SEPI DESARROLLO EMPRESARIAL, S.A., S.M.E.

PROCEDIMIENTO DE GESTIÓN DEL SISTEMA INTERNO DE INFORMACIÓN

SECRETARÍA GENERAL Y DIRECCIÓN DE ASESORÍA JURÍDICA

Código: SGC.INF.05
Fecha: 08/06/2023
Versión: 1.2
Nivel: Confidencial

Revisión y aprobación

Elaboración	Revisión	Aprobación
Secretaria General y Directora de Asesoría Jurídica		
Cristina Coto del Valle		
COTO DEL VALLE CRISTINA - 10878071Z Fecha: 08/06/2023		Firmado digitalmente por COTO DEL VALLE CRISTINA - 10878071Z Fecha: 2023.06.08 09:57:39 +02'00'

Control de versiones

Versión	Fecha	Páginas	Descripción
1.1	07/06/2023		PROCEDIMIENTO DE GESTION DEL SISTEMA INTERNO DE INFORMACIÓN
1.2	08/06/2023		REVISADO DIRECCIÓN DE CUMPLIMIENTO SEPI

ÍNDICE

I. OBJETO

El objeto del Procedimiento de Gestión del Sistema Interno de Información (el "**Procedimiento**"), pretende establecer las reglas necesarias para gestionar el Sistema Interno de información de SEPI DESARROLLLO EMPRESARIAL, S.A., S.M.E ("**SEPIDES")**, conforme los requisitos de la Ley 2/2023, de 20 de febrero, ("**Ley 2/2023**") reguladora de la protección de las personas que informen sobre infracciones normativas y lucha contra la corrupción.

La Ley 2/2023 incorpora al ordenamiento jurídico español 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.

II. ÁMBITO DE APLICACIÓN

2.1. Ámbito subjetivo

Esta Procedimiento resulta de aplicación a todo el personal de SEPIDES, así como a su órgano de administración. Igualmente será aplicable a todas aquellas personas que presten servicios de manera habitual, aunque no formen parte de la plantilla, conforme a lo dispuesto en el artículo 3.1 letra d):" *cualquier persona que trabaje para o bajo la supervisión y la dirección de contratistas, subcontratistas o proveedores*". Incluirá también a becarios.

Será igualmente aplicable al personal que comunique una información en el marco de una relación laboral ya finalizada, así como aquellos cuya relación laboral no ha comenzado en el marco de las infracciones que pudieran informarse respecto al procedimiento de selección.

En todo caso, se incluye en el ámbito de aplicación a cualquier persona, física o jurídica, que haya obtenido información sobre infracciones en un contexto profesional.

2.2. Ámbito objetivo

A través del sistema interno de información se podrán comunicar:

a) Infracciones del Derecho de la Unión Europea siempre que entren dentro del ámbito de aplicación de la UE enumerados en el anexo de la Directiva 2019/1937 del Parlamento Europeo y del Consejo, de 23 de octubre de 2019, y que afecten a los intereses financieros de la UE o incidan en el mercado interior.
b) En el ámbito del ordenamiento jurídico español las infracciones penales, infracciones administrativas graves y muy graves, infracciones del derecho laboral en materia de seguridad y salud en el trabajo.
c) Infracciones del Código ético de SEPIDES o de otras políticas debidamente aprobadas.

III. OBLIGACIONES EN RELACIÓN CON EL PRESENTE PROCEDIMIENTO

3.1. Obligaciones del personal de SEPIDES

3.1.1. Consejo de Administración de SEPIDES

Todos los integrantes del órgano de administración de SEPIDES y personal que le sea de aplicación el presente procedimiento deberán guardar la más estricta confidencialidad sobre: (i) la identidad del informante; (ii) la identidad de las personas afectadas por la comunicación; (iii) la identidad de cualesquiera otras personas mencionadas en la comunicación; (iv) cualquier tipo de información comunicada a través del Sistema interno de información.

3.1.2. Responsable de Sistema

El acceso a los datos contenidos en el Sistema interno de Información quedará limitado exclusivamente a quienes desarrollen las funciones de control interno y de cumplimiento, o a los encargados del tratamiento que eventualmente se designen a tal efecto. En concreto, el Responsable de Sistema es el Comité de Prevención de Delitos de SEPIDES (el "**Comité**"), quien delega las facultades de gestión del sistema interno de información y de tramitación de expedientes de investigación en su Secretaría.

