

# **SISTEMA INTERNO DE INFORMACIÓN**

**Procedimiento para la gestión de las informaciones sobre infracciones en CANAL  
ETHICA**

|   |    |
|---|----|
| 1. OBJETO .....   | 3  |
| 2. ÁMBITO DE APLICACIÓN .....   | 3  |
| 2.1. ÁMBITO DE APLICACIÓN PERSONAL.....   | 3  |
| 2.2. ÁMBITO DE APLICACIÓN MATERIAL .....  | 4  |
| 3. RESPONSABILIDADES.....   | 5  |
| 4. DESARROLLO.....  | 6  |
| 4.1. RESPONSABLE DEL SISTEMA INTERNO DE INFORMACIÓN .....                                     | 6  |
| 4.2. PROCEDIMIENTO DE GESTIÓN DE INFORMACIONES.....   | 7  |
| 4.2.1. Política General del Sistema Interno de Información .....                              | 7  |
| 4.2.2. Canales internos .....   | 7  |
| 4.2.3. Gestión de informaciones .....   | 8  |
| 4.2.4. Revelación Pública .....   | 11 |
| 4.3. DERECHOS DE LAS PERSONAS .....   | 12 |
| 4.3.1. Derechos de las personas investigadas .....  | 12 |
| 4.3.2. Derechos de las personas informantes .....   | 12 |
| 4.4. PROTECCIÓN DE DATOS PERSONALES.....  | 12 |
| 4.4.1. Datos personales .....   | 12 |
| 4.4.2. Información de datos personales.....   | 13 |
| 4.4.3. Tratamiento de datos personales en el Sistema Interno de Información.....              | 13 |
| 4.5. MEDIDAS DE PROTECCIÓN .....  | 14 |
| 4.5.1. Preservación de la identidad de la persona informante y de las personas afectadas..... | 14 |
| 4.5.2. Condiciones de protección para personas informantes.....                               | 14 |
| 4.5.3. Prohibición de represalias.....  | 14 |
| 4.5.4. Medidas para la protección de las personas afectadas por la información.....           | 15 |
| 4.5.5. Medidas de apoyo.....  | 16 |
| 4.6. RÉGIMEN DISCIPLINARIO.....   | 16 |
| 5. CANALES EXTERNOS DE INFORMACIÓN .....  | 16 |
| 6. DOCUMENTACIÓN DE REFERENCIA .....  | 17 |

## **1. OBJETO**

El presente documento se establece con objeto de diseñar, establecer y gestionar de forma segura el Sistema Interno de Información **CANAL ETHICA**, garantizando la confidencialidad de la identidad de la persona informante y de cualquier tercero/a mencionado/a en la información vertida. Asimismo, incluye las actuaciones necesarias para su gestión y tramitación, así como la protección de datos, impidiendo el acceso a personal no autorizado.

Este procedimiento ha sido desarrollado según 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.

Este documento se trata de las directrices comunes que utilizan todas las Empresas Responsables que comparten medios técnicos para su Sistema Interno de Información a través de CANAL ETHICA.

## **2. ÁMBITO DE APLICACIÓN**

### **2.1. ÁMBITO DE APLICACIÓN PERSONAL**

El presente sistema se aplicará a aquellas personas que hayan obtenido información sobre infracciones en un contexto laboral o profesional, comprendiendo en todo caso:

- a) las personas que tengan la condición de trabajadores por cuenta ajena;
- b) los autónomos;
- c) los accionistas, partícipes y personas pertenecientes al órgano de administración, alta dirección o supervisión de la empresa, incluidos los miembros no ejecutivos;
- d) cualquier persona que trabaje para o bajo la supervisión y la dirección de contratistas, subcontratistas y proveedores.

También se aplicará a las personas informantes que comuniquen o revelen públicamente información sobre infracciones obtenida en el marco de una relación laboral o estatutaria ya finalizada, voluntarios, becarios, trabajadores en periodos de formación con independencia de que perciban o no una remuneración, así como a aquellos cuya relación laboral todavía no haya comenzado, en los casos en que la información sobre infracciones haya sido obtenida durante el proceso de selección o de negociación precontractual.

Las medidas de protección de la persona informante también se aplicarán, en su caso, a los representantes legales de las personas trabajadoras en el ejercicio de sus funciones de asesoramiento y apoyo al informante.

