



PROCEDIMIENTO DE GESTIÓN DEL SISTEMA INTERNO DE INFORMACIÓN DEL COLEGIO OFICIAL DE INGENIEROS INDUSTRIALES DE ANDALUCÍA OCCIDENTAL

ÍNDICE

1. Introducción y objeto.
2. Comunicaciones a través del Canal externo de información.
3. Ámbito de aplicación.
 - 3.1. Ámbito objetivo de aplicación. Hechos que pueden ser objeto de comunicación.
 - 3.2. Ámbito subjetivo de aplicación. ¿Quién puede comunicar una información?
4. Principios que rigen el sistema interno de información.
 - 4.1. Confidencialidad.
 - 4.2. Anonimato.
 - 4.3. Gestión de conflictos de interés.
 - 4.4. Derecho a la información.
 - 4.5. No represalias. Protección del informante.
 - 4.6. Presunción de inocencia y derecho de defensa del afectado.
 - 4.7. Protección de los datos personales. Conservación de la información.
5. Procedimiento de gestión de las informaciones recibidas.
 - 5.1. Fase de Investigación.
 - 5.1.1. Acceso al canal interno de información. Vías externas de información.
 - 5.1.2. Formalización y admisión a trámite de la comunicación.
 - 5.1.3. Investigación.
 - 5.2. Fase de conclusiones.
 - 5.2.1. Informe y resolución.
6. Entrada en vigor.
7. Anexos:
 - 7.1. Anexo I. Categorías de comunicaciones al canal interno de información.
 - 7.2. Anexo II. Listado de acciones consideradas como represalias.



1. Introducción y objeto.

El objeto del presente procedimiento es regular la recepción, tratamiento, investigación y resolución de las comunicaciones sobre presuntas irregularidades o incumplimientos legales (de los que aparecen recogidos en el apartado 2.2. de este documento) cometidos por personal o directivos del COLEGIO OFICIAL DE INGENIEROS INDUSTRIALES DE ANDALUCÍA OCCIDENTAL en el ejercicio de su actividad.

Además, el procedimiento busca asegurar que durante todo el proceso se garantice eficazmente la protección de la persona informante frente a cualquier tipo de represalia, así como la privacidad de las personas involucradas y la confidencialidad sobre los datos contenidos en la información que se comunique, pudiendo realizarse la misma de forma anónima si así lo considera la persona informante.

El presente Canal interno de información cumple todos los requerimientos establecidos en la Directiva 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 de Derecho de la Unión, así como en 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 el caso de que un interesado utilice el presente canal para cualquier otra comunicación o información fuera del ámbito de lo recogido en el apartado 2.2 de este documento y en el artículo 2 de la referida Ley 2/2023, puede quedar excluido de la protección dispensada por la misma.

2. Comunicaciones a través del Canal externo de información.

De acuerdo con lo establecido en el artículo 16 de la Ley 2/2023, cualquier persona física podrá informar ante la **Autoridad Independiente de Protección del Informante, A.A.I.** de la comisión de cualquiera de las infracciones incluidas en el artículo 2 de la Ley anteriormente citada. Dicha información podrá ser directamente o con posterioridad a la comunicación a través del presente canal interno.

La Autoridad autonómica competente como canal externo de información en la Comunidad Autónoma de Andalucía es la **Oficina Andaluza contra el Fraude y la Corrupción**, con NIF nº: Q-4100967-A, y cuya sede está en el Hospital de las Cinco Llagas, calle San Juan de Ribera, s/n; DP.: 41009 de Sevilla, con teléfono 945 592 120 y dirección web: <https://antifraudeandalucia.es>



3. Ámbito de aplicación.

