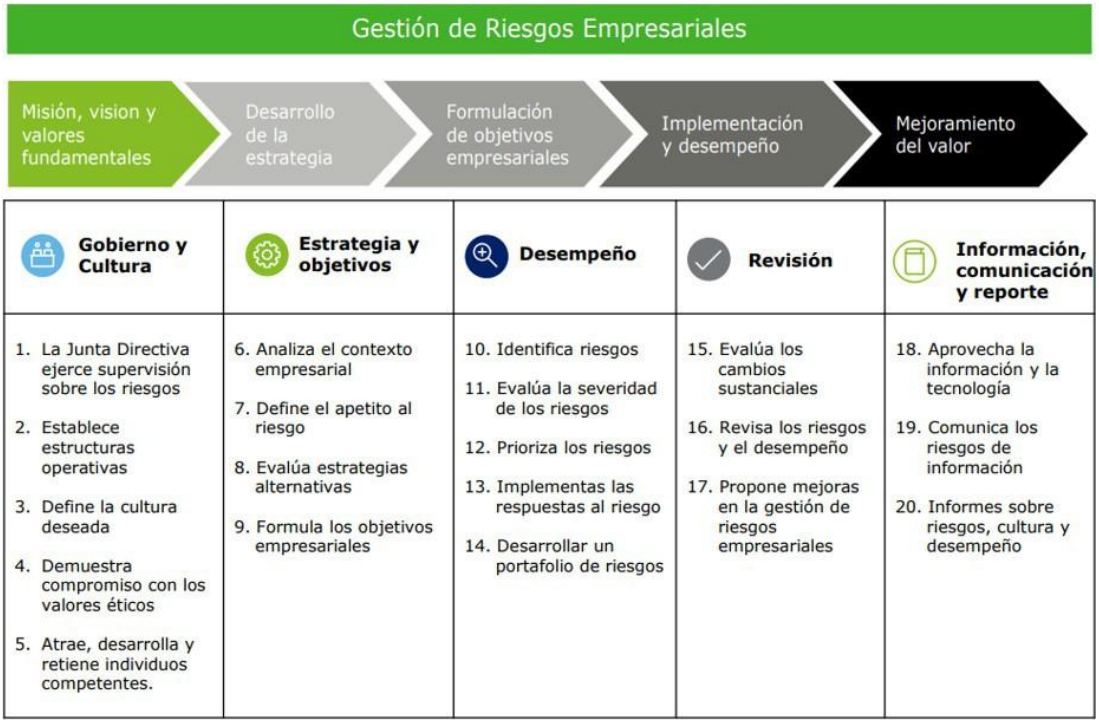
monitorizados.

5. Establecer los límites máximos para cada punto crítico de control (qué riesgos son tolerables y cuáles no). Para ello, es necesario analizar el impacto que ocasionaría la materialización del riesgo y la probabilidad de que ocurra.
6. Establecer un sistema de vigilancia y control de dichos puntos críticos.
7. Promulgar las medidas correctivas que han de adoptarse cuando la vigilancia indica que determinado punto crítico se sale de los límites establecidos (dichas medidas pueden consistir en mitigar el riesgo, aceptarlo, evitarlo, transferirlo, etc.).
8. Implementar o poner en práctica las medidas adoptadas, en su caso.
9. Instaurar procedimientos de supervisión para verificar el funcionamiento del sistema y estructurar un sistema de documentación sobre todos los procedimientos y los registros apropiados para estos principios y su aplicación.
10. Evaluar periódicamente los riesgos del entorno para detectar nuevas amenazas (seguimiento que inicia de nuevo el proceso cíclico).

## 2. Metodología para el control y la gestión de riesgos

El Sistema de Gestión de Riesgos del Grupo MERLIN, basado en los principios, elementos clave y metodología establecidos en el **Marco COSO** ("***Committee of Sponsoring Organizations of the Treadway Commission***"), tiene por objeto minimizar la volatilidad de los resultados (rentabilidad) y, por tanto, maximizar el valor económico del Grupo, incorporando el riesgo y la incertidumbre en el proceso de toma de decisiones para proporcionar una seguridad razonable en la consecución de los objetivos estratégicos establecidos, aportando a los accionistas, a otros grupos de interés y al mercado en general un nivel de garantías adecuado que asegure la protección del valor generado.

Sobre la base de una visión integradora de la Gestión de Riesgos, MERLIN ha adoptado un enfoque metodológico basado en el **Marco de Gestión de Riesgos Empresariales – integrado con estrategia y desempeño (COSO 2017),** el cual aclara la importancia de la gestión de riesgos empresariales en la planificación estratégica y la incorpora a toda la organización, ya que el riesgo influye en la estrategia y en el desempeño en todas las áreas, departamentos y funciones.




## 3. Órganos de la Compañía que desarrollan el control y la gestión de los riesgos

MERLIN se encuentra sometido a diversos riesgos inherentes a los distintos negocios en los que opera y a las actividades que desarrolla. En este sentido, el Consejo de Administración considera la Gestión de Riesgos como un instrumento que contribuye a lograr una mayor eficiencia y eficacia de sus operaciones.

