EMPRESA

Denominación	**FITO & ASOCIADOS, GESTIÓN DE RIESGOS, S.L.** (en adelante, "la Empresa")
CIF	B-15.826.290

Índice de contenidos

Introducción

En la Empresa disponemos de un **Sistema Interno de Información** para proteger a las personas que en un contexto laboral o profesional detecten infracciones penales o administrativas graves o muy graves y las comuniquen a través de este canal. La puesta en funcionamiento de este Sistema Interno de Información tiene como finalidad detectar de forma temprana posibles irregularidades en el seno de la organización y adoptar medidas preventivas que impidan su futura comisión, contribuyendo a la mejora continua de nuestros procesos internos de control.

Para lograr este objetivo, disponemos de una herramienta web y una cuenta de correo electrónico, gestionadas por INADE, INSTITUTO ATLÁNTICO DEL SEGURO, S.L., concebidas como un cauce seguro de presentación de denuncias, que garantiza la confidencialidad y la indemnidad del informante de buena fe, a la vez que asegura la confidencialidad de la información que éste facilite, todo ello sin perjuicio de que puedan dirigir sus denuncias o informaciones a la **Autoridad Independiente de Protección del Informante** o a cualquier otra institución, órgano u organismo competente.

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 faculta a la Empresa a tratar los datos de carácter personal de informante y denunciado en base al cumplimiento de una obligación legal (apartado 6.1.c. del Reglamento General de Protección de Datos).

1. ¿Qué se puede denunciar?

A través del Sistema Interno de Información, se podrá poner en conocimiento:

a) Que se ha cometido en la Empresa cualquiera de las infracciones tipificadas, como:

- Acciones u omisiones que puedan constituir infracciones del Derecho de la Unión Europea, siempre que:

  - Entren dentro del ámbito de aplicación de los actos de la Unión enumerados en el Anexo de la Directiva (UE) 2019/1937, con independencia de la calificación que de las mismas realice el ordenamiento jurídico interno.

    A tal efecto, debe tenerse presente que la citada Directiva establece normas mínimas comunes para la protección de las personas que informen sobre infracciones del Derecho de la Unión; es decir, infracciones que entren dentro del ámbito de aplicación de los actos de la Unión (enumeradas en el anexo) relativas a los ámbitos de contratación pública, servicios, productos y mercados financieros, prevención del blanqueo de capitales y 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; o

  - 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); o

  - 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 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.

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

b) Que se ha producido en la misma cualquier otro incumplimiento normativo de las siguientes normas:

- La normativa en materia de distribución de seguros:
  - Libro Segundo, Título I del Real Decreto-ley 3/2020, de 4 de febrero, de medidas urgentes por el que se incorporan al ordenamiento jurídico español diversas directivas de la Unión Europea en el ámbito de la contratación pública en determinados sectores; de seguros privados; de planes y fondos de pensiones; del ámbito tributario y de litigios fiscales.

- La normativa en materia de prevención del blanqueo de capitales y de la financiación del terrorismo:
  - Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo.
  - Real Decreto 304/2014, de 5 de mayo, por el que se aprueba el Reglamento de la Ley 10/2010 de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo.

- La normativa en materia de protección de datos y garantía de los derechos digitales:
  - 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 por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).
  - Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

- La normativa en materia laboral:
  - Real Decreto Legislativo 2/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores.
  - Real Decreto Legislativo 5/2000, de 4 de agosto, por el que se aprueba el texto refundido de la Ley sobre Infracciones y Sanciones en el Orden Social.
  - Ley Orgánica 3/2007, de 22 de marzo, para la igualdad efectiva de mujeres y hombres.

- La normativa penal:
  - Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.

- Los códigos, protocolos y normas internas de la empresa.

Sin perjuicio de cualquier otra norma complementaria de las categorías anteriormente descritas que suponga una infracción penal o administrativa.

2. ¿Quién puede denunciar?

Podrán denunciar las siguientes **personas** vinculadas con la Empresa:

1. Trabajadores por cuenta ajena.

2. Que hayan tenido en el pasado la condición de trabajadores por cuenta ajena.

3. Que presten a la empresa servicios como trabajadores por cuenta propia (mediante contratos mercantiles, contratos de servicios profesionales o similares).