3.1. **Ámbito objetivo de aplicación. Hechos que pueden ser objeto de comunicación.**

El Canal interno de información no consiste en un sistema de contacto entre empleados, usuarios, proveedores y resto de interesados por una parte y el COLEGIO OFICIAL DE INGENIEROS INDUSTRIALES DE ANDALUCÍA OCCIDENTAL por otra, para trasladar quejas, reclamaciones, propuestas, etc. que se aparten de la auténtica finalidad de este instrumento, que no es otra que la de la información o denuncia de conductas, irregularidades o incumplimientos que puedan representar una infracción grave de la legislación vigente y especialmente en el ámbito penal y administrativo y del Derecho de la Unión Europea. En concreto, los hechos objeto de comunicación por este Canal interno serán los recogidos expresamente en el artículo 2 de la Ley 2/2023, reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción.

En el **Anexo I** se especifican posibles categorías de comunicaciones sobre hechos denunciados a través de este Canal.

3.2. **Ámbito subjetivo de aplicación. ¿Quién puede comunicar una información?**

En general, cualquier persona, formen parte o no de la Entidad, que tengan conocimiento de la comisión de un hecho denunciado en el seno de la misma, lo que incluye, en todo caso: Empleados, tanto antiguos como actuales o potenciales (que hayan participado en un proceso de selección), accionistas o directivos, incluidos miembros, ejecutivos o no, de los órganos de dirección, cualquier persona que trabaje para o bajo la supervisión y la dirección de contratistas, subcontratistas y proveedores, voluntarios, becarios.

A todos los mencionados en el párrafo anterior, así como a los representantes legales de las personas trabajadoras en el ejercicio de funciones de asesoramiento y apoyo al informante, a las personas físicas que estén relacionadas con el informante y que puedan sufrir represalias, como compañeros de trabajo o familiares, y a 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 participación significativa, les serán de aplicación las medidas de protección del informante que prevé la Ley 2/2023.



4. Principios que rigen el sistema interno de información.

4.1. Confidencialidad.

El Sistema Interno de Información del que forma parte este Canal está diseñado, establecido y gestionado de una forma segura, de modo que se garantiza la confidencialidad de la identidad del informante y de cualquier tercero mencionado en la comunicación, así como de las actuaciones que se desarrollen en la gestión y tramitación de la misma, así como la protección de datos, impidiendo el acceso de personal no autorizado.

Igualmente, se garantiza la confidencialidad cuando la comunicación sea remitida por canales de denuncia que no sean los establecidos en este Procedimiento o a miembros del personal no responsable de su tratamiento, al que se habrá formado en esta materia y advertido de la tipificación como infracción muy grave de su quebranto y, asimismo, el establecimiento de la obligación del receptor de la comunicación remitida inmediatamente al Responsable del Sistema.

La identidad del informante solo 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. Las revelaciones hechas en virtud de este apartado estarán sujetas a salvaguardas establecidas en la normativa aplicable. En particular, se trasladará al informante antes de revelar su identidad, salvo que dicha información pudiera comprometer la investigación o el procedimiento judicial. Cuando la autoridad competente lo comunique al informante, le remitirá un escrito explicando los motivos de la revelación de los datos confidenciales en cuestión.

4.2. Anonimato.

El informante que presente una comunicación a través del Canal interno de información podrá mantener el anonimato en torno a su identidad, garantizándose el mismo durante el proceso, siendo opcional para el informante incluir datos que permitan su identificación a través del formulario de comunicación habilitado.

Cuando se realice una comunicación anónima, al finalizar ésta, se generará un código a través del cual el informante podrá consultar en la página web donde estará alojado el Canal el estado de la comunicación y ampliar la información facilitada. Adicionalmente, el Canal interno de información proporcionará un



informe en PDF con la información facilitada y el código de acceso para su registro. El Canal no registrará ninguna información sobre la dirección IP o el ID del ordenador desde el que se plantea la comunicación.

Las personas que hayan realizado la comunicación de forma anónima pero que posteriormente hayan sido identificadas, siempre que cumplan las condiciones previstas en la Ley 2/2023 tendrán derecho a la protección que la misma concede y que se explicita en el apartado 3.5. de este Documento.

