

7

PROCOLO PARA
CANALS INTERNOS
DE INFORMACIÓN





7.1 ANTECEDENTES

El presente protocolo constituye la herramienta para la elaboración de canales o sistemas internos de información según los términos utilizados 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.

Se ha marcado como objetivo incorporar los elementos necesarios para la creación y funcionamiento de canales internos de información sobre infracciones, partiendo de la revisión de los antecedentes existentes sobre canales de denuncia internos de irregularidades en las distintas administraciones públicas, y sus características, funcionamiento y evolución junto con el análisis de la regulación sobre canales internos de denuncia. Asimismo, se plantea la necesidad de coordinarse con las tareas que está desarrollando el Servicio Nacional de Coordinación Antifraude (SNCA) con su canal de denuncias «Infotraude».

Las definiciones de los conceptos más relevantes utilizadas son las establecidas en 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 Europea (UE), en adelante Directiva (UE) 2019/1937, y en otras disposiciones europeas o nacionales, se incluyen en el anexo 7.1.

Se ha llevado a cabo el análisis de las características de un conjunto de canales de denuncia o comunicación de fraude o corrupción propios (canales internos) de entidades públicas pertenecientes a los tres niveles de administración pública. En el caso de la AGE, se trata en muchos casos de los canales de denuncia/comunicación de fraude/corrupción que se han contemplado en los Planes de Medida Antifraude (PMA) del Plan de Recuperación, Transformación y Resiliencia (PRTR) propios de entidades públicas.

Las conclusiones principales de dicho análisis son las siguientes:

En gran parte de los PMA del PRTR no consta la previsión de canales propios de denuncia (canales internos), sino la referencia a la existencia de canales de naturaleza transversal como el canal Infotraude del Servicio Nacional de Coordinación Antifraude (SNCA) de la IGAE, actual canal externo nacional existente en materia de protección de los intereses financieros de la Unión Europea y canal de denuncias propio de la

ejecución del Plan de Recuperación, Transformación y Resiliencia (según se establece en el apartado 4.6 del mismo) o el Sistema de Notificación de Fraudes de la Oficina Europea de Lucha contra el Fraude (OLAF).

No todos los restantes canales propios sobre los que han informado algunos departamentos están disponibles en línea o son accesibles a cualquier persona física o jurídica, existiendo canales internos de denuncia únicamente abiertos a las empleadas y empleados públicos de la entidad en cuestión.

En líneas generales, se trata de canales internos de denuncia específicos de fraude o corrupción, si bien el canal de denuncias que se utiliza para el tratamiento conjunto de consultas, quejas, o comunicaciones sobre el código ético y de conducta del personal relacionado con la función de compras y los buzones de Guardia Civil y Policía Nacional, parecen ser de uso general para cualquier denuncia.

El canal Infofraude del SNCA está destinado a la comunicación de denuncias relacionadas con operaciones financiadas con fondos europeos, tanto de gestión compartida como de gestión directa, en el ámbito estatal, autonómico y local, y sus aspectos fundamentales están regulados en la Comunicación 1/2017, de 6 de abril, del Servicio Nacional de Coordinación Antifraude, sobre la forma en la que pueden proceder las personas que tengan conocimiento de hechos que puedan ser constitutivos de fraude o irregularidad en relación con proyectos u operaciones financiados total o parcialmente con cargo a fondos procedentes de la Unión Europea.

Recientemente Infofraude ha sido modificado para albergar las denuncias procedentes de la ejecución del Mecanismo, puesto que fue designado como el canal externo oficial de denuncias relativas a los fondos procedentes de la ejecución del PRTR.

A la vista del análisis realizado, se deduce la existencia de algunos canales internos para entidades de la AGE, complementarias al canal externo Infofraude del SNCA. Estos canales internos parecen estar más extendidos en otros niveles de administración, a la vista del muestreo realizado.

Es desigual el grado de difusión y operatividad de estos canales, y su accesibilidad no siempre es universal a cualquier ciudadano o persona jurídica. No en todos los casos se admiten denuncias anónimas, ni por vías alternativas al correo electrónico o formulario en línea; es residual la admisión de denuncias por correo postal o verbales (vía telefónica u otros sistemas de mensajería de voz, o por medio de una reunión presencial).