**El Consejo de Administración es el órgano de gobierno responsable de fijar los niveles de riesgo que considere aceptables**, consciente de la importancia de este aspecto, establece, a través de la presente Política, los mecanismos y principios básicos para una adecuada gestión de los riesgos clave a los que se enfrenta, y todo ello con el fin de:

- ✓ favorecer el cumplimiento de los objetivos empresariales propuestos;
- ✓ evitar pérdidas derivadas de la materialización de los riesgos;
- ✓ preservar la imagen y reputación de la Compañía y de su marca; y
- ✓ tener una continuidad en el análisis y la detección de posibles amenazas y nuevos riesgos para analizar su impacto y probabilidad de ocurrencia.

Para el desarrollo del control y la gestión de los riesgos, el Consejo de Administración cuenta con la colaboración de la Comisión de Auditoría y Control que supervisa e informa sobre la adecuación y eficacia del sistema de control y gestión de riesgos.

En este sentido, la **Comisión de Auditoría y Control** apoya al Consejo en la supervisión del sistema de gestión de riesgos y es el órgano responsable de revisar de la efectividad del sistema de gestión de riesgos y control interno durante el ejercicio, con el apoyo de la Dirección de Auditoría Interna.

La Comisión de Auditoría y Control es el órgano de gobierno encargado de la supervisión de todo lo relativo a los distintos tipos de riesgo a los que se enfrenta MERLIN, incluyendo riesgos financieros o económicos, pasivos contingentes, otros riesgos fuera de balance, operativos, medioambientales, tecnológicos, legales, sociales, políticos y reputacionales. Así mismo, la Comisión de Auditoría y Control debe evaluar, al menos anualmente, la lista de los riesgos, financieros y no financieros, más significativos y el nivel de tolerancia establecido para cada uno a partir de la información proporcionada por la Dirección.

Por su parte, la **Comisión de Nombramientos y de Retribuciones y la Comisión de Sostenibilidad e Innovación**, en coordinación con la Comisión de Auditoría y Control, serán responsables en la identificación y supervisión de riesgos de gobierno, medioambientales y sociales, dentro del ámbito de actuación de cada uno.

El **Comité de Riesgos,** compuesto por representantes de las distintas ramas de actividad y áreas corporativas, es un órgano dependiente de la Comisión de Auditoría y Control que coordina el trabajo de los risk owners de primera línea y supervisa el diseño de controles de segunda línea. Dicho Comité se encarga de la coordinación de la gestión de riesgos, integrando la información recibida de los distintos responsables directos de la gestión de riesgos y reportando al Consejo de Administración con carácter semestral junto con la actualización del Mapa de Riesgos.

Por su parte, el **Operating Committee (OpCo)** es el responsable de la gestión diaria de riesgo, que incluye la identificación, evaluación y mitigación de los riesgos, así como el diseño e implementación de los planes de acción y evaluación del sistema de control interno, garantizando su efectividad operacional. MERLIN considera que toda la compañía debe estar implicada en la gestión de riesgos de forma activa, siendo la Dirección de MERLIN la responsable de liderar, implantar, transmitir y gestionar la estrategia y recursos que constituyen el Sistema de Gestión de Riesgos.

Por último, la **Dirección de Auditoría Interna**, como tercera línea de defensa se encarga de la auditoría y supervisión del Sistema de gestión de Riesgos de MERLN en su conjunto.

**Segregación de funciones en la gestión y control de riesgos en MERLIN**

| | Consejo de Administración | Comisión de Auditoría y Control | Comisión de Sostenibilidad | Comisión de Nombramientos y Retribuciones | Alta Dirección y Equipo Directivo | Comité de Riesgos | Dirección de Auditoría interna | Resto de Empleados |
|---|---|---|---|---|---|---|---|---|
| **Identificación de riesgos** | | X | X | X | X | X | | X |
| **Definición nivel de tolerancia** | X | | | | | | | |
| **Evaluación de riesgos** | | | | | X | X | | |
| **Ejecución planes de acción** | | | | | X | | | X |
| **Supervisión del SGR** | X | X | X | X | | X | X | |
| **Reporte y Control** | | | | | X | X | X | X |

La Comisión de Auditoría y Control de Merlin desarrollará las funciones en materia de supervisión de la gestión de riesgos y de la información financiera y no financiera que le han sido delegadas por el Consejo de Administración.

**Coordinación entre Comisiones del Consejo**

Por su parte y de acuerdo con sus respectivos Reglamentos, la Comisión de Nombramientos y Retribuciones y la Comisión de Sostenibilidad e Innovación, tienen encomendada la supervisión de la información no financiera y de sostenibilidad dentro de los respectivos ámbitos de actuación.

En este sentido, ambas Comisiones, en coordinación con la Comisión de Auditoría y Control, serán responsables en la identificación y supervisión de riesgos de gobierno, medioambientales y sociales, así como en la supervisión de la información no financiera relativa, a la gobernanza del Grupo, el desempeño ambiental de los activos, la gestión del cambio climático, el uso responsable de los recursos, la gestión de los grupos de interés, el impacto social de las actividades, la organización del trabajo y el empleo, el cumplimiento de los derechos humanos, entre otros.