4. Que hayan prestado a la empresa en el pasado servicios como trabajadores por cuenta propia (mediante contratos mercantiles, contratos de servicios profesionales o similares).

5. Los accionistas o titulares de participaciones sociales de la misma, así como sus administradores y directivos. Si la empresa tiene un órgano colegiado de administración se consideran incluidos en este punto también sus miembros no ejecutivos.

6. Cualquier persona que trabaje para o bajo la supervisión y la dirección de contratistas, subcontratistas y proveedores.

7. El personal que se encuentre realizando prácticas, ya sean estas remuneradas o no.

8. Los colaboradores externos.

9. Que participen en procesos de selección.

10. Que se encuentren en cualquiera de las categorías anteriores con respecto a otras personas jurídicas integradas en el mismo grupo de empresas al que pertenece la Empresa.

3. ¿Qué requisitos tienen que cumplir las denuncias?

El Sistema Interno de Información admite **denuncias anónimas o nominales**, sin perjuicio de la confidencialidad, indemnidad y protección de la identidad de los informantes, así como la confidencialidad de las informaciones facilitadas.

Sin perjuicio de la herramienta web, se ofrece también la posibilidad de comunicar cualquier conducta de manera verbal mediante la petición por parte del informante de una reunión presencial con el Responsable del Sistema Interno de Información.

El presente procedimiento resultará de aplicación para todas aquellas comunicaciones e informaciones recibidas en el Sistema Interno de Información, con independencia de si se reciben o no por alguna de las vías previstas.

La denuncia debe contener unos requisitos mínimos que posibiliten una investigación posterior. A fin de que pueda ser considerada como tal, deberá contener los siguientes datos:

- Nombre y NIF de la Empresa (no será necesario en caso de que la denuncia sea registrada en la herramienta web)
- En caso de no ser anónima: nombre y correo electrónico a efectos de notificaciones de la persona o personas autoras de la denuncia.
- Relación con la empresa denunciada.
- Cuando sea posible, identificación del denunciado y/o indicación de su cargo.
- Cuando sea posible, identificación de testigos y/o indicación de su cargo.
- ¿El hecho ha sido comentado con algún miembro de la dirección?
- Descripción detallada de la conducta potencialmente ilegal, ilícita o irregular (medios empleados para su comisión, fecha aproximada en que tuvo lugar, área de la empresa o lugar en que se cometió, y persona/s presuntamente implicada/s).

El autor de la denuncia podrá acompañarla de cuantos documentos, vídeos, audios o pruebas de cualquier tipo estime convenientes para acreditar los hechos denunciados.

4. Principios que rigen el Sistema Interno de Información

El Sistema Interno de Información se rige por los siguientes principios:

- Ausencia de represalias y protección al informante.
- Seguridad, confidencialidad y, en su caso, anonimato, en el uso del Sistema Interno de Información.
- Sometimiento de las actuaciones de verificación a la presunción de inocencia y al respeto al derecho al honor para los afectados por las informaciones remitidas.
- Respeto al derecho a la protección de datos de carácter personal.
- Autonomía e independencia del Responsable y del Gestor del Sistema Interno de Información en el ejercicio de sus funciones, así como deber de sigilo y reserva respecto de toda información de la que tenga conocimiento como consecuencia de las mismas.

5. Protección y garantía de confidencialidad e indemnidad de los informantes

Los informantes deben tener motivos razonables para creer, a la luz de las circunstancias y de la información de que dispongan en el momento de la denuncia, que los hechos que denuncian son ciertos.

El Sistema Interno de Información protegerá, en la máxima medida posible, la confidencialidad de la identidad del informante de buena fe. Igualmente, se garantizará la indemnidad del informante de buena fe, sin que se pueda producir reacción o represalia alguna contra él, como consecuencia del hecho de denunciar e informar a través del Sistema.

El informante sólo perderá su derecho a la confidencialidad y la indemnidad en el caso de que su denuncia haya sido efectuada de mala fe. Se entiende que una denuncia es realizada de mala fe cuando el informante:

1. Sea consciente de la falsedad de los hechos que denuncia.

2. Actúe con manifiesto desprecio de la verdad, tergiversando o manipulando los hechos que denuncia con:

    - la intención de venganza o de perjudicar a la persona denunciada y/o a la Empresa, o

    - con la intención de lesionar el honor o perjudicar la reputación laboral, profesional o empresarial de cualquier persona o entidad vinculada a la misma.