Estas medidas de protección de la persona informante también se aplicarán a:

- a) personas físicas que, en el marco de la organización en la que preste servicios la persona informante, asistan al mismo en el proceso,
- b) personas físicas que estén relacionadas con la persona informante y que puedan sufrir represalias, como compañeros de trabajo o familiares de la persona informante, y
- c) personas jurídicas, para las que trabaje o con las que mantenga cualquier otro tipo de relación en un contexto laboral o en las que ostente una participación significativa. A estos efectos, se entiende que la participación en el capital o en los derechos de voto correspondientes a acciones o participaciones es significativa cuando, por su proporción, permite a la persona que la posea tener capacidad de influencia en la persona jurídica participada.

## 2.2. ÁMBITO DE APLICACIÓN MATERIAL

El presente procedimiento establece normas mínimas comunes para la protección de las personas que informen sobre:

a) Infracciones del Derecho de la Unión:

1) Infracciones que entren dentro del ámbito de aplicación de los actos de la Unión enumerados en el anexo de la Directiva (UE) 2019/1937 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 23 de octubre de 2019 relativa a la protección de las personas que informen sobre infracciones del Derecho de la Unión, relativas a los ámbitos siguientes:

- contratación pública,
- servicios, productos y mercados financieros, y prevención del blanqueo de capitales y la financiación del terrorismo,
- seguridad de los productos y conformidad,
- seguridad del transporte,
- protección del medio ambiente,
- protección frente a las radiaciones y seguridad nuclear,
- seguridad de los alimentos y los piensos, sanidad animal y bienestar de los animales,
- salud pública,
- protección de las personas consumidoras,
- protección de la privacidad y de los datos personales, y seguridad de las redes y los sistemas de información.

2) Infracciones que afecten a los intereses financieros de la Unión tal como se contemplan en el artículo 325 del TFUE y tal como se concretan en las correspondientes medidas de la Unión.

3) Infracciones relativas al mercado interior, tal como se contemplan 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 a prácticas cuya finalidad sea obtener una ventaja fiscal que desvirtúe el objeto o la finalidad de la legislación aplicable del impuesto sobre sociedades.

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

Esta protección no excluirá la aplicación de las normas relativas al proceso penal, incluyendo las diligencias de investigación.

La protección prevista para las personas trabajadoras que informen sobre infracciones del Derecho laboral en materia de seguridad y salud en el trabajo, se entiende sin perjuicio de la establecida en su normativa específica.

## EXCLUSIONES:

- Informaciones que afecten a la información clasificada.
- Tampoco afectará a las obligaciones que resultan de la protección del secreto profesional de los profesionales de la medicina y de la abogacía, del deber de confidencialidad de las Fuerzas y Cuerpos de Seguridad en el ámbito de sus actuaciones, así como del secreto de las deliberaciones judiciales.
- Informaciones relativas a infracciones en la tramitación de procedimientos de contratación que contengan información clasificada o que hayan sido declarados secretos o reservados, o aquellos cuya ejecución deba ir acompañada de medidas de seguridad especiales conforme a la legislación vigente, o en los que lo exija la protección de intereses esenciales para la seguridad del Estado.

## **3. RESPONSABILIDADES**

### **ÓRGANO DE GOBIERNO**

- Implantar el Sistema Interno de Información, previa consulta con la representación legal de las personas trabajadoras.
- Tendrá la condición de responsable del tratamiento de los datos personales de conformidad con lo dispuesto en la normativa sobre protección de datos personales.
- Designación, destitución y/o, cese de los miembros del Sistema Interno de Información.
- Definir y aprobar la Política que define los principios básicos del Sistema Interno de Información.
- Aprobación del procedimiento de gestión de informaciones del Sistema Interno de Información, definido en el presente documento.

### **RESPONSABLE DEL SISTEMA INTERNO DE INFORMACIÓN**

- Garantizar el correcto funcionamiento del Sistema.
- Recibir, gestionar e investigar las informaciones recibidas por el canal formal del Sistema Interno de Información, haciendo un seguimiento con la máxima diligencia.
- Tramitar de manera diligente las comunicaciones que se reciban.
- Desarrollar sus funciones de forma independiente y autónoma respeto del resto de órganos de la empresa
- Mantener comunicación con la persona informante.
- Proporcionar respuesta.
- Cumplir con las disposiciones sobre protección de datos personales.
- Garantizar la confidencialidad de la persona informante y de la persona afectada por la información.