En caso de ausencia, vacante o enfermedad del Responsable de Sistemas, o cuando en el concurra algún tipo de conflicto de interés, las funciones serán desarrolladas por el miembro del Comité designado por la Dirección de Planificación y Control.

No obstante, será lícito su acceso por otras personas, o incluso su comunicación a terceros, cuando resulte necesario para la adopción de medidas disciplinarias. En todo caso, cualquiera de estas

personas legitimadas para conocer la identidad del informante serán garantes de la confidencialidad de su identidad y de cualquier tercero mencionado en la comunicación.

Cualquier persona que sea receptor de una comunicación y que no sea responsable de su tratamiento, deberá remitirla de forma inmediata al Responsable del Sistema, teniendo un deber de confidencialidad absoluto de lo que haya podido conocer.

3.1.3. Deber de colaboración y confidencialidad

Todo el personal de SEPIDES y a quien le sea de aplicación el presente procedimiento, tendrá el deber de colaboración absoluta en todas las diligencias de investigación, en los plazos señalados por el Responsable de Sistema, compareciendo cuando así sean requeridos para contestar a todo aquello que se le formule, aportando la documentación que el Responsable de Sistema requiera, manteniendo la confidencialidad de la existencia de la investigación y su contenido.

Este procedimiento busca que todas las personas a las que les sea de aplicación el presente procedimiento actúen con buena fe y mantengan constantemente una actitud colaborativa con SEPIDES en la lucha contra el incumplimiento normativo. Para el cumplimiento de este objetivo, se han creado sistemas que permitan una comunicación fluida con el Responsable de Sistema de forma que puedan manifestar, comunicar o denunciar cualquier irregularidad que detecten en el desempeño de sus funciones, así como resolver cualquier cuestión que se les pueda plantear para una correcta actuación.

Así las cosas, las investigaciones se dirigirán con el debido secreto respecto de la información relativa a informantes y a los afectados por la información, todo ello con la intención de evitar perjudicar el buen nombre de cualquier de ellos.

Toda comunicación o investigación que se lleve a cabo solo será conocida por el Comité de Prevención de Delitos, así como por las personas que éste designe para una adecuada investigación de los hechos, los cuales deberán mantener en estricta confidencialidad la información que se reciba o recabe al respecto

La falta de colaboración del informante con el Responsable del Sistema podrá determinar el archivo del expediente.

3.1.4. Prohibición de represalias

Todo el personal de SEPIDES, el órgano de Administración y a quienes se les aplique el presente Procedimiento deberán abstenerse:

- de obstaculizar, impedir, frustrar, ralentizar, la presentación o seguimiento de las comunicaciones
- Aportar documentación que le sea requerida con datos falsos o falseados o incompletos.
- Adoptar cualquier represalia, incluidas las amenazas, o tentativa de amenaza

SEPIDES adoptará las medidas adecuadas para garantizar que ningún informante se vea perjudicado por comunicar en el sistema interno de información cualquier incumplimiento normativo.

3.1.5. Prohibición de comunicaciones falsas a sabiendas

En el sistema interno de comunicaciones no deben comunicarse informaciones falsas a sabiendas. Las comunicaciones o informaciones deben formularse siempre bajo criterios de veracidad, claridad y de forma completa y detallada, no debiendo ser inveraces o maliciosas, ya que de la imputación de hechos con conocimiento de su falsedad o con temerario desprecio hacia la verdad, podrían derivarse responsabilidades penales, laborales o civiles para el informante.

De igual forma, considerará toda acusación falsa o maliciosa realizada de manera deliberada como una infracción muy grave, que podrá ser sancionada de conformidad con lo establecido en el Código Ético y de Conducta, por aplicación de la normativa laboral y/o penal.

En el caso de SEPIDES el Convenio aplicable es el de Oficinas y Despachos de la Comunidad de Madrid.

3.2. Obligaciones del personal ajeno a SEPIDES

Las obligaciones que se acaban de enumerar para el personal de SEPIDES serán aplicables *mutatis mutandi* al personal ajeno que esté incluido en el ámbito de aplicación.