Queda, por tanto, cierto margen de desarrollo de los canales internos existentes, con vistas a la aplicación de las previsiones de la citada Ley 2/2023, de 20 de febrero.

7.2 OBJETO DE ESTE PROTOCOLO

Con arreglo a las previsiones del Título II de la Ley 2/2023, de 20 de febrero, relativa al sistema interno de información, el presente documento tiene por objeto exponer el conjunto mínimo de elementos necesarios para la creación y el funcionamiento de canales internos de información, en el ámbito de la Administración General del

Estado incluyendo unas directrices para el establecimiento de su procedimiento de gestión que, con arreglo a lo establecido por el artículo 9.1 de la citada ley, deberá ser aprobado por cada uno de los departamentos ministeriales sobre la base del contenido mínimo y principios establecidos en ese precepto.

De acuerdo con la normativa aplicable, se incluyen, por lo tanto, en el objeto de este procedimiento los elementos requeridos a los sistemas internos de información sobre infracciones, en los que deben encuadrarse los referidos canales.

Hay que resaltar que el Sistema de Integridad distingue entre buzones de ética institucional, a utilizar para solicitar información o resolver dudas de interpretación o concreción sobre la materia o dilemas éticos, y los canales internos de información en los que, en su caso, pueden plantearse denuncias sobre conductas irregulares o contrarias a las reglas éticas. Todo ello además al margen de los buzones de quejas y sugerencias, que mantiene su función actual sin verse afectados por el Sistema de Integridad de la AGE.

7.3 CONTEXTO NORMATIVO Y ESTRATÉGICO

7.3.1 Normativa

Las disposiciones más relevantes que resultan de aplicación a los canales internos de información son las siguientes:

- a) 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.
- b) Ley 47/2003, de 26 de noviembre, General Presupuestaria.
- c) Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, por la que se transponen al ordenamiento jurídico español las Directivas del Parlamento Europeo y del Consejo 2014/23/UE y 2014/24/UE, de 26 de febrero de 2014.
- d) 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 de Derecho de la Unión y la Ley, en virtud de la cual se produzca su transposición a nuestro Ordenamiento Jurídico.
- e) Reglamento (CE, EURATOM) No 2988/95 del Consejo de 18 de diciembre de 1995 relativo a la protección de los intereses financieros de las Comunidades Europeas.
- f) Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).

7.3.2 Otros planes, disposiciones o programas relevantes

Además de la mencionada normativa, los canales internos de información se pueden ver afectados por los siguientes planes o programas que resulte de aplicación en cada caso:

- a) IV Plan de Gobierno Abierto de España 2020-2024.
- b) Planes de medidas antifraude propios del órgano o entidad, tanto si se refieren a los fondos europeos denominados «*Next Generation*», como a cualquier otra tipología de fondos europeos, nacionales o de cualquier otra fuente de financiación.
- c) Norma UNE-ISO 37002. Sistemas de gestión de denuncias de irregularidades. Directrices.

7.4 ÁMBITO Y FINALIDAD DEL CANAL INTERNO DE INFORMACIÓN SOBRE INFRACCIONES

7.4.1 Finalidad

El canal interno de información sobre infracciones tiene como finalidad poner en conocimiento a las personas responsables en el ámbito de la Administración General del Estado de posibles casos de fraude, así como otras irregularidades, que afecten al ámbito de aplicación de la Ley 2/2023, de 20 de febrero, en el ámbito de su departamento.

7.4.2 Ámbito material del canal interno de información

Los canales internos de información sobre infracciones objeto de este protocolo que se creen e implanten deben canalizar comunicaciones de información relativa a:

- a) Cualesquiera acciones u omisiones que puedan constituir infracciones del Derecho de la Unión Europea siempre que:
 - 1.º Entren dentro del ámbito de aplicación de los actos de la Unión Europea 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, con independencia de la calificación que de las mismas realice el ordenamiento jurídico interno.
 - 2.º Afecten a los intereses financieros de la Unión Europea tal y como se contemplan en el artículo 325 del Tratado de Funcionamiento de la Unión Europea (TFUE), o
 - 3.º Incidan en el mercado interior, tal y como se contemplan en el artículo 26, apartado 2 del TFUE, incluidas las infracciones de las normas de la Unión Europea en materia de competencia y ayudas otorgadas por los Estados, así como las infracciones relativas al mercado interior en relación con los actos que infrinjan las normas del impuesto sobre sociedades o con prácticas cuya finalidad sea obtener una ventaja fiscal que desvirtúe el objeto o la finalidad de la legislación aplicable al impuesto sobre sociedades.