## 4. Modelo de las 3 líneas de defensa

Para la gestión de riesgos, MERLIN aplica el modelo de las tres líneas de defensa, consistente con la metodología COSO y el posicionamiento del Instituto de Auditores Internos, por el que los roles y responsabilidades en la gestión de riesgos se estructuran en tres ámbitos claramente diferenciados:

- **La primera línea** se corresponde con los gestores del negocio (Operating Committee, Divisiones de Negocio y Funciones ejecutivas) que son los responsables de mantener un control interno efectivo y de ejecutar procedimientos de control sobre los riesgos de manera constante en el día a día. En este sentido son los responsables de identificar, evaluar, controlar y mitigar los riesgos, orientando el desarrollo e implementación de políticas y procedimientos internos que aseguren que las actividades desarrolladas son consistentes con los objetivos establecidos.

- **La segunda línea** corresponde con el Comité de Riesgos y el resto de las funciones de control (Órgano de Cumplimiento Normativo, Órgano de Control en materia del Reglamento Interno de Conducta del Mercado de Valores, Órgano de Control Interno en materia de prevención de blanqueo de capitales, CISO y Comité de Seguridad de la Información) que deben monitorizar los riesgos y controles para asegurar que la primera línea de defensa está apropiadamente diseñada, implementada y operando según lo previsto.

- **La tercera línea** de defensa corresponde a la Dirección de Auditoría Interna, que tiene como misión proveer aseguramiento independiente al Consejo de Administración y a la Comisión de Auditoría y Control sobre la efectividad y eficacia de los controles implementados en la gestión de riesgos.

## 5. Mapa de Riesgos de MERLIN

Merlin utiliza el Mapa de Riesgos como una herramienta que tiene por objeto mostrar gráficamente el resultado del proceso de evaluación de riesgos durante un periodo de medición determinado.

La Comisión de Auditoría y Control, tal y como establece su propio Reglamento, revisará el mapa de riesgos del Grupo con la periodicidad necesaria para un seguimiento adecuado de los riesgos. La actualización

periódica del Mapa de riesgos se realiza, al menos, semestralmente, de forma coordinada y por parte de cada uno de los responsables de las diferentes divisiones de negocio mediante el seguimiento de los KPIs asociados a cada riesgo y juntamente con la actualización del presupuesto anual del Grupo Merlin.

En este sentido, la Comisión de Auditoría y Control mantendrá, al menos con carácter anual, una reunión con los responsables de las unidades de negocio en la que éstos expliquen las tendencias del negocio y los riesgos asociados, y reforzar la idea de que es a los responsables de las unidades de negocio a quienes corresponde de modo directo gestionar eficazmente los riesgos, como el principio de que es conveniente que exista un responsable asignado para cada riesgo identificado.

Para la identificación y supervisión de los riesgos medioambientales, sociales y de gobernanza, la Comisión de Auditoría se coordinará con las Comisiones de Sostenibilidad e Innovación, así como con la Comisión de Nombramientos y Retribuciones.

La Dirección de Auditoría Interna y Gestión de Riesgos es la función encargada de la elaboración del marco de actuación con el fin de homogeneizar la identificación, clasificación, evaluación, gestión y seguimiento de los riesgos de los distintos segmentos de negocio.

El Mapa de Riesgos de MERLIN está dividido en sectores (Riesgos Estratégicos, Riesgos de Negocio, Riesgos de Recursos -económicos, tecnológicos y humanos- y Riesgos ESG) que representan los distintos ejes de la estrategia de MERLIN y que engloban a los distintos riesgos identificados (factores internos y externos) que pueden afectar a los objetivos de MERLIN respecto de su Plan Estratégico (largo plazo), su Presupuesto anual (corto plazo), así como a los distintos grupos de interés con los que interactúa (y según se establece en la Política de gestión de grupos de interés).

La evaluación de la criticidad de cada uno de los riesgos se determina mediante el binomio de la probabilidad y el impacto de los riesgos en los diferentes procesos, actividades o funciones de cada división de negocio.

Posteriormente, y una vez identificados los riesgos, evaluado su impacto y probabilidad, así como los indicadores para su seguimiento, se elabora el Mapa de Riesgos con la participación de cada una de las divisiones de negocio, así como de la Alta Dirección, para su posterior revisión y validación de las comisiones del consejo involucradas, para su validación final por la Comisión de Auditoría y Control y su presentación final al Consejo de Administración.

Cada uno de los riesgos incluidos en el Mapa de Riesgos tiene asignado un responsable para el seguimiento y reporte de los diferentes indicadores asociados a los riesgos.

En general, todos aquellos riesgos que se han identificado como de criticidad Alta son objeto de seguimiento continuo tanto por el Comité de Riesgos, como por la Alta Dirección en sus reuniones del Operating Committee (OpCo), como por el Consejo de Administración a través de las presentaciones, con periodicidad trimestral o semestral según sea el caso, que se realizan a la Comisión de Auditoría y Control, con los diferentes indicadores cuantitativos y/o cualitativos con el fin de analizar la situación y los riesgos a los que se enfrenta el Grupo.

## 6. Nivel de tolerancia al Riesgo

**La fijación del apetito y del nivel de tolerancia al riesgo son funciones ejecutivas atribuidas al Consejo de Administración.**

Se entiende el apetito al riesgo como el nivel de riesgos que la Compañía está dispuesta a asumir o rechazar en base a sus objetivos estratégicos, considerando las expectativas de sus grupos de interés, y la tolerancia al riesgo como la determinación de las fluctuaciones del nivel de riesgos, entendidas como normales alrededor de su apetito al riesgo.