Al margen de lo dispuesto en el número 2 del párrafo anterior, los motivos de los informantes al denunciar deben ser irrelevantes para determinar si esas personas deben recibir protección.

6. Medidas de Protección del Informante

Aquellas personas que utilicen este Sistema Interno de Comunicación para enviar sus comunicaciones están protegidas por las **disposiciones de salvaguardia del informante** establecidas en el Título VII de la Ley 2/2023, de 20 de febrero.

En cualquier caso, únicamente otorgarán la condición de informante conforme a lo dispuesto en la Ley 2/2023 y los derechos establecidos en el Título V en su integridad, aquellas comunicaciones que se refieran a infracciones descritas en el apartado 1 letra a) de esta política, que se presenten por las personas descritas en el apartado 2.

Estas medidas de protección se resumen de la siguiente manera:

- Se prohíben de manera expresa los **actos de represalia** (incluyendo las amenazas y los intentos de represalia) contra quienes presenten una comunicación. Entre dichas represalias se incluyen, entre otras, el despido, la suspensión del contrato, la no renovación o finalización anticipada de contratos temporales, la imposición de sanciones disciplinarias, la degradación profesional, la denegación de ascensos, la modificación sustancial de las condiciones de trabajo, la intimidación, el acoso, la discriminación o cualquier trato desfavorable derivado de la comunicación realizada.

  Esta protección se extenderá durante el plazo legalmente previsto de dos años desde la finalización de la investigación o desde la finalización del procedimiento correspondiente, pudiendo prorrogarse en los supuestos legalmente establecidos.

  No obstante, podrán adoptarse medidas laborales o disciplinarias cuando estas respondan a causas objetivas, debidamente acreditadas y completamente ajenas a la presentación de la comunicación, correspondiendo a la entidad justificar dicha desvinculación cuando resulte procedente.

  Los actos administrativos o decisiones empresariales que tengan por finalidad impedir o dificultar la presentación de comunicaciones, así como aquellos que constituyan represalias o discriminación, serán nulos de pleno derecho.

- Se brindan **medidas de apoyo** que incluyen información y asesoramiento sobre los procedimientos y recursos disponibles para protegerse de las represalias, asistencia legal en procesos penales y civiles transfronterizos, así como apoyo financiero y psicológico en caso de necesidad.

- Se establecen medidas de **protección contra las represalias**. Aquellas personas que informen sobre acciones u omisiones contempladas en la Ley 2/2023, de 20 de febrero, o que hagan una revelación pública, no serán consideradas como infractoras de ninguna restricción de

divulgación de información. No se les imputará responsabilidad alguna en relación con dicha comunicación ni en relación con la adquisición o acceso a la información comunicada, siempre y cuando esa adquisición o acceso no constituya un delito. En los procedimientos judiciales u otras instancias relacionadas con los daños sufridos por los informantes, la carga de la prueba recae sobre la persona que haya causado perjuicio al informante.

- Se contempla la **exención o reducción de sanciones para los informantes** que hayan participado en la infracción de la cual informan, siempre y cuando dicha comunicación se realice antes de la notificación oficial de un procedimiento de investigación o sancionador.

7. ¿A quién dirigirse?

La gestión externa del Sistema Interno de Información ha sido encomendada a INADE, INSTITUTO ATLÁNTICO DEL SEGURO S.L., con N.I.F. B-36.851.350, que actúa en calidad de encargado del tratamiento de datos personales conforme a la normativa vigente.

Las comunicaciones podrán presentarse a través de cualquiera de los siguientes canales habilitados:

- Mediante mensaje de correo electrónico dirigido a denuncias@inade.org
- A través de la plataforma accesible mediante el enlace facilitado.
- Telefónicamente, a través del número 986 485 228.

El Sistema permite la presentación de comunicaciones tanto identificadas como anónimas, garantizándose en todo caso la máxima confidencialidad durante todo el procedimiento y el acceso restringido exclusivamente al personal autorizado.

