Contenido

1. Objetivo

Con la entrada en vigor 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 de protección del informante) se transpone en el ordenamiento jurídico español la *Directiva (UE) 2019/1937 del Parlamento Europeo y del Consejo, de 23 de octubre, relativa a la protección de las personas que informen sobre infracciones del Derecho de la Unión* (conocida como Directiva *Whistleblowing*) y se da un paso más en la cultura de la información y del cumplimiento empresarial, para prevenir y detectar determinadas amenazas al interés público.

Mediante la nueva ley se regulan, por un lado, la protección de las personas físicas que, en el contexto laboral o profesional, informen sobre prácticas irregulares cometidas por entidades públicas o privadas y, por otro, los requisitos y garantías que deben cumplir los mecanismos de comunicación efectivos de estas informaciones (canales de denuncia) por parte de las empresas y demás organismos públicos obligados.

PROA CAPITAL DE INVERSIONES SGEIC, S.A. (en adelante, "PROA CAPITAL" o "PROA") está comprometida con la prevención de vulneraciones del ordenamiento jurídico y ha aprobado una Política de protección del informante e implementado el presente Protocolo de Sistema interno de información, de conformidad con la normativa vigente.

De esta manera, se pone a disposición de aquellas personas, que tengan la condición de informantes en el seno de PROA CAPITAL, el Sistema interno de información para comunicar, dentro de la propia entidad, la información sobre prácticas irregulares de las que tengan conocimiento, garantizándose, en todo momento, la aplicación de los derechos del informante y de las medidas de protección por ley establecidas.

2. Rasgos del Sistema

PROA CAPITAL reconoce como propios los principios generales en materia de Sistemas interno de información y defensa del informante establecidos en la Ley de protección del informante y ha establecido las previsiones necesarias para dar cumplimiento y garantizar los siguientes requisitos:

- Contar con un procedimiento de gestión de las informaciones recibidas.
- Permitir a los informantes comunicar la información, a través de canales seguros y fácilmente accesibles.
- Garantizar la confidencialidad de la identidad del informante, de los terceros mencionados en la comunicación y de las actuaciones que se desarrollen en su gestión y tramitación.
- Velar asimismo por los derechos de la persona afectada. En todo caso, el derecho a que se le informe de las irregularidades que se le atribuyen, el derecho a ser oído en cualquier momento, el derecho a la presunción de inocencia y el derecho al honor.
- Permitir la presentación de la información por escrito (a través de correo electrónico o correo postal) o mediante reunión presencial.

- Permitir la presentación de la información de forma anónima.

- Informar sobre los canales externos de información ante las autoridades competentes y, en su caso, ante las instituciones, órganos u organismos de la Unión Europea.

- Contar con un Responsable del Sistema.

- Establecer las garantías para la protección de los informantes.

- Remitir la información al Ministerio Fiscal o a la Fiscalía Europea, con carácter inmediato, cuando los hechos puedan ser indiciariamente constitutivos de delito.

- Realizar el tratamiento de los datos personales de conformidad con la normativa vigente.

3. Ámbito de aplicación material

Mediante el Sistema interno de información puede reportarse cualquier tipo de infracción que se refiera a:

- Acciones u omisiones que puedan constituir una infracción del Derecho de la Unión Europea que:

    - Entren dentro del ámbito de aplicación de los actos de la Unión Europea enumerados en el anexo de la Directiva (UE) 2019/1937, con independencia de la calificación que de las mismas realice el ordenamiento jurídico interno:
        - 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 los consumidores.
        - Protección de la privacidad y de los datos personales, y seguridad de las redes y los sistemas de información.

    - Afecten a los intereses financieros de la Unión Europea tal y como se contemplan en el artículo 325 del Tratado de Funcionamiento de la Unión Europea (TFUE).

    - Incidan en el mercado interior, tal y como se contempla en el artículo 26, apartado 2 del TFUE, incluidas las infracciones de las normas de la Unión Europea 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 con prácticas cuya finalidad sea obtener una ventaja fiscal que desvirtúe el objeto o la finalidad de la legislación aplicable al impuesto sobre sociedades.

