

Guía AVAF

Ley 2/2023: Principales obligaciones y recursos de la AVAF



AGENCIA VALENCIANA ANTIFRAUDE
AGENCIA DE PREVENCIÓN Y LUCHA CONTRA EL FRAUDE Y LA CORRUPCIÓN DE LA COMUNIDAD VALENCIANA

València, marzo de 2023

Versión actualizada julio de 2023*

La versión digital de este documento está accesible en la web: <http://www.antifraucv.es>



This work is licensed under the Creative Commons
Reconocimiento-NoComercial-SinObraDerivada 4.0 Internacional License.
No se permite el uso comercial de la obra original ni la generación de derivadas.
Para ver una copia de esta licencia <http://creativecommons.org/licenses/by-nc-nd/4.0/>

Tabla de contenidos

1. Obligación de implementar un canal interno de recepción de informaciones, de uso preferente	3
2. Obligación de los órganos de gobierno de las entidades de designar un responsable del Sistema interno de información.	12
3. Obligación de las entidades de establecer, publicar y actualizar una política o estrategia del Sistema interno de información y defensa del informante	14
4. Obligación de las entidades de establecer, publicar y actualizar un procedimiento de gestión de informaciones recibidas.	14
5. Obligación de establecer las garantías para la protección de los informantes en el ámbito de la propia entidad u organismo	17
6. Sobre la obligación de identificar el canal externo de información.....	23
7. Sobre las obligaciones en materia de tratamiento y protección de datos personales	28
8. Sobre el régimen sancionador.....	31
9. Plazos para adaptarse a la ley	37
10. Posibilidad de suscribir un Protocolo de colaboración con la AVAF y direcciones de contacto para consultas y apoyo en nuestro ámbito de aplicación...	38
Anexo I: Marco normativo	41
Anexo II: Documentos de consulta	42

Por 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 incorporado al ordenamiento interno español la Directiva 2019/1937 del Parlamento Europeo y del Consejo, de 23 de octubre de 2019, relativa a la protección de las personas que informen sobre infracciones del Derecho de la Unión.

La finalidad de la norma es la de proteger frente a represalias a las personas que en un contexto laboral o profesional detecten infracciones penales o administrativas graves o muy graves y las comuniquen mediante los mecanismos regulados en la misma. Pero lo es también el fortalecimiento de la cultura de la información, de las infraestructuras de integridad de las organizaciones y el fomento de la cultura de la información o comunicación como mecanismo para prevenir y detectar amenazas al interés público. De ahí que se amplíe el ámbito de aplicación de la Directiva a las infracciones del ordenamiento nacional, pero limitado a las penales y a las administrativas graves o muy graves para permitir que tanto los canales internos de información como los externos puedan concentrar su actividad investigadora en las vulneraciones que se considera que afectan con mayor impacto al conjunto de la sociedad.

Sin perjuicio de que la citada Ley deja para un desarrollo reglamentario y de elaboración de una estrategia de lucha contra la corrupción posterior (el primero sine die y la segunda a 18 meses vista), y de la necesidad de habilitar los mecanismos legales procedentes para la coexistencia de dicha norma con las regulaciones autonómicas de forma que no se produzca inseguridad jurídica, incertidumbres o contradicciones para la ciudadanía, desde la AVAF, consideramos fundamental recordar a las entidades incluidas en nuestro ámbito subjetivo de aplicación (que a su vez lo están en el de la Ley 2/2023), tanto sus OBLIGACIONES como los MEDIOS GRATUITOS que la Agencia Valenciana Antifraude pone a su disposición para darles cumplimiento, así como una serie de consideraciones que, por su interés, exponemos a continuación.

De igual manera, la Agencia ha publicado en su página web www.antifraucv.es un documento de 36 preguntas y respuestas referidas tanto a cuestiones básicas sobre la Ley como a específicas sobre los Sistemas internos de información (SII), su responsable, los plazos de implementación y la firma al efecto de protocolos con la AVAF.