8. Obligaciones de INADE, INSTITUTO ATLÁNTICO DEL SEGURO S.L.

1. INADE Deberá adoptar las medidas necesarias para salvaguardar la identidad del informante.

2. INADE en ningún momento revelará el nombre del informante, salvo que:

   - Sea requerida para ello, judicialmente o por la autoridad competente.

   - Existan fundadas razones objetivas para entender que la denuncia se ha formulado de mala fe y el responsable del Sistema Interno de Información solicitase por escrito que le facilite la identidad del informante, a los solos efectos de promover las medidas disciplinarias que resulten de aplicación.

     Para que existan fundadas razones objetivas de que la denuncia se ha formulado de mala fe, será imprescindible:

     a) Que el responsable Sistema Interno de Información de la Empresa u órgano equivalente aporte pruebas objetivas suficientes de la presencia de mala fe.

     b) Y que se hayan trasladado esas pruebas al informante, dándole la oportunidad de defenderse frente a la acusación de mala fe.

     Sólo si tras estos trámites persisten las fundadas razones objetivas para entender que la denuncia es de mala fe, se podrá revelar la identidad del informante.

     Fuera de estos supuestos, si el responsable del Sistema Interno de Información de la empresa considerase necesario contactar con el informante con el fin de obtener más información para el adecuado análisis y gestión de la denuncia, ese contacto se realizará a través de INADE, preservando el carácter confidencial de su identidad.

3. INADE enviará al informante acuse de recibo en un plazo máximo de siete días desde la recepción de la denuncia.

4. INADE comunicará la información tratada únicamente al responsable del Sistema Interno de Información para que pueda proceder a la averiguación de los hechos de los que se informa y, en su caso, adoptar las medidas que pudieran corresponder.

9. Protección de datos

INADE gestionará el Sistema Interno de Información garantizando el cumplimiento de las normas de protección de datos de la Unión Europea ya que la puesta en marcha de este programa implica el tratamiento de datos personales tanto del informante como del denunciado y/o de otros terceros involucrados en los hechos objeto de denuncia.

INADE tratará los datos personales de forma leal y lícita; sólo los recogerá para cumplir con los fines determinados, explícitos y legítimos que se señalan en el presente documento y nunca los utilizará para fines incompatibles con aquellos. Asimismo, se limitará a tratar los datos que sean adecuados, pertinentes y no excesivos en relación con los fines para los que se recaban y/o para los que se traten posteriormente.

INADE adoptará las medidas adecuadas para garantizar que los datos que sean imprecisos o incompletos se supriman o rectifiquen.

Igualmente, INADE tomará todas las precauciones técnicas y de organización adecuadas para preservar la seguridad de los datos en el momento de su recopilación, circulación o conservación con el objetivo de protegerlos de su destrucción accidental o ilícita o de su pérdida accidental y difusión o acceso no autorizado.

Estas medidas de seguridad serán proporcionadas al objetivo de investigar las cuestiones planteadas.

10. Derechos del denunciado

El denunciado y las terceras partes implicadas (responsables de la actividad del denunciado u otros posibles afectados), tienen derecho a conocer en un plazo máximo de tres meses la existencia de una denuncia en su contra. Este deber de información no implica en ningún caso revelar al denunciado la identidad del informante, o datos que permitan conocer o deducir su identidad, sino únicamente:

1. Que ha sido denunciado a través del Sistema Interno de Información implantado en la Empresa.

2. Cuáles son los hechos denunciados.

3. De la confidencialidad del sistema.

4. De la posible comunicación de los datos a Jueces y Tribunales o a las personas, físicas o jurídicas, que se considere pertinentes, implicadas en cualquier fase de la investigación.

5. De la razón social y dirección del responsable del fichero que realice el tratamiento de la información.

6. De la finalidad del tratamiento de los datos.

7. De la forma y dirección para ejercer los derechos de acceso (en ningún caso a la identidad y datos personales del informante), rectificación, cancelación y oposición.

8. No podrá obtener información sobre la identidad del informante salvo cuando este realice una declaración falsa de mala fe.