- Infracciones penales y administrativas graves o muy graves (incluidas las que provoquen quebranto para Hacienda y Seguridad Social).

- Infracciones en material laboral relativas a la salud y seguridad en el trabajo.

Quedan excluidas expresamente del ámbito de protección del presente Protocolo:

- Las irregularidades que se rigen por su normativa específica en las leyes sectoriales (incluyendo las que se refieran al ámbito de aplicación de las enumeradas en la parte II del Anexo de la Directiva UE 2019/1937).

- Las informaciones que afecten a la información secreta o clasificada.

- Las informaciones vinculadas a reclamaciones sobre conflictos interpersonales.

- Las informaciones cuya adquisición o acceso constituya un delito.

- Las informaciones que impliquen vulneración de secretos de abogados o médicos.

- Las informaciones relativas al secreto de deliberaciones judiciales.

- Las informaciones sujetas a confidencialidad de las fuerzas armadas y Cuerpos de Seguridad.

- Las informaciones relativas a infracciones en la tramitación de procedimientos de contratación.

- La comunicación sobre informaciones ya disponibles públicamente o que constituyan meros rumores.

Adicionalmente, PROA CAPITAL prevé la posibilidad de utilizar el Sistema interno de información para recibir cualesquiera otras comunicaciones o informaciones que pudieran constituir un incumplimiento de la legalidad vigente, fuera del ámbito de aplicación de la Ley de protección del informante. Si bien, en estos casos, dichas comunicaciones y sus remitentes no estarán amparados por la protección dispensada por Ley de protección del informante.

4. Ámbito de aplicación subjetivo

El presente Protocolo es de aplicación para todas aquellas personas que pongan en conocimiento de PROA CAPITAL información sobre las infracciones obtenida en el contexto laboral o profesional, y concretamente, a:

- Los empleados de PROA CAPITAL (incluyendo: las personas que hayan finalizado su relación profesional, los trabajadores en prácticas, en periodo de formación, becarios y voluntarios).

- Las personas que se encuentren participando en procesos de selección o negociación contractual con PROA CAPITAL.

- Las personas autónomas que trabajen para o bajo la supervisión de PROA CAPITAL.

- Los accionistas, los partícipes y las personas pertenecientes al órgano de administración, dirección o supervisión de PROA CAPITAL (incluidos los miembros no ejecutivos).

- Cualquier otra persona que trabaje para o bajo la supervisión y la dirección de contratistas, subcontratistas y proveedores de PROA CAPITAL.

Asimismo, el Sistema interno de información y las medidas de protección previstas en el mismo se extienden a:

- Las personas físicas que, en el marco de la organización en la que preste servicios el informante, asistan al mismo en el proceso.

- Las personas físicas que estén relacionadas con el informante y que puedan sufrir represalias, como compañeros de trabajo o familiares del informante.

- Las 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.

5. Responsable del Sistema

El Órgano de Administración de PROA CAPITAL ha designado como Responsable del Sistema a Paloma de Carlos, quien velará por el correcto funcionamiento del Sistema interno de información, y desempeñará sus funciones de manera independiente y autónoma.

En el caso de que el Responsable del Sistema fuera la persona afectada por la información comunicada, para evitar posibles situaciones de conflicto de interés, podrá dirigirse la comunicación a Lourdes Martínez, quien asumirá, a los solos efectos de esta gestión, las funciones del Responsable del Sistema.

El Responsable del Sistema podrá contar con el apoyo de diferentes delegados dentro de PROA CAPITAL para la tramitación de las investigaciones, quienes estarán igualmente obligados a cumplir con los derechos y garantías de protección del informante.

6. Canal interno de información

La información sobre los canales internos de información consta en la página web PROA CAPITAL (www.proacapital.com) de forma clara y fácilmente accesible.

Los canales internos para la recepción de la información cumplen, en todo caso, las garantías legales de protección del informante.

PROA CAPITAL ha habilitado los siguientes canales internos de información:

- Por correo electrónico remitido a canaletico@proacapital.com, que será el canal interno preferente para la recepción de las comunicaciones.

