

**Sistema Interno de
Información.
Canal de denuncias.**



Sistema Interno de Información de Código Gestión, conforme a 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.

08/02/2024

1. DESCRIPCIÓN DEL SISTEMA INTERNO DE INFORMACIÓN.

El Sistema Interno de Información de Código Gestión de la Información S.L. (en adelante Código Gestión) es un el **cauce o canal seguro de participación** que permite informar sobre cualquier acción u omisión contraria a los principios de buen gobierno y, en particular, sobre cualquier infracción de las normas que puedan constituir un delito o una infracción administrativa grave, así como de las normas de la Unión Europea.

Incluye mecanismos para garantizar la **confidencialidad** de todas las informaciones y **ofrece un espacio de comunicación seguro que permite el anonimato** para mantener el contacto con la empresa. Se quiere garantizar que **cualquier empleado o persona relacionada con Código Gestión pueda facilitar información libremente, sin sufrir represalias.**

Se trata de un medio de prevención y resolución de conflictos que **preserva la identidad de la persona que hace la comunicación** y también incorpora herramientas para **garantizar los derechos de las personas afectadas por la comunicación.**

El Sistema Interno de Información se articula en torno a los **siguientes elementos:**

- Canales de recepción de la información.
- Responsable del Sistema.
- Procedimiento de gestión de informaciones.

2. CANALES DE RECEPCIÓN DE LA INFORMACIÓN.

El personal de Código Gestión dispone de un Sistema Interno de Información con las siguientes características:

2.1. BUZONES O CANALES DE RECEPCIÓN DE LA INFORMACIÓN.

Todo canal interno de información de que dispone Código Gestión para posibilitar la presentación de información respecto de las infracciones del Código ético, de los protocolos de obligado cumplimiento o del Derecho de la Unión Europea, así como infracciones penales o administrativas graves.

El Sistema Interno de Información de Código Gestión está integrado por los siguientes canales:

2.1.1. Canal ético.

Es el cauce general para informar de las infracciones del Código ético de Códice Gestión que no tengan un canal de denuncias específico, así como cualquier otra infracción del Derecho de la Unión Europea o las acciones que puedan ser constitutivas de infracción penal o administrativa grave o muy grave.

2.1.2. Canal de protocolo contra el acoso sexual o por razón de sexo.

Es el cauce para informar de los comportamientos constitutivos de acoso sexual o por razón de sexo.

2.2. HECHOS DE LOS QUE SE PUEDE INFORMAR.

Podrán ser comunicados cualquier hecho o actividad, con independencia de su cuantía, que, por su naturaleza pueda ser constitutivo de:

- Infracción del Derecho de la Unión Europea en materia de:
 - Contratación pública y concesión de subvenciones.
 - 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.
 - Normas relativas a la protección y gestión de aguas y suelos, normas relativas a la protección de la naturaleza y biodiversidad.
 - Normas relativas a las sustancias y mezclas químicas.
 - Normas relativas a los productos ecológicos.
 - 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.
 - Intereses financieros de la Unión Europea.
 - Mercado interior, incluidas las infracciones de las normas de la Unión Europea en materia de competencia y ayudas otorgadas por los Estados, así como las infracciones de las normas del impuesto sobre sociedades o 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.

2.3. SUJETOS DENUNCIABLES: Todo el personal directivo y empleado de Códice Gestión podrá ser denunciado a través del sistema.

2.4. INFORMANTES:

Podrán actuar como informantes cualquiera que haya obtenido información sobre infracciones en un contexto laboral o profesional, comprendiendo en todo caso:

- Las personas que tengan la condición de empleados públicos o trabajadores por cuenta ajena.
- Los autónomos.
- Los accionistas, partícipes y personas pertenecientes al órgano de administración, dirección o supervisión de una empresa, incluidos los miembros no ejecutivos.
- Cualquier persona que trabaje para o bajo la supervisión y la dirección de contratistas, subcontratistas y proveedores.

2.5. INFORMACIÓN:

El personal será previamente informado de la existencia y finalidad del sistema, su funcionamiento, la garantía de confidencialidad de los datos del denunciante y la garantía de información al denunciado de la existencia de la denuncia.