1. OBLIGACIÓN DE IMPLEMENTAR UN CANAL INTERNO DE RECEPCIÓN DE INFORMACIONES, DE USO PREFERENTE

El título II de la ley contiene el régimen jurídico del Sistema interno de información que abarca tanto el canal, entendido como buzón o cauce para recepción de la información, como el responsable del Sistema y el procedimiento. El Sistema interno de información debería utilizarse de manera preferente para canalizar la información, pues una actuación diligente y eficaz en el seno de la propia organización podría paralizar las consecuencias perjudiciales de las actuaciones investigadas. No obstante, declarada esta preferencia, el informante puede elegir el cauce a seguir, interno o externo, según las circunstancias y los riesgos de represalias que considere:

Artículo 4. Comunicación de infracciones a través del Sistema interno de información.

1. El Sistema interno de información es el cauce preferente para informar sobre las acciones u omisiones previstas en el artículo 2, siempre que se pueda tratar de manera efectiva la infracción y si el denunciante considera que no hay riesgo de represalia.

2. Las personas jurídicas obligadas por las disposiciones del presente título dispondrán de un Sistema interno de información en los términos establecidos en esta ley.

La configuración del Sistema interno de información **debe reunir determinados requisitos**, entre otros, su uso asequible, las garantías de confidencialidad, las prácticas correctas de seguimiento, investigación y protección del informante.

Artículo 5. Sistema interno de información.

1. El órgano de administración u órgano de gobierno de cada entidad u organismo obligado por esta ley será el responsable de la implantación del Sistema interno de información, previa consulta con la representación legal de las personas trabajadoras, y tendrá la condición de responsable del tratamiento de los datos personales de conformidad con lo dispuesto en la normativa sobre protección de datos personales.

2. El Sistema interno de información, en cualquiera de sus fórmulas de gestión, deberá:

a) Permitir a todas las personas referidas en el artículo 3 comunicar información sobre las infracciones previstas en el artículo 2.

b) Estar diseñado, establecido y gestionado de una forma segura, de modo que se garantice la confidencialidad de la identidad del informante y de cualquier tercero mencionado en la comunicación, y de las actuaciones que se desarrollen en la gestión y tramitación de la misma, así como la protección de datos, impidiendo el acceso de personal no autorizado.

c) Permitir la presentación de comunicaciones por escrito o verbalmente, o de ambos modos.

d) Integrar los distintos canales internos de información que pudieran establecerse dentro de la entidad.

e) Garantizar que las comunicaciones presentadas puedan tratarse de manera efectiva dentro de la correspondiente entidad u organismo con el objetivo de que el primero en conocer la posible irregularidad sea la propia entidad u organismo.

f) Ser independientes y aparecer diferenciados respecto de los sistemas internos de información de otras entidades u organismos, sin perjuicio de lo establecido en los artículos 12 y 14.

g) Contar con un responsable del sistema en los términos previstos en el artículo 8.

h) Contar con una política o estrategia que enuncie los principios generales en materia de Sistema interno de información y defensa del informante y que sea debidamente publicitada en el seno de la entidad u organismo.

i) Contar con un procedimiento de gestión de las informaciones recibidas.

j) Establecer las garantías para la protección de los informantes en el ámbito de la propia entidad u organismo, respetando, en todo caso, lo dispuesto en el artículo 9.

Se ha de destacar que **se permite la comunicación anónima**. Cuando se traslade una comunicación en el marco del Sistema interno de información, que entre dentro del ámbito de aplicación de la ley, se aplicará la regla específica contenida en esta ley en cuanto a la posibilidad de presentación y tramitación de comunicaciones anónimas, en línea con el

artículo 24.1 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

Artículo 7. Canal interno de información.

1. Todo canal interno de información de que disponga una entidad para posibilitar la presentación de información respecto de las infracciones previstas en el artículo 2 estará integrado dentro del Sistema interno de información a que se refiere el artículo 5.

*2. **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 de acuerdo a lo que establece el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016.

***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 a 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.

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

4. Los canales internos de información podrán estar habilitados por la entidad que los gestione para la recepción de cualesquiera otras comunicaciones o informaciones fuera del ámbito establecido en el artículo 2, si bien dichas comunicaciones y sus remitentes quedarán fuera del ámbito de protección dispensado por la misma.