- Respetar la presunción de inocencia, el derecho de defensa y el honor de las personas afectadas.
- Informar a las personas afectadas de las acciones u omisiones que se le atribuyen, así como mantener comunicación con la persona afectada en tiempo y forma para garantizar la investigación.
- Prohibir las represalias a las personas informantes, sean amenazas y/o tentativas de represalias, y asegurar que se toman las medidas necesarias para prevenirlas.
- Adoptar las decisiones necesarias en cuestiones relacionadas con las medidas cautelares de protección de la persona informante o de las personas sobre las que verse la información recibida, no pudiendo proceder en ningún caso a la delegación de dichas facultades.

#### **RESTO DEL PERSONAL**

- Derivar en el Responsable del Sistema de Información cualquier comunicación que reciban en relación con esta materia.
- Garantizar la confidencialidad de la información recibida y comunicada al Responsable del Sistema Interno de Información.

#### **4. DESARROLLO**

Las personas que trabajan para una organización pública o privada o están en contacto con ella en el contexto de sus actividades laborales o profesionales son a menudo las primeras en tener conocimiento de amenazas o perjuicios para el interés público que surgen en ese contexto. Al informar sobre infracciones dichas personas actúan como personas informantes y por ello desempeñan un papel clave a la hora de descubrir y prevenir esas infracciones y de proteger el bienestar de la sociedad. Sin embargo, las personas informantes potenciales suelen renunciar a informar sobre sus preocupaciones o sospechas por temor a represalias. Debido a esto, y considerando además que la protección de las personas informantes es necesaria para mejorar la aplicación del derecho en materia de contratación pública, en cumplimiento de la normativa legal, **la empresa responsable** establece un Sistema de Interno de Información, que canalizará formalmente las posibles comunicaciones sobre infracciones penales o administrativas (graves o muy graves) que ocurran en la Organización.

Por ello se ha diseñado, establecido y gestionado un sistema que funciona de forma segura y que garantice la confidencialidad de la identidad del informante y de cualquier tercera persona comprendida en la información, otorgando protección adecuada frente a posibles represalias que pueden sufrir las personas informantes.

##### **4.1. RESPONSABLE DEL SISTEMA INTERNO DE INFORMACIÓN**

El Órgano de Administración o de Gobierno será el competente para la designación de las personas físicas responsables de la gestión de dicho sistema u «Órgano Responsable del Sistema Interno de Información», y de su destitución o cese. Deberá ser personal directivo de la Empresa, que ejercerá su cargo con independencia del Órgano de Administración o de Gobierno.

Cada empresa responsable ha designado a un responsable de la gestión del Sistema Interno de Información .

A pesar de esto, todas las empresas responsables delegarán en una persona física la gestión del Sistema y la tramitación de los expedientes de investigación. Una vez recibida la información, esta persona será la responsable de convocar al Órgano Responsable del Sistema Interno de Información para decidir sobre las medidas a adoptar, en cada caso, para la procedencia o no de la investigación de los hechos y el procedimiento de actuación al respecto. La persona designada para la tramitación de los expedientes no podrá tomar decisiones de manera independiente al resto del Órgano.

Tanto el nombramiento como el cese de la persona física individualmente designada, así como de las integrantes del órgano colegiado, si lo hubiese, 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.

Dichas personas desarrollarán sus funciones de forma independiente y autónoma respecto del resto de los órganos de la entidad u organismo, no podrán recibir instrucciones de ningún tipo en su ejercicio, y deberán disponer de todos los medios personales y materiales necesarios para llevarlas a cabo.

Dicha designación ha sido aprobada por el Órgano Administración o de Gobierno.

#### 4.2. PROCEDIMIENTO DE GESTIÓN DE INFORMACIONES

##### 4.2.1. Política General del Sistema Interno de Información

**Cada empresa responsable** se ha adscrito a la presente política que incluye los principios básicos generales del Sistema Interno de Información y defensa de la persona informante. Esta se comunica a todas las personas integrantes de las empresa y estará disponible en el propio canal.

##### 4.2.2. Canales internos

Las informaciones deben hacerse llegar por los diferentes canales internos de información disponibles, pudiendo realizar la comunicación por escrito o verbalmente. **La empresa responsable** ha establecido el siguiente canal de comunicación:

###### ➤ Por escrito

- **Plataforma web TALESO:** <https://taleso.es/CanalEthica>

Taleso.es es una herramienta online constituida como una plataforma informática especializada y accesible a través de la página web corporativa. A través de la plataforma las comunicaciones serán por escrito y permitirá la posibilidad de realizarlas de manera totalmente anónima.

