SISTEMA INTERNO DE INFORMACIÓN DE BIGMALL IBERICA S.L.

TABLA DE REVISIONES			
Revisión Nº:	**Aprobación por:**	**Fecha:**	**Modificación realizada:**
00	Gerencia	12/01/2025	Emisión Inicial

Este documento es propiedad de BIGMALL IBERICA, S.L.. La persona receptora del mismo se compromete a no realizar ninguna copia total o parcial y a no distribuirlo a terceros. Al mismo tiempo, acepta el compromiso de devolverlo cuando sea requerido por BIGMALL IBERICA, S.L..

1. OBJETO 3
2. ÁMBITO DE APLICACIÓN 3
2.1. ÁMBITO DE APLICACIÓN PERSONAL 3
2.2. ÁMBITO DE APLICACIÓN MATERIAL 4
3. RESPONSABILIDADES 5
4. DESARROLLO 6
4.1. RESPONSABLE DEL SISTEMA INTERNO DE INFORMACIÓN 7
4.2. PROCEDIMIENTO DE GESTIÓN DE INFORMACIONES 7
4.2.1. Política General del Sistema Interno de Información 7
4.2.2. Canales internos 8
4.2.3. Gestión de informaciones 9
4.2.4. Revelación Pública 11
4.3. PRESERVACIÓN DE LA IDENTIDAD DEL INFORMANTE Y DE LAS PERSONAS AFECTADAS 11
4.4. MEDIDAS PARA LA PROTECCIÓN DE LAS PERSONAS AFECTADAS 12
4.5. PROTECCIÓN DE DATOS PERSONALES 12
4.5.1. Datos personales 12
4.5.2. Información de datos personales 12
4.6. MEDIDAS DE PROTECCIÓN 13
4.6.1. Condiciones de protección para personas informantes 13
4.6.2. Prohibición de represalias 13
4.6.3. Medidas de apoyo 15
4.7. RÉGIMEN DISCIPLINARIO 15
5. CANALES EXTERNOS DE INFORMACIÓN 15
6. DOCUMENTACIÓN DE REFERENCIA 16

1. OBJETO

El presente documento se establece con objeto de diseñar, establecer y gestionar de forma segura el Sistema Interno de Información de BIGMALL IBERICA S.L.., garantizando la confidencialidad de la identidad de la persona informante y de cualquier tercero mencionado. Asimismo, incluye las actuaciones necesarias para su gestión y tramitación, así como la protección de datos, impidiendo el acceso a personal no autorizado.

Este procedimiento ha sido desarrollado según 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.

2. ÁMBITO DE APLICACIÓN

2.1. ÁMBITO DE APLICACIÓN PERSONAL

El presente sistema se aplicará a aquellas personas que hayan obtenido información sobre infracciones en un contexto laboral o profesional, comprendiendo en todo caso:

a) las personas que tengan la condición de trabajadores por cuenta ajena;

b) los autónomos;

c) los accionistas, partícipes y personas pertenecientes al órgano de administración, alta dirección o supervisión de la empresa, incluidos los miembros no ejecutivos;

d) cualquier persona que trabaje para o bajo la supervisión y la dirección de contratistas, subcontratistas y proveedores.

También se aplicará a las personas informantes que comuniquen o revelen públicamente información sobre infracciones obtenida en el marco de una relación laboral o estatutaria ya finalizada, voluntarios, becarios, trabajadores en periodos de formación con independencia de que perciban o no una remuneración, así como a aquellos cuya relación laboral todavía no haya comenzado, en los casos en que la información sobre infracciones haya sido obtenida durante el proceso de selección o de negociación precontractual.

Las medidas de protección de la persona informante también se aplicarán, en su caso, a los representantes legales de las personas trabajadoras en el ejercicio de sus funciones de asesoramiento y apoyo al informante.

Estas medidas de protección de la persona informante también se aplicarán a:

a) personas físicas que, en el marco de la organización en la que preste servicios la persona informante, asistan al mismo en el proceso,

b) personas físicas que estén relacionadas con la persona informante y que puedan sufrir represalias, como compañeros de trabajo o familiares de la persona informante, y

c) personas jurídicas, para las que trabaje o con las que mantenga cualquier otro tipo de relación en un contexto laboral o en las que ostente una participación significativa. A estos efectos, se entiende que la participación en el capital o en los derechos de voto correspondientes a acciones o participaciones es significativa cuando, por su proporción, permite a la persona que la posea tener capacidad de influencia en la persona jurídica participada.