Artículo 25. Información sobre los canales interno y externo de información.

Los sujetos comprendidos dentro del ámbito de aplicación de esta ley proporcionarán la información adecuada de forma clara y fácilmente accesible, sobre el uso de todo canal interno de información que hayan implantado, así como sobre los principios esenciales del procedimiento de gestión. En caso de contar con una página web, dicha información deberá constar en la página de inicio, en una sección separada y fácilmente identificable.

(...)

Artículo 26. Registro de informaciones.

*1. Todos los sujetos obligados, de acuerdo con lo dispuesto en esta ley, a disponer de un canal interno de informaciones, con independencia de que formen parte del sector público o del sector privado, **deberán contar 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 esta 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.

2. 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 esta ley. En particular, se tendrá

*en cuenta lo previsto en los apartados 3 y 4 del artículo 32. En ningún caso podrán conservarse los datos por un período superior a **diez años**.*

La ley diferencia la extensión de la obligación de configurar estos canales internos en el ámbito de las organizaciones privadas de las que pertenecen al sector público.

En el ámbito privado, siguiendo la previsión de la Directiva, **estarán obligadas a configurar un Sistema interno de información todas aquellas empresas que tengan más de cincuenta trabajadores**. En los grupos de empresas será la sociedad dominante la que pueda implantar los principios y políticas que inspiren la organización del Sistema para la adecuada organización y coordinación de los canales en cada una de las entidades que forman parte de aquel.

Siendo conscientes del coste que esta nueva carga pueda generar en las empresas, la ley admite que aquellas que, superando la cifra de cincuenta trabajadores cuenten con menos de doscientos cincuenta, puedan compartir medios y recursos para la gestión de las informaciones que reciban, quedando siempre clara la existencia de canales propios en cada empresa.

No obstante, con independencia del número de empleados, se obliga a contar con un Sistema interno de información a todos los partidos políticos, sindicatos, organizaciones empresariales, así como a las fundaciones que de los mismos dependan, siempre que reciban fondos públicos para su financiación. La generalización de un Sistema interno de información facilitará la erradicación de cualquier sospecha de nepotismo, clientelismo, derroche de fondos públicos, financiación irregular u otras prácticas corruptas.

Artículo 10. Entidades obligadas del sector privado.

1. Estarán obligadas a disponer un Sistema interno de información en los términos previstos en esta ley:

a) Las personas físicas o jurídicas del sector privado que tengan contratados cincuenta o más trabajadores.

b) Las personas jurídicas del sector privado que entren en el ámbito de aplicación de los actos de la Unión Europea en materia de servicios, productos y mercados financieros, prevención del blanqueo de capitales o de la financiación del terrorismo, seguridad del transporte y protección del medio ambiente a que se refieren las partes I.B y II del anexo

de la Directiva (UE) 2019/1937, del Parlamento Europeo y del Consejo, de 23 de octubre de 2019, deberán disponer de un Sistema interno de información que se regulará por su normativa específica con independencia del número de trabajadores con que cuenten. En estos casos, esta ley será de aplicación en lo no regulado por su normativa específica.

Se considerarán incluidas en el párrafo anterior las personas jurídicas que, pese a no tener su domicilio en territorio nacional, desarrollen en España actividades a través de sucursales o agentes o mediante prestación de servicios sin establecimiento permanente.

c) Los partidos políticos, los sindicatos, las organizaciones empresariales y las fundaciones creadas por unos y otros, siempre que reciban o gestionen fondos públicos.

2. Las personas jurídicas del sector privado que no estén vinculadas por la obligación impuesta en el apartado 1 podrán establecer su propio Sistema interno de información, que deberá cumplir, en todo caso, los requisitos previstos en esta ley.

Con relación al **sector público**, la ley ha extendido en toda su amplitud la obligación de contar con un Sistema interno de información. En consecuencia, **han de configurar tal Sistema las Administraciones públicas, ya sean territoriales o institucionales, las autoridades independientes u otros organismos que gestionan los servicios de la Seguridad Social, las universidades, las sociedades y fundaciones pertenecientes al sector público, así como las corporaciones de Derecho Público.** En el mismo sentido, se impone también contar con un Sistema interno de información a todos los órganos constitucionales y de relevancia constitucional, así como aquellos mencionados en los Estatutos de Autonomía.