La plataforma será gestionada exclusivamente por una empresa externa, según las previsiones del artículo 6 de la ley 2/2023, de 20 de febrero, de modo que ninguna persona que forme parte de la empresa tendrá acceso a la misma.

**Se garantiza la confidencialidad de la persona informante en todo momento.** La plataforma requiere la inclusión de una dirección de correo electrónico que quedará almacenada de manera cifrada en la propia plataforma, de modo que no es accesible bajo ningún concepto a las personas Responsables del Sistema Interno de Información ni a la empresa externa de recepción de las

informaciones, siempre que se decida hacer la comunicación de manera anónima.

Dicho canal se mantendrá accesible en todo momento en la página web de modo que puedan acceder al mismo todas aquellas personas que se encuentren dentro del ámbito de aplicación personal de la normativa de aplicación.

#### ➤ **Verbal**

- **Reunión presencial:** se ofrece también la posibilidad de comunicar cualquier conducta de manera verbal mediante la petición por parte de la persona informante de una reunión con cualquiera de los miembros del Órgano Responsable del Sistema Interno de Información. Dicha reunión se deberá llevar a cabo en un plazo máximo de 7 días desde la petición. Las comunicaciones verbales se documentarán según las previsiones que establece la Ley, preferentemente a través de una transcripción completa de la conversación por el personal responsable de tratarla, que se facilitará en el acto a la persona informante para comprobar, rectificar, y aceptar, mediante su firma, la transcripción de la reunión y se le informará de las condiciones en el tratamiento de sus datos personales.

Cualquier comunicación que sea realizada a través de vías diferentes se cursará por los canales establecidos en este procedimiento, se trasladará al Responsable del Sistema Interno de Información.

#### **4.2.3. Gestión de informaciones**

El Sistema Interno de Información debe garantizar que las comunicaciones presentadas puedan tratarse de manera efectiva, con el fin de que la Empresa sea la primera en conocer la posible irregularidad. Para ello, el Sistema Interno de Información se gestionará del siguiente modo:

- **CONTENIDO DE LA INFORMACIÓN:** Todas las informaciones serán comunicadas y gestionadas por el canal interno definido en el apartado anterior.

Toda comunicación debe recoger la siguiente información a fin de facilitar su comprensión y posible gestión de la misma:

- a. Identidad del informante cuando se opte por realizar la comunicación de forma confidencial y no anónima. En este caso se deberá indicar nombre, apellidos y una dirección de correo electrónico para mantener comunicaciones.
- b. Una descripción clara, concisa y objetiva de los hechos de los que se informa o de las cuestiones o sugerencias que se plantean, acompañando, en su caso, los elementos de prueba necesarios que fundamenten el hecho o hechos objeto de la comunicación.
- c. Motivos por los que considera que los hechos descritos son irregulares.

La falta de información en una comunicación puede dificultar su entendimiento, así como su gestión. En caso de no poder obtener datos suficientes para poder tramitar la comunicación, el expediente será sobreesido.

- **RECEPCIÓN INFORMACIÓN:** Todas las informaciones serán comunicadas y gestionadas por el canal interno definido en el apartado anterior.

Siempre que se trate de una persona informante no anónima, al hacer la comunicación, ésta podrá indicar

un domicilio, correo electrónico o lugar seguro a efectos de recibir las notificaciones.

Las comunicaciones también podrán ser realizadas de manera anónima, siendo gestionadas y tramitadas como cualquier otra información recibida a través del Sistema Interno de Información.

En caso de recibirse informaciones no incluidas en el objeto del presente procedimiento, dichas comunicaciones y sus remitentes quedarán fuera del ámbito de protección dispensado por el Sistema, derivando el contenido de la información a las personas responsables de su gestión.

Cuando la comunicación recibida sea o pueda ser objeto del Protocolo de Acoso, la persona delegada o la persona que reciba la información, deberá informar inmediatamente al Órgano Responsable que se reunirá para dar traslado a la Comisión Instructora de Acoso con el objeto de hacer valoración de la información.

En estos casos, el Órgano Responsable cumplirá con su función informando al Comité Instructor de Acoso y recogiendo en el Libro Registro las principales diligencias de investigación y resoluciones.