- b) 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.
- c) Infracciones del derecho laboral en materia de seguridad y salud en el trabajo de las que informen las trabajadoras y trabajadores, sin perjuicio de lo establecido en su normativa específica.

No estarán incluidas en el ámbito de aplicación de los canales internos las consultas de cualquier tipo sobre información administrativa, ni aquellas comunicaciones cuya exclusión está expresamente contemplada en la Ley 2/2023, de 20 de febrero.

En el caso de que el canal no admita algún tipo de información por razón de la especialización de la materia, se dejará clara esa información en el sistema de acceso al canal interno, indicando, en su caso, los canales de referencia para el ámbito material excluido de este canal interno.

En el caso de que el organismo tenga competencias de investigación, tendrá dos canales de información:

- a) Uno, respecto a los propios incumplimientos e irregularidades cometidas en el seno de su organización, en el ejercicio de las actividades de su personal, en materias que pueden ser de ámbitos normativos diferentes al de su competencia de investigación.
- b) Su canal especializado, en el que reciba las comunicaciones escaladas de terceros organismos, respecto de investigaciones de su competencia sectorial respecto a irregularidades e incumplimientos de terceros.

7.4.3 Ámbito subjetivo de la tipología de las personas informantes

Se indica la siguiente tipología de posibles informantes, como orientación para la definición del ámbito del canal interno de información integrado en el Sistema interno de información.

Serán objeto de recepción, tramitación y seguimiento las informaciones recibidas de las personas informantes que trabajen en el sector privado o público y que hayan obtenido información sobre infracciones en un contexto laboral o profesional, comprendiendo en todo caso:

- a) Las personas que tengan la condición de empleadas o empleados públicos (del propio órgano o entidad, o de cualesquiera de cualquier nivel administrativo) o trabajadoras y trabajadores por cuenta ajena.
- b) Los autónomos.
- c) Accionistas, partícipes y personas pertenecientes al órgano de administración, dirección o supervisión de una empresa, incluidas las no ejecutivas.

- d) Cualquier persona que trabaje para o bajo la supervisión y la dirección de contratistas, subcontratistas y proveedores.
- e) Personas informantes que comuniquen o revelen públicamente información sobre infracciones obtenida en el marco de una relación laboral o estatutaria ya finalizada, voluntarias, becarias, trabajadoras en periodos de formación con independencia de que perciban o no una remuneración, así como aquellas 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.
- f) Representantes legales de las personas trabajadoras en el ejercicio de sus funciones de asesoramiento y apoyo a la persona informante.

7.4.4 Características del Sistema interno de información para comunicación de informaciones

Todos los ministerios habrán de formalizar un canal interno, que deberá estar integrado en sus sistemas internos de información y aprobar su procedimiento de gestión, así como designar a un responsable, con arreglo a las previsiones del Capítulo I del Título II de la Ley 2/2023, de 20 de febrero.

Este canal interno de información integrado en el Sistema interno de información se implantará previa consulta con la representación de las empleadas y empleados públicos.

El Sistema interno de información debe cumplir con los requisitos establecidos en el artículo 5.2 de la Ley 2/2023, de 20 de febrero, contemplar la implantación de todas las funcionalidades y requisitos del procedimiento de gestión de informaciones del artículo 9 de ese texto legal, y el seguimiento posterior de las actuaciones, el registro de las comunicaciones de informaciones, las comunicaciones con las personas informantes y las interconexiones e integraciones con otros canales y las autoridades y órganos competentes en investigación.

7.4.5 Responsable del canal interno de información

Deberá dictarse una resolución departamental de designación de la persona responsable del Sistema interno de información.

Con arreglo al modelo de organización propuesto en el Sistema de Integridad de la Administración General del Estado, la designación puede recaer en el coordinador o coordinadora de integridad departamental. Con arreglo a lo establecido por el artículo 8 de la Ley 2/2023, de 20 de febrero, la persona responsable del Sistema deberá desarrollar sus funciones de forma independiente y autónoma respecto del resto de órganos departamentales y no podrá recibir instrucciones de ningún tipo en su ejercicio. Deberá disponer de todos los medios personales y materiales necesarios para llevarlas a cabo.