Como se advierte, **preocupa que todas las instituciones, organismos y otras personificaciones que ejercen funciones públicas tengan un sistema eficaz para detectar las prácticas irregulares descritas en esta norma**, sin que a estos efectos parezca relevante el tamaño de la entidad o el ámbito territorial en el que ejerza sus competencias.

Artículo 13. Entidades obligadas en el sector público.

1. Todas las entidades que integran el sector público estarán obligadas a disponer de un Sistema interno de información en los términos previstos en esta ley.

A los efectos de esta ley se entienden comprendidos en el sector público:

a) La Administración General del Estado, las Administraciones de las comunidades autónomas, ciudades con Estatuto de Autonomía y las entidades que integran la Administración Local.

b) Los organismos y entidades públicas vinculadas o dependientes de alguna Administración pública, así como aquellas otras asociaciones y corporaciones en las que participen Administraciones y organismos públicos.

c) Las autoridades administrativas independientes, el Banco de España y las entidades gestoras y servicios comunes de la Seguridad Social.

d) Las universidades públicas.

e) Las corporaciones de Derecho público.

f) Las fundaciones del sector público. A efectos de esta ley, se entenderá por fundaciones del sector público aquellas que reúnan alguno de los siguientes requisitos:

1.º Que se constituyan de forma inicial, con una aportación mayoritaria, directa o indirecta, de una o varias entidades integradas en el sector público, o bien reciban dicha aportación con posterioridad a su constitución.

2.º Que el patrimonio de la fundación esté integrado en más de un cincuenta por ciento por bienes o derechos aportados o cedidos por sujetos integrantes del sector público con carácter permanente.

3.º Que la mayoría de derechos de voto en su patronato corresponda a representantes del sector público.

g) Las sociedades mercantiles en cuyo capital social la participación, directa o indirecta, de entidades de las mencionadas en las letras a), b), c), d) y g) del presente apartado sea superior al cincuenta por ciento, o en los casos en que, sin superar ese porcentaje, se encuentre respecto de las referidas entidades en el supuesto previsto en el artículo 5 del texto refundido de la Ley del Mercado de Valores, aprobado por Real Decreto Legislativo 4/2015, de 23 de octubre.

2. También deberán dotarse de un Sistema interno de información, en los mismos términos requeridos para las entidades del sector público enunciados en el apartado anterior, los órganos constitucionales, los de relevancia constitucional e instituciones autonómicas análogas a los anteriores.

3. *En caso de organismos públicos con funciones de comprobación o investigación de incumplimientos sujetos a esta norma, se distinguirá, al menos, entre un canal interno referente a los propios incumplimientos del organismo o su personal, y el canal externo referente a las comunicaciones que reciba de los incumplimientos de terceros cuya investigación corresponda a sus competencias.*

4. *En caso de que un organismo público con competencias en materia de investigación reciba informaciones referentes a los incumplimientos de terceros en el plazo de duración establecido en la letra d) del artículo 9.2, se resolverá si procede o no iniciar una comprobación o investigación del sujeto afectado dando traslado de ello al informante.*

Una vez ultimado el procedimiento de comprobación o investigación, se comunicará al informante el resultado de la comprobación. Si los datos e informes que figuran en el expediente tienen carácter reservado o confidencial de acuerdo con alguna disposición con rango de ley, el contenido del resultado que se traslade al informante tendrá carácter genérico.