4.3. Gestión de conflictos de interés.

La presentación de una comunicación de información que afecte directamente a personas que puedan participar activamente en la gestión e investigación de la misma, es decir, a uno o varios miembros del órgano Responsable del Sistema Interno de Información, y, en caso de ser requerido, del órgano de dirección de la Entidad, serán excluidos de forma automática durante todo el proceso de investigación y análisis hasta su resolución, con el fin de evitar cualquier tipo de conflicto de interés e incompatibilidad, y garantizar así la objetividad e independencia de las actuaciones realizadas por el propio órgano Responsable del Sistema Interno de Información.

Los miembros excluidos, estarán obligados a mantener la máxima confidencialidad sobre la comunicación, estando prohibido el acceso directo o indirecto a cualquier información sobre la identidad de la persona informante y del proceso de investigación en curso.

4.4. Derecho a la información.

La persona informante tendrá derecho a ser informada en todo momento del progreso de la investigación de su comunicación. Así, el informante será informado por escrito, una vez analizada la información comunicada, si es considerada procedente para ser analizada. Por otro lado, una vez finalizada la investigación, el informante deberá ser informado sobre las medidas de seguimiento previstas, por ejemplo, la remisión a una autoridad competente, así como del resultado de las investigaciones, debiendo explicar la razón por la que se han adoptado las medidas o acciones disciplinarias sobre las personas afectadas.

Por su parte, las personas afectadas por la comunicación deberán ser informados del proceso de investigación que se esté llevando a cabo para que, ante la imputación de determinadas conductas, puedan ejercer su derecho de defensa y alegar todo aquello que le permita acreditar su inocencia. En dicha información no se incluirá, en ningún caso, la identidad del informante.

En aquellos casos en que la información del proceso de investigación suponga un riesgo importante en la capacidad para investigar de manera eficaz, la



comunicación a los afectados podrá retrasarse mientras exista dicho riesgo, siendo el objetivo evitar la destrucción o alteración de evidencias por los afectados.

4.5. No represalias. Protección del informante.

Se prohíben expresamente los actos constitutivos de represalia, incluidas las amenazas de represalia y las tentativas de represalia contra las personas que presenten comunicaciones a través de este Canal interno de información. La transgresión de esta prohibición supondrá la sanción correspondiente para el autor.

Se entiende por represalia cualquier acto u omisión 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, solo por su condición de informantes.

En el **Anexo II** de este Procedimiento de Gestión, se recoge una relación de las acciones que se consideran como represalia.

La Entidad proporcionará la debida protección a todas las personas que presenten una comunicación de acuerdo con las directrices del presente Procedimiento.

En el caso de que el informante haga público el contenido de la comunicación sólo podrá acogerse a las medidas de protección en el caso de que haya primero comunicado la información a través del Canal interno de información y con los plazos y medidas establecidos.

También será objeto de protección en el caso de que haga público el contenido de la información bien porque exista riesgo manifiesto para el interés público, como puede ser una situación de emergencia o riesgo de daños irreversibles, bien porque en el caso de que se realice una comunicación a través de un canal externo existan riesgos de represalias o haya bajas probabilidades de que se le dé un tratamiento efectivo a la comunicación debido a las circunstancias concretas del caso, como puede ser la ocultación o destrucción de pruebas o que la autoridad actúe en connivencia con el autor de la infracción o se encuentre implicada en ella.

Quedarán expresamente excluidos de la protección prevista en este Procedimiento y en la Ley 2/2023, aquellas personas que comuniquen: a) Informaciones contenidas en comunicaciones que hayan sido inadmitidas por algún canal interno de información o cuando los hechos carezcan de toda verosimilitud, no sean constitutivos de infracción del ordenamiento jurídico, la



comunicación carezca manifiestamente de fundamento o existan indicios racionales de haberse obtenido mediante la comisión de un delito; b) Informaciones vinculadas a reclamaciones sobre conflictos interpersonales o que afecten únicamente al informante y a las personas a las que se refiera la comunicación; c) Informaciones que ya estén completamente disponibles para el público o que constituyan meros rumores; d) Informaciones que se refieran a acciones u omisiones no comprendidas en el apartado 2.1. del presente Procedimiento y en el artículo 2 de la Ley 2/2023.

