Política de gestión del sistema interno de información de Bewater Asset Management SGEIC, SA

Versión 01/12/2024

Emisor: Cumplimiento Normativo

Cumplimiento Normativo: Director de Cumplimiento Normativo

Órgano de aprobación: Consejo de Administración

Contenido

0. Registro de actualizaciones

Versión	Fecha de elaboración	Fecha de aprobación	Descripción de la revisión
1	01/12/2024	11/12/2024	Versión inicial

1. Introducción

1.1. Antecedentes

El 21 de febrero de 2023 se publicó en el Boletín Oficial del Estado la Ley 2/2023, de 20 de febrero, reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción. Con la aprobación de esta ley se incorpora al Derecho español la Directiva (UE) 2019/1937 del Parlamento y del Consejo, de 23 de octubre de 2019, relativa a la protección de las personas que informen sobre infracciones del Derecho de la Unión.

La referida Ley 2/2023, de conformidad con la Directiva, tiene como finalidad la protección de las personas que en un contexto laboral o profesional detecten determinadas infracciones normativas y lo comuniquen a través de los canales internos de información que deberán habilitarse al respecto, otorgando una protección adecuada frente a cualquier tipo de represalias.

1.2. Objeto

La presente política tiene por objeto incluir dentro del marco normativo general ya existente en Bewater Asset Management SGEIC, SA, en adelante (en adelante, "Bewater" o "la Entidad"), las nuevas disposiciones normativas legales en materia de protección de las personas informantes.

1.3. Normativa de referencia

- Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal y sus posteriores modificaciones.
- Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo.
- Ley Orgánica 5/2010, de 22 de junio, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.
- Circular 1/2011 de la Fiscalía General del Estado, de 1 de junio, relativa a la responsabilidad penal de las personas jurídicas conforme a la reforma del Código Penal efectuada por Ley Orgánica número 5/2010.
- Circular 1/2016 de la Fiscalía General del Estado sobre la responsabilidad penal de la persona jurídica conforme a la reforma del Código Penal efectuada por LO 1/2015.
- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril del 2016 (RGPD) relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).
- Real Decreto-ley 11/2018, de 31 de agosto, de transposición de directivas en materia de prevención del blanqueo de capitales.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPD).

- Directiva (UE) 2019/1937 del Parlamento Europeo y del Consejo, de 23 de octubre de 2019, relativa a la protección de las personas que informen sobre infracciones del Derecho de la Unión.
- Ley 2/2023, de 20 de febrero, reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción.
- 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.
- Real Decreto 1101/2024, de 29 de octubre, por el que se aprueba el Estatuto de la Autoridad Independiente de Protección del Informante, A.A.I.
- Guía de la AEPD sobre la protección de datos en las relaciones laborales.

Adicionalmente, esta política tiene en cuenta otros estándares nacionales e internacionales en la materia, como es la Norma ISO 37002 de Sistemas de Gestión de la denuncia de canales de denuncia

2. Alcance

La presente política recoge el marco normativo de funcionamiento y gestión del sistema interno de información de Bewater y se aplica a todos los trabajadores, directivos, consejeros y demás personas relacionadas con la Entidad. El cumplimiento de la normativa es responsabilidad de todos y cada uno de los miembros de la organización y en este sentido, de acuerdo con el Código Ético, concurre el deber de informar sobre cualquier hecho conocido que pueda constituir delito, fraude e irregularidad.

3. Objetivo

De acuerdo con los principios de ética empresarial de Bewater (Código de Ética y Conducta), aprobados por el Consejo de Administración de Bewater Asset Management SGEIC, SA, todos los colaboradores de la Entidad tienen la obligación de actuar con integridad, transparencia, compromiso y respeto hacia la legislación y las normativas internas. Asimismo, tienen la responsabilidad de colaborar para prevenir que cualquier miembro de Bewater actúe de manera indebida o poco ética, fomentando activamente la comunicación de posibles irregularidades o incumplimientos.