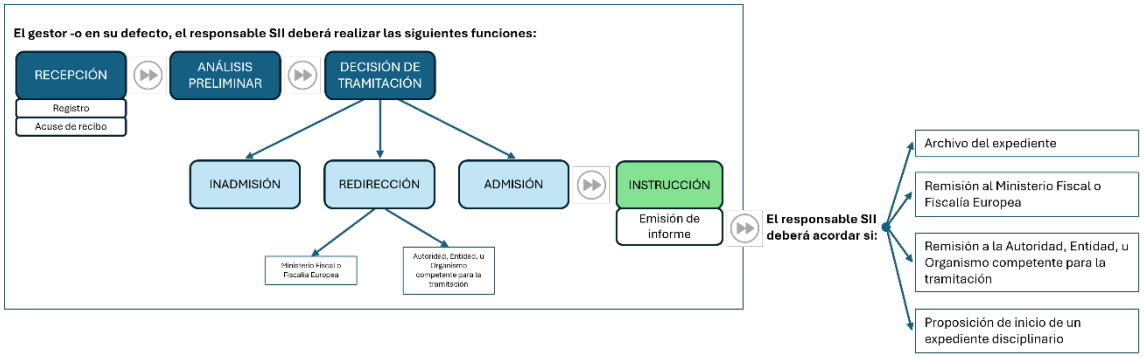
11. Plazos de conservación

Los datos personales tratados por el Sistema Interno de Información deberían suprimirse en un plazo máximo de tres meses desde la recepción de los datos.

Transcurridos los tres meses los datos podrán seguir siendo tratados por el órgano al que corresponda la investigación de los hechos denunciados, no conservándose en el propio Sistema Interno de Información.

Los datos personales relativos a las denuncias no fundamentadas se eliminarán sin dilación.

12. Procedimiento



PASO 1: RECEPCIÓN DE LA COMUNICACIÓN

El gestor -o en su defecto, el responsable del SII- recibe la comunicación.

1º. Registro

El gestor registra internamente la comunicación recibida con la siguiente información (si se ha recibido a través de la herramienta web se realiza automáticamente; para el resto de los casos se debe realizar de forma manual):

Fecha de recepción	Nombre, apellidos, e-mail y teléfono del informante (salvo si ha optado por mantener el anonimato)
Código de identificación	Descripción de la conducta o situación que el informante entiende que supone un incumplimiento.
Categoría de comunicación	Registro de documentos, archivos o cualquier otro medio de prueba de los cuales pueda disponer el informante en relación con los hechos comunicados.
Identificación de las personas involucradas y/o testigos	
Posición o relación con la entidad de las personas involucradas	

2º. Acuse de Recibo

El gestor debe emitir un acuse de recibo de la comunicación en el plazo de los 7 días naturales siguientes a la recepción, salvo que el informante haya renunciado expresamente a recibir comunicaciones relativas a la investigación, o que se considere razonablemente que el acuse de recibo de la información comprometería la confidencialidad de la comunicación.

En su caso, se debe proceder a la subsanación de defectos.

PASO 2: ANÁLISIS PRELIMINAR

El gestor -o en su defecto, el responsable del SII- procede a un análisis preliminar de la comunicación.

El GESTOR/RESPONSABLE SII, con el fin de decidir sobre su admisión o inadmisión a trámite, podrá solicitar al informante aclaración o que complemente de los hechos denunciados o la aportación de documentación acreditativa de la infracción.

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

PASO 3: DECISIÓN DE TRAMITACIÓN

Realizado el análisis preliminar, el gestor -o en su defecto, el responsable del SII- decidirá:

1º. INADMISIÓN

Se podrá proceder a no admitir la comunicación cuando:

- Los hechos carezcan de toda verosimilitud
- La comunicación carezca manifiestamente de fundamento
- Los hechos no sean constitutivos de infracción incluida en el ámbito de aplicación del SII.
- 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.
- En los casos de comunicaciones formuladas por personas que no estén incluidas en el ámbito subjetivo

2º. REDIRECCIÓN:

→ **Remisión al Ministerio Fiscal o Fiscalía Europea**

Cuando los hechos pudieran ser indiciariamente constitutivos de delito, se remitirá al Ministerio Fiscal.

