POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

ÍNDICE

1. INTRODUCCIÓN

El Consejo de Administración de Técnicas Reunidas, S.A. ("**Técnicas Reunidas**" o la "**Sociedad**") en su condición de sociedad cotizada, tiene legalmente atribuida como facultad indelegable la determinación de las políticas y estrategias generales de la Sociedad y del Grupo del que es entidad dominante ("**Grupo TR**" o "**Grupo**"), facultad que ha sido recogida asimismo en el Reglamento del Consejo de Administración.

Técnicas Reunidas y las sociedades que forman parte del Grupo tienen el compromiso de proteger la información como uno de sus activos más importantes, garantizando la seguridad de los Sistemas y Redes de Información en las que se apoyan los diferentes procesos de negocio, con el fin de reforzar su Resiliencia Operativa Digital, alineando sus prácticas con la normativa vigente que resulte de aplicación, así como con sus valores corporativos.

En este sentido, la estrategia y objetivos de seguridad que persigue el Grupo TR tienen como objetivo el desarrollo e implantación de las máximas capacidades en materia de Seguridad de la Información, con el fin de reducir las amenazas para los Sistemas y Redes de Información utilizados para prestar los servicios, teniendo en cuenta, en particular, su presencia en sectores críticos como el desarrollo de infraestructuras sostenibles y plantas para la creación de energías renovables, de modo que sus productos y servicios generen beneficios sostenibles y se alineen con los más altos estándares éticos y legales.

De conformidad con los objetivos referidos, el Consejo de Administración de Técnicas Reunidas ha aprobado la presente *Política de Seguridad de la Información* (la "**Política**") que forma parte del Sistema de Gestión de Seguridad de la Información (el "**SGSI**"), se proyecta sobre el Grupo TR y se integra en el Sistema de Gobernanza de la Sociedad.

2. DEFINICIONES

A los efectos de la presente Política, se deberán tener en cuenta las siguientes definiciones:

- **Comité de Seguridad de la Información, Privacidad e Inteligencia Artificial**: Comité de composición interdisciplinar con responsabilidades de supervisión y regulación para adoptar cualquier resolución, con relevancia en materia de Seguridad de la Información en la organización de Grupo TR, con el objetivo de garantizar que las medidas para la Gestión de Riesgos en la seguridad de los Sistemas y Redes de Información sean idóneas y que su implementación esté alineada con los valores, políticas y regulaciones que se proyectan sobre el Grupo TR en las distintas jurisdicciones en que está presente.

- **Seguridad de la Información**: todas las actividades que integran una correcta Gestión de Riesgos para asegurar la protección de los Sistemas y Redes de Información, de los Usuarios de tales sistemas y de otras personas que puedan verse afectadas por las Ciberamenazas en el Grupo TR.

- **Responsable de Seguridad de la Información (CISO)**: miembro del Comité de Seguridad de la Información, Privacidad e Inteligencia Artificial, y responsable en materia de Seguridad de la Información.

- **Director de Sistemas, Seguridad y Comunicaciones (CIO)**: miembro del Comité de Seguridad de la Información, Privacidad e Inteligencia Artificial en su condición de Director de Sistemas, Seguridad y Comunicaciones, y responsable en materia de seguridad de los Sistemas y Redes de Información.

- **Gestión de Riesgos**: actividades coordinadas para dirigir y controlar en Grupo TR los riesgos identificados.

- **Gestión de Incidentes**: conjunto de medidas y procedimientos destinados a prevenir, detectar, analizar y limitar un Incidente, resolviéndose e incorporando medidas de desempeño que permitan conocer la calidad del sistema de protección y detectar tendencias antes de que se conviertan en grandes problemas.

- **Incidente de Seguridad de la Información o *Ciberincidente***: suceso inesperado o no deseado que pueda comprometer la disponibilidad, autenticidad, trazabilidad, integridad o confidencialidad de los datos almacenados, transmitidos o tratados, o los servicios ofrecidos, por Sistemas y Redes de Información, o accesibles a través de ellos.

- **Profesional**: los miembros de los órganos de administración, directivos, trabajadores, colaboradores, estudiantes en prácticas y becarios, con independencia de cuál sea la modalidad jurídica que determine su relación laboral o de servicios, su nivel jerárquico, su ubicación geográfica o funcional y de la sociedad del Grupo TR para la que presten sus servicios.