IV. PROTECCIÓN DE DATOS PERSONALES

En cumplimiento del principio de responsabilidad proactiva, SEPIDES ha implantado las medidas técnicas y organizativas necesarias para garantizar la correcta aplicación de las obligaciones establecidas en la normativa de protección de datos. SEPIDES cuenta para ello con manuales y procedimientos específicos que deben ser cumplidos por los Destinatarios.

El tratamiento de los datos personales que deriven de la aplicación de este Procedimiento se regirán por lo dispuesto en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Conejo de 27 de abril de 2016, en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales, en la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales, y en el Título IV de la ley 2/2023, de 20 de febrero, reguladora de la protección de las personas que informen sobre infracciones normativas y lucha contra la corrupción.

En el sistema interno de información, se deberán respetar la confidencialidad de los datos, así como velar en todo momento porque el tratamiento de éstos se adecúe a las medidas de seguridad, técnicas y organizativas de SEPIDES evitando su uso no autorizado o ilícito, su pérdida, destrucción o daño accidental. Los datos serán utilizados exclusivamente para los fines y funciones para los que fueron recabados.

Las obligaciones anteriormente indicadas de secreto y confidencialidad que subsisten una vez finalizada la relación entre las partes.

A fin de comprobar el cumplimiento de las obligaciones establecidas en la normativa de protección de datos, SEPIDES, realizará una revisión sistemática para evaluar el cumplimiento de las obligaciones establecidas en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, 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 Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, mediante la

realización de auditorías de protección de datos periódicas. SEPIDES adoptará las medidas correctoras que resulten preceptivas a la vista del resultado de dichas auditorías.

El responsable del tratamiento de los datos personales en el sistema interno de la información es SEPIDES. El tratamiento de los datos personales está basado en el cumplimiento de una obligación legal, de conformidad con el artículo 30 de la Ley 2/2023.

La identidad de los informantes será en todo caso reservada, de tal forma que no se comunicará a las personas que se refieren los hechos ni a terceros.

Los datos de carácter personal y demás información que, en su caso, se facilite a través del sistema interno de información serán tratados con la finalidad de recibir comunicaciones de infracciones normativas, analizar su contenido y gestionar el expediente correspondiente.

El acceso a los datos personales del sistema interno de la información quedará limitado, dentro del ámbito de sus competencias y funciones exclusivamente a: (i) el Responsable del Sistema Interno de Información y a quien gestione el expediente; (ii) la persona titular de la dirección de Recursos Humanos, únicamente cuando pueda proceder la adopción de las medidas disciplinarias contra un trabajador o trabajadora; (iii) el titular de la Secretaría del Consejo y director de Asuntos Jurídicos de SEPIDES, si procediera la adopción de medidas legales; (iv) los encargados de tratamiento designados; (v) el delegado de protección de datos.

En todo caso, podrá ejercer sus derechos de acceso, rectificación, supresión, portabilidad y la licitación u oposición a través de correo postal a SEPIDES, calle Velázquez número 134, 28006, Madrid (España), aportando copia de su DNI o documento equivalente, con la referencia "Protección de Datos" o al correo electrónico: "*protecciónde datossepides@sepides.es*"

Será lícito el tratamiento de datos para otras personas, o incluso su comunicación a terceros, cuando resulte necesario para la adopción de medidas correctoras en la entidad o la tramitación de los procedimientos sancionadores o penales que, en su caso, procedan.

En ningún caso serán objeto de tratamiento los datos personales que no sean necesarios para el conocimiento e investigación de las infracciones normativas incluidas en el ámbito de aplicación del presente Procedimiento, procediéndose, en su caso, a su supresión. Se suprimirán los datos personales que se hubieran comunicado y que se refieran a conductas que no estén en dicho ámbito de aplicación.

Si se acreditara que la información comunicada no es veraz, se procederá a su inmediata supresión desde el momento que se tenga conocimiento de esta circunstancia.

En todo caso, transcurridos tres meses desde la recepción de la comunicación sin que se hubieren iniciado actuaciones de investigación, deberá procederse a la supresión de los datos salvo que la finalidad de conservación responda a dejar evidencia sobre el funcionamiento del sistema. Las comunicaciones a las que no se haya dado curso solamente podrán constar de forma anonimizada, sin que resulte de aplicación la obligación de bloqueo prevista en el artículo 32 de la Ley Orgánica 3/2018, de 5 de diciembre.