En la determinación del nivel de tolerancia al riesgo se tienen en cuenta:

- Elementos cualitativos, que establecen los riesgos específicos que la organización está dispuesta a aceptar en función de los riesgos propios de la actividad y que están vinculados a la estrategia y a los planes de negocio.

- Elementos cuantitativos, mediante las que se describen los límites, umbrales o indicadores clave de riesgo, que establecen cómo han de valorarse los riesgos y sus beneficios y/o cómo evaluar y vigilar el impacto agregado de estos riesgos, y ello con la premisa de que no todos los riesgos son medibles.

En este sentido, con carácter anual, la Comisión de Auditoría y Control, a propuesta de la Alta Dirección, eleva al Consejo de Administración para su aprobación la **fijación de los indicadores, umbrales y límites de los principales indicadores de riesgo** corporativos (i.e: LTV, ICR, FFO, etc..) y los propios de cada rama de actividad (GRI, NOI, tasa de ocupación, etc.), realizando un seguimiento del cumplimiento de los mismos con carácter semestral, estableciendo, en su caso, los pertinentes planes de acción.

**En todo caso, el objetivo último de la compañía es mantener un perfil de riesgo (apetito al riesgo) alineado con una tolerancia al riesgo media-baja, propia de un modelo de negocio de una SOCIMI comprometida con la creación de valor a largo plazo y a la generación de dividendo sostenible y creciente para los accionistas dentro de un entorno de valores de transparencia, ética y responsabilidad en el ámbito empresarial y social.**

Es importante destacar la existencia de riesgos con **"tolerancia cero"**, esto es, riesgos para cuya estrategia de respuesta es "evitar", lo que implica no proceder con la actividad que ocasiona el riesgo o cambiar la forma de actuar.

La organización incluye en esta tipología todos los riesgos relacionados con el cumplimiento de las condiciones del Régimen SOCIMI, con cualesquiera otros incumplimientos legales o regulatorios, con el cumplimiento de las condiciones de financiación y reparto de dividendos, los riesgos relacionados con ilícitos penales, los riesgos relacionados con cualquier tipo de fraude, corrupción o soborno (por parte de directivos y empleados, clientes o proveedores de la sociedad) y los relacionados con la prevención de blanqueo de capitales y financiación del terrorismo.

En este sentido, ha de tenerse en cuenta los establecido por la **Estrategia Fiscal y la Política Fiscal** del Grupo, que establecen una serie de principios de actuación, entre los que destacan el cumplimiento estricto de las obligaciones tributarias y abono de los tributos que resulten legalmente exigibles, no utilizar estructuras artificiosas o carentes de sentido económico o empresarial con el fin de minorar la carga fiscal de la compañía o de sus accionistas y el compromiso de no operar en territorios calificados como paraísos fiscales con la finalidad principal de reducir la carga fiscal de la compañía o de sus accionistas.

Así mismo, dentro del Sistema de Gobierno del Grupo MERLIN existen distintas políticas que expresan la voluntad de la Compañía en el cumplimiento estricto de lo más altos estándares de comportamiento ético y legal. Entre estas políticas destacan la **Política de Cumplimiento Penal, Política de Respeto a los Derechos Humanos y la Política de prevención del blanqueo de capitales, corrupción y soborno**, basadas en el principio de tolerancia cero hacia la comisión de actos ilícitos o delictivos, por lo que no permite que ninguno de sus empleados, con independencia de su nivel jerárquico o funcional, se involucre ni participe en ninguna operación o negocio dentro de su actividad empresarial que lleve consigo algún acto delictivo o de fraude, corrupción o soborno, o que vaya contra de los principios recogidos en su **Código de Conducta** que tiene como objetivo establecer los principios básicos por los que se rige el Grupo, y las normas y criterios de comportamiento de los empleados del Grupo MERLIN para imponer una actuación preventiva y proactiva en la lucha contra la corrupción y soborno en todos los ámbitos de su actividad empresarial.

## 7. Marco de continuidad de negocio

MERLIN dispone de un Plan de Continuidad de Negocio (PCN) cuyo propósito es reforzar la resiliencia organizacional y asegurar la continuidad de las operaciones y servicios críticos ante eventos disruptivos, minimizando el impacto y garantizando una recuperación eficaz.

El PCN se alinea con los principios de la ISO 22.301 para la gestión de continuidad de negocio y se integra con el enfoque corporativo de gestión de riesgos y con el **Sistema de Gestión de Seguridad de la Información (SGSI)**. El documento es de uso corporativo, revisable periódicamente (al menos anual) y orientado a la mejora continua.

**Alcance y enfoque basado en riesgo**
El PCN cubre todos los procesos y actividades de MERLIN, sus dependencias funcionales y los recursos asociados (personas, proveedores, aplicaciones TI y datos), tomando como base los análisis de impacto (BIA) y los objetivos de recuperación RTO/RPO. Considera escenarios de riesgo relevantes (incluyendo indisponibilidad de edificios, personal, tecnología, proveedores y datos) y define estrategias y planes de recuperación asociados a dichos escenarios, priorizados según criticidad.

**Gobernanza, responsabilidades y activación**
La gestión de la continuidad se articula mediante un marco de gobierno en el que destaca el **Comité de Seguridad y Continuidad**, con capacidad de decisión y escalado hacia los órganos de dirección, y con posibilidad de activar el **Equipo de Gestión de Crisis** y equipos de gestión ante incidentes. Se establecen roles y responsabilidades para: definición de líneas estratégicas, aprobación y supervisión del PCN, coordinación durante contingencias, y reporte del estado y evolución de crisis.