En conformidad con la Directiva (UE) 2019/1937 del Parlamento Europeo y del Consejo, del 23 de octubre de 2019, sobre la protección de los denunciantes de infracciones del Derecho de la Unión y la Ley 2/2023, de 20 de febrero, reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción; Bewater ha establecido un canal de denuncias que cumple con las normativas específicas correspondientes para permitir que, cualquier persona que quiera informar sobre conductas de carácter ilícito o irregular, pueda hacerlo sabiendo que se encontrará protegido frente a represalias

El objetivo último es fomentar la transparencia, ética y responsabilidad, a través de la promoción de una cultura de integridad y prevención de la corrupción.

4. Principios generales

- El sistema interno de información se configura como una herramienta clave para fomentar una cultura sólida de información y comunicación, y actúa como componente esencial en la

prevención, detección y corrección de posibles amenazas al interés público y de incumplimientos normativos.

- El sistema interno de información refuerza el marco de supervisión del riesgo de integridad y simplifica el cumplimiento, tanto del Código Ético en general, como de las normativas internas específicas.
- Todos los trabajadores, directivos y consejeros de Bewater tienen la responsabilidad de informar sobre cualquier posible irregularidad o conducta contraria a la legalidad o a las normas internas que conozcan. Solo de esta manera será posible investigar cualquier sospecha o duda acerca de posibles irregularidades o incumplimientos, y en caso necesario, tomar las medidas apropiadas para corregir sus consecuencias y evitar la repetición de dichas irregularidades en el futuro. Esto contribuirá a mejorar el entorno profesional, social, ético y el compromiso con el cumplimiento de leyes y normativas de Bewater.

Esta política se complementa con los criterios de gestión detallados en el Procedimiento de Gestión del Sistema Interno de Información de Bewater Asset Management SGEIC, SA (en adelante, el "Procedimiento de gestión del sistema interno de información de Bewater ") y demás normativa de desarrollo.

5. Principios específicos

Los principios específicos sobre los que se articula el sistema interno de información son los siguientes:

- Compromiso de los órganos de gobierno: El Consejo de Administración de Bewater es el responsable de la implantación del sistema interno de información a través de la aprobación de esta Política y del Procedimiento de gestión. Mediante la presente Política, el máximo órgano de gobierno pone de manifiesto su compromiso con respecto a su dimensión y relevancia.

- Independencia y autonomía: Dentro del sistema interno de información de la Entidad, la responsabilidad del sistema recae en el Comité de Defensa Corporativa, quien desempeña sus funciones de manera independiente y autónoma en comparación con otros órganos de la Entidad. Además, cuenta con todos los recursos personales y materiales necesarios para llevar a cabo sus tareas de manera efectiva.
  Con el fin de garantizar la objetividad de sus decisiones, el Comité de Defensa Corporativa opera bajo el principio de independencia funcional con respecto al resto de áreas.
  Todos los individuos que participan en la gestión del sistema interno de información poseen los conocimientos, experiencia, cualificaciones y requisitos de integridad profesional necesarios para cumplir adecuadamente con sus responsabilidades.

- Integración de canales: El sistema interno de información de Bewater , se integra dentro del sistema interno de información de Indexa Capital Group SA, lo que permite garantizar el cumplimiento de los estándares y garantías de gestión en todos ellos. Los accesos se encuentran publicitados en los entornos internos y en la página web corporativa o en la página web de sus filiales en los casos que fuese necesario.

- Buena fe: Todas las comunicaciones transmitidas a través del sistema de información deben realizarse con integridad y sinceridad. Se considerarán como comunicaciones deshonestas aquellas que se efectúen con el propósito de suplantar la identidad del informante o proporcionar información falsa o engañosa sobre hechos conocidos como inciertos, así como implicar a individuos que no están relacionados con dichos eventos, incluso si estos son verdaderos.
  La presentación de una comunicación falsa o deshonesta resultará en la aplicación de las medidas legales o disciplinarias correspondientes contra la persona responsable de tal acción. Además, de acuerdo con la legislación vigente, podría constituir un delito.