2.6. PROCEDIMIENTO DE REALIZACIÓN DE COMUNICACIONES.

El canal interno deberá permitir realizar comunicaciones por escrito o verbalmente, o de las dos formas. La información se podrá realizar bien por escrito, a través de correo postal o a través de cualquier medio electrónico habilitado al efecto, o verbalmente, por vía telefónica o a través de sistema de mensajería de voz. A solicitud del informante, también podrá presentarse mediante una reunión presencial dentro del plazo máximo de siete días.

En su caso, se advertirá al informante de que la comunicación será grabada y se le informará del tratamiento de sus datos.

Además, a quienes realicen la comunicación a través de canales internos se les informará, de forma clara y accesible, sobre los canales externos de información ante las autoridades

competentes y, en su caso, ante las instituciones, órganos u organismos de la Unión Europea.

Al hacer la comunicación, el informante podrá indicar un domicilio, correo electrónico o lugar seguro a efectos de recibir las notificaciones.

Las comunicaciones verbales, incluidas las realizadas a través de reunión presencial, telefónicamente o mediante sistema de mensajería de voz, deberán documentarse de alguna de las maneras siguientes, previo consentimiento del informante:

- a) mediante una 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.

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

Los canales internos de información permitirán incluso la presentación y posterior tramitación de comunicaciones anónimas.

3. RESPONSABLE DEL SISTEMA INTERNO DE INFORMACIÓN.

3.1. DESIGNACIÓN.

El órgano de administración de Códice Gestión será el competente para la designación de la persona física responsable de la gestión del sistema o «Responsable del Sistema», y de su destitución o cese.

Si se optase por que el Responsable del Sistema fuese un órgano colegiado, este deberá delegar en uno de sus miembros las facultades de gestión del Sistema interno de información y de tramitación de expedientes de investigación.

Tanto el nombramiento como el cese de la persona física individualmente designada, así como de las integrantes del órgano colegiado deberán ser notificados a la Autoridad Independiente de Protección del Informante, A.A.I., o, en su caso, a las autoridades u órganos competentes de las comunidades autónomas, en el ámbito de sus respectivas

competencias, en el plazo de los diez días hábiles siguientes, especificando, en el caso de su cese, las razones que han justificado el mismo.

3.2. ESTATUTO.

El Responsable del Sistema deberá desarrollar sus funciones de forma independiente y autónoma respecto del resto de los órganos de la entidad u organismo, no podrá recibir instrucciones de ningún tipo en su ejercicio, y deberá disponer de todos los medios personales y materiales necesarios para llevarlas a cabo

3.3. FUNCIONES.

El Responsable del Sistema se ocupará de la tramitación diligente de las informaciones recibidas, y en particular, de que se cumplan los principios siguientes:

- a) Identificación del canal o canales internos de información a los que se asocian.
- b) Inclusión de información clara y accesible sobre los canales externos de información ante las autoridades competentes y, en su caso, ante las instituciones, órganos u organismos de la Unión Europea.
- c) Envío de acuse de recibo de la comunicación al informante, en el plazo de siete días naturales siguientes a su recepción, salvo que ello pueda poner en peligro la confidencialidad de la comunicación.
- d) Cumplimiento del plazo máximo para dar respuesta a las actuaciones de investigación.
- e) Mantener, en su caso, la comunicación con el informante y, si se considera necesario, de solicitar a la persona informante información adicional.
- f) Garantizar el derecho de la persona afectada a que se le informe de las acciones u omisiones que se le atribuyen, y a ser oída en cualquier momento. Dicha comunicación tendrá lugar en el tiempo y forma que se considere adecuado para garantizar el buen fin de la investigación.
- g) Garantía de la confidencialidad de la información.
- h) Respeto a la presunción de inocencia y al honor de las personas afectadas.
- i) Respeto de las disposiciones sobre protección de datos personales.

j) Remisión de la información al Ministerio Fiscal con carácter inmediato cuando los hechos pudieran ser indiciariamente constitutivos de delito. En el caso de que los hechos afecten a los intereses financieros de la Unión Europea, se remitirá a la Fiscalía Europea.

