

## —ADHESIÓN A LAS GUÍAS DE AUTORREGULACIÓN

Mutua Madrileña está adscrita de forma voluntaria y sigue las recomendaciones contenidas en las Guías de autorregulación de UNESPA que regulan aspectos vinculados tanto al gobierno de las sociedades, como a la relación con clientes, entre otros, con el objetivo de desarrollar y promover negocios responsables y sostenibles. Algunas de las guías que seguimos son las siguientes:

- ◉ Guía de buen gobierno de las entidades aseguradoras.
- ◉ Guía de buenas prácticas en materia de seguros Individuales de Vida Ahorro.
- ◉ Guía de buenas prácticas en los procesos de suscripción de seguros de vida por parte de personas con VIH.
- ◉ Guía de buenas prácticas en el uso terminológico utilizado en el documento de información de productos de seguros No Vida.
- ◉ Guía de buenas prácticas en materia de seguros individuales de Vida Riesgo.
- ◉ Guía de buenas prácticas: principios sobre el tratamiento de datos de tomadores del seguro en pólizas intervenidas por corredor de seguro.
- ◉ Guía de buenas prácticas para el tratamiento de los datos personales por las entidades aseguradoras.
- ◉ Guía de buenas prácticas sobre la aplicación del derecho al olvido oncológico a los seguros contratados antes del 30 de junio de 2023.
- ◉ Guía de buenas prácticas del seguro de automóvil.
- ◉ Guía de buenas prácticas en materia de información previa a la contratación de los seguros multirriesgo.

## —SISTEMAS DE PREVENCIÓN Y CONTROL INTERNO

### Gestión de riesgos

Mutua Madrileña cuenta con un Sistema de Gestión de Riesgos cuyo objetivo es controlar y gestionar las amenazas a las que está o podría verse expuesta la compañía, debido a las actividades propias de su negocio. Las responsabilidades sobre la gestión de riesgos recaen fundamentalmente en los siguientes órganos:

— Consejo de Administración

— Comisión de Auditoría y Cumplimiento

— Comisión Delegada de Inversiones

— Comité de Dirección

— Comité de Riesgos

— Funciones clave

— Unidades de negocio

» Los riesgos se gestionan de forma integral mediante un Sistema de Control Interno basado en las tres líneas de defensa, combinando políticas, comités y órganos especializados.

## Modelo de tres líneas de defensa

Nuestro Sistema de Gestión de Riesgos se estructura en base al modelo de las “tres líneas de defensa”:

1—

**La primera línea** de defensa se encuentra en las áreas de negocio y soporte (propietarias de los procesos cuyas actividades se ven expuestas a los riesgos).

2—

**La segunda línea**, constituida, entre otras, por las Funciones de Control de Riesgos, Cumplimiento Normativo y Función Actuarial. Velan porque los riesgos se gestionen de acuerdo con el apetito por el riesgo y los límites establecidos, fomentan una sólida cultura de riesgos en toda la organización y facilitan herramientas y juicio experto en aquellas materias relevantes sobre los riesgos.

3—

**La tercera línea**, Auditoría Interna, comprueba la adecuación y eficacia del sistema de control interno y de otros elementos del sistema de gobierno.

Este modelo de “tres líneas de defensa” está sustentado por la existencia de unas políticas de gestión de riesgos que establecen las directrices que deben seguir todas las unidades de negocio, operaciones, funciones y, en general, todo el personal del grupo.

Estas políticas han sido aprobadas por el Consejo de Administración y se actualizan con una periodicidad mínima anual. De acuerdo con nuestra actividad, realizamos una clasificación de los principales riesgos a los que está expuesta nuestra compañía.