No se considerará que las personas que comuniquen información de buena fe mediante este Canal y de acuerdo con las directrices del presente Procedimiento, hayan infringido ninguna restricción de revelación de información y no incurrirán en responsabilidad de ningún tipo en relación con dicha comunicación, siempre que tuvieran motivos razonables para pensar que la comunicación de dicha información era necesaria para revelar una acción u omisión en virtud de la finalidad de este Canal y de la Ley 20/2023. Los informantes no incurrirán en responsabilidad respecto de la adquisición o el acceso a la información que es comunicada, siempre que dicha adquisición o acceso no constituya un delito.

4.6. Presunción de inocencia y derecho de defensa del afectado.

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

Los afectados tendrán derecho a una investigación basada en el análisis objetivo de las evidencias recabadas, garantizando una investigación eficaz y transparente.

4.7. Protección de los datos personales. Conservación de la información.

El Canal interno de información garantiza el cumplimiento de todas las obligaciones exigibles en materia de protección de datos. Sus datos personales serán tratados por la Entidad para gestionar de manera efectiva su comunicación e investigar los hechos comunicados a través del Canal. Este tratamiento de datos se legitima en el cumplimiento de las obligaciones legales establecidas en la Ley 2/2023 o, en su caso, en la necesidad de cumplir con una misión realizada en interés público.

La finalidad del tratamiento de los datos personales de los informantes y afectados por las comunicaciones realizadas será procesar e investigar, de manera confidencial, las mismas relativas a infracciones e incumplimientos legales, así como de la normativa interna de la Entidad.



En cuanto a la legitimidad o base jurídica del tratamiento de los datos personales será el artículo 6.1.c) del RGPD en cuanto que estamos ante un tratamiento necesario por la obligación legal impuesta en 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; Si dicho tratamiento de datos no fuese obligatorio, la base de legitimación es la necesidad de cumplir con una misión de interés público, de acuerdo con lo establecido en la mencionada Ley (artículo 6.1.e) RGPD).

Los datos personales se conservarán durante el tiempo imprescindible para cumplir con la finalidad para la que se recabaron y para determinar las posibles responsabilidades que se pudieran derivar de dicha finalidad y del tratamiento de los datos, así como para el cumplimiento de las obligaciones legales que correspondan. Si se acreditara que la información facilitada o parte de ella no es veraz, se procederá 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. Transcurridos tres meses desde la recepción de la comunicación sin que se hubiesen iniciado actuaciones de investigación, se procederá 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 constarán de forma anonimizada.

Los datos aportados serán tratados y, cuando sea imprescindible, cedidos a terceras partes interesadas, asesores o autoridades públicas con el fin de investigar y esclarecer los hechos comunicados, así como interponer las acciones legales y/o disciplinarias correspondientes, todo ello, de acuerdo con lo establecido en los artículos 32.1 y 33.3 de la Ley 2/2023. En ningún caso se desvelará la identidad de la persona informante a aquellas a los que se refieren los hechos comunicados.

En cuanto a los derechos que amparan a los interesados en este tratamiento de datos personales, se prevén los habituales de acceso, rectificación, supresión, oposición o a solicitar la limitación del tratamiento. No obstante, se contempla una puntualización respecto a las personas afectadas, en el caso de que éstas ejerciesen el derecho de oposición, se presumirá que, salvo prueba en contrario, existen motivos legítimos imperiosos que legitiman el tratamiento de sus datos personales y, por lo tanto, no sería reconocido.

No se recopilarán datos personales cuya pertinencia no resulte manifiesta para tratar la información específica o, si se recopilan por accidente, se eliminarán de forma inmediata.



Respecto al tratamiento de categorías especiales de datos personales por razones de interés público esencial se podrá realizar por razones de interés público esencial, sobre la base del Derecho de la Unión o de los Estados miembros (artículo 9.2.g) RGPD).