- **Responsable(s)**: directores, mandos intermedios o cualquier otra persona con responsabilidad para tomar decisiones en materia de Seguridad de la Información.

- **Resiliencia Operativa Digital**: la capacidad del Grupo TR para construir, asegurar y revisar su integridad y fiabilidad operativas garantizando, directa, o indirectamente a través del uso de servicios prestados por proveedores terceros de servicios de tecnologías de la información y comunicaciones, toda la gama de capacidades relacionadas con las TIC necesarias para preservar la seguridad de los Sistemas y Redes de Información que utiliza el Grupo TR y que sustentan la prestación continuada de servicios y su calidad, incluso en caso de perturbaciones.

- **Sistema de Gestión de Seguridad de la Información (SGSI)**: conjunto de políticas y procedimientos de seguridad de la información que tratan de componer un sistema de organización y gestión, diseñado para implantar, mantener y mejorar dichas políticas y procedimientos, cuya base es la *Política de Seguridad de la Información* del Grupo TR. El SGSI trata de asegurar la

confidencialidad, integridad y disponibilidad de los activos de información, minimizando a la vez los riesgos de seguridad de la Información teniendo en cuenta los riesgos analizados dentro de los procesos de negocio.

- **Sistemas y Redes de Información**: conjunto organizado de personas, procesos y herramientas que se utilizan para recolectar, procesar, almacenar y distribuir información. Estos sistemas permiten que los datos sean fácilmente accesibles y utilizables para tomar decisiones, gestionar operaciones y apoyar actividades organizativas.

- **Tecnologías de la Información y Comunicación ("TIC")**: conjunto organizado de personas, procesos y herramientas que se utilizan para recolectar, procesar, almacenar y distribuir información.

- **Usuario**: cualquier persona vinculada a una sociedad del Grupo TR por una relación civil o mercantil, así como clientes, proveedores, subcontratistas, consultores o cualesquiera otras personas o entidades a los que se autorice a utilizar, custodiar o acceder a los Sistemas y Redes de Información del Grupo TR.

- **Vulnerabilidad**: cualquier debilidad, susceptibilidad o defecto de un activo, sistema, proceso o control que puede ser explotado.

Salvo que se disponga expresamente lo contrario en cualquier apartado de la presente Política, las definiciones en singular incluyen el plural y viceversa.

3. OBJETO Y ALCANCE

La presente Política tiene por objeto establecer los principios básicos y las reglas generales que permitan a Técnicas Reunidas, con proyección sobre las sociedades del Grupo, desarrollar las estrategias, tecnologías, procedimientos y estándares de Seguridad de la Información para mantener un elevado nivel de Resiliencia Operativa Digital, enmarcándose dentro del SGSI , fortaleciendo el marco operativo y de control adecuado, alineados con los objetivos de negocio, para la gestión de la Seguridad de la Información del Grupo TR de manera que permitan a las empresas del Grupo cumplir su objeto social, todo ello de conformidad con la normativa vigente, así como con los valores corporativos del Grupo.

Sin perjuicio de lo dispuesto en el párrafo anterior, en aquellas sociedades participadas en las que esta Política no sea de aplicación, Técnicas Reunidas promoverá en lo posible, a través de sus representantes en sus órganos de administración, el alineamiento de sus políticas propias con las de Técnicas Reunidas, en el marco en todo caso del respeto a la autonomía de decisión de las sociedades participadas.

Además, esta Política resultará también aplicable, en lo que proceda, a las uniones temporales de empresas, *joint ventures* y otras asociaciones equivalentes, ya sean estas nacionales o extranjeras, cuando cualesquiera de las sociedades que integran el Grupo TR tengan el control de su gestión y siempre dentro de los límites legalmente establecidos.

4. PRINCIPIOS GENERALES DE ACTUACIÓN

El Grupo TR entiende la Seguridad de la Información como un elemento fundamental para proteger los activos de negocio, considerándola como un proceso integral basado en gestión y control de riesgos con el fin de lograr sus objetivos y cumplir con su misión. En este sentido, Técnicas Reunidas se compromete a dotar a las diferentes áreas del Grupo de todos los recursos técnicos, humanos, materiales y organizativos necesarios para garantizar una adecuada gestión de la seguridad de los Sistemas y Redes de Información del Grupo TR.