En ningún caso los datos personales relativos a infracciones recibidas y a las investigaciones internas podrán conservarse por un periodo superior a diez años.

V. VIAS PARA COMUNICAR LAS INFRACCIONES NORMATIVAS

- **Cuenta de correo electrónico**: *comiteprevenciondelitos@sepides.es*
- **De forma anónima**: mediante la remisión de la comunicación y de la documentación necesaria para la investigación en un sobre cerrado y confidencial al Responsable Comité de prevención de Delitos, calle Velázquez, 134bis, Madrid, 28006.
- **De manera verbal:** A solicitud del informante o denunciante, también podrá presentarse mediante una reunión presencial, dentro del plazo máximo de 7 días. En tal caso el Responsable de Sistema podrá asistir con otro miembro del Comité de Prevención de Delitos que designe.

Las comunicaciones verbales, realizadas a través de reunión presencial, se documentarán de alguna de las maneras siguientes, previo consentimiento del informante:

- mediante una grabación de la conversación en un formato seguro, duradero y accesible, o
- a través de una transcripción completa y exacta de la conversación realizada por el personal responsable de tratarla.

Sin perjuicio de los derechos que le corresponden de acuerdo con la normativa sobre protección de datos, se ofrecerá al informante la oportunidad de comprobar, rectificar y aceptar mediante su firma la transcripción de la conversación.

Asimismo, se informará que también podrán comunicar o informar de cualquier irregularidad a través de los canales externos de información ante la Autoridad Independiente de Protección del Informante, o, en su caso, ante las instituciones, órganos u organismos de la Unión Europea.

VI. TRAMITACIÓN DE LAS COMUNICACIONES

6.1. Fase de formulación de la comunicación

SEPIDES, consciente de su compromiso invertirá los recursos personales y económicos necesarios para implantar y mantener la efectividad del Canal interno, comprometiéndose a la investigación de cualquier comunicación recibida.

Cualquier comunicación en el sistema interno de un posible incumplimiento de la legalidad, deberá cumplir los siguientes requisitos:

- Descripción detallada y completa de los hechos que den lugar a la posible infracción.
- Identificación, si se conoce, de la persona que ha llevado a cabo la actuación posiblemente infractora.
- La fecha o fechas en que se hubieran cometido los hechos denunciados, aunque sea de forma aproximada.
- El tipo de vinculo que mantiene con SEPIDES
- Documentos, datos y demás fuentes de prueba o información que, en su caso, pudieran permitir la investigación de los hechos.

El Responsable de Sistema procederá a acusar recibo de la comunicación en el plazo de siete días naturales siguientes a su recepción, salvo que pueda poner en peligro la confidencialidad de la comunicación.

Los datos de quien formule la comunicación y de los empleados y terceros deberán conservarse en el sistema interno de comunicaciones únicamente durante el tiempo imprescindible para decidir sobre la procedencia de iniciar una investigación sobre los hechos denunciados.

En todo caso, transcurridos tres meses desde la introducción de los datos, deberá procederse a su supresión del sistema de comunicaciones, salvo que la finalidad de la conservación sea dejar evidencia del funcionamiento del modelo de prevención de la comisión de delitos por la persona jurídica. Las comunicaciones a las que no se haya dado curso solamente podrán constar de forma anonimizada.

Deberán adoptarse las medidas necesarias para preservar la identidad y garantizar la confidencialidad de los datos correspondientes a las personas afectadas por la información suministrada, especialmente la de la persona que hubiera puesto los hechos en conocimiento de la entidad, en caso de que se hubiera identificado.

En función de la materia, se derivará la comunicación al gestor del expediente, de tal forma que:

- Si la comunicación se refiere a protección de datos, se derivará al Delegado de Prevención.
- Si la comunicación se refiere al Blanqueo de Capitales se derivará a la Unidad Técnica de blanqueo de SEPIDES.
- Las comunicaciones que versen sobre cualquier otra materia serán tramitadas por el Responsable de Sistema como gestor del expediente.