5. Procedimiento de gestión de las informaciones recibidas.

Desde el COLEGIO OFICIAL DE INGENIEROS INDUSTRIALES DE ANDALUCÍA OCCIDENTAL, el órgano de gobierno con el impulso del Responsable del Sistema Interno de Información ha desarrollado este Procedimiento interno, que regula todo el ciclo de vida de las informaciones recibidas, desde su comunicación inicial hasta su resolución, con la finalidad de comprobar la veracidad de las mismas, la correcta obtención de evidencias y garantizar los derechos del informante y afectados. Este procedimiento se divide en dos fases:

- **Fase de investigación:** Esta fase comprende la recepción y evaluación inicial, hasta la investigación de los hechos informados y la recopilación de las evidencias que aporten validez a los mismos.
- **Fase de Conclusiones:** Esta fase comprende el análisis de las evidencias, pruebas aportadas y la posterior redacción del informe, por parte del Responsable del Sistema, con las eventuales propuestas de las medidas sancionadoras al Órgano de Dirección.

5.1. Fase de investigación.

5.1.1. Acceso al canal interno de información. Vías externas de información.

La persona informante, en caso de optar por el uso del Canal interno de información de la Entidad, tendrá que rellenar el formulario de comunicación que está a su disposición en la web corporativa: <https://coiiaoc.com>.

El informante también podrá optar por comunicar la información mediante una reunión presencial dentro del plazo máximo de siete días desde dicha solicitud al Responsable del Sistema. Las comunicaciones verbales realizadas a través de reunión presencial, deberán documentarse de alguna de las siguientes maneras, previo consentimiento del informante:

- a) Mediante grabación de la conversación en un formato seguro, duradero y accesible, o



- b) A través de una transcripción completa y exacta de la conversación realizada por el personal responsable de tratarla.

Se ofrecerá al informante la oportunidad de comprobar, rectificar y aceptar mediante su firma la transcripción de la conversación.

5.1.2. Formalización y admisión a trámite de la comunicación.

La comunicación deberá ser individual. En caso de que varias personas tengan conocimiento del mismo hecho o circunstancia que deba ser comunicado a la Entidad, cada una de ellas deberá hacerlo de forma individual a través del Canal interno de información.

En el propio formulario, se pone a disposición de la persona informante las disposiciones normativas vigentes que garantizan la protección de sus datos durante el tratamiento de los mismos, así como el ejercicio de derechos sobre ellos.

Una vez realizada la comunicación, el Sistema interno remitirá automáticamente, en ese mismo momento, un acuse de recibo de la presentación de la misma a la dirección de correo electrónico que indique la persona informante. En el caso de que la persona informante opte por el anonimato, se procederá de acuerdo a lo recogido en el apartado 3.2. de este Procedimiento.

Será importante que la persona informante aporte detalle suficiente sobre los hechos, conductas o actividades sospechosas, para que el Responsable del Sistema pueda realizar un análisis preliminar del contenido, permitiendo incluso el envío de ficheros o documentos adjuntos en relación a los hechos comunicados.

Dicho análisis, podrá generar los siguientes resultados:

- **Admisión de la comunicación:** Los hechos descritos son hechos de entidad suficiente que pueden suponer un acto ilícito de los descritos en el apartado 2 y en el Anexo I de este Procedimiento.
- **Inadmisión de la comunicación:** Los hechos descritos son de una naturaleza distinta a los recogidos en el apartado 2.1. de este Procedimiento.

En ambos casos el Responsable del Sistema deberá informar, de forma escrita, a la persona informante, de la decisión adoptada y el motivo del archivo o de la admisión de la comunicación, excepto si se hubiera utilizado el Canal interno de información para un uso inadecuado y no fuera



necesario informar a la persona informante del área más adecuada para tratar su comunicación.

5.1.3. Investigación.

El Responsable del Sistema, una vez evaluada y admitida la comunicación, procederá a la elaboración de un expediente de apertura que contendrá:

- Información descriptiva de los hechos informados.
- Datos aportados, diferenciando los datos objetivos y subjetivos.
- Valoración del contenido de la comunicación y de la fiabilidad de la persona informante.
- Personas afectadas.
- Proposición de medidas de urgencia a corto plazo, entre ellas, medidas cautelares que permitan minimizar el daño actual o inminente.