**ACUSE DE RECIBO:** una vez recibida la información a través de la plataforma, esta enviará un acuse de recibo a la persona informante de manera instantánea (plazo máximo de 7 días naturales), desde la recepción de ésta. Dicho acuse de recibo consistirá en un código numérico con el que se dará acceso al seguimiento del informe. Si la comunicación se realiza a través de las vías restantes, igualmente se aportará acuse de recibo a la persona en el mismo plazo de 7 días.

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.

• **TRAMITACIÓN / INVESTIGACIÓN:** Una vez se reciba la información y tras emitir el acuse de recibo, el Órgano Responsable del Sistema Interno de Información valorará la información y decidirá sobre la tramitación e inicio de actuaciones de investigación dejando constancia de ésta en la plataforma, el cual comprenderá los siguientes ítems:

- a. N.º de Registro.
- b. Fecha de entrada.
- c. Persona informante: este campo se completará con el nombre y apellidos de la persona informante. En caso de que la información recibida sea anónima se indicará el término “anónima”.
- d. Descripción de los hechos: se incluirá un breve extracto de la información recibida.
- e. Investigación: la investigación incluirá consultas internas y con asesores jurídicos externos; entrevistas a las personas afectadas, a la persona informante y/o a cualquier otra que pudiera resultar implicada; solicitud de antecedentes y aclaraciones, así como cualquier otra prueba documental.
- f. Sospechas de mala fe.
- g. Conclusiones y acciones tomadas.
- h. Verificación de la información.
- i. Fecha de respuesta a la persona informante (máximo 3 meses prorrogable por 3 meses más en caso de expediente de gran complejidad).
- j. Puesta en conocimiento de la Autoridad Competente y fecha (si se da el caso).
- k. Propuesta de sanciones disciplinarias.
- l. Fecha de cierre.

Una vez recibida la información de una presunta infracción, se efectuará un análisis preliminar de la información aportada pudiendo solicitar de la persona informante una ampliación o mayor detalle de aspectos concretos. Se analizará el alcance de la información, las personas que se puedan encontrar en riesgo, la existencia de un posible conflicto de intereses de algún actor con el rol en el sistema, necesidad de tomar medidas urgentes para preservar las pruebas, evitar su destrucción o alteración y/o proteger a la víctima. Se procederá al archivo sin investigación para aquellas informaciones que se revelen claramente inverosímiles, cuando los hechos relatados no sean constitutivos de ninguna infracción, informaciones carentes de buena fe o sin fundamento, cuando sean sobreesídas por falta de información solicitada y no aportada, dejando constancia de este hecho y de las razones que lo avalan, 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 de hecho o de derecho que justifiquen un seguimiento distinto.

Admitida a trámite la comunicación se abre la fase de instrucción que comprenderá todas aquellas actuaciones encaminadas a comprobar la verosimilitud de los hechos relatados y si éstos son constitutivos de algún incumplimiento normativo, tanto interno como externo.

Durante la investigación el Órgano Responsable del Sistema Interno de Información podrá mantener comunicación a través de la plataforma con la persona informante para solicitar información adicional tanto si se ha identificado como si no.

La persona afectada por la información será informada de las acciones u omisiones que se le atribuyen, así como será oída en cualquier momento. Esta comunicación se realizará cuando se finalice la investigación para no afectar a su desarrollo.

Durante todo el proceso de gestión de la información y hasta la finalización de la investigación, se debe de mantener la presunción de inocencia y respetar el honor de las personas afectadas, así como respetar las disposiciones en materia de protección de datos.

En caso de que la comunicación recibida sea o pueda ser objeto del Protocolo de Acoso, la valoración de los hechos y todo el desarrollo del procedimiento de investigación se realizará por parte del Comité Instructor en base al Protocolo de Acoso aprobado e implantado en la organización.

En cualquier momento del proceso, se deberá informar al Ministerio Fiscal de manera inmediata cuando se disponga de indicios de que se haya podido cometer un delito.

Se dispone de un plazo máximo de respuesta de tres meses, a partir del acuse de recibo, y en caso de que éste no se facilite, el plazo será de tres meses a partir del vencimiento del plazo de 7 días después de la facilitación de la información. En el caso de expedientes de especial complejidad, se podrá posponer el plazo máximo hasta 3 meses más.