De conformidad con lo anterior, todos los Profesionales y Usuarios del Grupo TR, deberán respetar y guiar su actuación con base en los siguientes principios:

I. **Definición, desarrollo y mantenimiento**: para alcanzar los objetivos, valores, estrategia y compromisos adquiridos, la Sociedad promoverá la definición, el desarrollo y la conservación de los controles técnicos, legales y de administración de la Seguridad de la Información incorporados en el SGSI esenciales para asegurar en todo momento el cumplimiento de las exigencias legales, reglamentarias y contractuales pertinentes en el asunto que sea relevante.

II. **Promoción de una cultura de Seguridad de la Información**: Técnicas Reunidas asume el compromiso de impulsar activamente una cultura de Seguridad de la Información entre todos sus Profesionales y Usuarios, tanto internamente como entre sus clientes y proveedores.

III. **Gestión diaria:** conlleva la obligación del Grupo TR de salvaguardar la seguridad de los Sistemas y Redes de Información, elaborando estrategias de seguridad sólidas, acordes con las demandas de los distintos interesados, así como con la legislación actual en vigor en el tema. Para ello, Técnicas Reunidas validará las políticas y/o procedimientos específicos por área que establecerán los principios y requerimientos fundamentales de seguridad de la información y Seguridad de la Información establecidos.

IV. **Protección proactiva**: de tal forma que se mantenga de manera activa la protección de los niveles definidos de privacidad, disponibilidad, autenticidad, seguimiento e integridad para proteger sus activos de información y garantizar la Resiliencia Operativa Digital del Grupo TR.

V. **Mejora continua**: comprendiendo la Seguridad de la Información como un pilar fundamental en todos los sectores y procesos empresariales, con el objetivo de alcanzar un avance constante en todos los procesos relacionados con el SGSI y la administración de la seguridad de los Sistemas y Redes de Información, con el fin de fortalecer la fiabilidad de la relación con todos los involucrados y/o potenciar la reputación positiva del Grupo TR.

5. REQUISITOS BÁSICOS DE SEGURIDAD DE LA INFORMACIÓN

Para llevar a cabo la gestión diaria de la seguridad y Seguridad de la Información, se procederá siempre conforme a los siguientes requisitos básicos:

- **Prevención, detección, respuesta y conservación.**

  Se definirán, registrarán e implementarán procesos, políticas y/o procedimientos para la prevención y administración de Incidentes de Seguridad de la Información, asegurando que sean conocidos por todos los Profesionales del Grupo TR y otros sujetos vinculados a esta Política, con el fin de identificar, examinar, contener o reaccionar ante Incidentes, recuperarse de estos, registrarlos y notificarlos a tiempo.

- **Diferenciación de responsabilidades.**

  Se definirán de manera precisa las tareas y obligaciones relacionadas con la Seguridad de la Información, para que todos los Profesionales del Grupo TR y otros sujetos vinculados a esta Política, las entiendan y conozcan.

- **Análisis y gestión de los riesgos y vulnerabilidades.**
  Se llevarán a cabo y registrarán evaluaciones de riesgos basándose en una monitorización continuada, conforme a la metodología de análisis de riesgos interna aprobada por Grupo TR, revisándose estas de forma regular tomando siempre como referencia los niveles de riesgo del análisis anterior.
  Igualmente, se llevarán a cabo periódicamente escaneos para detectar vulnerabilidades en los Sistemas y Redes de Información que puedan ser potencialmente explotadas. A partir de los resultados, se definirá, implementará y supervisará un plan de Gestión de Riesgos y vulnerabilidades.

- **Gestión del personal.**

  Todos los Profesionales y, en caso de ser necesario, los demás sujetos vinculados a esta Política entenderán y asumirán sus obligaciones en relación con la Seguridad de la Información. Por otro lado, se implementarán programas de concienciación y capacitación, para que todos los Profesionales, incluyendo a los integrantes de los órganos directivos, junto con los proveedores directos y proveedores de servicios, y otras personas sujetas a esta Política estén concienciados de la relevancia de la Seguridad de la Información y adopten las prácticas de ciberhigiene recomendadas.

- **Autorización y control de los accesos.**

  Se deberán establecer, documentar y aplicar procedimientos y/o políticas de control de acceso lógico y físico, gestionando los derechos de acceso a los Sistemas y Redes de Información, así como a las instalaciones físicas, sobre la base del principio de mínimo privilegio.

