

POLÍTICA DEL SISTEMA INTERNO DE INFORMACIÓN Y CANAL ÉTICO DE BEWOR TECH, S.L.

INFORMACIÓN GENERAL

Control Documental

Clasificación de seguridad: Público
Versión: 1.0.
Fecha edición: 27.07.2026
Fichero: 01_Política_SII_Bewor_v1.0.pdf
Código: 01_Pol-SII
Estado formal
Preparado por: Responsable de Cumplimiento (miembro del RSII)
Revisado por: Directora Operaciones (miembro del RSII)
Aprobado por: Administrador Solidario

Control de Versiones

Versión	Partes que cambian	Descripción cambio	Autor Cambio	Fecha de Cambio
1.0	Original	Creación documento	Responsable de Cumplimiento	27.07.2026

1.- Objeto y finalidad del Sistema Interno de Información

La presente Política tiene por objeto regular el funcionamiento del Sistema Interno de Información y del canal interno de información (en adelante, el “Canal” o el “Canal Ético”) de BEWOR TECH, S.L. (en adelante, “BEWOR” o “la Sociedad”), como cauce preferente para comunicar, de forma segura y confidencial, información sobre acciones u omisiones que puedan constituir infracciones incluidas en el ámbito de aplicación de 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 (en adelante, “Ley 2/2023” o “LPI”). El Canal se integra en el Sistema Interno de Información de la entidad (en adelante, “el Sistema” o “SI”), y su diseño se orienta a proteger frente a represalias a las personas informantes, a reforzar la cultura de la información y a facilitar la detección temprana de amenazas al interés público, preservando en todo momento los derechos de las personas afectadas y el cumplimiento de las exigencias de protección de datos.

BEWOR queda sujeta a la obligación de disponer de un Sistema Interno de Información en virtud del artículo 10.1.a) de la Ley 2/2023, por superar el umbral de cincuenta trabajadores en España, sin que le resulte de aplicación ningún régimen sectorial específico adicional de los previstos en el artículo 10.1.b) de la misma Ley.

2.- Ámbito material de las comunicaciones admisibles

A través del Canal podrán comunicarse hechos o conductas que, en un contexto laboral o profesional, puedan constituir: (i) infracciones del Derecho de la Unión Europea dentro de las materias contempladas por la normativa aplicable; o (ii) infracciones penales o administrativas graves o muy graves del ordenamiento español, incluyendo, en todo caso, aquellas que impliquen quebranto económico para la Hacienda Pública o para la Seguridad Social. Quedan fuera del ámbito de protección específico del régimen de protección al informante las comunicaciones relativas a materias excluidas por la normativa, y, en particular, las que afecten a información clasificada o a ámbitos amparados por secreto profesional y deberes de confidencialidad en los términos legalmente previstos.

3.- Ámbito personal: quién puede comunicar y quién queda protegido

Podrán presentar comunicaciones, entre otros, quienes hayan obtenido información sobre infracciones en un contexto laboral o profesional, incluyendo personal empleado, personas trabajadoras autónomas, socios y personas integrantes del órgano de administración, así como quienes trabajen para o bajo la supervisión de contratistas, subcontratistas y proveedores de BEWOR. También podrán comunicar información quienes mantengan o hayan mantenido relaciones profesionales o laborales con la Sociedad (incluidas personas candidatas en procesos de selección cuando la información se haya obtenido en ese contexto). Asimismo, podrán quedar amparadas por medidas de protección determinadas personas vinculadas con el informante (representantes legales de las personas trabajadoras, personas que asistan al informante, familiares o compañeros) y determinadas personas jurídicas vinculadas al informante, conforme a lo previsto en la normativa aplicable.

4.- Principios rectores del Canal

El Canal se regirá por los principios de independencia, confidencialidad, diligencia, accesibilidad y seguridad, asegurando que: (i) la identidad del informante se preserva y no se revela a terceras personas, salvo en los supuestos legalmente previstos; (ii) se impide el acceso a la información por personal no autorizado; (iii) se respetan la presunción de inocencia, el honor y el derecho de defensa de las personas afectadas; y (iv) se tramitan las comunicaciones de manera efectiva y en plazos razonables, con posibilidad de mantener la comunicación con el informante para solicitar información adicional cuando resulte necesario.