- **RESOLUCIÓN:** Una vez se haya finalizado la investigación se entregará un informe de conclusiones a la persona informante y a la/s persona/s sobre quien/es se esté informando, donde se incluirán las conclusiones obtenidas por el Órgano Responsable del Sistema Interno de Información o por la Comisión de Instrucción en los casos de acoso, así como la propuesta de posibles acciones disciplinarias que podrían llevarse a cabo, si proceden. Teniendo en cuenta las conclusiones del informe de instrucción, la Dirección de la Empresa procederá a la adopción de las medidas que considere oportunas en función de la naturaleza de los hechos constatados, la decisión final del órgano de gobierno será comunicada a la persona del informante y afectado (archivo del expediente, iniciar un procedimiento disciplinario, activación de cualquier otro protocolo vigente en la Compañía ...)
- **REGISTRO:** La información recibida y la investigación de la misma se archivarán en la plataforma del Registro del Sistema Interno de Información. Este registro no será público y únicamente se entregará a la Autoridad Judicial previa petición razonada, mediante auto y bajo su tutela.

El plazo de conservación será el que corresponda a la prescripción de cada delito y, en todo caso, por un plazo mínimo de 5 años y máximo de 10 años. Los datos personales de las informaciones serán tratados según se indica en el apartado correspondiente del presente procedimiento.

#### **4.2.4. Revelación Pública**

Cuando una persona pone a disposición del público la información sobre acciones y omisiones que puedan ser constitutivas de infracción penal o administrativa grave o muy grave, dispondrá de protección siempre y cuando:

- Haya realizado la comunicación a través de canales internos o externos y no se hayan tomado medidas apropiadas al respecto.

- Tenga motivos razonables para pensar que la infracción puede constituir un peligro inminente o manifiesto para el interés público o existe un riesgo de daños irreversibles, incluido un peligro para la integridad física de una persona, exista riesgo de represalias o pocas probabilidades de que se lleve a cabo un tratamiento efectivo de la información, mediante la ocultación o destrucción de pruebas.

#### 4.3. DERECHOS DE LAS PERSONAS

##### 4.3.1. Derechos de las personas investigadas.

Las personas afectadas por informaciones recibidas tienen el derecho a que la investigación y la decisión en torno a los resultados de la misma sean adoptados por personas imparciales, guiadas únicamente por la normativa que regula su función. Asimismo, tienen derecho a ser informadas de la existencia de la investigación y de la razón de la misma lo antes posible, siempre que no ponga en riesgo los fines de la investigación. En todo caso deberá ser informada antes de su finalización. Tendrá derecho a la presunción de inocencia, el derecho de defensa y de acceso al expediente en los términos previstos en la Ley 2/2023, así como a la misma protección que las personas informantes, preservándose su identidad y garantizándose la confidencialidad de los hechos y datos del procedimiento.

##### 4.3.2. Derechos de las personas informantes:

Las personas informantes tendrán los siguientes derechos:

- a. Derecho a que se tramite su comunicación conforme a este procedimiento.
- b. Derecho de confidencialidad en caso de haber revelado su identidad y derecho al anonimato cuando no se haya revelado.
- c. Derecho a que se le informe de la resolución o archivo de la comunicación en un plazo máximo de tres meses o de seis en aquellos casos de especial complejidad.
- d. Medidas de protección y apoyo según se relatan más adelante.
- e. Deber de actuar de buena fe. Los abusos realizados a través del Sistema Interno de Información implicarán la pérdida de la protección otorgada por la normativa de aplicación y podrán dar lugar a medidas disciplinarias / sancionadoras que en su caso procedan contra la persona informante o autora del abuso. Este deber de buena fe aplica también para aquellas personas que colaboren en la investigación para comprobar la veracidad de los hechos.
- f. Deber de aportar elementos de juicio y los datos y documentos de los que disponga que tengan relación con los hechos informados.
- g. Deber de confidencialidad sobre la realización de la comunicación y el contenido de ésta, en tanto en cuanto se analiza y resuelva la misma (salvo lo previsto en el punto 4.2.4).

#### 4.4. PROTECCIÓN DE DATOS PERSONALES

##### 4.4.1. Datos personales

Todos los datos personales necesarios para la aplicación del presente procedimiento serán considerados lícitos debiendo ser tratados respetando la normativa en esta materia. Se consideran datos personales los

relativos a la persona informante, así como datos de terceras personas, cuando resulte necesarios para la adopción de medidas correctoras o la tramitación de expediente.