- **Protección de las instalaciones.**

  Se implementarán controles y acciones para prevenir la pérdida, el perjuicio o la afectación de las instalaciones donde se ubican los Sistemas y Redes de Información

y otros activos, además de la interrupción de sus operaciones a causa de la falla o la interrupción de los servicios de soporte.

- **Integridad y actualización.**

  Se establecerán y aplicarán procesos para establecer los requisitos relativos a las actualizaciones de seguridad aplicables a los Sistemas y Redes de Información durante su vida útil.

- **Protección de la Información almacenada y en tránsito.**

  Se establecerán, implantarán y aplicarán los controles oportunos, con vistas a garantizar un uso adecuado y eficaz de la criptografía para proteger la confidencialidad, autenticidad e integridad de la información, tanto almacenada como en tránsito, en consonancia con la clasificación de activos y los resultados de la evaluación de riesgos realizada.

- **Segmentación de red.**

  Se implementarán acciones para segmentar los Sistemas o Redes de Información en redes o áreas (tanto los propios como los suministrados por terceros).

- **Registro de la actividad y detección de código dañino.**

  Se implementarán procesos y se emplearán instrumentos para monitorear y documentar las actividades en los Sistemas y Redes de Información del Grupo TR, con el objetivo de identificar eventos que puedan clasificarse como Incidentes y actuar de la manera que corresponda para atenuar su efecto, asegurando que los hallazgos de estas evaluaciones sean considerados en los procesos de aprendizaje y mejora.

- **Continuidad de la actividad.**

  Se definirá un plan de continuidad de la actividad y de recuperación ante catástrofes - que se mantendrá actualizado - para activarse en situaciones de Incidentes, que incluya, entre otros aspectos, condiciones para su activación, contactos esenciales, funciones y responsabilidades, y recursos requeridos. El objetivo es asegurar que las operaciones se reincorporan conforme a este plan, así como la continuidad del negocio en el Grupo TR.

- **Seguridad en la cadena de suministro.**

  Se implementarán y ejecutarán procedimientos y/o políticas de seguridad en la cadena de suministro que establezcan los criterios de homologación y supervisión de las relaciones con los proveedores, así como las acciones y los controles adecuados para minimizar los riesgos provenientes de estos terceros para la protección de los Sistemas y Redes de Información del Grupo TR.

El Grupo TR establecerá procedimientos específicos para que todos los Profesionales y las partes interesadas conozcan, comprenda y cumplan con la Política y toda su normativa de desarrollo.

En este sentido, toda la documentación de Seguridad de la Información que se desarrolle en ejecución de los mencionados principios y que se integrará junto con la presente

Política en el SGSI, se gestiona, estructura y conserva conforme a los procedimientos documentados que el Grupo TR ha desarrollado teniendo en cuenta la normativa, así como los estándares nacionales e internacionales que resulten aplicables en cada caso.

6. GOBERNANZA

La gobernanza de la Seguridad de la Información en el Grupo TR es esencial para gestionar y mitigar potenciales riesgos, para garantizar la toma de decisiones en función del riesgo real de la materialización de las amenazas sobre la organización, así como para la continuidad de las operaciones de negocio, siendo la presente Política una herramienta fundamental para la adecuada gestión y gobernanza de la Seguridad de la Información.

6.1. EL CONSEJO DE ADMINISTRACIÓN Y SUS COMISIONES

Corresponde al Consejo de Administración de Técnicas Reunidas el establecimiento de la estrategia y directrices de gestión del Grupo TR en materia de Seguridad de la Información, a través de la presente Política y, en su caso, de otras normas corporativas en desarrollo de la misma.

A su vez, es competencia de la Comisión de Auditoría y Control, velar por la implementación y desarrollo de la presente Política y de las medidas adoptadas en aplicación de la misma, así como revisar, y en su caso, proponer al Consejo de Administración la actualización de la presente Política.

Asimismo, corresponde a la Comisión de Auditoría y Control la supervisión de la eficacia de los sistemas de control y Gestión de Riesgos en materia de Seguridad de la Información de la Sociedad y su Grupo, así como del reporte acerca de los mismos.