5. *Las decisiones adoptadas por los organismos públicos con funciones de comprobación o investigación en relación con las informaciones no serán recurribles en vía administrativa ni en vía contencioso-administrativa.*

Así, **si bien es cierto que la Directiva atribuye a los Estados miembros la decisión de dispensar de algunas obligaciones a los municipios de menos de diez mil habitantes, esta ley no contempla esta excepción.** En consecuencia, atendiendo a la necesidad de ofrecer un marco común y general de protección de los informantes, de no facilitar resquicios que puedan dañar gravemente el interés general, **se extiende a todos los municipios la obligación de contar con un Sistema interno de información.** Ahora bien, tal obligación se acompaña de ciertas precisiones con el fin de facilitar su cumplimiento a aquellos municipios cuya población no supere los diez mil habitantes. **La ley permite que estos municipios puedan compartir medios para la recepción de informaciones con otras Administraciones que ejerzan sus competencias en la misma comunidad autónoma. Esta posibilidad no exime de que cada administración local tenga un responsable de su sistema interno de informaciones.**

En todo caso, hay que insistir en que se considera adecuado que cada municipio cuente con su propio sistema interno de información y de ahí que **se destaque la asistencia que pueden prestar otras Administraciones territoriales.**

Artículo 14. Medios compartidos en el sector público.

1. Los municipios de menos de 10.000 habitantes, entre sí o con cualesquiera otras Administraciones públicas que se ubiquen dentro del territorio de la comunidad autónoma, podrán compartir el Sistema interno de información y los recursos destinados a las investigaciones y las tramitaciones.

2. Asimismo, las entidades pertenecientes al sector público con personalidad jurídica propia vinculadas o dependientes de órganos de las Administraciones territoriales, y que cuenten con menos de cincuenta trabajadores, podrán compartir con la Administración de adscripción el Sistema interno de información y los recursos destinados a las investigaciones y las tramitaciones.

3. En todo caso, deberá garantizarse que los sistemas resulten independientes entre sí y los canales aparezcan diferenciados respecto del resto de entidades u organismos, de modo que no se genere confusión a los ciudadanos.

Para facilitar la implementación y puesta en marcha del canal interno a las entidades incluidas en el ámbito de actuación de la Agencia Valenciana Antifraude (Ley 11/2016, de 28 de noviembre, y su Reglamento de funcionamiento y régimen interior), se pueden suscribir protocolos de colaboración para asesorarles, colaborar en su implementación, así como **facilitar el uso gratuito del software libre de gestión que utiliza esta Agencia** para sus buzones de denuncias, tecnologías que cumplen todos los requisitos requeridos por la Ley 2/2023 para el canal interno de información.

Recordamos asimismo que, tal y como dispone el artículo 157.3 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, siempre que existan soluciones públicas (aplicaciones o herramientas) a su disposición para su reutilización, deberán justificar que la elección de otras tecnologías privadas que puedan comercializarse en el mercado (con el correspondiente gasto público) resultan más eficientes que las primeras conforme al artículo 7 de la LO 2/2012 de Estabilidad Presupuestaria y Sostenibilidad Financiera.

Recordamos que el sector público está obligado a proteger el interés general poniendo en práctica los principios de buena administración pública ex artículo 103 de la Constitución que desarrollan otras normas (entre ellas, el artículo 3 de la Ley 40/2015, de Régimen Jurídico del Sector Público), debiendo proteger asimismo la información pública y los datos personales frente a cualquier injerencia particular, para evitar fugas de información, conflictos de intereses y otros riesgos contrarios a la integridad institucional que pueden consultar en los Catálogos y Recomendaciones AVAF.

2. OBLIGACIÓN DE LOS ÓRGANOS DE GOBIERNO DE LAS ENTIDADES DE DESIGNAR UN RESPONSABLE DEL SISTEMA INTERNO DE INFORMACIÓN.

Resulta indispensable para la eficacia del Sistema interno de información la designación del responsable de su correcto funcionamiento. En el mismo sentido, se configura como elemento esencial del sistema en el **artículo 5 g)**.

Artículo 8. Responsable del Sistema interno de información.

1. El órgano de administración u órgano de gobierno de cada entidad u organismo obligado por esta ley será el competente para la designación de la persona física responsable de la gestión de dicho sistema o «Responsable del Sistema», y de su destitución o cese.

*2. 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**.*

*3. 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.*

*4. 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.