**Riesgos y escenarios de indisponibilidad**
El PCN incorpora un análisis de riesgos para priorizar amenazas y orientar medidas de mitigación y recuperación. Se estructuran escenarios de indisponibilidad que abarcan, entre otros: gobierno y cumplimiento, indisponibilidad tecnológica, indisponibilidad de personal, indisponibilidad de edificios e indisponibilidad de proveedores, que sirven como base para el diseño de estrategias y planes.

**Estrategias y planes de recuperación**
Para cada escenario se define un catálogo de estrategias preventivas y reactivas (por ejemplo: teletrabajo y reubicación, formación cruzada y protección del conocimiento, redundancias/CPD alterno y copias de seguridad, diversificación o sustitución de proveedores, medidas específicas ante indisponibilidad de datos/ransomware). Los planes de recuperación detallan fases típicas: validación/activación, comunicaciones, evaluación de situación, ejecución de medidas, coordinación con proveedores/clientes/reguladores cuando aplique, monitorización, documentación, retorno a la normalidad y lecciones aprendidas.

**Mantenimiento, formación y pruebas**
El PCN se gestiona como un documento vivo con revisión mínima anual y actualización ante cambios relevantes (estructura, procesos, tecnología, ubicaciones, proveedores, resultados de pruebas e incidentes). Se establece un enfoque formal de formación y concienciación y un programa de pruebas, con evaluación de resultados y planes de acción para reforzar la mejora continua.

## 8. Gestión de Riesgos de Terceros - Cadena de suministro

La gestión de riesgos de terceros (en adelante, "TPRM" por sus siglas en inglés, Third-Party Risk Management) constituye un componente esencial del Sistema de Gestión de Riesgos del Grupo, en la medida en que MERLIN externaliza actividades críticas —entre otras, la gestión de facility management, la ejecución de obras y reformas, la intermediación financiera y la prestación de servicios tecnológicos— cuya materialización deficiente puede generar pérdidas económicas, daños reputacionales, incumplimientos regulatorios o interrupciones operacionales.

Esta sección es de aplicación a todas las relaciones con terceros que, por su naturaleza, volumen o criticidad para las operaciones del Grupo, sean identificadas como relevantes en el proceso de evaluación periódica del Mapa de Riesgos Corporativo.

La gestión de riesgos de terceros en el Grupo MERLIN se rige por los siguientes principios:

- **Proporcionalidad**: el nivel de diligencia aplicado en la evaluación del riesgo de terceros será proporcional al impacto potencial de la relación sobre los objetivos del Grupo, considerando el volumen económico del contrato, la criticidad del servicio prestado, el acceso a activos o sistemas de información del Grupo y la posibilidad de contagio reputacional.

- **Ciclo de vida completo**: la gestión del riesgo de terceros abarcará todas las fases de la relación contractual, incluyendo la selección y homologación previa a la contratación, el seguimiento durante la vigencia del contrato y la gestión de la extinción o sustitución del proveedor.

- **Integración con el Mapa de Riesgos**: los riesgos identificados en el proceso TPRM se integrarán en el Mapa de Riesgos Corporativo del Grupo, bajo las categorías correspondientes según la taxonomía establecida en la presente Política.

- **Coherencia con otras políticas del Grupo**: la gestión de riesgos de terceros se desarrollará en coordinación con lo establecido en la **Política de Compras** del Grupo y, en su caso, con las instrucciones de la **Política de Prevención del Blanqueo de Capitales, Corrupción y Soborno** y la **Política de Seguridad de la Información.**

- **Tolerancia cero ante conductas indebidas**: con independencia del nivel de criticidad asignado al proveedor, el Grupo MERLIN no tolerará la relación con terceros que incumplan sus compromisos en materia de conducta ética, derechos humanos, medio ambiente o cumplimiento legal, en los términos establecidos en el Código de Conducta del Grupo.

## 9. Riesgos emergentes y de Inteligencia Artificial

En el contexto del Sistema de Gestión de Riesgos del Grupo, MERLIN dispone de un marco de identificación, evaluación y gestión de los riesgos emergentes, con especial atención a los riesgos derivados de la adopción y uso de sistemas de inteligencia artificial (en adelante, "IA").

A los efectos de la presente Política, se entiende por riesgo emergente toda amenaza de naturaleza nueva o evolutiva, cuyo impacto sobre los objetivos del Grupo es incierto y cuya probabilidad de materialización resulta indefinida, pero que presenta una tendencia creciente en el entorno operativo, tecnológico, regulatorio o social de la Compañía y podría adquirir relevancia significativa a medio o largo plazo.

Los riesgos emergentes se caracterizan por su transversalidad —pueden afectar simultáneamente a varias categorías de riesgos y por la limitada disponibilidad de datos históricos que permitan una cuantificación precisa de su impacto y probabilidad. Esta naturaleza exige una metodología de gestión diferenciada de la aplicable a los riesgos maduros del Mapa de Riesgos Corporativo.