En todos los supuestos el Responsable de Sistema velará por la tramitación diligente del expediente. La comunicación, que será recibida por el Responsable de Sistema como persona en quien delega el Comité de Prevención de Delitos, será trasladada al resto de miembros del Comité, siempre que no exista conflicto de interés por su parte.

6.2. Trámite de admisión o inadmisión

Una vez analizada la comunicación, el gestor del expediente decidirá:

a) Inadmitir a trámite la comunicación, en alguno de los siguientes casos:

i. Cuando los hechos relatados carezcan de toda verosimilitud.

ii. Cuando los hechos relatados no sean constitutivos de infracción del ordenamiento jurídico incluida en el ámbito de aplicación de este Procedimiento.

iii. Cuando la comunicación carezca manifiestamente de fundamento por no reunir los requisitos expresados en el apartado 6.1 de este Procedimiento o

iv. Cuando la comunicación no contenga información nueva y significativa sobre infracciones en comparación con una comunicación anterior respecto de la cual han concluido los correspondientes procedimientos, a menos que se den nuevas circunstancias que justifiquen un seguimiento distinto.

Ante la eventual inadmisión de la comunicación, el Responsable del Sistema velará por que no se produzca ningún efecto desfavorable para el informante por el hecho de haber formulado la comunicación.

b) Admitir a trámite la comunicación, desplegando efectos el régimen de protección frente a posibles represalias en los términos previstos en el presente Procedimiento.

En los casos de comunicaciones formuladas por personas que no estén incluidas en el ámbito subjetivo del presente Procedimiento, se procederá a inadmitir la comunicación sin perjuicio de darle el curso legal que proceda.

Con el fin de decidir sobre su admisión a trámite, se podrá solicitar al informante la aclaración o complemento de los hechos comunicados, aportando aquella documentación que pudiera ser necesaria para acreditar la existencia de la infracción normativa.

La decisión de admisión o inadmisión a trámite se comunicará al informante a la mayor brevedad posible. La comunicación de inadmisión a trámite se motivará de forma sucinta.

6.3. Diligencias de investigación

El gestor del expediente practicará todas las diligencias de investigación que estime oportunas para comprobar la veracidad de los hechos relatados, dejando constancia de las mismas en el expediente. Se detallan a continuación algunas de las principales diligencias que podrán conformar la investigación:

- Realizar entrevistas con el informante, con las personas mencionadas en la comunicación o con personal de Sepides, que deberán ser documentadas adecuadamente.
- Recabar toda la información o documentación que estime necesaria a cualesquiera de las Direcciones de la entidad.
- Acceder a los sistemas informáticos y dispositivos que la entidad pone a disposición de sus empleados para fines profesionales (por ejemplo, ordenadores portátiles, cuentas de correo electrónico, dispositivos de almacenamiento, etc.), dentro de los límites establecidos en la normativa laboral y la normativa de protección de datos que resulte de aplicación.

Si fuera preciso, el gestor del expediente podrá contar con el auxilio necesario para la práctica de las diligencias de investigación que, en todo caso, deberá respetar los principios establecidos en la Política del Sistema Interno de Información. Los procedimientos de contratación que se deban seguir se llevarán a cabo con la celeridad necesaria que demande el cumplimiento de los plazos de la investigación.

La persona afectada por la comunicación será informada de los hechos que se le atribuyen, si bien esta información se proporcionará en el momento y en la forma que se consideren adecuados para garantizar el buen fin de la investigación. En ningún caso se le comunicará la identidad del informante ni tendrá acceso a la comunicación. Asimismo, tendrá derecho a ser oída en cualquier momento con el objeto de exponer su versión de los hechos y aportar aquellos medios de prueba que considere adecuados y pertinentes, siempre con absoluto respeto a la presunción de inocencia. Se le deberá informar de la posibilidad de comparecer asistido por un abogado.

6.4. Terminación de las actuaciones:

Una vez analizada toda la información y documentación recabada, el Responsable de Sistema o la persona/s que éste designe deberá elaborar un informe escrito en el que se hará constar (i) descripción detallada de los hechos; (ii) detalle de las pruebas obtenidas y (iii) propuesta de resolución y, en su caso, de sanción.