Para el ejercicio de sus funciones de supervisión, la Comisión de Auditoría y Control recibirá periódicamente del Comité de Seguridad de la Información, Privacidad e Inteligencia Artificial, a través del Responsable de Seguridad de la Información, con apoyo del Director de Sistemas, Seguridad y Comunicaciones, información sobre la gestión desarrollada por el Comité de Seguridad de la Información, Privacidad e Inteligencia Artificial.

6.2. EL COMITÉ DE SEGURIDAD DE LA INFORMACIÓN, PRIVACIDAD E INTELIGENCIA ARTIFICAL

6.2.1. Principios de actuación

Técnicas Reunidas, a través del Responsable de Seguridad de la Información y del Director de Sistemas, Seguridad y Comunicaciones, que contarán con el apoyo del Comité de Seguridad de la Información, Privacidad e Inteligencia Artificial, observará y promoverá en el Grupo TR los siguientes principios en relación con la gobernanza de la Seguridad de la Información:

a) **Principio de alineamiento estratégico y visión de futuro**: se considerará la Seguridad de la Información como una parte más del negocio, entendiéndose como una herramienta que ayuda al Grupo TR a alcanzar sus objetivos, alineada con la misión y perspectiva del Grupo. En consecuencia, el Comité de Seguridad de la Información, Privacidad e Inteligencia Artificial impulsará en el Grupo TR un enfoque holístico con el fin de que la Seguridad de la Información no sea considerada como un obstáculo, sino como una herramienta más, imprescindible para el desarrollo de su negocio.

b) **Principio de ética y cumplimiento**: el gobierno de la Seguridad de la Información en el Grupo TR, deberá no solo enfocarse en el cumplimiento de la normativa establecida, sino también en las buenas prácticas de seguridad y el uso ético de los recursos del Grupo.

c) **Principio de responsabilidad y rendición de cuentas**: la Seguridad de la Información es un campo interdisciplinario y complejo que impacta en todas las operaciones de una entidad. Por lo tanto, necesita de un liderazgo apropiado y una estructura que, para ser establecida y administrada correctamente, debe estar conformada por profesionales con la formación y experiencia idóneas.

   El Comité de Seguridad de la Información, Privacidad e Inteligencia Artificial se encargará de establecer, fomentar y regular la Seguridad de la Información, además de participar en la toma de decisiones y estrategias en este campo. Además, el Comité de Seguridad de la Información, Privacidad e Inteligencia Artificial asumirá la responsabilidad de proporcionar un informe periódico apropiado y a los niveles adecuados, sobre los riesgos asociados a la Seguridad de la Información, junto con los mecanismos de mitigación y control que sean requeridos.

6.2.2. Composición y funciones del Comité de Seguridad de la Información, Privacidad e Inteligencia Artificial

El Comité de Seguridad de la Información, Privacidad e Inteligencia Artificial actuará como instancia de apoyo al Responsable de Seguridad de la Información y al Director de Sistemas, Seguridad y Comunicaciones para el desarrollo de sus funciones.

Al Comité de Seguridad de la Información, Privacidad e Inteligencia Artificial, con carácter adicional a cualesquiera otras funciones que se le atribuyen, le corresponderá:

- Revisar la presente Política, asegurando que cumple con la normativa aplicable y los principios éticos de Técnicas Reunidas, así como con las mejores prácticas del sector. En este sentido, cuando lo considere conveniente, podrá elevar propuestas de modificación de la presente Política al Consejo de Administración para su aprobación.

- Revisar y promover la mejora continua del SGSI de Técnicas Reunidas, incluyendo en su caso, la identificación y evaluación de nuevos riesgos asociados al SGSI.

- Coordinar los planes de continuidad de las diferentes áreas de Técnicas Reunidas para asegurar una actuación sin fisuras en el caso de que deban ser activados.

- Resolver los conflictos de responsabilidad que puedan aparecer entre los diferentes Responsables y/o entre diferentes áreas de Técnicas Reunidas, elevando aquellos casos en los que no tenga suficiente autoridad para decidir.

- Informar regularmente a la alta dirección y diferentes áreas de Técnicas Reunidas en relación con medidas de seguridad y control adoptadas, recomendando posibles actuaciones al respecto.

- Coordinar y monitorizar el desempeño de los procesos de gestión de Ciberincidentes.

- Promover procesos de auditorías periódicas para verificar el cumplimiento de la normativa aplicable.