Los riesgos derivados de la adopción y uso de sistemas de IA constituyen, en el momento actual, la categoría de riesgo emergente de mayor relevancia para el Grupo, tanto por la incorporación activa de estas tecnologías en las operaciones de MERLIN como por el impacto del marco regulatorio.

Sin perjuicio de lo establecido en la **Política de Uso Responsable de Sistemas de Inteligencia Artificial de MERLIN**, aprobada por el Consejo de Administración en diciembre de 2025, la presente sección integra los riesgos derivados del uso de sistemas de IA en el marco del Sistema de Gestión de Riesgos del Grupo, de conformidad con lo establecido en el AI Act de la UE y en el Marco COSO ERM 2017.

El proceso de identificación y seguimiento de riesgos emergentes se integrará en el ciclo anual de actualización del Mapa de Riesgos del Grupo, con las siguientes especificidades:

- **Análisis de horizonte**: con carácter anual, y con carácter previo a la elaboración del Mapa de Riesgos, el Comité de Riesgos, con el apoyo de las Divisiones de Negocio, realizará un análisis de las tendencias tecnológicas, regulatorias, geopolíticas y sociales relevantes para el Grupo, con el objeto de identificar amenazas emergentes que pudieran no estar recogidas en la taxonomía de riesgos vigente.

- **Registro de riesgos emergentes**: los riesgos emergentes identificados se registrarán en un apartado específico del Mapa de Riesgos Corporativo, diferenciado de los riesgos maduros, con

indicación del nivel de incertidumbre, el horizonte temporal estimado de materialización y los indicadores de seguimiento disponibles.

- **Revisión de la taxonomía**: cuando un riesgo emergente sea considerado, por su evolución, como maduro —esto es, cuando su impacto y probabilidad sean cuantificables con suficiente fiabilidad— la Dirección de Auditoría Interna propondrá su integración formal en la taxonomía de riesgos, para su elevación a la Comisión de Auditoría y Control.

- **Monitorización regulatoria:** la Dirección de MERLIN junto al Comité de Riesgos y en coordinación con la Dirección de Auditoría Interna y el Órgano de Cumplimiento Normativo, realizará un seguimiento activo de las iniciativas regulatorias en materia de IA, ciberseguridad, protección de datos y sostenibilidad, con el objeto de anticipar la emergencia de nuevos riesgos de cumplimiento.

El **Comité de Seguridad de la Información** (CSI-Seguridad), en cumplimiento de sus funciones como segunda línea de defensa, supervisará la adecuación de los controles implantados para los sistemas de IA, reportando semestralmente a la Comisión de Auditoría y Control sobre el estado del riesgo de IA en el Grupo.

## 10. Gestión de riesgos de sostenibilidad: TCFD y análisis de escenarios climáticos

Este marco se fundamenta en las recomendaciones de la Task Force on Climate-related Financial Disclosures (en adelante, "TCFD") del Financial Stability Board, que el Grupo MERLIN ha adoptado voluntariamente como referencia para el reporte de riesgos climáticos, tal y como se recoge en el Anexo IV del Estado de Información No Financiera (EINF) del Grupo. Su incorporación al Sistema de Gestión de Riesgos tiene por objeto garantizar que los riesgos climáticos y de sostenibilidad reciben, a efectos internos, el mismo tratamiento sistemático y periódico que el resto de las categorías del Mapa de Riesgos Corporativo.

El alcance de este marco de gestión de riesgos de sostenibilidad comprende todos los activos gestionados por el Grupo, incluyendo la cartera de oficinas, centros comerciales, naves logísticas y centros de datos, atendiendo a que cada tipología de activo presenta un perfil de exposición diferenciado a los riesgos físicos y de transición asociados al cambio climático.

El Grupo MERLIN clasifica los riesgos de sostenibilidad en dos grandes grupos, conforme a la metodología TCFD:

**A) <u>RIESGOS FÍSICOS</u>**

- **Agudos (eventos extremos):** Inundaciones y lluvias torrenciales que afecten a activos logísticos en zonas costeras o de llanura aluvial; olas de calor que incrementen el consumo energético y deterioren la experiencia en activos de oficinas; granizadas y vientos extremos con daños estructurales en cubiertas fotovoltaicas.

- **Crónicos (cambio gradual):** Incremento sostenido de las temperaturas medias que eleve los costes de refrigeración en los Data Centers del Grupo (mayor consumo de agua para enfriamiento); elevación del nivel del mar con impacto en valoraciones de activos en zonas costeras; estrés hídrico en regiones donde se ubican activos de alto consumo de agua.

**B) <u>RIESGOS DE TRANSICIÓN:</u>**

- **Regulatorios y legales**: Endurecimiento de los requisitos de eficiencia energética de los edificios (Directiva Europea de Eficiencia Energética de los Edificios); introducción o ampliación del mercado de CO2; nuevas exigencias de reporting de sostenibilidad (CSRD) para inquilinos que afecten a los requisitos de las cláusulas verdes del Grupo.

- **Mercado y competitivos**: Preferencia creciente de los inquilinos por edificios con altas certificaciones de sostenibilidad (BREEAM/LEED Excellent o Outstanding) que pudiera afectar a la ocupación de activos con menor certificación; reducción del valor de tasación de activos no adaptados a la transición energética (stranded assets); presión de inversores institucionales con mandatos ESG sobre el perfil de sostenibilidad del portfolio.