2.2. ÁMBITO DE APLICACIÓN MATERIAL

El presente procedimiento establece normas mínimas comunes para la protección de las personas que informen sobre:

a) Infracciones del Derecho de la Unión:

1) infracciones que entren dentro del ámbito de aplicación de los actos de la Unión enumerados en el anexo de la 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, relativas a los ámbitos siguientes:
    - contratación pública,
    - servicios, productos y mercados financieros, y prevención del blanqueo de capitales y la financiación del terrorismo,
    - seguridad de los productos y conformidad,
    - seguridad del transporte,
    - protección del medio ambiente,
    - protección frente a las radiaciones y seguridad nuclear,
    - seguridad de los alimentos y los piensos, sanidad animal y bienestar de los animales,
    - salud pública,
    - protección de las personas consumidoras,
    - protección de la privacidad y de los datos personales, y seguridad de las redes y los sistemas de información;
2) infracciones que afecten a los intereses financieros de la Unión tal como se contemplan en el artículo 325 del TFUE y tal como se concretan en las correspondientes medidas de la Unión;
3) infracciones relativas al mercado interior, tal como se contemplan en el artículo 26, apartado 2, del TFUE, incluidas las infracciones de las normas de la Unión en materia de competencia y ayudas otorgadas por los Estados, así como las infracciones relativas al mercado interior en relación con los actos que infrinjan las normas del impuesto sobre sociedades o a prácticas cuya finalidad sea obtener una ventaja fiscal que desvirtúe el objeto o la finalidad de la legislación aplicable del impuesto sobre sociedades.

b) Acciones u Omisiones que pueden ser constitutivas de infracción penal o administrativa grave o muy grave. En todo caso, se entenderán todas aquellas infracciones penales o administrativas graves o muy graves que impliquen quebranto económico para la Hacienda Pública y para la Seguridad Social.

Esta protección no excluirá la aplicación de las normas relativas al proceso penal, incluyendo las diligencias de investigación.

La protección prevista para las personas trabajadoras que informen sobre infracciones del Derecho laboral en materia de seguridad y salud en el trabajo, se entiende sin perjuicio de la establecida en su normativa específica.

EXCLUSIONES:

- Informaciones que afecten a la información clasificada.
- Tampoco afectará a las obligaciones que resultan de la protección del secreto profesional de los profesionales de la medicina y de la abogacía, del deber de confidencialidad de las Fuerzas y Cuerpos de Seguridad en el ámbito de sus actuaciones, así como del secreto de las deliberaciones judiciales.
- Informaciones relativas a infracciones en la tramitación de procedimientos de contratación que contengan información clasificada o que hayan sido declarados secretos o reservados, o aquellos cuya ejecución deba ir acompañada de medidas de seguridad especiales conforme a la legislación vigente, o en los que lo exija la protección de intereses esenciales para la seguridad del Estado.

3. RESPONSABILIDADES

ÓRGANO DE GOBIERNO

- Implantar el Sistema interno de información, previa consulta con la representación legal de las personas trabajadoras.
- Tendrá la condición de responsable del tratamiento de los datos personales de conformidad con lo dispuesto en la normativa sobre protección de datos personales.
- Designación, destitución y/o, cese de los miembros del Sistema Interno de Información.
- Definir y aprobar la Política o Estrategia que define los principios básicos del Sistema Interno de información.
- Aprobación del procedimiento de gestión de informaciones del Sistema Interno de Información, definido en el presente documento.

RESPONSABLE DEL SISTEMA INTERNO DE INFORMACIÓN

- Recibir, gestionar e investigar las informaciones recibidas por el canal formal del sistema interno de información, haciendo un seguimiento con la máxima diligencia.
- Desarrollar sus funciones de forma independiente y autónoma respeto del resto de órganos de la entidad, disponiendo de medios materiales y personales necesarios para llevarlas a cabo.
- Mantener comunicación con la persona informante.
- Proporcionar respuesta.
- Cumplir con las disposiciones sobre protección de datos personales.
- Garantizar la confidencialidad del informante y de la persona afectada por la información.
- Respetar la presunción de inocencia y al honor de las personas afectadas.
- Informar a los afectados de las acciones u omisiones que se le atribuyen, así como mantener comunicación con el afectado en tiempo y forma para garantizar la investigación.
- Prohibir las represalias a los informantes, sean amenazas y/o tentativas de represalias, y asegurar que se toman las medidas necesarias para prevenirlas.