- Por correo postal, dirigido a la atención del Responsable del Sistema, en las oficinas que PROA CAPITAL tiene en la dirección C/ Zurbano 76, 6ª, 28010, de Madrid.

- Mediante comparecencia personal ante el Responsable del Sistema, que se celebrará en el plazo máximo de siete días, previa solicitud de una reunión presencial, efectuada a través de correo electrónico o correo postal.
  Dicha conversación será documentada mediante grabación, siempre que el informante preste su consentimiento para ello; o través de transcripción completa, que el informante podrá comprobar y aceptar mediante la firma de la misma.

Las comunicaciones pueden realizarse de forma identificada o anónima y deben contener, en el mayor grado posible, la siguiente información:

- Nombre y apellidos de la persona (o personas) a las que se atribuye la conducta irregular.

- Fecha de los hechos.

- Descripción de la conducta irregular objeto de la comunicación y/o cualquier información obtenida de la que disponga.

- Documentos u otros medios de prueba que sirvan para acreditar las conductas irregulares objeto de la comunicación.

Al presentar la información, el informante puede indicar un domicilio, correo electrónico o lugar seguro, para recibir notificaciones. En el caso de que no lo facilite o renuncie expresamente a ello, no se le comunicará ninguna actuación llevada a cabo.

El plazo máximo para dar respuesta al informante sobre las actuaciones de investigación es de tres meses, a contar desde la recepción de la información. Para los casos de especial complejidad, se prevé que el plazo pueda ampliarse hasta un máximo de otros tres meses (seis meses en total).

7. Procedimiento de actuación

7.1. Trámite de recepción y registro de la información

Una vez recibida la comunicación, en un plazo no superior a siete días naturales desde su presentación, se procederá a acusar recibo al informante, siempre que haya indicado domicilio, correo electrónico o lugar seguro de recepción de comunicaciones.

En el caso de que la información se haya presentado de forma anónima o de que el informante expresamente haya renunciado a la recepción de comunicaciones relativas a las actuaciones llevadas a cabo, no se confirmará tal recepción. Tampoco se acusará recibo cuando el Responsable del Sistema considere razonablemente que el acuse de la información comprometería la protección de la identidad del informante.

Con el acuse de recibo, también se informará al informante de los derechos y garantías que le asisten durante el transcurso de la investigación.

Recibida la información, se anotará en un libro-registro, de forma segura y con acceso restringido al personal designado por el Responsable del Sistema, asignándole un código de identificación correlativo. En el referido registro se cumplimentarán los siguientes datos:

- La fecha de recepción.
- El código de identificación.
- Si procede, los datos de contacto del informante.
- Los hechos comunicados.
- Las actuaciones desarrolladas.
- Las medidas adoptadas.
- La fecha de cierre.

Los datos que se hagan constar en el registro no serán públicos y serán tratados con carácter confidencial. No obstante, y sólo en el caso de petición razonada de la autoridad judicial competente, podrá accederse al contenido del referido registro.

7.2. Trámite de admisión

Registrada la información, el Responsable del Sistema realizará un análisis preliminar, para comprobar si la información constituye algún hecho o conducta que entre dentro del ámbito de aplicación del Sistema interno de información.

Para ello, el Responsable del Sistema podrá ponerse en contacto con el informante para obtener aclaraciones o solicitar información o documentación adicional.

Realizadas las comprobaciones pertinentes, en un plazo no superior a diez días, desde la fecha de recepción de la información, el Responsable del Sistema, decidirá inadmitir o admitir a trámite la comunicación, o remitir la información al organismo público competente.

- Inadmitir la comunicación

Se inadmitirá la información, cuando se dé alguno de los siguientes supuestos:

  - Cuando los hechos relatados carezcan de toda verosimilitud.
  - Cuando los hechos relatados no sean constitutivos de infracción del ordenamiento jurídico incluida en el ámbito de aplicación del Sistema interno de información.
  - Cuando la comunicación carezca manifiestamente de fundamento o existan, a juicio del Responsable del Sistema, indicios racionales de haberse obtenido mediante la comisión de un delito. En este último caso, además de la inadmisión, se remitirá al Ministerio Fiscal relación circunstanciada de los hechos que se estimen constitutivos de delito.