5.- Canales habilitados y modalidades de presentación

El Canal permite realizar comunicaciones por escrito y verbalmente, a través de las siguientes vías habilitadas:

- *Vía escrita — formulario web*: formulario disponible en el apartado de cumplimiento de la página web corporativa de BEWOR.
- *Vía verbal — teléfono*: línea de teléfono móvil dedicada, gestionada directamente por el Responsable del Sistema.
- *Vía verbal — reunión presencial*: a solicitud del informante, a celebrar en un plazo máximo de siete días desde la solicitud.

En los casos en que la comunicación verbal sea grabada o transcrita, se advertirá previamente al informante y se le informará sobre el tratamiento de sus datos personales, conforme a lo previsto en el apartado 11 siguiente.

6.- Comunicaciones anónimas y preservación reforzada de la identidad

El Canal permite la presentación y posterior tramitación de comunicaciones anónimas. Incluso cuando el informante se identifique, el Sistema cuenta con medidas técnicas y organizativas para preservar su identidad y garantizar la confidencialidad de los datos de las personas afectadas y de cualquier tercero mencionado. La identidad del informante solo podrá comunicarse, con carácter excepcional y limitado a lo estrictamente necesario:

- i) a la autoridad judicial, al Ministerio Fiscal o a la autoridad administrativa competente, en el marco de una investigación penal, disciplinaria o sancionadora;
- ii) al personal interno de BEWOR o a asesores externos que intervengan en la tramitación del expediente, cuando resulte imprescindible y debidamente justificado para la adopción de medidas disciplinarias, legales, cautelares o de protección frente a represalias, limitándose en todo caso la información facilitada a la estrictamente necesaria para dicha finalidad, con las salvaguardas legalmente previstas.

Estas garantías se desarrollan en detalle en el Protocolo de Seguridad, Confidencialidad y Control de Accesos del Sistema, que concreta los perfiles internos autorizados a este acceso excepcional y las reglas bajo las que se podrá compartir el expediente.

7.- Información al informante sobre canales externos

BEWOR pondrá a disposición de las personas usuarias del Canal, de forma clara y accesible, información sobre la existencia de canales externos ante las autoridades competentes (la Autoridad Independiente de Protección del Informante (AIPI) y, en su caso, la autoridad autonómica competente) y, cuando proceda, ante instituciones, órganos u organismos de la Unión Europea. Esta información se facilitará junto con los principios esenciales del procedimiento de gestión del Canal y el régimen de confidencialidad y protección de datos aplicable, publicándose en el apartado de cumplimiento de la página web corporativa.

Adicionalmente, y sin que ello resulte exigido por la Ley 2/2023, BEWOR informa de que, en su condición de prestador de servicios de confianza cualificado conforme al Reglamento (UE) n.º 910/2014 (eIDAS), las cuestiones relativas a certificados cualificados y a la prestación de servicios de confianza pueden asimismo comunicarse a la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales. Se advierte expresamente que estas comunicaciones quedan fuera del ámbito de protección específico dispensado por el régimen de protección al informante de la Ley 2/2023, salvo que los hechos comunicados encajen, además, en el ámbito material definido en el apartado 2 de esta Política.

8.- Responsable del Sistema Interno de Información y garantías de independencia

El órgano de administración de BEWOR ha designado como Responsable del Sistema Interno de Información (RSII), en su modalidad de órgano colegiado conforme al artículo 8 de la Ley 2/2023, a:

- **Dña. Patricia Bodelón Álvarez**, Directora de Operaciones (COO), a quien corresponde la representación institucional del Sistema y la interlocución con terceros.
- **Dña. Noemí Vique Fernández**, Compliance & Risk Manager, en quien se delegan expresamente las facultades de gestión ordinaria, tramitación de expedientes e instrucción de las comunicaciones recibidas.

Ambos miembros del órgano colegiado ejercen sus funciones con plena independencia y autonomía respecto del resto de órganos de la Sociedad, sin recibir instrucciones de ningún tipo en el ejercicio de las mismas, y garantizando en todo momento la ausencia de conflictos de interés.

En caso de que una comunicación afectase a uno de los miembros del órgano colegiado, este se abstendrá de intervenir en su tramitación, asumiendo la instrucción el otro miembro en exclusiva. En ese supuesto, la persona informante podrá dirigir su comunicación directamente al correo electrónico profesional de la persona no afectada por el conflicto de interés, dado que el correo electrónico del Canal al que llegan las Comunicaciones resulta accesible para ambos miembros del órgano colegiado:

-Dña. Patricia Bodelón: pbodelon@bework.com

-Dña. Noemí Vique: nvique@legal.bework.com

El Delegado de Protección de Datos de BEWOR, de carácter externo, no forma parte del órgano de cumplimiento ni del RSII, sin perjuicio de su intervención, dentro del ámbito de sus funciones, en la supervisión del tratamiento de datos personales asociado al Sistema.