RESTO DE PERSONAL

- Derivar en el Responsable del Sistema de Información cualquier comunicación que reciban en relación con esta materia.
- Garantizar la confidencialidad de la información recibida y comunicada al Responsable del Sistema Interno de Información.

4. DESARROLLO

Las personas que trabajan para una organización pública o privada o están en contacto con ella en el contexto de sus actividades laborales o profesionales son a menudo las primeras en tener conocimiento de amenazas o perjuicios para el interés público que surgen en ese contexto. Al informar sobre infracciones dichas personas actúan como personas informantes y por ello desempeñan un papel clave a la hora de descubrir y prevenir esas infracciones y de proteger el bienestar de la sociedad. Sin embargo, las personas informantes potenciales suelen renunciar a informar sobre sus preocupaciones o sospechas por temor a represalias. Debido a esto, y considerando además que la protección de las personas informantes es necesaria para mejorar la aplicación del derecho en materia de contratación pública, en cumplimiento de la normativa legal, BIGMALL IBERICA S.L. acuerdan establecer un Sistema de Interno de Información, que canalizará formalmente las posibles comunicaciones sobre infracciones penales o administrativas (graves o muy graves) que ocurran en la Organización.

Por ello se ha diseñado, establecido y gestionado un sistema que funciona de forma segura y que garantice la confidencialidad de la identidad del informante y de cualquier tercera persona comprendida en la información, otorgando protección adecuada frente a posibles represalias que pueden sufrir las personas informantes.

4.1. RESPONSABLE DEL SISTEMA INTERNO DE INFORMACIÓN

El Administración o de Órgano de Gobierno será el competente para la designación de las personas físicas responsables de la gestión de dicho sistema o «Responsables del Sistema Interno de Información», y de su destitución o cese. Deberán ser directivos, que ejercerán su cargo con independencia del Órgano de Administración o de Gobierno.

Si el Responsable del Sistema de Información es un órgano colegiado, se debe delegar en uno de sus miembros las facultades de gestión del Sistema interno de información y de tramitación de expedientes de investigación.

Tanto el nombramiento como el cese de la persona física individualmente designada, así como de las integrantes del órgano colegiado, si lo hubiese, deberán ser notificados a la Autoridad Independiente de Protección del Informante, A.A.I., o, en su caso, a las autoridades u órganos competentes de las comunidades autónomas, en el ámbito de sus respectivas competencias, en el plazo de los diez días hábiles siguientes, especificando, en el caso de su cese, las razones que han justificado el mismo.

Dichas personas desarrollarán sus funciones de forma independiente y autónoma respecto del resto de los órganos de la entidad u organismo, no podrán recibir instrucciones de ningún tipo en su ejercicio, y deberán disponer de todos los medios personales y materiales necesarios para llevarlas a cabo.

Dicha designación ha sido aprobada por el Órgano de Gestión o de Gobierno.

4.2. PROCEDIMIENTO DE GESTIÓN DE INFORMACIONES

4.2.1. Política General del Sistema Interno de Información

BIGMALL IBERICA S.L. ha definido una política o estrategia que incluye los principios básicos generales del Sistema interno de información y defensa del informante. Esta política es comunicada en el seno de laempresa.

4.2.2.Canales internos

Las informaciones deben hacerse llegar por los diferentes canales internos de información disponibles, pudiendo realizar la comunicación por escrito o verbalmente:

a. Por escrito

- Entregándosela directamente a la persona o personas Responsable del Sistema Interno de Información.
- Remitiéndola por correo postal a la dirección C/ Marcial del Adalid, 1, 4º Derecha, 15005, A Coruña. Las informaciones remitidas por correo postal podrán ser enviadas de manera anónima, especificando que es "A la atención del Responsable del SII" de la empresa correspondiente.

En caso de facilitar la información de manera anónima y no indicar un correo electrónico, domicilio, apartado postal o similar a la que enviar acuse de recibo, no se podrá cumplir con el requisito de facilitar acuse de recibo ni el de informar acerca del procedimiento.

b. Verbalmente

- Comunicándola directamente a la persona Responsable del Sistema Interno de Información de manera presencial, previa solicitud del informante, mediante reunión en un plazo máximo de 7 días. De esta reunión se levantará un acta que firmarán las personas intervinientes.