- **Tecnológicos:** Costes asociados a la implantación de tecnologías de eficiencia energética en activos existentes para cumplir con los estándares de eficiencia requeridos (retrofitting); incertidumbre sobre el coste y disponibilidad de tecnologías de almacenamiento energético que soporten el autoconsumo fotovoltaico del Grupo.

- **Reputacionales**: Percepción negativa de inversores, analistas de sostenibilidad o agencias de rating ESG ante insuficiente avance en los objetivos del Plan "Camino a Neto Cero" del Grupo o ante discrepancias entre los compromisos declarados y el desempeño real de los activos.

El Grupo MERLIN realizará, con periodicidad mínima bienal (coincidiendo con la actualización de su estrategia de sostenibilidad), un análisis de escenarios climáticos orientado a evaluar la resiliencia del portfolio de activos y del modelo de negocio del Grupo ante diferentes trayectorias de cambio climático.

Los resultados del análisis de escenarios se integrarán en el Mapa de Riesgos Corporativo, bajo la categoría (g) de riesgos climáticos y de sostenibilidad, y se reportarán al Consejo de Administración como parte de la revisión anual del Sistema de Gestión de Riesgos. Adicionalmente, los resultados del análisis serán la base del Anexo TCFD que el Grupo publica en su Estado de Información No Financiera, asegurando la coherencia entre el reporte externo y la gestión interna del riesgo climático.

La gestión de riesgos de sostenibilidad establecida en la presente sección se articulará de forma coherente con la estrategia "**Camino a Neto Cero**" del Grupo, garantizando que:

- **Los objetivos de reducción de emisiones del Grupo, validados por la Science Based Targets initiative (SBTi), se reflejan en el Mapa de Riesgos** como objetivos estratégicos cuyo incumplimiento constituye un riesgo de reputación y de mercado.

- **Las oportunidades asociadas a la transición energética serán evaluadas sistemáticamente** como contrapartida a los riesgos identificados, en aplicación del enfoque de gestión del binomio riesgo-oportunidad establecido en la sección 2 de la presente Política.

- **El reporte externo de riesgos climáticos conforme a la metodología TCFD (publicado en el Anexo IV del EINF del Grupo) reflejará fielmente los resultados de la gestión interna** establecida en la presente sección, asegurando la coherencia entre la información publicada y el Sistema de Gestión de Riesgos del Grupo.

Respecto a los riesgos de sostenibilidad, la **Comisión de Auditoría y Control**, se encargará de la supervisión de la efectividad del proceso de identificación y evaluación de riesgos de sostenibilidad, de la revisión semestral de los KRIs de sostenibilidad, de la aprobación del análisis de escenarios TCFD para su publicación en el EINF y de la coordinación con la Comisión de Sostenibilidad e Innovación.

Por su parte, la **Comisión de Sostenibilidad e Innovación**, será la responsable de la supervisión de la estrategia de sostenibilidad del Grupo y su coherencia con el Sistema de Gestión de Riesgos, de la revisión trimestral de los KRIs de sostenibilidad, del seguimiento del plan de actualización de los objetivos climáticos y de la supervisión del reporte TCFD.

## 11. Supervisión Global del Sistema de Control y Gestión del riesgo

El Grupo MERLIN dispone de un **Sistema de Gestión de Riesgos** fundamentado en un enfoque integral y sistemático. Este sistema está concebido como una herramienta clave en la gestión de la incertidumbre, y como tal, el objetivo es ayudar a reducir las amenazas y

a aprovechar las oportunidades que puedan surgir en los negocios de la Sociedad y su Grupo.

El Sistema de Gestión de Riesgos del Grupo MERLIN tiene por objeto minimizar la volatilidad de la rentabilidad y, por tanto, maximizar el valor económico del Grupo, incorporando el riesgo y la incertidumbre en el proceso de toma de decisiones para proporcionar una seguridad razonable en la consecución de los objetivos estratégicos establecidos, aportando a los accionistas, a otros grupos de interés y al mercado en general un nivel de garantías adecuado que asegure la protección del valor generado.

Para el desarrollo del control y la gestión de los riesgos, el Consejo de Administración cuenta con la colaboración de la Comisión de Auditoría y Control que supervisa e informa sobre la adecuación y eficacia del sistema de control y gestión de riesgos.

**La Comisión de Auditoría y Control es el órgano encargado de supervisar el sistema de control y gestión de riesgos (incluyendo los controles internos) de la Sociedad y comprobar su adecuación e integridad.**

Para la supervisión de los riesgos medioambientales, sociales y de gobernanza, la Comisión de Auditoría se coordinará con las Comisiones de Sostenibilidad e Innovación, así como con la Comisión de Nombramientos y Retribuciones.

Así, la Comisión de Auditoría y Control lleva a cabo esta función de supervisión a través de la Dirección de Auditoría Interna, quien comprueba con periodicidad anual la adecuación e integridad del Sistema de Gestión de Riesgos implantado por la Dirección de la Compañía.

A partir del análisis de la Visión, valores y estrategia de MERLIN se realiza un análisis de los distintos componentes, según la agrupación de los distintos objetivos estratégicos que se engloban en dichos elementos (ser la SOCIMI de referencia, creación de valor a largo plazo, generación de dividendo sostenible y creciente, valores de transparencia, ética y responsabilidad).