Tanto el nombramiento como el cese de la persona designada deberá ser notificado a la Autoridad Independiente de Protección de la persona Informante, una vez que esta se constituya, en el plazo de los diez días hábiles siguientes, especificando, en el caso de su cese, las razones que han justificado el mismo.

La persona responsable del Sistema está obligada a guardar secreto sobre las informaciones que conozca con ocasión del ejercicio de sus funciones.

Se deberá identificar a las personas encargadas del tratamiento en función de qué implementación concreta se haga del sistema de información y la división que se haga de las tareas asociadas de gestión del canal interno, de la información y de los elementos técnicos que lo constituyan.

7.4.6 Información sobre el canal interno

Deberá proporcionarse información adecuada de forma clara y fácilmente accesible sobre el uso de todo canal interno de información que se haya implantado, así como sobre los principios esenciales del procedimiento de gestión a través del portal de internet.

Esta información deberá constar en la página de inicio, en una sección separada y fácilmente identificable.

Asimismo, se publicará, en una sección separada, fácilmente identificable y accesible de la sede electrónica, como mínimo, la información siguiente:

- a) las condiciones para poder acogerse a la protección con arreglo al ordenamiento;
- b) los datos de contacto para los canales internos de información previstos, en particular, las direcciones electrónica y postal y los números de teléfono asociados a dichos canales, indicando si se graban las conversaciones telefónicas;
- c) los procedimientos de gestión, incluida la manera en que la autoridad competente puede solicitar a la persona informante aclaraciones sobre la información comunicada o que proporcione información adicional, el plazo para dar respuesta, en su caso, y el tipo y contenido de esta;
- d) el régimen de confidencialidad aplicable a las comunicaciones, y en particular, la información sobre el tratamiento de los datos personales de conformidad con lo dispuesto en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales y en el título VII de la Ley 2/2023, de 20 de febrero;
- e) las vías de recurso y los procedimientos para la protección frente a represalias, y la disponibilidad de asesoramiento confidencial. En particular, se contemplarán las condiciones de exención de responsabilidad y los programas de clemencia.

Deberá asimismo indicarse de forma clara las distintas formas de presentación de la información a través de los distintos canales que se indican en el siguiente apartado. Los canales internos de información permitirán la presentación y posterior tramitación de comunicaciones anónimas.

Asimismo, deberá incluirse 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.

Se fomentará entre el personal propio una cultura favorable a facilitar información interna sobre posibles casos de fraude o infracciones de las que puedan tener conocimiento en el ámbito de su departamento o entidad, y se valorará esto como un acto de lealtad, así como una oportunidad para conocer eventuales irregularidades y remediarlas.

7.5 DIRECTRICES DE PROCEDIMIENTO

7.5.1 Recepción de información de irregularidades

1. Formas de presentación de la información

La persona informante podrá presentar la información:

- a) Presencialmente:
 - i. Deberá asegurarse que las conversaciones se desarrollan en una ubicación en la que pueda garantizarse la confidencialidad.
 - ii. Deberá solicitarse el consentimiento de la persona informante para la grabación de la conversación, así como de sus derechos conforme a la normativa de protección de datos de carácter personal.
 - iii. La información deberá documentarse mediante una grabación de la conversación en un formato seguro, duradero y accesible, o a través de una transcripción completa y exacta de la conversación realizada por el personal responsable de tratarla.
 - iv. Sin perjuicio de los derechos que le corresponden de acuerdo con la normativa sobre protección de datos, se ofrecerá a la persona informante la oportunidad de comprobar, rectificar y aceptar mediante su firma la transcripción del mensaje.
- b) Por teléfono o mensajería de voz:
 - i. Deberá habilitarse una línea exclusivamente para esta finalidad, atendida por una persona designada por el responsable del canal interno de denuncias y con una ubicación segura que garantice la confidencialidad.
 - ii. Deberá solicitarse el consentimiento de la persona informante para la grabación de la conversación, así como de sus derechos conforme a la normativa de protección de datos de carácter personal.
 - iii. La información deberá documentarse mediante una grabación de la conversación en un formato seguro, duradero y accesible, o a través de una transcripción completa y exacta de la conversación realizada por el personal responsable de tratarla.

c) En línea:

Se contienen en el anexo 7.2 buenas prácticas identificadas para la gestión de las informaciones en línea.

d) Por correo postal:

Deberá habilitarse una dirección específica bajo la responsabilidad de la persona responsable del sistema interno de información, que se utilice de manera segura.