*5. En el caso del **sector privado**, el Responsable del Sistema persona física o la entidad en quien el órgano colegiado responsable haya delegado sus funciones, será un directivo de la entidad, que ejercerá su cargo con independencia del órgano de administración o de gobierno de la misma. Cuando la naturaleza o la dimensión de las actividades de la entidad no justifiquen o permitan la existencia de un directivo Responsable del Sistema, será posible el desempeño ordinario de las funciones del puesto o cargo con las de Responsable del Sistema, tratando en todo caso de evitar posibles situaciones de conflicto de interés.*

*6. En las entidades u organismos en que ya existiera una persona responsable de la función de cumplimiento normativo o de políticas de integridad, cualquiera que fuese su denominación, podrá ser esta la persona designada como **Responsable del Sistema**, siempre que cumpla los requisitos establecidos en esta ley.*

Desde la Agencia Valenciana Antifraude animamos a todas las entidades a designar un responsable de integridad (que asumiría las funciones vinculadas a los canales internos de información arriba indicadas, pero también todas aquellas que requiera la ejecución del plan de integridad institucional y/o de cada uno de los marcos de integridad que impone la vigente legislación autonómica en materia de transparencia y buen gobierno, tales como: códigos éticos, procedimientos de prevención y control de los conflictos de interés, formación, etc). Dicha persona u órgano designado como tal sería “puente” y “palanca” con esta Agencia así como con el resto de órganos de control, propiciando así una comunicación fluida y la creación de una futura red autonómica de responsables de integridad con mayor capacidad de afrontar cuestiones similares en la práctica.

Sobre este particular, se hace preciso anotar que por Resolución número 504, de 10 de mayo de 2023, del director de la AVAF (DOGV núm. 9601 de 23.05.2023), se creó el Registro de responsables de sistemas internos de información de la Agencia de Prevención y Lucha contra el Fraude y la Corrupción de la Comunitat Valenciana (RRSII), regulándose su funcionamiento.

3. OBLIGACIÓN DE LAS ENTIDADES DE ESTABLECER, PUBLICAR Y ACTUALIZAR UNA POLÍTICA O ESTRATEGIA DEL SISTEMA INTERNO DE INFORMACIÓN Y DEFENSA DEL INFORMANTE

Las entidades públicas y privadas obligadas por la Ley deberán contar con una política o estrategia que enuncie los principios generales en materia de Sistema interno de información y defensa del informante y que sea debidamente publicitada en el seno de la entidad u organismo.

A tal efecto, se puede consultar el decálogo de principios de protección de las personas denunciantes de la AVAF.

4. OBLIGACIÓN DE LAS ENTIDADES DE ESTABLECER, PUBLICAR Y ACTUALIZAR UN PROCEDIMIENTO DE GESTIÓN DE INFORMACIONES RECIBIDAS.

Artículo 9. Procedimiento de gestión de informaciones.

1. El órgano de administración u órgano de gobierno de cada entidad u organismo obligado por esta ley aprobará el procedimiento de gestión de informaciones. El Responsable del Sistema responderá de su tramitación diligente.

2. El procedimiento establecerá las previsiones necesarias para que el Sistema interno de información y los canales internos de información existentes cumplan con los requisitos establecidos en esta ley. En particular, el procedimiento responderá al contenido mínimo y 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) Determinación del plazo máximo para dar respuesta a las actuaciones de investigación, que no podrá ser superior a tres meses a contar desde la recepción de la comunicación o, si no se remitió un acuse de recibo al informante, a 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 tres meses adicionales.

e) Previsión de la posibilidad de mantener la comunicación con el informante y, si se considera necesario, de solicitar a la persona informante información adicional.

f) Establecimiento del 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 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.

h) Exigencia del respeto a la presunción de inocencia y al honor de las personas afectadas.

i) Respeto de las disposiciones sobre protección de datos personales de acuerdo a lo previsto en el título VI.

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.

Por otra parte, se prevé que **la gestión material del Sistema interno de información se realice mediante modalidades de gestión indirecta**, si bien la atribución por parte de las Administraciones territoriales a un tercero de la gestión del Sistema interno de información requerirá que acrediten la **insuficiencia de medios propios** para poder realizar la función.

Artículo 6. Gestión del Sistema interno de información por tercero externo.