9.- Gestión del Sistema

A la fecha de la presente Política, la gestión y tramitación del Sistema se realiza íntegramente por medios propios de BEWOR, sin intervención de terceros externos como encargados del tratamiento. Si en el futuro la recepción de informaciones se gestionase mediante un tercero externo, este debería ofrecer garantías adecuadas de independencia, confidencialidad, protección de datos y secreto de las comunicaciones, sin que ello pudiera menoscabar las garantías del Sistema ni desplazar la responsabilidad del mismo en una persona distinta del RSII, debiendo formalizarse el correspondiente contrato de encargado del tratamiento en los términos exigidos por la normativa aplicable.

10.- Procedimiento de gestión de informaciones, acuse de recibo y plazos

BEWOR acusará recibo de la comunicación al informante dentro del plazo máximo de siete días naturales desde su recepción, salvo que ello pueda poner en peligro la confidencialidad de la comunicación. El procedimiento establece un plazo máximo para dar respuesta a las actuaciones de investigación que no podrá ser superior a tres meses desde la recepción, o, si no se remitió acuse de recibo, tres meses desde el vencimiento del plazo de siete días desde la comunicación. En supuestos de especial complejidad, podrá ampliarse el plazo hasta un máximo de otros tres meses adicionales. El desarrollo íntegro de este procedimiento se recoge en el Procedimiento de Gestión de Informaciones, documento independiente que forma parte del Sistema.

11.- Documentación de comunicaciones verbales

Las comunicaciones verbales, incluidas las realizadas telefónicamente o mediante reunión presencial, se documentarán, mediante: (i) grabación en un formato seguro, duradero y accesible; o (ii) transcripción completa y exacta realizada por el personal responsable de su tratamiento.

Con carácter previo a proceder a la grabación o transcripción, se informará al informante de esta obligación legal de documentación y se recabará su consentimiento expreso, no procediéndose a grabar ni a transcribir la comunicación sin haberlo obtenido; si el informante no prestara su consentimiento, el personal responsable elaborará una nota o acta resumen de la reunión o llamada. Se ofrecerá al informante la oportunidad de comprobar, rectificar y aceptar mediante su firma la transcripción, sin perjuicio de los derechos que le correspondan en materia de protección de datos.

12.- Recepción por canales no previstos o por personal no autorizado

Si una comunicación se recibiera por canales distintos a los habilitados o por personal no autorizado para su tratamiento, se garantizará la confidencialidad, impidiéndose que quien la reciba revele cualquier información que pueda permitir identificar al informante o a la persona afectada. La persona receptora deberá remitir inmediatamente la comunicación al RSII, sin modificarla, conforme a las previsiones del Protocolo de Seguridad, Confidencialidad y Control de Accesos y a la formación impartida.

13.- Derechos de la persona afectada e instrucción de las actuaciones

La instrucción incluirá las actuaciones necesarias para comprobar la verosimilitud de los hechos relatados. Se garantizará que la persona afectada tenga noticia de la comunicación y de los hechos relatados de manera sucinta, así como de su derecho a presentar alegaciones por escrito y de la información sobre el tratamiento de sus datos personales. En ningún caso se comunicará a la persona afectada la identidad del informante ni se le dará acceso a la comunicación original. En la medida de lo posible, se celebrará una entrevista con la persona afectada, con respeto a la presunción de inocencia, invitándole a exponer su versión y aportar pruebas; asimismo, cuando resulte imprescindible para el ejercicio efectivo de su derecho de defensa, se le podrá poner de manifiesto o facilitar únicamente la documentación o los extractos estrictamente necesarios, sin que en ningún caso se le facilite información que permita identificar, directa o indirectamente, al informante, y podrá ser asistida de abogado.

14.- Remisión al Ministerio Fiscal cuando existan indicios de delito

Cuando de los hechos comunicados pudieran derivarse indicios de delito, BEWOR remitirá la información al Ministerio Fiscal con carácter inmediato. Si los hechos afectaran a los intereses financieros de la Unión Europea, se remitirá igualmente a la Fiscalía Europea.