- Conservación de los registros: Todas las denuncias y consultas que se reciban a través del sistema interno de información, las contestaciones que se den a la persona denunciante, toda la documentación que se genere en la investigación, entrevistas, etc. serán conservados en el registro del sistema interno de información de la Entidad de acuerdo con lo dispuesto en la normativa aplicable en materia de protección de datos personales y durante el tiempo estrictamente necesario a los efectos de desarrollar la investigación o para aplicar las medidas oportunas a los efectos de defender los intereses de la Entidad. En caso de que los hechos denunciados hubieran resultado probados, en ningún caso podrán conservarse los datos por un período superior a diez (10) años.
  Los datos de quien formule la comunicación y de los trabajadore y terceros deberán conservarse en el sistema interno de información únicamente durante el tiempo imprescindible para decidir sobre la procedencia de iniciar una investigación sobre los hechos denunciados.
  Si se acreditara que la información facilitada o parte de ella no es veraz, deberá procederse a su inmediata supresión desde el momento en que se tenga constancia de dicha circunstancia, salvo que dicha falta de veracidad pueda constituir un ilícito penal, en cuyo caso se guardará la información por el tiempo necesario durante el que se tramite el procedimiento judicial.
  En todo caso, transcurridos tres (3) meses desde la introducción de los datos sin que se hubiesen iniciado actuaciones de investigación, deberá procederse a su supresión, salvo que la finalidad de la conservación sea dejar evidencia del funcionamiento del sistema interno de información. En tal caso, las comunicaciones a las que no se haya dado curso solamente podrán constar de forma anonimizada, sin que sea de aplicación la obligación de bloqueo prevista en el artículo 32 de la Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales.
  Transcurrido el plazo mencionado en el párrafo anterior, los datos podrán seguir siendo tratados por el órgano al que corresponda para la investigación de los hechos denunciados, no conservándose en el propio sistema interno de información.

6. Medidas de protección al informante

El sistema interno de comunicación de Bewater otorga las siguientes garantías:

- Confidencialidad: La preservación de la confidencialidad emerge como un principio fundamental que orienta todas las actividades dentro del ámbito de gestión del sistema interno de información.

El sistema ha sido diseñado, establecido y operado de manera segura para asegurar la confidencialidad de la identidad de los informantes y terceros mencionados en las comunicaciones, así como de las acciones llevadas a cabo en la gestión y procesamiento de estas, incluyendo la protección de datos personales.
El acceso a la información está limitado únicamente a aquellas personas autorizadas conforme a las responsabilidades asignadas, quedando terminantemente prohibida la divulgación de cualquier tipo de información relacionada con las comunicaciones.

- Medidas de protección al informante: Para garantizar el cumplimiento de este principio, se adoptarán las medidas que sean necesarias para garantizar la protección del informante. Por ello, se prohíben expresamente los actos constitutivos de represalia, incluidas las amenazas de represalia y las tentativas de represalia contra las personas que presenten una comunicación conforme a lo previsto en el "Procedimiento del Sistema Interno de Información" como por ejemplo suspensión del contrato de trabajo, despido o extinción de la relación laboral o estatutaria, incluyendo la no renovación o la terminación anticipada de un contrato de trabajo temporal una vez superado el periodo de prueba. Es decir, las personas que denuncien posibles infracciones tendrán derecho a protección siempre que tengan motivos razonables para pensar que la información referida es veraz en el momento de la comunicación o revelación, aun cuando no aporten pruebas concluyentes.
  Se entiende por represalia cualesquiera actos u omisiones que estén prohibidos por la ley, o que, de forma directa o indirecta, supongan un trato desfavorable que sitúe a las personas que las sufren en desventaja particular con respecto a otra en el contexto laboral o profesional, sólo por su condición de informantes, o por haber realizado una revelación pública. Se exceptúa el supuesto en que dicha acción u omisión pueda justificarse objetivamente en atención a una finalidad legítima y que los medios para alcanzar dicha finalidad sean necesarios y adecuados.
- A los efectos del artículo 36.3 de la Ley 2/2023, de 20 de febrero se consideran represalias:
  a. Suspensión del contrato de trabajo, despido o extinción de la relación laboral o estatutaria, incluyendo la no renovación o la terminación anticipada de un contrato de trabajo temporal una vez superado el período de prueba, o terminación anticipada o anulación de contratos de bienes o servicios, imposición de cualquier medida disciplinaria, degradación o denegación de ascensos y cualquier otra modificación sustancial de las condiciones de trabajo y la no conversión de un contrato de trabajo temporal en uno indefinido, en caso de que el trabajador tuviera expectativas legítimas de que se le ofrecería un trabajo indefinido; salvo que estas medidas se llevaran a cabo dentro del ejercicio regular del poder de dirección al amparo de la legislación laboral o reguladora del estatuto del empleado público correspondiente, por circunstancias, hechos o infracciones acreditadas, y ajenas a la presentación de la comunicación.
  b. Daños, incluidos los de carácter reputacional, o pérdidas económicas, coacciones, intimidaciones, acoso u ostracismo.
  c. Evaluación o referencias negativas respecto al desempeño laboral o profesional.