4. PROCEDIMIENTO DE GESTIÓN DE INFORMACIÓN.

4.1. RECEPCIÓN DE INFORMACIONES.

Recibida la información, se procederá a su registro en el Sistema de Gestión de Información, y le será asignado un código de identificación.

Se procederá al envío de acuse de recibo de la comunicación al informante, en el plazo de siete días naturales siguientes a su recepción, salvo que ello pueda poner en peligro la confidencialidad de la comunicación o que el informante expresamente haya renunciado a recibir comunicaciones relativas a la investigación.

Se garantizará la confidencialidad cuando la comunicación sea remitida por canales de denuncia que no sean los establecidos 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 de remitirla inmediatamente al Responsable del Sistema.

4.2. TRÁMITE DE ADMISIÓN.

Registrada la información, el responsable de la tramitación deberá comprobar si aquella expone hechos o conductas que se encuentran dentro del ámbito de aplicación del Sistema.

Realizado este análisis preliminar, decidirá, en un plazo que no podrá ser superior a diez días desde la fecha de entrada en el registro de la información:

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

- 1.º Cuando los hechos relatados carezcan de toda verosimilitud.
- 2.º Cuando los hechos relatados no sean constitutivos de infracción del ordenamiento jurídico.
- 3.º Cuando la comunicación carezca manifiestamente de fundamento o existan 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.

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

La inadmisión se comunicará al informante dentro de los cinco días hábiles siguientes, salvo que la comunicación fuera anónima o el informante hubiera renunciado a recibir comunicaciones.

b) Admitir a trámite la comunicación.

La admisión a trámite se comunicará al informante dentro de los cinco días hábiles siguientes, salvo que la comunicación fuera anónima o el informante hubiera renunciado a recibir comunicaciones del Responsable del Sistema.

c) Remitir con carácter inmediato la información al Ministerio Fiscal cuando los hechos pudieran ser indiciariamente constitutivos de delito o a la Fiscalía Europea en el caso de que los hechos afecten a los intereses financieros de la Unión Europea.

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

4.3. INSTRUCCIÓN.

La instrucción comprenderá todas aquellas actuaciones encaminadas a comprobar la verosimilitud de los hechos relatados.

Se garantizará que la persona afectada por la información tenga noticia de la misma, así como de los hechos relatados de manera sucinta. Adicionalmente se le informará del derecho que tiene a presentar alegaciones por escrito y del tratamiento de sus datos personales. No obstante, esta información podrá efectuarse en el trámite de audiencia si se considerara que su aportación con anterioridad pudiera facilitar la ocultación, destrucción o alteración de las pruebas.

Sin perjuicio del derecho a formular alegaciones por escrito, 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.

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.

Todos los empleados deberán colaborar con el instructor del expediente y aportar documentación, datos o cualquier información relacionada con los procedimientos que se estén tramitando, incluso los datos personales que le fueran requeridos.

El plazo máximo para dar respuesta a las actuaciones de investigación no podrá ser superior a dos/tres meses a contar desde la recepción de la comunicación o, si no se remitió un acuse de recibo al informante, a dos/tres meses a partir del vencimiento del plazo de siete días después de efectuarse la comunicación, salvo casos de especial complejidad que requieran una ampliación del plazo, en cuyo caso, este podrá extenderse hasta un máximo de otros dos/tres meses adicionales.

Podrá mantenerse la comunicación con el informante y, si se considera necesario, de solicitar a la persona informante información adicional.

Se respetará la presunción de inocencia y al honor de las personas afectadas.

Se procederá a la remisión de la información al Ministerio Fiscal con carácter inmediato cuando los hechos pudieran ser indiciariamente constitutivos de delito. En el caso de que los hechos afecten a los intereses financieros de la Unión Europea, se remitirá a la Fiscalía Europea.

4.4. TERMINACIÓN DE LAS ACTUACIONES.

Concluidas todas las actuaciones, el instructor emitirá un informe que contendrá al menos:

- a) Una exposición de los hechos relatados junto con el código de identificación de la comunicación y la fecha de registro.
- b) Las actuaciones realizadas con el fin de comprobar la verosimilitud de los hechos.
- c) Las conclusiones alcanzadas en la instrucción y la valoración de las diligencias y de los indicios que las sustentan.