15.- Libro-registro de informaciones y confidencialidad del registro

BEWOR mantendrá un libro-registro de las informaciones recibidas y de las investigaciones internas a que hayan dado lugar, garantizando la confidencialidad exigida por la normativa. Dicho registro no será público y solo podrá accederse a su contenido total o parcial en virtud de petición razonada de la autoridad judicial competente, en el marco de un procedimiento judicial y bajo su tutela.

16.- Protección de datos: acceso restringido y deber de minimización

El acceso a los datos personales contenidos en el Sistema queda limitado exclusivamente a los miembros del RSII; al responsable de recursos humanos, solo cuando pudiera proceder la adopción de medidas disciplinarias o cautelares de protección frente a represalias; a los servicios jurídicos internos o externos, cuando proceda adoptar medidas legales; y al Delegado de Protección de Datos, en el ámbito de sus funciones de supervisión. En ningún caso se tratarán datos personales que no sean necesarios para conocer e investigar los hechos; si se hubieran recopilado por accidente o se constatará su innecesariedad, se suprimirán de inmediato.

17.- Categorías especiales de datos y supresión inmediata

Si la comunicación recibida contuviera datos personales incluidos dentro de categorías especiales, se procederá a su inmediata supresión, sin que se registren ni traten en el Sistema, salvo que resulten estrictamente imprescindibles para el objeto de la comunicación.

18.- Conservación y supresión de datos

Los datos personales se conservarán únicamente durante el tiempo imprescindible para decidir sobre la procedencia de iniciar una investigación. Transcurridos tres meses desde la recepción de la comunicación 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, en cuyo caso las comunicaciones a las que no se haya dado curso solo podrán constar de forma anonimizada. El periodo total de conservación de los datos personales en el marco del libro-registro no podrá superar los diez años. Si se acreditara que la información facilitada no es veraz, deberá suprimirse desde que se tenga constancia, salvo que dicha falta de veracidad pudiera constituir ilícito penal, en cuyo caso se conservará por el tiempo necesario durante la tramitación del procedimiento judicial.

19.- Deber de información a empleados y terceros

BEWOR informará a empleados y terceros acerca de la existencia del Sistema y del tratamiento de datos personales que se realice en su marco, mediante la publicación de la presente Política y del Canal Ético en el apartado de cumplimiento de la página web corporativa, así como mediante las acciones de formación y difusión interna que se determinen.

20.- Confidencialidad y secreto de las actuaciones

Toda persona que intervenga en la recepción, gestión, análisis o investigación de una comunicación deberá guardar secreto sobre cualquier aspecto relacionado con la información. El quebranto de la confidencialidad o del deber de secreto podrá dar lugar a responsabilidades internas y, en su caso, a responsabilidades conforme al régimen sancionador aplicable.

21.- Protección frente a represalias

BEWOR prohíbe expresamente cualquier forma de represalia, amenaza de represalia o tentativa de represalia contra quienes presenten comunicaciones conforme a esta Política. Se entenderá por represalia cualquier acto u omisión prohibidos por la normativa o que suponga un trato desfavorable que sitúe al informante en desventaja en el contexto laboral o profesional por razón de su comunicación, pudiendo manifestarse, entre otras, en las siguientes conductas:

- a) La suspensión del contrato de trabajo, el despido o la extinción de la relación laboral, incluida la no renovación o la terminación anticipada de un contrato temporal.
- b) La denegación de ascenso o la degradación en el puesto de trabajo.
- c) El cambio de funciones, el cambio de lugar de trabajo, la reducción salarial o la modificación del horario de trabajo.

- d) La denegación de formación.
- e) Una evaluación de rendimiento o un certificado de trabajo negativos.
- f) La imposición de una medida disciplinaria, amonestación u otra sanción.
- g) La coacción, intimidación, el acoso o el ostracismo.
- h) La discriminación o el trato desfavorable o injusto.

Esta enumeración tiene carácter meramente ejemplificativo y no exhaustivo.

22.- Condiciones para acceder a la protección del informante

Para que resulte aplicable la protección prevista, deberá concurrir que: (i) existan motivos razonables para considerar veraz la información en el momento de la comunicación, aunque no se aporten pruebas concluyentes, y que dicha información se refiera a materias incluidas en el ámbito de aplicación; y (ii) que la comunicación se realice conforme a los requerimientos del Sistema. Quedan excluidas de la protección, en todo caso, las comunicaciones relativas a hechos o conductas ajenos al ámbito material de la Ley 2/2023 (apartado 2 de esta Política), así como, entre otras, las comunicaciones inadmitidas, las vinculadas a conflictos interpersonales que afecten únicamente al informante y a las personas a las que se refiera la comunicación y las que versen sobre informaciones ya completamente públicas o meros rumores.