En el caso de que la información se realice por escrito, ésta podrá realizarse por cualquiera de los canales anteriormente descritos; en el caso de que la persona informante se identifique la persona Responsable del Sistema le ofrecerá ampliar la información facilitándole el Formulario de Comunicación del Sistema Interno de Información.

En el caso de que se realice la comunicación de manera verbal, deben ser documentadas mediante una de las dos opciones:

- Grabación de la conversación en formato duradero y accesible. En cualquier caso, se advertirá al informante de que la comunicación será grabada y se le informará del tratamiento de sus datos de acuerdo con lo que establece el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016.
- A través de una transcripción completa y exacta de la conversación realizada por el personal responsable de tratarla. En estos casos, se ofrecerá al informante la oportunidad de comprobar, rectificar y aceptar mediante su firma la transcripción de la conversación.

En cualquier caso, los canales disponibles han de ser debidamente publicitados en el seno de la empresa para que cualquier persona incluida en el ámbito de aplicación del presente documento pueda informar de posibles infracciones.

4.2.3.Gestión de informaciones

El Sistema Interno de Información debe garantizar que las comunicaciones presentadas puedan tratarse de manera efectiva dentro de la empresa, con el fin de que éstas sean las primeras en conocer la posible irregularidad. Para ello, el Sistema Interno de Información se gestionará del siguiente modo:

- RECEPCIÓN INFORMACIÓN: Todas las informaciones serán comunicadas y gestionadas por los canales internos definidos en el apartado anterior.

Siempre que se trate de un informante no anónimo, al hacer la comunicación, el informante podrá indicar un domicilio, correo electrónico o lugar seguro a efectos de recibir las notificaciones.

Las comunicaciones también podrán ser realizadas de manera anónima a través de los canales disponibles, siendo gestionadas y tramitadas como cualquier otra información recibida a través del Sistema Interno de Información.

Si, a través de estos canales, se reciben informaciones no incluidas en el objeto del presente procedimiento, dichas comunicaciones y sus remitentes quedarán fuera del ámbito de protección dispensado por el sistema. Derivando el contenido de la información a las personas responsables de su gestión.

- ACUSE DE RECIBO: una vez recibida la información a través de los canales dispuestos, se debe facilitar un acuse de recibo a la persona informante en un plazo máximo de 7 días, desde la recepción de ésta, salvo que ello pueda poner en peligro la confidencialidad de la información.

A quienes realicen la comunicación a través de canales internos se les informará, de forma clara y accesible, sobre los canales externos de información ante las autoridades competentes y, en su caso, ante las instituciones, órganos u organismos de la Unión Europea.

- TRAMITACIÓN / INVESTIGACIÓN: Una vez se reciba la información y tras emitir el acuse de recibo, la persona Responsable del Sistema Interno de Información iniciará su investigación dejando constancia de ésta en la Registro de Investigaciones del Sistema Interno de Información, el cual comprenderá los siguientes ítems:

a. N.º de Registro: el cual seguirá la estructura (XX/YYYY donde XX es nº correlativo empezando por el 01 y donde YYYY es el año en curso).
b. Fecha de entrada.

c. Persona informante: Este campo se completará con el nombre y apellidos de la persona informante y, en caso de tratarse de una persona que no pertenezca a BIGMALL IBERICA, S.L., se indicará la empresa a la que pertenece. En caso de que la información recibida sea anónima se indicará el término "anónima".
d. Descripción de los hechos: Se incluirá un breve extracto de la información recibida.
e. Investigación: La investigación incluirá consultas internas y con asesores jurídicos externos; entrevistas a las personas afectadas, a la persona informante y/o a cualquier otra que pudiera resultar implicada; solicitud de antecedentes y aclaraciones, así como cualquier otra prueba documental.
f. Sospechas de mala fe.
g. Conclusiones y acciones tomadas.
h. Verificación de la información.
i. Fecha de respuesta a la persona informante (máximo 3 meses prorrogable por 3 meses más en caso de expediente de gran complejidad).
j. Puesta en conocimiento de la Autoridad Competente y fecha (si se da el caso).
k. Sanciones disciplinarias.
l. Fecha de cierre.

Se dispone de un plazo máximo de respuesta de tres meses, a partir del acuse de recibo, y en caso de que éste no se facilitase, el plazo será de tres meses a partir del vencimiento del plazo de 7 días después de la facilitación de la información. En el caso de expedientes de especial complejidad, se podrá posponer el plazo máximo hasta 3 meses más.