Emitido el informe, el Responsable del Sistema de Información adoptará alguna de las siguientes decisiones:

- a) Archivo del expediente, que será notificado al informante y, en su caso, a la persona afectada. En estos supuestos, el informante tendrá derecho a protección, salvo que, como

consecuencia de las actuaciones llevadas a cabo en fase de instrucción, se concluyera que la información, a la vista de la información recabada, debía haber sido inadmitida.

b) 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, se remitirá a la Fiscalía Europea.

c) Adopción de acuerdo de inicio de un procedimiento sancionador.

El plazo para finalizar las actuaciones y dar respuesta al informante, en su caso, no podrá ser superior a tres meses desde la entrada en registro de la información. Cualquiera que sea la decisión, se comunicará al informante, salvo que haya renunciado a ello o que la comunicación sea anónima.

5. REGISTRO DE INFORMACIONES.

El Sistema de Gestión de Información estará contenido en una base de datos segura y de acceso restringido exclusivamente al personal de la Autoridad Independiente de Protección del Informante, A.A.I. convenientemente autorizado

Códice Gestión contará con un libro-registro de las informaciones recibidas y de las investigaciones internas a que hayan dado lugar, garantizando, en todo caso, los requisitos de confidencialidad previstos en la ley.

Este registro no será público y únicamente a petición razonada de la Autoridad judicial competente, mediante auto, y en el marco de un procedimiento judicial y bajo la tutela de aquella, podrá accederse total o parcialmente al contenido del referido registro.

En el libro se registrarán todas las comunicaciones recibidas, cumplimentando los siguientes datos:

- a) Fecha de recepción.
- b) Código de identificación.
- c) Actuaciones desarrolladas.
- d) Medidas adoptadas.
- e) Fecha de cierre.

Los datos personales relativos a las informaciones recibidas y a las investigaciones internas a que se refiere el apartado anterior solo se conservarán durante el período que sea necesario y proporcionado a efectos de cumplir con la ley. En particular, se tendrán en cuenta lo dispuesto en el apartado 6 relativo a los plazos de conservación.

6. PROTECCIÓN DE DATOS

6.1. Régimen jurídico del tratamiento de datos personales.

Los tratamientos de datos personales del SII se regirán por lo dispuesto en el Reglamento Europeo de Protección de Datos, la Ley Orgánica 3/2018, de Protección de Datos Personales y garantía de los derechos digitales, la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales, y en el presente título.

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

6.2. Información sobre protección de datos personales y ejercicio de derechos:

- Cuando se obtengan directamente de los interesados sus datos personales se les facilitará la información a que se refieren los artículos 13 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, y 11 de la Ley Orgánica de protección de datos personales y garantía de los derechos digitales.
- A los informantes y a quienes lleven a cabo una revelación pública se les informará, además, de forma expresa, de que su identidad será en todo caso reservada, que no se comunicará a las personas a las que se refieren los hechos relatados ni a terceros.
- La persona a la que se refieran los hechos relatados no será en ningún caso informada de la identidad del informante o de quien haya llevado a cabo la revelación pública.
- Los interesados podrán ejercer los derechos a que se refieren los artículos 15 a 22 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016. 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.

6.3 Tratamiento de datos personales en el Sistema interno de información.

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:

- a) El Responsable del Sistema y a quien lo gestione directamente.
- b) El responsable de recursos humanos o el órgano competente debidamente designado, solo cuando pudiera proceder la adopción de medidas disciplinarias contra un trabajador. En el caso de los empleados públicos, el órgano competente para la tramitación del mismo.
- c) 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.
- d) Los encargados del tratamiento que eventualmente se designen.
- e) El delegado de protección de datos.

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

En ningún caso serán objeto de tratamiento los datos personales que no sean necesarios para el conocimiento e investigación de las acciones u omisiones que vulneren el Derecho de la Unión o sean constitutivas de infracción penal o administrativa grave o muy grave, procediéndose, en su caso, a su inmediata supresión. Asimismo, se suprimirán todos aquellos datos personales que se puedan haber comunicado y que se refieran a conductas que no estén incluidas en el ámbito de aplicación de la ley.