El objetivo del expediente de apertura es recabar la máxima trazabilidad del proceso de investigación, en caso de que la comunicación pueda ser requerida por cualquier autoridad judicial competente.

En el transcurso de la investigación, se podrá recurrir a otras áreas de la Organización para desarrollar de forma efectiva la reclamación de pruebas y análisis que permita contrastar los hechos denunciados.

Los órganos de dirección de la Entidad podrán ser requeridos en cualquier momento por el Responsable del Sistema para complementar, de forma coordinada, las acciones de investigación llevadas a cabo por este último, siempre con la máxima confidencialidad y discreción.

Por último, en caso de encontrarse alguna incompatibilidad del Responsable del Sistema con la investigación en curso, se actuará de acuerdo a lo establecido en el apartado 3.3. del presente Procedimiento.

El Responsable del Sistema emprenderá, si lo considera necesario, acciones tendentes a profundizar en los hechos y a recabar información adicional para tomar una correcta decisión, de forma objetiva, en base a las evidencias recabadas. Las acciones de investigación pueden contemplar:

- Requerir nuevas evidencias y/o pruebas al denunciante para mejorar el proceso de investigación.
- Concertar entrevistas con las personas implicadas.
- Revisar toda aquella información relativa a la relación profesional de los implicados con la Organización, siempre con respeto a las leyes de protección de datos y privacidad de los implicados.
- Análisis forense por un experto externo independiente.



- Cualquier otra acción que considere necesaria para continuar con el proceso de investigación, respetando la normativa vigente en Protección de Datos.

La investigación consistirá, en todo momento, en un análisis objetivo de la documentación disponible, la obtención de evidencias, recolección de pruebas y análisis de las mismas.

El proceso de investigación durará como máximo 3 meses desde el día en que se recibió la comunicación de la información. Transcurridos los 3 meses, los datos podrán seguir siendo tratados para la investigación de los hechos comunicados y en su caso por las autoridades competentes o en procesos judiciales, pero no se conservarán en el propio Sistema Interno de Información.

5.2. Fase de conclusiones.

5.2.1. Informe y Resolución.

Una vez recabadas las pruebas y analizada las mismas por parte del Responsable del Sistema, se cierra la fase de investigación y se procede a la toma de decisiones acerca de la comunicación analizada, proponiendo a los órganos de gobierno de la Entidad las medidas que se deberán adoptar.

Para ello, el Responsable del Sistema emitirá un informe que contendrá al menos:

- a) Aspectos técnicos: Título, autor, fecha, finalidad, nivel de confidencialidad.
- b) Antecedentes del expediente: Hechos que produjeron la comunicación, personas o departamentos objeto de la investigación.
- c) Objeto de la investigación y su finalidad.
- d) Actuaciones, hechos relevantes investigados y detectados, evidencias y pruebas analizadas.
- e) Conclusiones determinadas, en base al objetivo y alcance de la investigación.
- f) Propuesta de medidas sancionadoras que deberán adoptar los órganos de gobierno de la Entidad, de conformidad con la legislación laboral y el resto de obligaciones civiles y mercantiles que haya contraído la plantilla de la Entidad, personal directivo o de los órganos de gobierno, sin perjuicio de las responsabilidades penales que pudieran derivarse de la comisión de posibles delitos.

El Responsable del Sistema recogerá dichas conclusiones de manera clara y concisa. Además, si existiera alguna limitación en el transcurso de la investigación, debe quedar reflejado en el informe.



Los informes resultantes de las comunicaciones recibidas y las posibles medidas adoptadas serán informadas a los órganos de gobierno de la Entidad.