2. Información sobre los derechos que asisten a la persona informante

La persona que informe sobre las irregularidades será debidamente informada de los derechos que le asisten:

- a) Protección en el transcurso de la investigación. A las personas informantes y a quienes lleven a cabo una revelación pública se les informará de forma expresa de que su identidad será en todo caso reservada y que no se comunicará a las personas a las que se refieren los hechos relatados ni a terceros.
- b) Prohibición de represalias.
- c) Acuse de recibo de la comunicación en el plazo de siete días naturales siguientes a su recepción, salvo que ello pueda poner en peligro la confidencialidad de la comunicación.
- d) Ser informada por escrito sobre el resultado del trámite de admisión de la información para ser investigada en un plazo máximo de diez días hábiles desde la comunicación.
- e) Ser informada por escrito del resultado de las investigaciones en el plazo de máximo de 3 meses desde la comunicación o, en caso de que no se hubiera remitido acuse de recibo, desde la finalización del plazo de siete días naturales posterior a realizarse la comunicación.
- f) Indicación de un domicilio, correo electrónico o lugar seguro a efectos de recibir las notificaciones, pudiendo asimismo renunciar expresamente a la recepción de cualquier comunicación de actuaciones llevadas a cabo por las personas responsables del canal interno como consecuencia de la información.
- g) Ser informada sobre la identidad de la persona responsable del tratamiento, la finalidad del tratamiento y la posibilidad de ejercer los derechos establecidos en los artículos 15 a 22 del Reglamento (UE) 2016/679.
- h) Al anonimato, en caso de que lo desee.
- i) A la supresión de datos transcurridos tres meses, salvo que se deriven de la información procedimientos disciplinarios o de carácter penal.

La información sobre los derechos de la persona informante estará claramente visible junto a la información relativa al canal interno de información disponible en el portal web y le será asimismo remitida o entregada por escrito en el caso de remisión de la

información por correo electrónico o postal o leída mediante locución automática en caso de que la información se formule telefónicamente.

3. Preguntas formuladas por las personas responsables del Sistema interno

Las preguntas que pueden formularse por las personas responsables de los sistemas de información pueden incluir cuestiones relativas al lugar de la irregularidad, el momento en el que se ha producido, las personas que pueden estar involucradas, si se ha remitido anteriormente esta información a través del canal interno de otras vías, si la dirección u otras personas de la organización están involucradas, si existe algún riesgo para la persona informante o para las demás, si se pueden aportar documentos adicionales para apoyar la información, si hay otras personas de contacto o si ha habido intentos de disuasión por parte de otras personas, entre otras.

4. Registro en el sistema de gestión de la información

Presentada la información, se procederá a su registro en el sistema de gestión de la información, siéndole asignado un código de identificación.

El sistema de gestión de la información estará contenido en una base de datos segura y de acceso restringido exclusivamente al personal designado por la persona responsable del Sistema interno de información convenientemente autorizada, en la que se registrarán todas las comunicaciones recibidas, cumplimentando los datos relativos a la fecha de recepción, el código de identificación, las actuaciones desarrolladas, las medidas adoptadas y la fecha de cierre.

Con arreglo a lo establecido por el artículo 26 de la Ley 2/2023, de 20 de febrero, este registro no será público y únicamente a petición razonada de la autoridad competente, y en el marco de un procedimiento judicial y bajo la tutela de aquella, podrá accederse total o parcialmente al contenido del referido registro.

5. Acuse de recibo de la información

Recibida la información, en un plazo no superior a siete días naturales desde dicha recepción, se procederá a acusar recibo, a menos que aquella sea anónima, que la persona informante expresamente haya renunciado a recibir comunicaciones relativas a la investigación o, que la responsable del Sistema interno de información considere razonablemente que el acuse de recibo de la información comprometería la protección de la identidad de la persona informante.

7.5.2 Evaluación de información de irregularidades

La evaluación de la información tiene por finalidad la comprobación de la veracidad de las comunicaciones, la correcta obtención de evidencias y garantizar los derechos de la persona informante y de la afectada por la información.