Si la información recibida contuviera datos personales incluidos dentro de las categorías especiales de datos, se procederá a su inmediata supresión, sin que se proceda al registro y tratamiento de los mismos.

En particular, se tendrán en cuenta lo siguientes aspectos:

- Los datos que sean objeto de tratamiento podrán conservarse en el sistema de informaciones únicamente durante el tiempo imprescindible para decidir sobre la procedencia de iniciar una investigación sobre los hechos informados.
- 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 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.
- En ningún caso podrán conservarse los datos por un período superior a diez años.

Los empleados y terceros deberán ser informados acerca del tratamiento de datos personales en el marco de los Sistemas de información a que se refiere el presente artículo.

6.4. Prohibición de revelación de identidad.

Quien presente una comunicación o lleve a cabo una revelación pública tiene derecho a que su identidad no sea revelada a terceras personas.

Los sistemas internos de información, los canales externos y quienes reciban revelaciones públicas no obtendrán datos que permitan la identificación del informante y deberán contar con medidas técnicas y organizativas adecuadas para preservar la identidad y garantizar la confidencialidad de los datos correspondientes a las personas afectadas y a cualquier tercero que se mencione en la información suministrada, especialmente la identidad del informante en caso de que se hubiera identificado.

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.

7. MEDIDAS DE PROTECCIÓN

7.1. CONDICIONES DE PROTECCIÓN.

Las personas que comuniquen o revelen infracciones tendrán derecho a protección siempre que concurren las circunstancias siguientes:

- a) 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 entra dentro del ámbito de aplicación de la ley,
- b) la comunicación o revelación se haya realizado conforme a los requerimientos previstos en la ley.

Quedan expresamente excluidos de la protección aquellas personas que comuniquen o revelen:

- a) Informaciones contenidas en comunicaciones que hayan sido inadmitidas por algún canal interno de información.
- 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 o revelación.
- 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 constitutivas de infracción penal o administrativa grave o muy grave.

7.2. PROHIBICIÓN DE REPRESALIAS.

Se prohíben expresamente los actos constitutivos de represalia, incluidas las amenazas de represalia y las tentativas de represalia contra las personas que presenten una comunicación.

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, solo por su condición de informantes, o por haber realizado una revelación pública.

A título enunciativo, se consideran represalias las que se adopten en forma de:

- a) 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.

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

c) Evaluación o referencias negativas respecto al desempeño laboral o profesional.

d) 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.

e) Denegación o anulación de una licencia o permiso.

f) Denegación de formación.

g) Discriminación, o trato desfavorable o injusto.

7.3. MEDIDAS DE APOYO.

Las personas que comuniquen o revelen infracciones a través de los procedimientos previstos accederán a las medidas de apoyo siguientes:

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

b) Asistencia efectiva por parte de las autoridades competentes ante cualquier autoridad pertinente implicada en su protección frente a represalias, incluida la certificación de que pueden acogerse a protección al amparo de la presente ley.

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

d) Apoyo financiero y psicológico, de forma excepcional, si así lo decidiese la Autoridad Independiente de Protección del Informante, A.A.I. tras la valoración de las circunstancias derivadas de la presentación de la comunicación.

7.4. MEDIDAS DE PROTECCIÓN FRENTE A REPRESALIAS.

No se considerará que las personas que comuniquen información sobre las acciones u omisiones o que hagan una revelación pública hayan infringido ninguna restricción de revelación de información, y aquellas no incurrirán en responsabilidad de ningún tipo en relación con dicha comunicación o revelación pública, siempre que tuvieran motivos razonables para pensar que la comunicación o revelación pública de dicha información era necesaria para revelar una acción u omisión en virtud de la ley. Esta medida no afectará a las responsabilidades de carácter penal.

Lo previsto en el párrafo anterior se extiende a la comunicación de informaciones realizadas por los representantes de las personas trabajadoras, aunque se encuentren sometidas a obligaciones legales de sigilo o de no revelar información reservada. Todo ello sin perjuicio de las normas específicas de protección aplicables conforme a la normativa laboral.

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.

7.5. MEDIDAS PARA LA PROTECCIÓN DE LAS PERSONAS AFECTADAS.

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