Durante la investigación, y en caso de disponer de la identidad del informante, la persona Responsable del Sistema Interno de información, podrá mantener comunicación con el informante para solicitar información adicional.

La persona afectada por la información será informada de las acciones u omisiones que se le atribuyen, así como ser oída en cualquier momento. Esta comunicación se realizará cuando se considere más adecuado para no entorpecer la investigación.

Durante todo el proceso de gestión de la información y hasta la finalización de la investigación, se debe de mantener la presunción de inocencia y respetar el honor de las personas afectadas. Así como respetar las disposiciones en materia de protección de datos.

En cualquier momento del proceso, se deberá informar al Ministerio Fiscal de manera inmediata cuando se disponga de indicios de que se haya podido cometer un delito.

• RESOLUCIÓN: Una vez se haya finalizado la investigación se entregará informe al informante y a la persona sobre quien se esté informando, donde se incluirán las conclusiones a las que ha llegado la persona Responsable del Sistema Interno de Información, así como las acciones disciplinarias que se llevarán a cabo.

• REGISTRO: La información recibida y la investigación de la misma se archivarán en el Registro del Sistema Interno de Información, así mismo se dispondrá de un libro-registro de las informaciones recibidas e investigaciones internas a través del Registro de Investigaciones del Sistema de Interno de Información. Este registro no será público y únicamente se entregará a la Autoridad Judicial previa petición razonada, mediante auto y bajo su tutela.

El plazo de conservación será el que corresponda a la prescripción de cada delito y, en todo caso, por un plazo mínimo de 5 años y máximo de 10 años. Los datos personales de las informaciones serán tratados según se indica en el apartado correspondiente del presente procedimiento.

4.2.4. Revelación Pública

Cuando una persona pone a disposición del público la información sobre acciones y omisiones que puedan ser constitutivas de infracción penal o administrativa grave o muy grave, dispondrá de protección siempre y cuando:

- Haya realizado la comunicación a través de canales internos o externos y no se hayan tomado medidas apropiadas al respecto.
- Tenga motivos razonables para pensar que la infracción puede constituir un peligro inminente o manifiesto para el interés público o existe un riesgo de daños irreversibles, incluido un peligro para la integridad física de una persona, exista riesgo de represalias o pocas probabilidades de que se lleve a cabo un tratamiento efectivo de la información, mediante la ocultación o destrucción de pruebas.

4.3. PRESERVACIÓN DE LA IDENTIDAD DEL INFORMANTE Y DE LAS PERSONAS AFECTADAS

La persona Responsable del Sistema Interno de Información, se asegurará de que se preserva tanto la identidad del informante como la de cualquier tercero que se mencione. Asimismo, se deberá preservar la identidad y garantizar la confidencialidad de los datos de las personas afectadas. En el caso de revelación pública, se asegurará que no se facilita información que permita la identificación del informante, de un tercero que se mencione o de las personas afectadas.

Únicamente se facilitará la identidad del informante a la Autoridad Judicial, al Ministerio Fiscal o la Autoridad Administrativa competente en el marco de una investigación penal, disciplinaria o sancionadora, teniendo que comunicar al informante, previamente, que su identidad va a ser revelada, salvo que esta comunicación pueda comprometer la investigación o el procedimiento judicial.

Durante el proceso de investigación, y cuando se comunique al afectado las informaciones recibidas, no se podrá, en ningún caso, informar sobre la identidad del informante o de quien ha llevado a cabo la revelación pública.

4.4. MEDIDAS PARA LA PROTECCIÓN DE LAS PERSONAS AFECTADAS

Durante la tramitación del expediente, las personas afectadas por la comunicación tendrán derecho a la presunción de inocencia, al derecho de defensa y al derecho de acceso al expediente, así como a la misma protección establecida para los informantes, preservándole su identidad y garantizándose la confidencialidad de los hechos y datos del expediente.

4.5. PROTECCIÓN DE DATOS PERSONALES

4.5.1. Datos personales

Todos los datos personales necesarios para la aplicación del presente procedimiento serán considerados lícitos debiendo ser tratados respetando la normativa en esta materia. Se consideran datos personales los relativos a la persona informante, así como datos de terceras personas, cuando resulte necesarios para la adopción de medidas correctoras o la tramitación de expediente.