- 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 de hecho o de Derecho que justifiquen un seguimiento distinto. En estos casos, el Responsable del Sistema notificará la resolución de manera motivada.

La inadmisión se comunicará al informante, salvo que la comunicación fuera anónima o se hubiera renunciado a recibir comunicaciones.

- Admitir a trámite la comunicación

La admisión a trámite se comunicará al informante, salvo que la comunicación fuera anónima o éste hubiera renunciado a recibir comunicaciones.

- Remitir la información al Ministerio Fiscal

En el caso de que los hechos pudieran ser indiciariamente constitutivos de delito, se remitirán, con carácter inmediato, al Ministerio Fiscal o a la Fiscalía Europea (en el caso de que los hechos afecten a los intereses financieros de la Unión Europea).

- Remitir la comunicación a la autoridad, entidad u organismo que se considere competente para su tramitación.

7.3. Trámite de instrucción

Una vez admitida a trámite la comunicación, el Responsable del Sistema iniciará un procedimiento de investigación, que comprenderá todas aquellas actuaciones encaminadas a comprobar la verosimilitud de los hechos relatados.

La persona afectada por la información deberá ser informada:

- De la información y de los hechos relatados de forma sucinta.
- Del derecho que tiene a presentar alegaciones por escrito.
- Del tratamiento de sus datos personales.

No obstante, esta comunicación podría efectuarse con posterioridad, si se considerara que con su aportación pudiera facilitar la ocultación, destrucción o alteración de las pruebas.

En ningún caso se comunicará a los sujetos afectados la identidad del informante ni se dará acceso a la comunicación.

La instrucción comprenderá, siempre que sea posible, una entrevista con la persona afectada en la que, siempre con absoluto respeto a la presunción de inocencia, se le invitará a exponer su versión de los hechos y a aportar aquellos medios de prueba que considere adecuados y pertinentes para su defensa.

La persona afectada tendrá acceso al expediente, sin revelar información que pudiera identificar a la persona informante, pudiendo ser oída en cualquier momento y se le advertirá de la posibilidad de comparecer asistida de abogado.

7.4. Terminación de las actuaciones

Concluidas todas las actuaciones, el Responsable del Sistema emitirá un informe que contendrá:

- La exposición de los hechos relatados, el código de identificación y la fecha de registro.
- Las actuaciones realizadas con el fin de comprobar la verosimilitud de los hechos.
- Las conclusiones alcanzadas en la instrucción y valoración de los hechos y los indicios que las sustentan.

El informe concluirá con la adopción de alguna de las decisiones siguientes:

- Archivo del expediente, que será notificado al informante y a la persona afectada.
  En estos supuestos, el informante tendrá derecho a la protección prevista en el ordenamiento, salvo que se concluyera en la instrucción que la información debería haber sido inadmitida.
- Remisión al Ministerio Fiscal, Fiscalía Europea o autoridad u organismo que se considere competente para su tramitación si, pese a no apreciar inicialmente indicios de que los hechos pudieran revestir el carácter de delito, así resultase del curso de la instrucción.

Cualquiera que sea la decisión, se comunicará al informante, salvo que la comunicación fuera anónima o hubiese renunciado expresamente a ello.

8. Canal externo de información

Además del canal de comunicación interno de PROA CAPITAL, toda persona física dispone de canales externos de información, que puede utilizar, directamente o con posterioridad a la previa formulación de información por el canal interno, para informar de las irregularidades ante la Autoridad Independiente de Protección del Informante (A.A.I.), o ante las autoridades u organismos autonómicos correspondientes:

- Servicio Nacional de Coordinación Antifraude
  https://www.igae.pap.hacienda.gob.es/sitios/igae/es-ES/snca/Paginas/inicio.aspx
- Fiscalía contra la Corrupción y la Criminalidad Organizada
  https://www.fiscal.es/
- Policía Nacional
  https://www.policia.es/_es/denuncias.php
- Tribunal de Cuentas
  https://www.tcu.es/es
- Defensor del Pueblo
  https://www.defensordelpueblo.es/
- Tribunal de Cuentas Europeo

https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/search-all-eu-institutions-and-bodies/european-court-auditors-eca_es

- Oficina Europea Antifraude
  https://anti-fraud.ec.europa.eu/about-us/what-we-do_es

A la fecha en la que se aprueba este protocolo, la Autoridad Independiente de Protección del Informante (A.A.I.) aún no ha sido creada, contando el Gobierno con un año para la aprobación de su Estatuto a partir de la entrada en vigor de la Ley de Protección del Informante.

9. Revelación pública

Se entiende por revelación pública cualquier puesta a disposición del público de información sobre irregularidades que se refieran al ámbito de protección de este Protocolo y de la Ley de protección del informante.

La persona que haga una revelación pública goza de la misma protección que los informantes que comuniquen mediante el canal de información interno o externo, siempre que se cumpla alguna de las siguientes condiciones:

- Que se haya realizado previamente la comunicación por los canales internos y externos, o directamente por canales externos, sin que se hayan tomado medidas apropiadas al respecto en el plazo establecido.

- Que tenga motivos razonables para pensar que, o bien la infracción puede constituir un peligro inminente o manifiesto para el interés público, en particular cuando se da una situación de emergencia, o existe un riesgo de daños irreversibles, incluido un peligro para la integridad física de una persona; o bien, en caso de comunicación a través de canal externo de información, exista riesgo de represalias o haya pocas probabilidades de que se dé un tratamiento efectivo a la información debido a las circunstancias particulares del caso, tales como la ocultación o destrucción de pruebas, la connivencia de una autoridad con el autor de la infracción, o que esta esté implicada en la infracción.

Cuando la persona haya revelado la información directamente a la prensa, con arreglo al ejercicio de la libertad de expresión y de información veraz previstas constitucionalmente y en su legislación de desarrollo, las condiciones para acogerse a protección no podrán ser exigibles.

10. Medidas de protección

10.1. Del informante

Las personas que comuniquen o revelen informaciones susceptibles de ser consideradas 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, y que la citada información entre dentro del ámbito de aplicación del presente Protocolo y de la Ley de protección del informante.

- La comunicación o revelación se haya realizado conforme a los requerimientos previstos en el presente Protocolo y la Ley de protección del informante.

Gozarán de la misma protección:

- Las personas que hayan comunicado o revelado públicamente información sobre acciones u omisiones, de forma anónima, pero que posteriormente hayan sido identificadas.

- Las personas que informen ante las instituciones, órganos u organismos pertinentes de la Unión Europea infracciones que entren en el ámbito de aplicación de la Directiva 2019/1937.

Por el contrario, quedan expresamente excluidos de la protección aquellas personas que comuniquen o revelen:

- Informaciones contenidas en comunicaciones que hayan sido inadmitidas por algún canal interno de información o por alguna de las causas:

    - Cuando los hechos relatados carezcan de toda verosimilitud.

    - Cuando los hechos relatados no sean constitutivos de infracción del ordenamiento jurídico incluida en el ámbito de aplicación de la Ley de protección del informante.

    - Cuando la comunicación carezca manifiestamente de fundamento o existan, a juicio del Responsable del Sistema, indicios racionales de haberse obtenido mediante la comisión de un delito.

    - 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 de hecho o de Derecho que justifiquen un seguimiento distinto.

- Informaciones vinculadas a reclamaciones sobre conflictos interpersonales o que afecten únicamente al informante y a las personas a las que se refiera la comunicación o revelación.

- Informaciones que ya estén completamente disponibles para el público o que constituyan meros rumores.

- Informaciones que se refieran a acciones u omisiones no comprendidas en el ámbito de aplicación del presente Protocolo y la Ley de protección del informante.

Prohibición de represalias

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.