1. Admisión

Desarrollo

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

Realizado este análisis preliminar, la persona responsable del Sistema interno de información decidirá, en un plazo que no podrá ser superior a diez días hábiles desde la comunicación:

- 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 incluida en el ámbito de aplicación del Sistema.
 - 3.º Cuando la comunicación carezca manifiestamente de fundamento o existan, a juicio de la persona responsable del Sistema interno de información, 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 de hecho o de Derecho que justifiquen un seguimiento distinto. En estos casos, la persona responsable del Sistema interno de información notificará la resolución de manera motivada.

La inadmisión se comunicará a la persona informante dentro de los siete días naturales siguientes a su recepción, salvo que la comunicación fuera anónima o la persona informante hubiera renunciado a recibir comunicaciones.

- b) Admitir a trámite la comunicación.

La admisión a trámite se comunicará a la persona informante dentro de los siete días naturales siguientes a su recepción, salvo que la comunicación fuera anónima o aquella hubiera renunciado a recibir comunicaciones.
- 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.

Actuaciones para la protección y apoyo a la persona que informa de las irregularidades.

Ha de asegurarse en todo momento la protección a las personas que informen de las irregularidades frente a posibles perjuicios derivados de la comunicación de la información.

La protección implica dar todos los pasos razonables para evitar que se produzca un perjuicio o para contener un perjuicio ya identificado o para evitar un daño mayor.

Las estrategias implementadas dependerán de las posibles fuentes de daño identificadas a través de la evaluación del riesgo.

Ha de proporcionarse:

- 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 la persona responsable del Sistema interno ante cualquier autoridad pertinente implicada en su protección frente a represalias, incluida la emisión de una certificación de que la persona informante puede acogerse a protección al amparo de las previsiones del ordenamiento.
- c) Apoyo práctico consistente en tranquilizar a la persona informante acerca del desarrollo del procedimiento y del valor de su conducta.

2. Instrucción

Actuaciones de comprobación de verosimilitud

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

Las preguntas pueden incluir las siguientes:

- ¿Cuándo sucedió la irregularidad?, ¿está a punto de suceder?
- ¿Existe una necesidad inmediata de cesar las actividades?
- ¿Existe un riesgo inmediato para la salud o la seguridad?
- ¿Existe un riesgo inmediato para los derechos de las personas o el medio ambiente?
- ¿Existe una necesidad inmediata de asegurar y proteger las pruebas antes de eliminarlas o destruirlas?
- ¿Existe algún riesgo para las funciones, servicios o reputación de la organización?
- ¿La continuidad de las actividades se verá afectada por la denuncia que se está investigando?
- ¿Podría haber interés de los medios de comunicación en la denuncia de irregularidades?
- ¿Cómo se puede gestionar este proceso de evaluación, asegurando al mismo tiempo la confianza, la protección y la imparcialidad?
- ¿Hay disponible más información que la corrobore?
- ¿Cuál es la naturaleza de la irregularidad (es decir, tipo, frecuencia, prevalencia, función y antigüedad de los sujetos de la denuncia)?

¿Existe la posibilidad de que se denuncie la irregularidad fuera de la organización?

¿Se ha denunciado previamente la irregularidad?

¿Cómo obtuvo la persona denunciante la información? ¿La información es de primera mano o proviene de rumores?

Actuaciones para la garantía de derechos de la persona afectada por la información

Una vez admitida a trámite la comunicación, la persona afectada deberá ser informada por escrito:

- a) De las acciones u omisiones que se le atribuyen. Dicha comunicación podrá efectuarse en el trámite de audiencia si se considera que su aportación con anterioridad pudiera facilitar la ocultación, destrucción o alteración de las pruebas.
- b) De su derecho a la defensa.
- c) De su derecho a la presunción de inocencia.
- d) De su derecho a la protección al honor, mediante la preservación de su identidad y la garantía de la confidencialidad de los hechos y datos del procedimiento.
- e) De su derecho a ser oída y a presentar alegaciones por escrito en cualquier momento del procedimiento y, en cualquier caso, en el trámite de audiencia.
- f) De su derecho al tratamiento de datos personales.

Deberá celebrarse una entrevista con la persona afectada en la que, siempre con absoluto respeto a la presunción de inocencia, se la invitará a exponer su versión de los hechos y a aportar aquellos medios de prueba que considere pertinentes para su defensa.