23.- Medidas de apoyo y asistencia al informante

Las personas que comuniquen infracciones incluidas en el ámbito material a través de los procedimientos previstos podrán acceder a medidas de apoyo consistentes en información y asesoramiento sobre procedimientos y recursos disponibles, protección frente a represalias y derechos de la persona afectada, así como asistencia efectiva por parte de las autoridades competentes cuando proceda.

24.- Relación con canales externos y derecho a comunicar externamente

Sin perjuicio del carácter preferente del Sistema interno, toda persona física podrá informar ante la Autoridad Independiente de Protección del Informante (AIPI) o ante las autoridades u órganos autonómicos competentes sobre acciones u omisiones incluidas en el ámbito de aplicación, ya sea directamente o tras haber comunicado a través del Canal interno.

Asimismo, en su condición de prestador de servicios de confianza cualificado, BEWOR informa de que las cuestiones relativas a certificados y servicios de confianza pueden comunicarse a la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales, sin perjuicio de que dichas comunicaciones queden fuera del régimen de protección específico de la Ley 2/2023 salvo que concurren, además, los presupuestos del apartado 2.

25.- Medidas de seguridad y control de accesos

BEWOR implementa medidas técnicas y organizativas adecuadas para garantizar la autenticidad, integridad, disponibilidad, trazabilidad y confidencialidad de la información tratada en el Sistema, con especial atención a la prevención de accesos no autorizados y a la limitación de acceso según

perfiles estrictamente necesarios. Estas medidas se desarrollan en el Protocolo de Seguridad, Confidencialidad y Control de Accesos del Sistema, y se revisarán periódicamente.

26.- Uso del Canal para comunicaciones ajenas al ámbito material de la Ley 2/2023

El Canal está habilitado, adicionalmente, para la recepción de otras comunicaciones o informaciones internas que no encajen en el ámbito material descrito en el apartado 2 anterior (por ejemplo, incumplimientos de normas internas de seguridad de la información, conflictos de interés u otras cuestiones de integridad organizativa). Se advierte expresamente que estas comunicaciones y sus remitentes quedan fuera del ámbito de protección específico dispensado por el régimen de protección al informante de la Ley 2/2023, si bien BEWOR mantendrá, en la medida de lo posible, las salvaguardas esenciales de confidencialidad y las exigencias de minimización y supresión de datos aplicables al Sistema.

27.- Prohibición de obstaculización y consecuencias internas

Queda prohibida cualquier actuación destinada a impedir o dificultar la presentación de comunicaciones o a frustrar, ralentizar o impedir su seguimiento, así como la aportación deliberada de información o documentación falsa en respuesta a requerimientos vinculados a la investigación. El incumplimiento de estas obligaciones y la vulneración de la confidencialidad y del secreto podrán dar lugar a la adopción de medidas disciplinarias internas y a cualesquiera otras responsabilidades que procedan.

28.- Canales de contacto, notificaciones y comunicaciones con el informante

Al presentar una comunicación, el informante podrá indicar un correo electrónico o lugar seguro a efectos de notificaciones. El formulario web permitirá, en todo caso, el envío de la comunicación de forma anónima, sin necesidad de facilitar correo electrónico ni ningún otro dato identificativo. En estos casos, se advertirá expresamente al informante de que, salvo que indique una vía alternativa de contacto, BEWOR no podrá comunicarse con él ni solicitarle aclaraciones o información adicional durante la tramitación. El procedimiento permitirá mantener comunicación con el informante y solicitar aclaraciones o información adicional cuando sea necesario y este haya facilitado un cauce de contacto.

29.- Aprobación, difusión, revisión y entrada en vigor

La presente Política ha sido aprobada por el Administrador Solidario de BEWOR TECH, S.L. mediante Acuerdo de fecha 3 de agosto de 2026, y entra en vigor en dicha fecha. La Política se difundirá internamente entre la plantilla y externamente a través de la página web corporativa, garantizando su fácil accesibilidad. BEWOR revisará periódicamente esta Política y el resto de documentos del Sistema para asegurar su adecuación a la normativa aplicable y a la evolución organizativa y tecnológica, dejando constancia documental de las versiones vigentes.