d. Inclusión en listas negras o difusión de información en un determinado ámbito sectorial, que dificulten o impidan el acceso al empleo o la contratación de obras o servicios.
e. Denegación o anulación de una licencia o permiso.
f. Denegación de formación.
g. Discriminación, o trato desfavorable o injusto.

-

El denunciante que viera lesionados sus derechos por causa de su comunicación una vez transcurrido el plazo de dos (2) años, podrá solicitar la protección de la autoridad competente que, excepcionalmente y de forma justificada, podrá extender el periodo de protección, previa audiencia de las personas u órganos que pudieran verse afectados.

- Anonimato y no rastreabilidad: Las comunicaciones enviadas al sistema interno de información pueden ser tanto nominativas, es decir, con identificación del informante, como anónimas. Bewater mantiene un firme compromiso con el respeto a la anonimidad cuando esta sea la opción elegida por el informante. Queda prohibido el rastreo y trazabilidad de las comunicaciones anónimas. La vulneración de este extremo supondrá la adopción de las medidas disciplinarias correspondientes.

- Derechos de las personas afectadas: Se asegura el principio de presunción de inocencia y se respeta el honor de las personas implicadas, así como su derecho a ser escuchadas. Aquellas personas que puedan estar involucradas en una investigación interna tienen el derecho de ser informadas sobre la comunicación presentada en su contra tan pronto como se hayan realizado las verificaciones pertinentes, se haya iniciado el procedimiento y se considere apropiado para asegurar el éxito de la investigación.
  El momento en el que se informe a la persona investigada variará según las circunstancias de cada caso. Se procurará informar a la persona investigada tan pronto como sea posible, pero siempre persiguiendo el objetivo de conservar las pruebas evitando su alteración o destrucción por parte del denunciado.
  En los casos en los que el responsable del sistema interno de información considere que existe el riesgo de que la persona investigada pueda alterar o destruir pruebas relacionadas con los hechos denunciados, o bien la información al denunciante pueda suponer una obstaculización de los logros de la eventual investigación, de conformidad con las excepciones del artículo 14.5 RGPD, y siempre a criterio del responsable del sistema interno de información, podrán evitar comunicar dicha información al denunciante hasta el momento del trámite de audiencia.
  Asimismo, de acuerdo con lo exigido por la normativa aplicable en materia de protección de datos, el denunciante podrá ejercer sus derechos de acceso, rectificación, supresión y oposición, limitación del tratamiento y portabilidad obtenidos a través de este sistema poniéndose en contacto a través del correo electrónico del delegado de protección de datos (dpo@bewaterfunds.com.).

7. Grupos de interés

Los grupos con acceso al sistema interno de información de la Entidad son los siguientes:

- Trabajadores, directivos y miembros de los órganos de gobierno de Bewater .

- Proveedores y personas que trabajen para o bajo su supervisión
- Accionistas
- Ex - trabajadores y candidatos a un puesto de trabajo

Cabe mencionar que las "medidas de protección al informante" serán de aplicación, en su caso, a las siguientes personas:

- Los representantes legales de las personas trabajadoras en el ejercicio de sus funciones de asesoramiento y apoyo al informante.
- Personas físicas que, en el marco de la organización en la que preste servicios el informante, asistan al mismo en el proceso.
- Personas físicas que estén relacionadas con el informante y que puedan sufrir represalias, como compañeros de trabajo o familiares del informante.
- Personas jurídicas, para las que trabaje o con las que mantengan cualquier otro tipo de relación en un contexto laboral o en las que ostente una participación significativa.