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

3. Terminación de las actuaciones

Concluidas todas las actuaciones, la persona responsable del Sistema interno de información emitirá un informe que contendrá al menos:

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

El informe será remitido al Comité de integridad departamental, a fin de que adopte alguna de las decisiones siguientes:

- a) Archivo del expediente, que será notificado a la persona informante y a la persona afectada. En estos supuestos, la persona informante tendrá derecho a la protección prevista en el ordenamiento, salvo que se concluyera en la instrucción que la información debería 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, lo remitirá a la Fiscalía Europea.
- c) Traslado de todo lo actuado a la autoridad u organismo que se considere competente para su tramitación.
- d) Traslado a la Subsecretaría para el inicio, en su caso, de un procedimiento disciplinario.

7.6 PROHIBICIÓN DE REPRESALIAS

Con arreglo a lo previsto por el artículo 36 de la Ley 2/2023, de 20 de febrero, 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 conforme a lo previsto en el ordenamiento.

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 la persona informante 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) Anulación de una licencia o permiso.
- f) Denegación de formación.
- g) 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 ante la persona responsable del Sistema interno que, excepcionalmente y de forma justificada, podrá someter la decisión de extender el periodo de protección al comité departamental de integridad, previa audiencia de las personas u órganos que pudieran verse afectados.

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 a la persona o personas perjudicadas.

Las personas que comuniquen o revelen infracciones tendrán derecho a protección siempre que:

- 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 esta ley, y
- b) la comunicación o revelación se haya realizado conforme a los requerimientos previstos en esta ley.

Quedan expresamente excluidas 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 a la persona 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 comprendidas en el ámbito de aplicación del canal.

Las personas que hayan comunicado o revelado públicamente información sobre acciones u omisiones incluidas en el ámbito de aplicación de forma anónima pero que posteriormente hayan sido identificadas y cumplan las condiciones previstas, tendrán derecho a la protección que la misma contiene.

7.7 PROTECCIÓN DE DATOS PERSONALES

Los tratamientos de datos personales que deriven de la gestión del canal interno de información se regirán por lo dispuesto en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, en la Ley Orgánica 3/2018, de 5 de diciembre, en 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 título VI de la Ley 2/2023.

Información sobre protección de datos personales y ejercicio de derechos

Cuando los datos personales se obtengan directamente de las personas interesadas 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 3/2018, de 5 de diciembre.

A las personas 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 de la persona informante o de quien haya llevado a cabo la revelación pública.

Las personas interesadas 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.

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.

Tratamiento de datos personales en el sistema interno de información

El acceso a los datos personales contenidos en el sistema interno quedará limitado, dentro del ámbito de sus competencias y funciones, exclusivamente a las siguientes personas:

- a) Responsable del Sistema interno y a quien lo gestione directamente.
- b) Responsable de recursos humanos o el órgano competente para la tramitación de expedientes disciplinarios.
- c) Abogacía del Estado en el departamento, si procediera la adopción de medidas legales en relación con los hechos relatados en la comunicación.
- d) Encargadas del tratamiento que eventualmente se designen.
- e) Delegado o delegada 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 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 incluidos en el ámbito de aplicación del canal, 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 2/2023, de 20 de febrero.. 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 estos.

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.

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, sin que sea de aplicación la obligación de bloqueo prevista en el artículo 32 de la Ley Orgánica 3/2018, de 5 de diciembre.

Las empleadas y empleados públicos y terceros deberán ser informados acerca del tratamiento de datos personales en el marco de la información relativa al Sistema interno.

Datos incluidos en el registro

Los datos personales relativos a las informaciones recibidas y a las investigaciones internas incluidos en el registro solo se conservarán durante el período que sea necesario y proporcionado a efectos de cumplir con las obligaciones establecidas por el ordenamiento.

En ningún caso podrán conservarse los datos por un período superior a diez años.

Preservación de la identidad de la persona informante y de las personas afectadas

Con arreglo a lo establecido por el artículo 33 de la Ley 2/2023, de 20 de febrero, quien presente una comunicación o lleve a cabo una revelación pública tiene derecho a que su identidad no sea revelada a terceras personas.

El Sistema interno y quienes reciban revelaciones públicas no obtendrán datos que permitan la identificación de la persona 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 de la persona informante en caso de que se hubiera identificado. A estos efectos, se establecen en el anexo 7.2 un boceto de las características técnicas del sistema.

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