No se recopilarán datos de personas cuya pertenencia no resulte necesaria para la información y posterior investigación, en caso de recopilar datos por accidente, éstos han de ser eliminados del expediente en cuanto se determine su no procedencia. Del mismo modo, serán tratados los datos de informaciones de conductas que no se incluyen en el ámbito de aplicación del presente procedimiento o informaciones de conductas cuando se evidencia que no son veraces, salvo que la falta de veracidad dé lugar a un procedimiento judicial.

Todos los datos de informaciones que, transcurridos 3 meses desde su recepción, no han iniciado actuaciones de investigación, deberán ser suprimidos del Sistema, salvo que sean necesarios para evidenciar el funcionamiento del Sistema Interno de Información.

#### **4.4.2. Información de datos personales**

Siempre que se obtengan los datos personales de las personas interesadas, se les ha de informar del tratamiento de sus datos, datos de contacto del Delegado de Protección de Datos y de sus derechos. En caso de que las personas interesadas ejerzan su derecho de acceso, se les informará de:

- Los fines del tratamiento de datos.
- Las categorías de los datos personales de que se tratan.
- Los destinatarios a los que se comunicaron o serán comunicados los datos.
- De ser posible, el plazo previsto de conservación o al menos, los criterios empleados para determinar el plazo de conservación.
- La posibilidad de solicitar rectificación o supresión de datos personales o la limitación de tratamiento de datos o a oponerse al tratamiento.

#### **4.4.3. Tratamiento de datos personales en el Sistema Interno de Información**

El acceso a datos personales contenido en el Sistema Interno de Información quedará limitado a:

- Personas Responsables del Sistema Interno de Información y, a quien lo gestione directamente.
- Personas Responsables de RRHH u órgano competente en dicha materia, cuando pudiera proceder la adopción de medidas disciplinarias contra el trabajador/a.
- Personas Responsables de Servicios jurídicos de la Empresa, siempre que proceda la adopción de medidas legales en relación con los hechos comunicados.
- Los encargados de tratamiento que eventualmente se designen.
- El Delegado de Protección de Datos, en caso de que se disponga del mismo.

#### 4.5. MEDIDAS DE PROTECCIÓN

##### 4.5.1. Preservación de la identidad de la persona informante y de las personas afectadas

El Órgano Responsable del Sistema Interno de Información, se asegurará de que se preserve tanto la identidad de la persona informante como la de cualquier tercera persona que se mencione. Asimismo, se deberá preservar la identidad y garantizar la confidencialidad de los datos de las personas afectadas. En el caso de revelación pública, se asegurará que no se facilita información que permita la identificación de la persona informante, de una tercera persona que se mencione o de las personas afectadas.

Únicamente se facilitará la identidad de la persona informante a la Autoridad Judicial, al Ministerio Fiscal o la Autoridad Administrativa competente en el marco de una investigación penal, disciplinaria o sancionadora, teniendo que informarle, previamente, que su identidad va a ser revelada, salvo que esta comunicación pueda comprometer la investigación o el procedimiento judicial.

Durante el proceso de investigación, y cuando se comunique a la persona afectada la información recibida, no se podrá, en ningún caso, informar sobre la identidad de la persona informante o de quien ha llevado a cabo la revelación pública.

##### 4.5.2. Condiciones de protección para personas informantes

Todas las personas que comuniquen o revelen infracciones objeto del presente procedimiento tendrán derecho a protección cuando haya motivos razonables para pensar que la información aportada es veraz en el momento de la comunicación o revelación, aun cuando no se aporten pruebas concluyentes, pero siempre que se haya realizado respetando lo previsto en el presente procedimiento y en la normativa vigente.

No dispondrán de derecho de protección todas aquellas personas que comuniquen o revelen:

- Informaciones contenidas en comunicaciones que hayan sido inadmitidas en canales internos o externos de información.
- Informaciones vinculadas a reclamaciones sobre conflictos interpersonales o que afecten únicamente al informante y a las personas a las que se refiere la comunicación.
- Informaciones que ya se encuentren disponibles para el público o que constituyan meros rumores.
- Informaciones sobre acciones u omisiones no contempladas en el presente procedimiento.

##### 4.5.3. Prohibición de represalias

Quedan prohibidos los actos constitutivos de represalias, sean amenazas o tentativas, contra las personas informantes, entendiéndose por represalias todas aquellas prohibidas por ley, así como cualquier trato desfavorable en el contexto laboral o profesional simplemente por su condición de informante o por haber realizado una revelación pública.

De manera general, se consideran represalias:

- a. suspensión, despido, destitución o medidas equivalentes.