8. Deber de comunicar posibles actividades y actos ilícitos

Todos los trabajadores, directivos, consejeros y demás personas relacionadas con la Entidad, que trabajen para o bajo su supervisión, así como los accionistas, ex - trabajadores y candidatos a un puesto de trabajo, están obligados a comunicar a Bewater Asset Management SGEIC, SA los hechos de los que tuvieran conocimiento y que se refieran o afecten al ámbito de las actividades de la Entidad o al desempeño de sus funciones profesionales y que pudieran constituir una posible irregularidad o actuación contraria a lo previsto en los Principios de la Entidad, a la legalidad o a cualquier normativa interna y, en particular, que pudieran ser constitutivas de una presunta infracción penal o administrativa, grave o muy grave.

9. Marco de gobierno

Los Órganos de Gobierno de Bewater , realizan determinadas funciones asociadas a su responsabilidad de aprobación y supervisión de las directrices estratégicas y de gestión establecidas en interés de la Entidad, así como de supervisión, seguimiento y control integrado de los riesgos de esta.

10. Marco de gestión

El marco de gestión se encuentra detallado en el "Procedimiento de Gestión del sistema interno de información de Bewater Asset Management SGEIC, SA", que deberá ser aprobado por el Consejo de Administración de Bewater y cuyos principales aspectos se detallan en la *web* corporativa, el cual establece las previsiones necesarias para que el sistema interno de información cumpla con los requisitos definidos legalmente. El procedimiento prevé la participación de diferentes áreas que garantizan la preservación de la autonomía e independencia en todas las fases del proceso.

11. Marco de control

El marco de control interno de Bewater se vertebra según el modelo de "Tres Líneas de Defensa", que garantiza la estricta segregación de funciones y la existencia de varias capas de control independiente.

El modelo de Tres Líneas de Defensa se articula de forma que las funciones de control interno de la Entidad desempeñan su misión con una visión consolidada. Así, la Dirección de cumplimiento

normativo y gestión de riesgos y la función delegada de Auditoría Interna, como áreas responsables, respectivamente, de las funciones de cumplimiento y auditoría Interna, asumen la orientación estratégica, la supervisión y la coordinación con respecto a las respectivas funciones de control interno, salvaguardando al mismo tiempo el ámbito propio de estas.

12. Marco de información

El responsable del sistema interno de información, designado por el consejo de administración podrá:

- Solicitar la información necesaria para garantizar el cumplimiento de las disposiciones legales en las diferentes áreas, en el marco de la organización en la que preste servicios el informante, asistan al mismo en el proceso.
- Facilitará de forma periódica información relevante sobre el sistema de información interno a los órganos de gobierno y a la alta dirección.

13. Tratamiento de datos personales

Los datos personales que pueden llegar a tratarse en el curso de un expediente dentro del procedimiento del sistema interno de información serán tratados con la máxima confidencialidad y en cumplimiento de la normativa aplicable en materia de protección de datos. El responsable del tratamiento de dichos datos es Bewater Asset Management SGEIC, SA, con domicilio en Calle Serrano, 213, planta 1, B1, 28016 Madrid.

La finalidad del tratamiento de datos personales del Canal de Denuncias es la de gestionar la denuncia y/o comunicación de una conducta irregular cuando el usuario desee informar sobre sospechas de conductas irregulares, actos ilícitos o incumplimientos normativos y, en su caso, investigar la realidad de los hechos objeto de la comunicación y/o denuncia.

El tratamiento de datos personales realizado en el marco del sistema interno de información se realiza sobre la base del artículo 6.1.c) del RGPD (cumplimiento de obligaciones legales). Adicionalmente, el tratamiento de categorías especiales de datos que se produzca en el marco del sistema queda amparado por la excepción del artículo 9.2. g) RGPD (razones de interés público esencial).