PROA CAPITAL adoptará las medidas necesarias para prohibir expresamente los actos constitutivos de represalia, incluidas las amenazas de represalia y las tentativas de represalia contra las personas que presenten una comunicación, dentro de los dos años siguientes a ultimar las investigaciones.

A los efectos de lo previsto en el presente Protocolo, y a título enunciativo, se consideran represalias las que se adopten en forma de:

- 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.

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

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

- 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.

- Denegación o anulación de una licencia o permiso.

- Denegación de formación.

- 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.

Serán nulos de pleno derecho y darán lugar, en su caso, a medidas correctoras disciplinarias o de responsabilidad (incluyendo la correspondiente indemnización de daños y perjuicios al perjudicado), los actos:

- Que tengan por objeto impedir o dificultar la presentación de comunicaciones y revelaciones.

- Que constituyan represalia o causen discriminación tras su presentación.

Medidas de apoyo

Asimismo, las personas que comuniquen o revelen informaciones, podrán tener acceso a las medidas de apoyo que preste la Autoridad Independiente de Protección del Informante (A.A.I.) (u órgano competente):

- Información y asesoramiento completos e independientes, fácilmente accesibles para el público y gratuitos, sobre los procedimientos y recursos disponibles, protección frente a represalias y derechos de la persona afectada.

- Asistencia efectiva por parte de las autoridades competentes en su protección frente a represalias.

- Asistencia jurídica en los procesos penales y en los procesos civiles transfronterizos de conformidad con la normativa comunitaria.

- Apoyo financiero y psicológico, de forma excepcional, si así lo decidiese la Autoridad Independiente de Protección del Informante (A.A.I.).

Del mismo modo, las personas que comuniquen o revelen informaciones, podrán tener acceso de asistencia jurídica gratuita, para la representación y defensa en procedimientos judiciales derivados de la presentación de la comunicación o revelación pública.

Medidas de protección frente a represalias

PROA CAPITAL se compromete a adoptar las siguientes medidas necesarias para garantizar a los informantes la protección frente a represalias:

- No se considerará que las personas que comuniquen la información o que hagan una revelación pública hayan infringido ninguna restricción de revelación de información, ni incurrirán en responsabilidad de ningún tipo en relación con dicha comunicación o revelación pública, siempre que tuvieran motivos razonables para pensar que era necesaria para revelar una irregularidad.

- Los informantes no incurrirán en responsabilidad respecto de la adquisición o el acceso a la información que es comunicada o revelada públicamente, siempre que dicha adquisición o acceso no constituya un delito.

- Cualquier otra posible responsabilidad de los informantes derivada de actos u omisiones que no estén relacionados con la comunicación o la revelación pública o que no sean necesarios para revelar una infracción será exigible conforme a la normativa aplicable.

- En los procedimientos ante un órgano jurisdiccional u otra autoridad relativos a los perjuicios sufridos por los informantes, una vez que el informante haya demostrado razonablemente que ha comunicado o ha hecho una revelación pública y que ha sufrido un perjuicio, se presumirá que el perjuicio se produjo como represalia por informar o por hacer una revelación pública. En tales casos, corresponderá a la persona que haya tomado la medida perjudicial probar que esa medida se basó en motivos debidamente justificados no vinculados a la comunicación o revelación pública.

- En los procesos judiciales, incluidos los relativos a difamación, violación de derechos de autor, vulneración de secreto, infracción de las normas de protección de datos, revelación de secretos empresariales, o a solicitudes de indemnización basadas en el derecho laboral o estatutario, los informantes no incurrirán en responsabilidad de ningún tipo como consecuencia de comunicaciones o de revelaciones públicas protegidas por la misma. Dichas personas tendrán derecho a alegar en su descargo y en el marco de los referidos procesos judiciales, el haber comunicado o haber hecho una

revelación pública, siempre que tuvieran motivos razonables para pensar que la comunicación o revelación pública era necesaria para poner de manifiesto una infracción.