## Clasificación de riesgos

⦿ **Riesgos técnicos y financieros establecidos en la normativa de Solvencia II o relacionados con la misma.**

⦿ **Riesgos operacionales y de cumplimiento normativo.**

⦿ **Otros riesgos globales o de entorno**

— Riesgos ambientales, sociales y de gobernanza (ASG/ESG)

— Riesgo estratégico

— Riesgo reputacional

— Riesgos derivados de las decisiones de la compañía

— Riesgos emergentes

— Riesgos macroeconómicos



## GESTIÓN Y MITIGACIÓN

Para todos los riesgos identificados se revisan de forma periódica los mecanismos para su gestión y mitigación y contamos con diferentes sistemas de control interno y de riesgos.

Además de las áreas de negocio y de soporte, en las que se originan los riesgos, y de las funciones clave, el Sistema de Control Interno lo componen un conjunto de sistemas, funciones y unidades especializadas y comités que en su globalidad permiten, siguiendo la definición de control interno, obtener seguridad razonable sobre las operaciones, la información financiera y no financiera, los objetivos estratégicos de la compañía y el cumplimiento de las leyes y procedimientos internos aplicables.

## SISTEMAS, FUNCIONES Y COMITÉS DE CONTROL



### Sistemas de gestión de riesgos

- ⦿ Sistema de Gestión del Riesgo Operacional
- ⦿ Sistema de Gestión de la Continuidad de Negocio
- ⦿ Sistema de Gestión de Seguridad de la información (incluye riesgos cibernéticos)
- ⦿ Sistema de Gestión de Riesgos Tecnológicos
- ⦿ Sistema de Control Interno de la Información Financiera
- ⦿ Sistema de Cumplimiento Fiscal
- ⦿ Sistema de Prevención del Blanqueo de Capitales y Financiación del Terrorismo
- ⦿ Sistema de Prevención de Riesgos Penales y Anticorrupción
- ⦿ Sistema de Gestión de la Privacidad
- ⦿ Sistema de Gestión de la Seguridad y Salud en el trabajo



### Funciones y unidades de control especializadas

- ⦿ Subdirección General de Control de Riesgos
- ⦿ Dirección de Regulación
- ⦿ Función de Verificación del Cumplimiento Normativo
- ⦿ Función Actuarial
- ⦿ Función de Auditoría Interna
- ⦿ Calidad Call Center
- ⦿ Control de Calidad y Procesos
- ⦿ Gestión del Fraude de Negocio
- ⦿ Red de Peritos e Inspectores
- ⦿ Seguridad Física
- ⦿ Unidad de Gestión de Reclamaciones
- ⦿ Gestión de Procesos
- ⦿ Departamento de compras y gestión de proveedores
- ⦿ Área de Delivery Office de Tecnología
- ⦿ CISO y Seguridad IT
- ⦿ Subdirección General de Datos y Analítica Avanzada
- ⦿ Prevención de Riesgos Laborales y Medioambiente
- ⦿ Asesoría Jurídica de Negocio
- ⦿ Control de Gestión
- ⦿ Dirección de la Estrategia y Desarrollo corporativo



### Comités de control

- ⦿ Comité de Gobernanza del Producto
- ⦿ Comité de Autorizaciones y Apoderamientos
- ⦿ Comité de Riesgos
- ⦿ Comité de Seguridad de la Información y Riesgos Tecnológicos
- ⦿ Comité de Reservas y Suscripción
- ⦿ Comité de Riesgos Financieros
- ⦿ Subcomité de Riesgos
- ⦿ Comité de Inteligencia Artificial
- ⦿ Comité de Cumplimiento Normativo
- ⦿ Comité de Prevención de Riesgos Penales
- ⦿ Comité de Prevención de Blanqueo de Capitales y Financiación del Terrorismo
- ⦿ Comité de Control de Protección de Datos



## —SISTEMA DE GESTIÓN DEL RIESGO DE PREVENCIÓN DEL BLANQUEO DE CAPITALES Y FINANCIACIÓN DEL TERRORISMO

La entidad cuenta con un Sistema de Prevención del Blanqueo de Capitales y Financiación del Terrorismo que tiene por objetivo establecer las reglas y procedimientos necesarios para el cumplimiento de aquello que se establece en la normativa española en materia de prevención del blanqueo de capitales y financiación del terrorismo.