En el caso de que los hechos afecten a los intereses financieros de la Unión Europea, se remitirá a la Fiscalía Europea

→ **Remisión a la Autoridad, Entidad, u Organismo competente para la tramitación**

Cuando, de acuerdo a la entidad de la información recibida, se considere que no debe procederse a una investigación complementaria, podrá decidirse remitir directamente los hechos a la autoridad, entidad u organismo competente. Los mismos, sin carácter limitativo, pueden ser:

- SEPBLAC (Servicio Ejecutivo de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias)
- Ministerio de Hacienda / Agencia Tributaria
- Inspección de Trabajo y Seguridad Social
- AEPD (Agencia Española de Protección de Datos)
- OLAF (Oficina Europea de Lucha contra el Fraude)
- CNMC (Comisión Nacional de los Mercados y la Competencia)

3º. ADMISIÓN

Una vez admitida a trámite la comunicación, ésta se remitirá al instructor, que llevará a cabo todas las actuaciones precisas para esclarecer los hechos comunicados.

Se debe levantar acta de todas las actuaciones.

Al finalizar las actuaciones, el instructor debe elaborar un informe sobre las conclusiones alcanzadas en la instrucción.

PASO 4: INSTRUCCIÓN

El órgano/persona encargada de la instrucción deberá revisar los hechos acontecidos a fin de emitir un Informe

La persona afectada será informada de las acciones u omisiones que se le atribuyen, al inicio de la instrucción o durante trámite de audiencia si su información previa pudiera suponer alteración, destrucción u ocultación de pruebas.

Se le informará de sus derechos de defensa, presunción de inocencia, protección del honor, derecho a ser oído y a presentar alegaciones.

En su caso, se puede acordar la adopción de medidas cautelares y urgentes de forma coordinada con los órganos o responsables correspondientes de la entidad.

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 pertinentes para su defensa.

A fin de garantizar el derecho de defensa de la persona afectada, la misma 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.

Concluidas todas las actuaciones, el instructor emitirá un INFORME que contendrá:

- Exposición de los hechos e información del registro de la comunicación.
- Actuaciones realizadas
- Conclusiones de la instrucción y valoración de hechos e indicios que las sustentan.

PASO 5: RESOLUCIÓN DEL EXPEDIENTE POR EL RESPONSABLE DEL SII

Tras el informe del instructor, el responsable del SII adoptará alguna de las siguientes decisiones:

❒ Archivo del expediente (se notificará a las partes). En este supuesto, el informante tendrá derecho a la protección prevista en la Ley 2/2023, de 20 de febrero, salvo que, a consecuencia de las actuaciones llevadas a cabo en fase de instrucción, se concluyera que la comunicación a la vista de la información recopilada tenía que haber sido inadmitida.

❒ Remisión al Ministerio Fiscal o a la Fiscalía Europea: Remisión al Ministerio Fiscal si, pese a no apreciar inicialmente indicios de que los hechos pudieran revestir el carácter de delito, así resultase del curso de la instrucción. Si el delito afectase a los intereses financieros de la Unión Europea, lo remitirá a la Fiscalía Europea.

❒ Remisión a la Autoridad, Entidad, u Organismo competente para la tramitación

❒ Proposición de inicio de un expediente disciplinario conforme a la normativa de aplicación y/o adopción de medidas por el órgano interno competente.

13. Conflicto de intereses

Con el fin de garantizar la imparcialidad, independencia y objetividad en la gestión de las informaciones recibidas a través del Sistema Interno de Información (SII), cualquier persona que intervenga en su tramitación —incluyendo al gestor del sistema, al Responsable del SII y, en su caso, a los instructores o personas designadas para la investigación— deberá abstenerse de participar cuando concurra alguna circunstancia que pueda comprometer su neutralidad o generar un conflicto de intereses.

Se entenderá que existe conflicto de intereses, entre otros supuestos, cuando exista una relación personal, familiar, económica o de cualquier otra naturaleza con la persona informante, la persona afectada o con los hechos objeto de investigación que pudiera influir, o aparentar influir, en la toma de decisiones.

En estos casos, la persona afectada deberá comunicarlo de forma inmediata al órgano competente y abstenerse de intervenir en el procedimiento hasta su finalización, siendo sustituida por la persona que se designe conforme a la organización interna de la entidad.