En este sentido, los riesgos que MERLIN identifica y evalúa se clasifican, tal y como se muestra a continuación:

a) **Riesgos de gobernanza y de estrategia**: riesgos derivados de un eventual incumplimiento de lo dispuesto por los sistemas de gobernanza del Grupo, así como los riesgos asociados al entorno macroeconómico, geopolítico y social, y a las decisiones de inversión y desinversión.

b) **Riesgos de negocio y mercado**: riesgos relacionados con variables clave intrínsecas a las distintas actividades del Grupo, a través de los distintas ramas de actividad sus negocios, como la gestión de los ciclos inmobiliarios de cada rama de actividad del Grupo, así como la

incertidumbre generada por la volatilidad del nivel de ocupación de los activos, fluctuación del nivel de rentas, concentración de rentas, pérdida de valor de los inmuebles de los activos inmobiliarios que componen cada rama de actividad del Grupo.

c) **Riesgos de crédito y financieros**: riesgos relacionados con la posibilidad de que una contraparte incumpla sus obligaciones contractuales y ocasione una pérdida económica o financiera, incluyendo los riesgos y costes de sustitución, así como los relativos a la volatilidad de los tipos de interés, la inflación y aquellos relacionados con la solvencia y la liquidez.

d) **Riesgos regulatorios, fiscales y legales**: así como los provenientes de cambios regulatorios o en la normativa fiscal del régimen SOCIMI.

e) **Riesgos operacionales**: riesgos referidos a las pérdidas económicas, directas o indirectas, ocasionadas por eventos externos, errores o procesos internos inadecuados, así como los que afecten a la capacidad de dar una respuesta adecuada ante eventos de cualquier naturaleza que afecten a la continuidad de los procesos prioritarios.

f) **Riesgos tecnológicos y de seguridad de la información**: riesgos relacionados con la gestión y el funcionamiento apropiado de las tecnologías de la información, así como los motivados por la adopción de nuevas tecnologías, incluyendo la inteligencia artificial. Incluye, también, los riesgos relacionados con la seguridad de los sistemas de información, incluyendo la ciberseguridad, así como de la privacidad de los datos personales tratados y el cumplimiento de la normativa relacionada.

g) **Riesgos climáticos y de sostenibilidad:** incluyendo los daños directos causados por fenómenos meteorológicos extremos (como inundaciones, sequías, olas de calor, etc.), así como la necesidad de adaptarse a nuevas normativas ambientales, exigencias de eficiencia energética y expectativas crecientes de inversores y clientes en materia de sostenibilidad.

Considerando la naturaleza multidimensional de los riesgos, la taxonomía incorpora variables de clasificación adicionales que facilitan su seguimiento, control y reporte. Entre estas variables se incluyen los riesgos emergentes, definidos como amenazas nuevas, cuyo impacto es incierto y cuya probabilidad resulta indefinida, pero que presentan una tendencia creciente y podrían adquirir relevancia significativa para las sociedades que integran el Grupo.

La Dirección de MERLIN desarrolla la presente Política de Control y Gestión de Riesgos a través de su **Sistema de Gestión de Riesgos** el cual desarrolla aspectos tales como las responsabilidades en la organización o el proceso interno de Gestión de los Riesgos identificados en el Mapa de Riesgos Corporativo Anual.

## 12. Comunicación de la Política y concienciación

La Política de Control y Gestión de Riesgos será puesta a disposición de todos los grupos de interés de la Compañía, tanto a nivel interno como externo mediante su **publicación en la página web corporativa** y será objeto de las adecuadas acciones de comunicación para su oportuna comprensión y puesta en práctica en toda la organización.

De manera adicional a la comunicación y como refuerzo de la cultura de gestión de riesgos en la organización, la Dirección de MERLIN estructurará un **Programa Anual de Cultura de Riesgos** con: (i) formación obligatoria diferenciada por nivel jerárquico; (ii) métricas de seguimiento; (iii) comunicaciones periódicas sobre el estado del sistema de riesgos; y (iv) una encuesta anual de cultura de riesgos para medir la madurez percibida. Los resultados de dicho programa se reportarán anualmente a la Comisión de Auditoría y Control.

## 13. Aprobación y actualización

El Consejo de Administración de MERLIN Properties SOCIMI, S.A. tiene atribuida la facultad de aprobar de las políticas y estrategias generales de la Sociedad.

La Política de Control y Gestión de Riesgos, de acuerdo con el artículo 9 del Reglamento de la Comisión de Auditoría y Control, se revisará periódicamente, para asegurar que recoge las recomendaciones y mejores prácticas internacionales en vigor en cada momento, y procediendo a su modificación cuando se produzcan variaciones en dicha materia que sugieran una revisión extraordinaria fuera del ciclo anual, tales como: materialización de un riesgo crítico, cambio regulatorio de impacto significativo, una adquisición o desinversión relevante, cambios en el entorno macroeconómico o geopolítico, o recomendación del auditor externo, entre otros.

La Dirección de Auditoría Interna será el encargado de presentar una propuesta de modificación a la Comisión de Auditoría y Control para que la eleve al Consejo de Administración para su aprobación.

**********

**Esta política fue inicialmente aprobada por el Consejo de Administración en febrero de 2016, posteriormente en abril de 2018, marzo 2019, marzo de 2021, abril 2022, abril 2025 y finalmente en su redacción actual en junio de 2026.**