La normativa aplicable en España establece la obligatoriedad de establecer canales de comunicación y reconocen en estos una excelente herramienta para la prevención de delitos de forma eficaz, incluyendo como destinatarios a la totalidad de sujetos de la empresa (trabajadores, directivos, etc.) como parte del control interno de esta en materia de gestión de riesgos. En particular:

- La Ley 2/2023, de 20 de febrero, reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción.
- El Código Penal establece en su artículo 31 bis 2. 4º la “obligación de informar de posibles riesgos e incumplimientos al organismo encargado de vigilar el funcionamiento y la observancia del modelo de prevención.” De manera implícita, las empresas deben proporcionar un canal a través del cual se pueda enviar la información.
- La Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo establece en su artículo 26.bis la obligación de los sujetos obligados a establecer procedimientos para que sus empleados, directivos puedan comunicar, incluso

anónimamente, información relevante sobre posibles incumplimientos de esa ley, su normativa de desarrollo o las políticas y procedimientos implantados.

Los datos personales que se tratarán por Bewater , en el sistema interno de información son los siguientes:

- Nombre y datos de contacto del informante, en caso de que se trate de una denuncia no anónima. El informante puede también identificarse voluntariamente en un momento posterior a la interposición de la denuncia o aportar en un momento posterior del proceso documentación o información adicional.
- Información facilitada tanto en el momento de la denuncia como durante toda la tramitación del expediente.
- Nombre y otros datos personales de las personas que menciona la denuncia (supuesto infractor, posibles testigos y otros), en el caso de que se proporcione dicha información.

Bewater puede obtener datos directamente del denunciante como de terceros (ej. testigos, investigado, áreas de Bewater , informes periciales o policiales), así como a través de los documentos facilitados o relacionados con el hecho denunciado y de los recursos tecnológicos de la información asignados al informante y denunciado, incluyendo, con carácter no limitativo, su correo corporativo, así como cualesquiera otros recursos informáticos suministrados por la Entidad.

Únicamente las personas indicadas en el apartado 9 de la presente Política, así como los encargados del tratamiento que eventualmente se designen, podrán tener acceso, dentro del ámbito de sus competencias y funciones, a los datos personales contenidos en el sistema interno de información.

Los plazos de conservación de los datos personales incluidos dentro del sistema interno de información se encuentran recogidos en el apartado de “conservación de los registros” de la presente política.

Los interesados pueden ejercitar sus derechos de acceso, rectificación, supresión, oposición, limitación del tratamiento y portabilidad, respecto del tratamiento del que es responsable Bewater mediante escrito dirigido a la propia Entidad, a la dirección postal Calle Serrano, 213, planta 1, B1, 28016 Madrid, acreditando su identidad o bien por correo electrónico a la dirección electrónica: info@bewaterfunds.com. El ejercicio del derecho de acceso por parte del denunciado no supone, en ningún caso, el acceso a los datos relativos a la identidad del informante ni a otros datos personales de terceros obrantes en el expediente.

Los interesados también pueden presentar reclamaciones ante la Agencia Española de Protección de Datos.

Para cualquier información adicional, Bewater cuenta con un Delegado de Protección de Datos que se encarga de supervisar el cumplimiento de la normativa aplicable en materia de protección de datos, con quien tanto los interesados como otros terceros pueden contactar a través de la dirección de correo electrónico dpo@bewaterfunds.com.

14. Publicidad

Sin perjuicio de la obligación que tienen los trabajadores de conocer y actuar de conformidad con lo dispuesto en la Normativa Interna, en el desempeño de sus funciones, se promoverá y velará

por la debida difusión de esta Política y de la existencia del Canal de Denuncias. Con el objetivo de lograr una mayor difusión, la presente Política ha sido publicada en la página *web* corporativa, y en la propia intranet de la Entidad.

15. Actualización

Esta Política se someterá a revisión del Consejo de Administración cada tres años. No obstante, el equipo de cumplimiento normativo y gestión de riesgos, como responsable de la política, revisará su contenido anualmente y, en caso de que lo estime pertinente, propondrá modificaciones que elevará para su aprobación por el Consejo de Administración.

La presente Política está a disposición de todos los profesionales y trabajadores de la Entidad, así como de socios de negocio y terceros, mediante su publicación en un apartado separado y fácilmente identificable de la página *web* corporativa de Bewater Asset Management SGEIC, SA, proporcionando una información adecuada y suficiente sobre los distintos aspectos de esta Política.