La propuesta de imposición de sanciones deberá ajustarse en todo caso a lo establecido en este Procedimiento y/o en la legislación laboral de aplicación. El referido informe deberá ser valorado y votado por el Comité de Prevención de Delitos. En cualquier caso, si el empleado cuya actuación está siendo analizada pertenece al Departamento o División de alguno de los miembros del Comité de Prevención de Delitos, el mismo podrá participar en la fase de deliberación facilitando su punto de vista, pero quedará prohibido que participe en la fase de votación.

En el supuesto que como resultado del informe el Responsable del Sistema detecte la existencia de indicios de la comisión de un delito por parte de uno de los informados, se procederá de inmediato a denunciar los hechos ante la Fiscalía, las autoridades judiciales pertinentes o las Fuerzas y Cuerpos de Seguridad del Estado, debiendo colaborar con los mismos en todo lo que fuere necesario y/o se le requiera para el esclarecimiento de los hechos.

Concluidas las diligencias de investigación, el gestor del expediente emitirá un informe que contendrá un resumen de las diligencias practicadas con el fin de comprobar la verosimilitud de los hechos, la valoración de estas y las conclusiones alcanzadas.

El gestor del expediente procederá a archivar el expediente en los siguientes supuestos:

i. Inexistencia de los hechos que pudieran constituir una infracción normativa incluida en el ámbito de aplicación de este Procedimiento.

ii. Cuando las diligencias practicadas no acrediten suficientemente la comisión de la infracción.

iii. Cuando los hechos probados no constituyan, de modo manifiesto, una infracción normativa incluida en el ámbito de aplicación de este Procedimiento.

iv. Cuando no se haya podido identificar a la persona o personas responsables.

v. Cuando se concluyera, en cualquier momento, que ha prescrito la infracción.

No obstante, si la investigación pusiera de manifiesto alguna deficiencia a subsanar, se elaborará un informe con propuestas de mejora que se trasladará a Presidencia.

El archivo del expediente será notificado al informante y, en su caso, a la persona afectada.

Si el gestor del expediente estima que las diligencias practicadas acreditan suficientemente la comisión de una infracción normativa incluida en el ámbito de aplicación de este Procedimiento, trasladará su informe al Comité de Prevención de Delitos.

Recibido el informe jurídico, si los hechos pudieran revestir carácter delictivo se deberá informar de forma inmediata al Ministerio Fiscal o a la Fiscalía Europea en el caso de que los hechos afecten a los intereses financieros de la Unión Europea.

Asimismo, el gestor del expediente deberá proponer las medidas preventivas adecuadas para mitigar el riesgo de reiteración en la conducta infractora. En el caso de que la conducta infractora no hubiera cesado, también deberá elaborar una propuesta sobre la forma de restaurar la situación.

En todos los supuestos en los que no se haya procedido al archivo del expediente, los informes del gestor del expediente y el informe del Comité de Prevención de Delitos, se trasladarán al Consejo de Administración para su información.

Asimismo, si pudiera proceder la adopción de medidas disciplinarias contra un trabajador o trabajadora de la entidad, los informes serán trasladados a la Dirección de Recursos Humanos.

De las resultas de la investigación se dará cuenta sucinta al informante y a la persona afectada.

El plazo para finalizar las actuaciones y dar respuesta al informante no podrá ser superior a tres meses a contar desde la recepción de la comunicación completa o, en su caso, desde la subsanación de los requisitos que hubieran determinado la inadmisión de la comunicación. De forma motivada, este plazo podrá extenderse hasta un máximo de otros tres meses adicionales en casos de especial complejidad.

Con carácter general, las actuaciones que hubiera que practicar tendrán lugar en las instalaciones de SEPIDES, en horario laboral de lunes a viernes.

El informante y la/s persona/s a la/s que se refiere la comunicación podrán formular alegaciones en relación con las decisiones adoptadas por el gestor del expediente, quedando este habilitado para revisarlas si considera que existen motivos para ello.

6.5. Medidas de protección frente a represalias

El principio rector de la Política del Sistema interno de información de Sepides es la protección del informante. En consecuencia, las personas que comuniquen alguna de las infracciones normativas previstas en el ámbito de aplicación de este Procedimiento tendrán derecho a protección siempre que concurran las circunstancias siguientes:

- tengan motivos razonables para pensar que la información referida es veraz en el momento de la comunicación, aun cuando no aporten pruebas concluyentes, y
- la comunicación se haya realizado conforme a los requisitos establecidos en el presente Procedimiento.