10.2. De la persona afectada

PROA CAPITAL garantiza a las personas afectadas por la información las siguientes medidas de protección:

- Derecho a la preservación de su identidad y confidencialidad de los hechos y datos del procedimiento.
- Derecho a que se le informe de las irregularidades que se le atribuyen.
- Derecho a la presunción de inocencia.
- Derecho a ser oído en cualquier momento.
- Derecho de defensa, a presentar alegaciones y a ser asistido por un abogado.
- Derecho de acceso al expediente.
- Derecho a que el tratamiento que se haga de sus datos personales sea de conformidad con la normativa de protección de datos.

11. Protección de datos personales

El tratamiento de los datos personales se regirá por lo dispuesto en el *Reglamento (UE) 2016/679 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* (en adelante, RGPD) y su normativa nacional específica.

Quien presente una comunicación o lleve a cabo una revelación pública tiene derecho a que su identidad no sea revelada a terceras personas. La identidad del informante sólo podrá ser comunicada a la Autoridad judicial, al Ministerio Fiscal o a la autoridad administrativa competente en el marco de una investigación penal, disciplinaria o sancionadora.

En ningún caso se comunicará la identidad del informante o de la persona que haya llevado a cabo la revelación pública, a la persona a la que se refieran los hechos relatados.

No se tratarán datos personales o, en su caso, se suprimirán aquéllos que se puedan haber comunicado, que no sean necesarios para el conocimiento de las irregularidades.

Tampoco se recopilarán datos personales cuya pertinencia no resulte manifiesta para tratar una información específica. Si se recopilan datos personales por accidente, se eliminarán sin dilación indebida.

Cualquier interesado puede ejercitar los derechos de acceso, rectificación, supresión, oposición, limitación del tratamiento y/ o portabilidad, respecto de sus datos de carácter personal, por escrito a la dirección de PROA CAPITAL, o bien enviando un correo electrónico a info@proacapital.com. Igualmente, puede presentar una reclamación ante la Agencia Española de Protección de Datos (www.aepd.es).

En caso de que la persona a la que se refieran los hechos relatados en la comunicación o a la que se refiera la revelación pública ejerciese el derecho de oposición, se presumirá que, salvo prueba en contrario, existen motivos legítimos imperiosos que legitiman el tratamiento de sus datos personales.

La licitud para el tratamiento de datos personales es la siguiente:

- Canal interno de información:

    - En virtud del art. 6.1.c) del RGPD (el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento), cuando el canal interno de información sea obligatorio.

    - En virtud del art. 6.1.e) del RGPD (el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento), cuando el canal interno de información no sea obligatorio.

- Canal externo de información: En virtud del art. 6.1.e) del RGPD.

- Revelación pública: En virtud del art. 6.1.e) del RGPD, cuando el canal interno de información no sea obligatorio.

- Tratamiento de categorías especiales de datos personales: En virtud del art. 9.2.g) del RGPD (el tratamiento es necesario por razones de un interés público esencial, sobre la base del Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado).

El tiempo de conservación de los datos personales será el imprescindible para decidir sobre la procedencia de iniciar una investigación sobre los hechos informados.

En todo caso, 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. Las comunicaciones a las que no se haya dado curso solamente podrán constar de forma anonimizada.

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 cualquier caso, el acceso a los datos personales contenidos en el Sistema interno de información quedará limitado, dentro del ámbito de sus competencias y funciones, exclusivamente, a:

- El Responsable del Sistema y a quien lo gestione directamente.

- El responsable de recursos humanos o el órgano competente debidamente designado, solo cuando pudiera proceder la adopción de medidas disciplinarias contra un trabajador.

- El responsable de los servicios jurídicos de la entidad u organismo, si procediera la adopción de medidas legales en relación con los hechos relatados en la comunicación.

- Los encargados del tratamiento que eventualmente se designen.

- 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 será lícito el tratamiento de los datos por otras personas, o incluso su comunicación a terceros.

12. Revisión y actualización

El presente Protocolo ha sido aprobado por el Órgano de Administración de PROA CAPITAL, en su reunión de 21 de agosto de 2023, entrando en vigor en este mismo momento.

Este Protocolo será revisado, actualizado, aprobado y difundido de manera periódica y siempre que resulte necesario practicar cualquier modificación.