- b. no renovación o terminación anticipada de un contrato de trabajo temporal.
- c. terminación anticipada o anulación de contratos de bienes o servicios.
- d. imposición de cualquier medida disciplinaria, amonestación u otra sanción, incluidas las sanciones pecuniarias.
- e. degradación o denegación de ascensos; y cualquier otra modificación sustancial de las condiciones de trabajo.
- f. no conversión de un contrato de trabajo temporal en uno indefinido, en caso de que la persona trabajadora tuviera expectativas legítimas de que se le ofrecería un trabajo indefinido.
- g. daños, incluidos a su reputación, en especial en los medios sociales, o pérdidas económicas, incluidas la pérdida de negocio y de ingresos.
- h. coacciones, intimidaciones, acoso u ostracismo.
- i. evaluación o referencias negativas con respecto a sus resultados laborales.
- j. inclusión en listas negras sobre la base de un acuerdo sectorial, informal o formal, que pueda implicar que en el futuro la persona no vaya a encontrar empleo en dicho sector.
- k. anulación de una licencia o permiso.
- l. denegación de formación.
- m. discriminación, o trato desfavorable o injusto.

La persona que viera lesionados sus derechos por causa de su comunicación o revelación una vez transcurrido el plazo de dos años podrá solicitar la protección de la autoridad competente que, excepcionalmente y de forma justificada, podrá extender el período de protección, previa audiencia de las personas u órganos que pudieran verse afectados. La denegación de la extensión del período de protección deberá estar motivada.

Los actos administrativos que tengan por objeto impedir o dificultar la presentación de comunicaciones y revelaciones, así como los que constituyan represalia o causen discriminación tras la presentación de aquellas al amparo de esta ley, serán nulos de pleno derecho y darán lugar, en su caso, a medidas correctoras disciplinarias o de responsabilidad, pudiendo incluir la correspondiente indemnización de daños y perjuicios al perjudicado.

#### **4.5.4. Medidas para la protección de las personas afectadas por la información**

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, preservándole su identidad y garantizándose la confidencialidad de los hechos y datos del expediente.

#### **4.5.5. Medidas de apoyo**

A las personas que comuniquen o revelen infracciones a través de los procedimientos previstos se les dará acceso 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 de la persona informante, A.A.I., tras la valoración de las circunstancias derivadas de la presentación de la comunicación.

#### **4.6. RÉGIMEN DISCIPLINARIO**

En el caso de confirmarse la falsedad de la información, la persona infractora puede tener como consecuencia la exigencia de responsabilidades y/o sanciones derivadas de la legislación aplicable y/o del régimen disciplinario establecido en el Convenio colectivo correspondiente.

### **5. CANALES EXTERNOS DE INFORMACIÓN**

Se informa de que están disponibles los canales externos de información, para informar de la comisión de cualesquiera acciones u omisiones incluidas en el ámbito de aplicación de la Ley 2/2023, ante la Autoridad Independiente de Protección del Informante, A.A.I., ante las autoridades u órganos autonómicos correspondientes, y, cuando proceda, a instituciones, organismos o agencias de la UE a través de los siguientes links:

❖ **Servicio Nacional de Coordinación Antifraude (S.N.C.A.)**

<https://www.igae.pap.hacienda.gob.es/sitios/igae/es-ES/snca/Paginas/ComunicacionSNCA.aspx>

❖ **Oficina Europea de Lucha contra el Fraude (OLAF)**

[https://anti-fraud.ec.europa.eu/olaf-and-you/report-fraud\\_es](https://anti-fraud.ec.europa.eu/olaf-and-you/report-fraud_es)

❖ **Fiscalía Europea**

<https://www.eppo.europa.eu/en/reporting-crime-eppo>

❖ **Dirección de Competencia de la Comisión Nacional de los Mercados y la Competencia**

<https://edi.cnmc.es/buzones-anonimos/sica>

❖ **Canal de denuncias de la Agencia Tributaria**

<https://sede.agenciatributaria.gob.es/Sede/colaborar-agencia-tributaria/denuncias.html>

❖ **Comunicación de indicios de Blanqueo de Capitales ante el SEPBLAC**

<https://www.sepblac.es/es/sujetos-obligados/tramites/comunicacion-por-indicio/>

**6. DOCUMENTACIÓN DE REFERENCIA**

Normas de referencia:

- *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.*
- *Directiva (UE) 2019/1937 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 23 de octubre de 2019.*

Otra documentación:

- *Archivo de información recibida.*