Adicionalmente, las medidas de protección 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.
- 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 el informante 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.

No obstante, quedan expresamente excluidos del régimen de protección aquellas personas que comuniquen:

- Informaciones contenidas en comunicaciones que hayan sido inadmitidas a trámite.
- Informaciones vinculadas a reclamaciones sobre conflictos interpersonales o que afecten únicamente al informante y a las personas a las que se refiera la comunicación.
- Informaciones que ya estén completamente disponibles para el público o que constituyan meros rumores.

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 este Procedimiento.

Se entiende por represalia cualesquiera actos u omisiones que estén prohibidos por la Ley 2/2023, 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, solo por su condición de informantes y siempre que tales actos u omisiones se produzcan mientras duren las diligencias de investigación y en los dos años siguientes a su finalización.

En concreto, se considerarán represalias las que se adopten en forma de:

i. 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.

ii. Daños, incluidos los de carácter reputacional, o pérdidas económicas, coacciones, intimidaciones, acoso u ostracismo.

iii. Evaluación o referencias negativas respecto al desempeño laboral o profesional.

iv. 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.

v. Denegación o anulación de una licencia o permiso.

vi. Denegación de formación.

vii. Discriminación, o trato desfavorable o injusto.

En caso de sufrir represalias, se deberá informar inmediatamente al Responsable del Sistema interno de información a través de la dirección de correo electrónico comiteprevenciondelitos@sepides.es . Adicionalmente, el Responsable del Sistema realizará un seguimiento periódico de la situación del informante y, en su caso, de aquellas personas incluidas en el régimen de protección.

Si el Responsable del Sistema constatase que durante la vigencia del régimen de protección se han adoptado represalias, además de las medidas disciplinarias y/o sanciones administrativas que pudieran resultar de aplicación, se adoptarán las medidas necesarias y para que el represaliado vuelva a la situación previa al perjuicio sufrido.

VII. INCUMPLIMIENTO DEL PROCEDIMIENTO

Con carácter general, todo el personal de SEPIDES, incluidas las personas pertenecientes al órgano de administración de la entidad, está obligado a cumplir con lo establecido en el presente

Procedimiento, pudiendo proceder la adopción de medidas disciplinarias en caso de incumplimiento.

Adicionalmente, la Ley 2/2023 establece un régimen sancionador al que están sujetas todas las personas físicas y jurídicas que cometan alguna de las infracciones tipificadas en la citada ley.

En el caso de que sean personas físicas las responsables de las infracciones, el importe de las multas oscilará entre 1.001 y 300.000 euros, dependiendo de si se ha cometido una infracción leve, grave o muy grave.

En el ámbito del sector público estatal, será competente para la aplicación del régimen sancionador la Autoridad Independiente de Protección del Informante (A.A.I.).

La obligación de cumplir con este Procedimiento se extiende a las personas ajenas a SEPIDES a través del Sistema interno de información de la entidad.

VIII. APROBACIÓN, ENTRADA EN VIGOR Y DIFUSIÓN

El Consejo de Administración de SEPIDES es el órgano competente para aprobar este Procedimiento.
El presente Procedimiento será efectivo desde el momento de su aprobación, procediendo a su publicación ese mismo día en la página web de SEPIDES y en su tablón

Por parte del Departamento de Recursos Humanos se promoverán las acciones formativas necesarias para la adecuada difusión de este Procedimiento y de la cultura de cumplimiento y los fines de la Ley 2/2023.

El Presente Procedimiento se ajustará, en su interpretación y aplicación a:

i. La Directiva (UE)2019/1937, Ley 2/2023, y demás legislación que le resulte de aplicación
ii. La doctrina y jurisprudencia de tribunales nacionales y europeos;
iii. Circulares, informes, guías emitidas por la Autoridad Independiente de Protección del Informante (A.A.I)

El Presente Procedimiento será revisado cada que vez que surja una modificación normativa, y, en todo caso, cada dos años para adecuarlo a las modificaciones normativas que puedan sucederse, así como para incorporar todas aquellas mejoras identificadas por el Responsable del Sistema en base a las mejores prácticas en la materia.