No se recopilarán datos de personas cuya pertenencia no resulte necesaria para la información y posterior investigación, en caso de recopilar datos por accidente, éstos han de ser eliminados del expediente en cuento se determine su no procedencia. Del mismo modo, serán tratados los datos de informaciones de conductas que no se incluyen en el ámbito de aplicación del presente procedimiento o informaciones de conductas cuando se evidencia que no son veraces, salvo que la falta de veracidad dé lugar a un procedimiento judicial.

Todos los datos de informaciones que, transcurridos 3 meses desde su recepción, no han iniciado actuaciones de investigación, deberán ser suprimidos del Sistema, salvo que sean necesarios para evidenciar el funcionamiento del Sistema Interno de Información.

4.5.2. Información de datos personales

Siempre que se obtengan los datos personales de los interesados, se les ha de informar del tratamiento de sus datos, datos de contacto del delegado de protección de datos, en caso de que se disponga del mismo, y de sus derechos. Los interesados podrán ejercer sus derechos de acceso facilitándole información sobre:

- Los fines del tratamiento de datos.
- Las categorías de los datos personales de que se tratan.
- Los destinatarios a los que se comunicaron o serán comunicados los datos.

- De ser posible, el plazo previsto de conservación o al menos, los criterios empleados para determinar el plazo de conservación.
- La posibilidad de solicitar rectificación o supresión de datos personales o la limitación de tratamiento de datos o a oponerse al tratamiento.

4.5.3. Tratamiento de datos personales en el Sistema Interno de Información

El acceso a datos personales contenido en el Sistema Interno de Información quedará limitado a:
- Persona Responsable del Sistema Interno de Información y, a quien lo gestione directamente.
- Persona Responsable de RRHH o el órgano competente, cuando pudiera proceder la adopción de medidas disciplinarias contra el trabajador/a.
- Persona Responsable de Servicios jurídicos de la Empresa, siempre que proceda la adopción de medidas legales en relación con los hechos comunicados.
- Los encargados de tratamiento que eventualmente se designen.
- El Delegado de Protección de Datos, en caso de que se disponga del mismo.

4.6. MEDIDAS DE PROTECCIÓN

4.6.1. Condiciones de protección para personas informantes

Todas las personas que comuniquen o revelen infracciones objeto del presente procedimiento tendrán derecho a protección cuando haya motivos razonables para pensar que la información aportada es veraz en el momento de la comunicación o revelación, aun cuando no se aporten pruebas concluyentes, pero siempre que se haya realizado respetando lo previsto en el presente procedimiento y en la normativa vigente.

No dispondrán de derecho de protección todas aquellas personas que comuniquen o revelen:

- Informaciones contenidas en comunicaciones que hayan sido inadmitidas en canales internos o externos de información.
- Informaciones vinculadas a reclamaciones sobre conflictos interpersonales o que afecten únicamente al informante y a las personas a las que se refiere la comunicación.
- Informaciones que ya se encuentren disponibles para el público o que constituyan meros rumores.
- Informaciones sobre acciones u omisiones no contempladas en el presente procedimiento.

4.6.2. Prohibición de represalias

Quedan prohibidos los actos constitutivos de represalias, sean amenazas o tentativas, contra las personas informantes, entendiendo por represalias todas aquellas prohibidas por ley, así como cualquier trato

desfavorable en el contexto laboral o profesional simplemente por su condición de informante o por haber realizado una revelación pública.

De manera general, se consideran represalias:

a. suspensión, despido, destitución o medidas equivalentes.
b. no renovación o terminación anticipada de un contrato de trabajo temporal.
c. terminación anticipada o anulación de contratos de bienes o servicios.
d. imposición de cualquier medida disciplinaria, amonestación u otra sanción, incluidas las sanciones pecuniarias.
e. degradación o denegación de ascensos; y cualquier otra modificación sustancial de las condiciones de trabajo.
f. no conversión de un contrato de trabajo temporal en uno indefinido, en caso de que la persona trabajadora tuviera expectativas legítimas de que se le ofrecería un trabajo indefinido.
g. daños, incluidos a su reputación, en especial en los medios sociales, o pérdidas económicas, incluidas la pérdida de negocio y de ingresos.
h. coacciones, intimidaciones, acoso u ostracismo.
i. evaluación o referencias negativas con respecto a sus resultados laborales.
j. inclusión en listas negras sobre la base de un acuerdo sectorial, informal o formal, que pueda implicar que en el futuro la persona no vaya a encontrar empleo en dicho sector.
k. anulación de una licencia o permiso.
l. denegación de formación.
m. discriminación, o trato desfavorable o injusto.