Este sistema también impide que los sujetos del grupo puedan ser utilizados en la financiación del terrorismo u otras actividades delictivas. Para ello, también cuenta con una política que establece los principios para garantizar la implantación de un sistema de supervisión integrado dentro del sistema de control interno del Grupo, determinándose las responsabilidades, competencias y deberes de información, así como sus procesos y procedimientos.

» Establecemos responsabilidades, competencias y procedimientos para supervisar y proteger las operaciones del Grupo.

## Función de cumplimiento normativo

La Función de cumplimiento normativo comprende el asesoramiento al órgano de administración acerca del cumplimiento de las disposiciones legales, reglamentarias y administrativas que afecten a la entidad, así como acerca del cumplimiento de su normativa interna. Comporta, asimismo, la evaluación del impacto de cualquier modificación del entorno legal en las operaciones de la entidad y la determinación y evaluación del riesgo de cumplimiento.

De esta manera, la Función de cumplimiento se define como una función independiente que, a través de políticas y procedimientos adecuados, detecta y gestiona el riesgo de incumplimiento de las obligaciones regulatorias, tanto externas como internas de diferentes entidades.

La Función de cumplimiento normativo se rige por su propia política, que tiene por objetivo establecer las responsabilidades, competencias y deberes de información, así como sus procesos y procedimientos necesarios para llevar a cabo su labor.

## —SISTEMA DE PREVENCIÓN DE RIESGOS PENALES Y ANTICORRUPCIÓN



El objetivo del Sistema de Prevención de Riesgos Penales y anticorrupción de Mutua Madrileña es prevenir situaciones que puedan desembocar en responsabilidades legales o afectar al estado financiero, patrimonial y reputacional de la compañía.

Nuestro sistema sigue la Norma UNE 19601 y la ISO 37001 antisoborno. En 2018, obtuvo la indicada certificación tras realizarse la correspondiente auditoría del sistema por parte de la entidad certificadora designada. En 2025, se ha sometido a la auditoría de recertificación conforme a la UNE 19601 con resultado favorable. Asimismo, en 2024 se certificó su modelo conforme a la ISO 37001 antisoborno y en 2025, se ha sometido a la primera auditoría de seguimiento, con resultado favorable. El objetivo del Sistema de Prevención de Riesgos Penales y Anticorrupción de Mutua Madrileña es prevenir situaciones que puedan desembocar en responsabilidades legales o afectar al estado financiero, patrimonial y reputacional de la compañía.

El modelo se sustenta, entre otros elementos, en una política que describe el alcance del sistema, una relación de los riesgos penales identificados, un conjunto de procedimientos, protocolos de actuación definidos y un sistema disciplinario en caso de incumplimiento.

El sistema se basa en los principios de prevención, control, denuncia y reparación e integra y coordina el conjunto de actuaciones necesarias para prevenir y combatir la posible comisión de actos ilícitos, generando un entorno de transparencia e integrando los diferentes sistemas desarrollados para la prevención de delitos.

» Los canales de denuncia y las políticas internas son los pilares que refuerzan la prevención de riesgos penales y anticorrupción.

Los elementos esenciales del sistema de cumplimiento pivotan sobre los siguientes elementos:

- Comité de Prevención de Riesgos Penales
- Política del Sistema Interno de Información
- Política de evaluación del desempeño
- Política de prevención de riesgos penales
- Sistema disciplinario
- Política Anticorrupción
- Guía Anticorrupción
- Protocolo para la prevención de riesgos penales
- Código de conducta ética para empleados
- Cláusulas de compromiso ético con proveedores
- Código de conducta de proveedores
- Canal de denuncias de la entidad, que está gestionado por una entidad externa de reconocido prestigio para garantizar la independencia en su gestión. Está disponible a través de: [www.grupomutua.es/informacion-corporativa/transparencia-etica/](http://www.grupomutua.es/informacion-corporativa/transparencia-etica/)