Por los órganos de gobierno de la Entidad, a la vista del informe de conclusiones, se podrán adoptar las siguientes medidas:

- Archivo del expediente: En el supuesto en el que la investigación de los hechos comunicados se manifieste la ausencia de incumplimiento. El Responsable del Sistema informará a la persona informante y a los afectados de dicha decisión, junto con los motivos que sustentan la decisión.
- Comunicación informativa procedente: En el supuesto que se pruebe que los hechos comunicados son ciertos, e implican la comisión de una infracción grave de la legislación vigente y especialmente en el ámbito penal y administrativo y del Derecho de la Unión Europea. En este caso, se deberán detallar las acciones que sustentan dicha conclusión. El régimen sancionador se aplicará de conformidad con la legislación laboral y el resto de obligaciones civiles y mercantiles que haya contraído la plantilla de la Entidad, personal directivo o de los órganos de gobierno, sin perjuicio de las responsabilidades penales que pudieran derivarse de la comisión de posibles delitos. El Responsable del Sistema deberá informar a la persona informante y en particular a los afectados para ofrecerle la posibilidad de defensa.

En el caso de que los hechos pudieran ser indiciariamente constitutivos de delito, deberán ser remitidos con carácter inmediato al Ministerio Fiscal, y si los hechos afectan a los intereses financieros de la Unión Europea, se remitirán a la Fiscalía Europea.

6. Entrada en vigor.

Este Procedimiento de Gestión del sistema interno de información entrará en vigor a partir de su aprobación por los órganos de gobierno del COLEGIO OFICIAL DE INGENIEROS INDUSTRIALES DE ANDALUCÍA OCCIDENTAL.

7. Anexos:

7.1. Anexo I. Categorías de comunicaciones al canal interno de información.

- Actuaciones con proveedores: Incumplimiento de procedimientos relacionados con la selección, adjudicación o supervisión de proveedores.



- Contabilidad: Irregularidades referidas a las obligaciones contables de la Entidad.
- Irregularidades referidas a la confidencialidad, los datos personales y los secretos de la empresa: Cualquier utilización no autorizada de la información no pública de la Entidad, de sus clientes, de datos personales o utilización inadecuada de la propiedad intelectual.
- Apropiación indebida, desvío de recursos o robo: Apropiarse fraudulentamente, para uso propio, de bienes confiados al cuidado de uno o utilización inadecuada de bienes o información propiedad de la Entidad en beneficio propio. Robar o sustraer bienes de la Entidad.
- Irregularidades en la contratación: Alterar, inventar o falsificar, total o parcialmente contratos con el propósito de obtener una ventaja o de alterar el contenido del mismo.
- Represalias: Actuaciones discriminatorias de la Entidad contra personas que de buena fe informan sobre posibles irregularidades.
- Conflictos de interés: Ejercicio irregular de los deberes de un profesional debido a un interés personal.
- Irregularidades sobre el medioambiente: Incumplimiento de la normativa interna o externa con respecto a aspectos relacionados con el medioambiente o con materias peligrosas.
- Soborno, corrupción y tráfico de influencias: Ofrecer o aceptar regalos de terceros para obtener una ventaja para la organización. Uso de influencia personal con el fin de obtener favores o tratamiento preferencial.
- Irregularidades respecto a la gestión de fondos públicos: Hechos que puedan ser constitutivos de fraude o irregularidad en relación con proyectos u operaciones financiadas con cargo a fondos públicos, tanto nacionales como europeos.
- Infracciones del Derecho de la Unión Europea: Acciones u omisiones que constituyen infracciones de Derecho de la Unión Europea de acuerdo con el Anexo de la Directiva (UE) 2019/1937, que afecten a los intereses financieros de la Unión Europea o incidan en el mercado interior.
- Acoso laboral, discriminación o malos tratos: Comportamientos hostiles contra los trabajadores en situaciones de discriminación hacia una persona o un grupo de personas. Acciones contrarias al Convenio Colectivo o al Estatuto de los Trabajadores.
- Acoso sexual o por razón de sexo: Comportamientos susceptibles de ser calificados como acoso sexual o por razón de sexo.

7.2. Anexo II. Listado de acciones consideradas como represalias.

- 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 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.