La persona que viera lesionados sus derechos por causa de su comunicación o revelación una vez transcurrido el plazo de dos años podrá solicitar la protección de la autoridad competente que, excepcionalmente y de forma justificada, podrá extender el período de protección, previa audiencia de las personas u órganos que pudieran verse afectados. La denegación de la extensión del período de protección deberá estar motivada.

Los actos administrativos que tengan por objeto impedir o dificultar la presentación de comunicaciones y revelaciones, así como los que constituyan represalia o causen discriminación tras la presentación de aquellas al amparo de esta ley, serán nulos de pleno derecho y darán lugar, en su caso, a medidas correctoras disciplinarias o de responsabilidad, pudiendo incluir la correspondiente indemnización de daños y perjuicios al perjudicado.

4.6.3. Medidas de apoyo

A las personas que comuniquen o revelen infracciones a través de los procedimientos previstos se les dará acceso a las medidas de apoyo siguientes:

a. Información y asesoramiento completos e independientes, que sean fácilmente accesibles para el público y gratuitos, sobre los procedimientos y recursos disponibles, protección frente a represalias y derechos de la persona afectada.
b. Asistencia efectiva por parte de las autoridades competentes ante cualquier autoridad pertinente implicada en su protección frente a represalias, incluida la certificación de que pueden acogerse a protección al amparo de la presente ley.
c. Asistencia jurídica en los procesos penales y en los procesos civiles transfronterizos de conformidad con la normativa comunitaria.
d. Apoyo financiero y psicológico, de forma excepcional, si así lo decidiese la Autoridad Independiente de Protección de la persona informante, A.A.I., tras la valoración de las circunstancias derivadas de la presentación de la comunicación.

4.7. RÉGIMEN DISCIPLINARIO

En el caso de confirmarse la falsedad de la información, la persona infractora puede tener como consecuencia la exigencia de responsabilidades y/o sanciones derivadas de la legislación aplicable y/o del régimen disciplinario establecido en el Convenio colectivo correspondiente.

5. CANALES EXTERNOS DE INFORMACIÓN

Igualmente, se le informa que, están disponibles los canales externos de información, para informar de la comisión de cualesquiera acciones u omisiones incluidas en el ámbito de aplicación de la Ley 2/2023, ante la Autoridad Independiente de Protección del Informante, A.A.I., ante las autoridades u órganos autonómicos correspondientes, y, cuando proceda, a instituciones, organismos o agencias de la UE a través de los siguientes links:

- Servicio Nacional de Coordinación Antifraude (S.N.C.A.)

  https://www.igae.pap.hacienda.gob.es/sitios/igae/es-ES/snca/Paginas/ComunicacionSNCA.aspx

- Oficina Europea de Lucha contra el Fraude (OLAF)

  https://anti-fraud.ec.europa.eu/olaf-and-you/report-fraud_es

- Fiscalía Europea

  https://www.eppo.europa.eu/en/reporting-crime-eppo

- Dirección de Competencia de la Comisión Nacional de los Mercados y la Competencia

  https://edi.cnmc.es/buzones-anonimos/sica

- Canal de denuncias de la Agencia Tributaria

  https://sede.agenciatributaria.gob.es/Sede/colaborar-agencia-tributaria/denuncias.html

- Comunicación de indicios de Blanqueo de Capitales ante el SEPBLAC

  https://www.sepblac.es/es/sujetos-obligados/tramites/comunicacion-por-indicio/

6. DOCUMENTACIÓN DE REFERENCIA

Normas de referencia:

- *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.*
- *Directiva (UE) 2019/1937 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 23 de octubre de 2019.*

Procedimientos:

- *Procedimiento del Sistema Interno de Información.*

Formatos:

- *Protocolo de Tramitación de Comunicaciones Interno*
- *Formulario de Comunicación del Sistema Interno de Información.*
- *Registro de Investigaciones del Sistema Interno de Información.*
- *Designación de facultades Sistema Interno de Información.*

Otra documentación:

- *Acuse de Recibo de Denuncia*
- *Confidencialidad Persona No Responsable*
- *Instrucciones de documentación*