Asimismo, cualquier persona interesada podrá promover su recusación mediante escrito motivado, cuando existan razones objetivas que justifiquen la falta de imparcialidad. La recusación será valorada y resuelta con la debida confidencialidad y sin dilaciones indebidas.

La falta de comunicación de una situación de conflicto de intereses podrá dar lugar a la adopción de las medidas internas que correspondan, sin perjuicio de las posibles responsabilidades legales o disciplinarias que pudieran derivarse.

14. Canales externos de información y Autoridad Independiente de protección del Informante

Sin perjuicio del Sistema Interno de Información establecido por la EMPRESA, las personas informantes podrán acudir igualmente a los canales externos habilitados por las distintas Administraciones Públicas y los organismos competentes en materia de protección del informante, lucha contra el fraude o prevención de infracciones normativas.

Con la finalidad de mantener permanentemente actualizada la información relativa a dichos canales externos y evitar modificaciones continuas de la presente Política, la relación completa de autoridades competentes, canales autonómicos y organismos supranacionales se encuentra disponible a través del siguiente enlace externo:

Canales Externos de Información

Entre otros, dicho enlace recoge información relativa a:

- La Autoridad Independiente de Protección del Informante (A.A.I.).
- Las autoridades autonómicas competentes.
- La Oficina Europea de Lucha contra el Fraude (OLAF).
- La Fiscalía Europea (EPPO).
- El Servicio Ejecutivo de la Comisión de Prevención de Blanqueo de Capitales e Infracciones Monetarias (SEPBLAC).
- El Servicio Nacional de Coordinación Antifraude (SNCA).

Se revisará periódicamente dicho enlace con el objetivo de procurar que la información facilitada se mantenga actualizada y accesible para todas las personas interesadas.

15. Responsable del Sistema Interno de Información

El Órgano de Administración de la organización designará formalmente a la persona Responsable del Sistema Interno de Información, de conformidad con lo establecido en el artículo 8 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.

El Responsable del SII debe desempeñar sus funciones con plena independencia y autonomía, sin recibir instrucciones en lo que respecta a la tramitación de las informaciones recibidas a través del Sistema Interno de Información.

Entre sus funciones principales se incluyen, entre otras, las siguientes:

- La correcta gestión y supervisión del Sistema Interno de Información.
- La recepción, análisis preliminar y tramitación de las comunicaciones recibidas.
- La adopción de las decisiones de admisión o inadmisión de las informaciones, cuando proceda.
- La coordinación de las actuaciones de investigación interna que puedan derivarse de las comunicaciones.
- La garantía de la confidencialidad de la identidad del informante y de las personas afectadas.
- La supervisión del cumplimiento de los plazos y garantías establecidos en la normativa aplicable.
- La propuesta de medidas correctoras o de mejora del sistema a los órganos de administración, cuando resulte procedente.

El Responsable del SII podrá contar con el apoyo de personal interno o externo para el desarrollo de sus funciones, sin perjuicio de que la responsabilidad última sobre el sistema recaiga en la persona designada.

Asimismo, deberá abstenerse de intervenir en aquellos procedimientos en los que pudiera existir conflicto de intereses, de conformidad con lo previsto en la presente política.

Asimismo, el nombramiento, identidad y cese del Responsable del SII serán debidamente notificados a la Autoridad Independiente de Protección del Informante (AIPI), de conformidad con lo establecido en la Ley 2/2023, de 20 de febrero.

16. Revisión de la política

INADE, como gestor del Sistema Interno de Información revisará regularmente el contenido de la Política, asegurándose de que recoge las recomendaciones y las mejores prácticas internacionales en vigor en cada momento, y propondrá al órgano de Administración las modificaciones y las actualizaciones que contribuyan a su desarrollo y a su mejora continua.

Versión del documento	Fecha de aprobación	Objeto de la actualización	Apartados afectados
PSII 01/2023	17/NOVIEMBRE/2023		
PSII 02/2026	26/JUNIO/2026	Ampliación de las medidas de protección al informante Ampliación del procedimiento de gestión Adaptación a la constitución de la Autoridad Independiente de Protección al Informante	6. Medidas de Protección del Informante 12. Procedimiento de gestión 13. Conflicto de intereses 14. Canales externos de información y autoridad independientes de protección del informante 15. Responsable del Sistema Interno de Información