- Promover la formación y el desarrollo de habilidades relacionadas con la Seguridad de la Información, así como prácticas básicas de ciberhigiene, en Técnicas Reunidas.

- Velar por el cumplimiento de la normativa de aplicación.

- Aprobar procedimientos, normas o protocolos internos dirigidos al desarrollo e implementación de la presente Política en Técnicas Reunidas.

- Hacer el seguimiento del desarrollo de estas funciones por los órganos o instancias correspondientes de las sociedades del Grupo TR con la finalidad de supervisar la implementación de los principios y compromisos que inspiran la presente Política, pudiendo recabar de las mismas cuanta información considere para el cumplimiento de esta función de coordinación a nivel de Grupo.

7. SEGUIMIENTO, INTERPRETACIÓN Y REVISIÓN

7.1. SEGUIMIENTO

El cumplimiento de esta Política será supervisado por el Comité de Seguridad de la Información, Privacidad e Inteligencia Artificial. Se establecerán mecanismos de auditoría y revisión periódica de las medidas establecidas en ejecución de la presente Política.

Es responsabilidad de todos los Usuarios y Profesionales leer y comprender el contenido de esta Política, así como observar y cumplir sus directrices, principios y procesos en el desarrollo de su trabajo, en la medida en que la comprensión y adherencia a las

definiciones y principios establecidos en la Política es fundamental para mantener un SGSI sólido.

El seguimiento y medición de la efectividad de las medidas que desarrollen los principios y reglas generales de la presente Política se ejecutará de conformidad con las políticas y/o procedimientos internos de objetivos e indicadores de revisión que Técnicas Reunidas apruebe internamente.

Corresponderá al Departamento de Seguridad de la Información establecer los indicadores de Seguridad de la Información a los que se les deberá dar seguimiento durante el año, y que se deberán analizar como mínimo en la revisión del sistema por la Dirección del Área de Sistemas de Información, Comunicaciones y Seguridad, dejando constancia en el acta de la misma.

Con base en los resultados de estas mediciones, así como de los resultados de auditorías de Seguridad de la Información, Ciberincidentes gestionados, vulnerabilidades detectadas y retroalimentación de las partes interesadas, se procederá a la revisión regular de las medidas de Seguridad de la Información establecidas con motivo del desarrollo de la presente Política integrándose en el marco de la revisión regular del SGSI.

7.2. INTERPRETACIÓN

El órgano de contacto para cualquier duda y/o consulta en relación con la interpretación y ejecución de la presente Política será el Comité de Seguridad de la Información, Privacidad e Inteligencia Artificial, que podrá ser contactado por los cauces habilitados al efecto.

7.3. REVISIÓN Y ACTUALIZACIÓN

Esta Política será revisada y actualizada al menos una vez al año, en el marco de la revisión anual del SGSI que se lleve a cabo por la Sociedad, y siempre que se produzcan Incidentes significativos o cambios importantes en las operaciones o los riesgos, para asegurar su eficacia y adecuación a los avances tecnológicos y cambios regulatorios, organizativos, técnicos y de procesos del Grupo TR, así como para incorporar las mejores prácticas identificadas en materia de Seguridad de la Información.

La modificación y/o actualización de la presente Política será aprobada por el Consejo de Administración de Técnicas Reunidas, previo informe de la Comisión de Auditoría y Control, y se difundirá a los Profesionales y Usuarios a través de los canales habituales.

8. DIFUSIÓN DE LA POLÍTICA

Esta Política se publicará en la página web corporativa de Técnicas Reunidas con el consiguiente conocimiento y asunción de su contenido íntegro por parte de los Profesionales y Usuarios.

Sin perjuicio de ello, Técnicas Reunidas llevará a cabo acciones de comunicación, formación y sensibilización para la comprensión y puesta en práctica de esta Política, así como de sus actualizaciones.

En todo caso, se recomienda acceder de forma periódica al contenido de esta Política a través de los canales disponibles para una mejor comprensión de la misma, debiendo tenerse en cuenta que el desconocimiento de todo o parte de su contenido no exime de su cumplimiento.

9. ENTRADA EN VIGOR

La presente Política fue aprobada por el Consejo de Administración de Técnicas Reunidas en su reunión de fecha 10 de abril de 2025, entrando en vigor desde el momento de su publicación en la página web corporativa de la Sociedad el 15 de abril de 2025.