1. La gestión del Sistema interno de información se podrá llevar a cabo dentro de la propia entidad u organismo o acudiendo a un tercero externo, en los términos previstos en esta ley. A estos efectos, se considera gestión del Sistema la recepción de informaciones.

2. La gestión del sistema por un tercero externo exigirá en todo caso que este ofrezca garantías adecuadas de respeto de la independencia, la confidencialidad, la protección de datos y el secreto de las comunicaciones.

La existencia de corresponsables del tratamiento de datos personales requiere la previa suscripción del acuerdo regulado en el artículo 26 del 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), y en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

3. La gestión del Sistema interno de información por un tercero no podrá suponer un menoscabo de las garantías y requisitos que para dicho sistema establece esta ley ni una atribución de la responsabilidad sobre el mismo en persona distinta del Responsable del Sistema previsto en el artículo 8.

4. El tercero externo que gestione el Sistema tendrá la consideración de encargado del tratamiento a efectos de la legislación sobre protección de datos personales. El tratamiento se registrará por el acto o contrato al que se refiere el artículo 28.3 del Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016.

Artículo 15. Gestión del Sistema interno de información por tercero externo.

La gestión del Sistema interno de información por un tercero externo en el ámbito de la Administración General del Estado, las Administraciones autonómicas y ciudades con Estatuto de Autonomía y las Entidades que integran la Administración Local solo podrá acordarse en aquellos casos en que se acredite insuficiencia de medios propios, conforme a lo dispuesto en el artículo 116 apartado 4 letra f) de la 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. Esta gestión comprenderá únicamente el procedimiento para la recepción de las informaciones sobre infracciones y, en todo caso, tendrá carácter exclusivamente instrumental.

Conviene destacar que la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (LPAC), aplicable con carácter básico a todos

los procedimientos administrativos, establece que **toda comunicación de hechos que puedan constituir una infracción ha de ser considerada como una denuncia (artículo 62.1 LPAC).**

Con respecto a la gestión indirecta del Sistema interno de información por un tercero, desde la AVAF queremos advertir que, en todo caso, deberá residenciarse su control en el ámbito interno de la organización.

La externalización, previa justificación de la insuficiencia de medios propios, únicamente podría ser de carácter instrumental y sin que pueda implicar ejercicio de potestades públicas y/o funciones reservadas a personal funcionario de carrera de acuerdo con el artículo 105 de la Constitución y de la Ley de Función Pública de la Comunidad Valenciana. A tal efecto, cada Administración y entidad del sector público deberá velar por implementar cuantas garantías y mecanismos resulten necesarios en el procedimiento de recepción de informaciones sobre infracciones para: detectar eventuales posibles conflictos de interés entre el tercero y las personas informantes (declaraciones de ausencia de conflictos de interés preceptivas y actualizadas, mecanismos de inhibición y abstención, control por las respectivas entidades públicas, etc.); prevenir y contener los riesgos de fuga de información institucional y los ciberataques; protección de datos personales de las personas informantes, garantías de confidencialidad, entre otras.

5. OBLIGACIÓN DE ESTABLECER LAS GARANTÍAS PARA LA PROTECCIÓN DE LOS INFORMANTES EN EL ÁMBITO DE LA PROPIA ENTIDAD U ORGANISMO

Habrán de establecerse, en el ámbito interno por parte de cada entidad, respetando lo dispuesto en el artículo 9 de la Ley.

A efectos orientativos, y como competencia de la Autoridad Independiente estatal y de las autonómicas, el **título VII** constituye, como ya se ha anticipado, el eje de la ley, las medidas de protección para amparar a aquellas personas que mantienen una actitud cívica y de respeto democrático al alertar sobre infracciones graves que dañan el interés general. Ha de conseguirse que nadie esté amedrentado ante futuros perjuicios. De ahí que la primera medida sea la contundente declaración de prohibir y declarar nulas aquellas conductas que puedan calificarse de represalias y se adopten dentro de los dos años siguientes a ultimar las investigaciones. En este sentido, la ley ofrece varios supuestos, sin ningún ánimo exhaustivo, que muestran conductas intolerables hacia los

informantes: resolución de contratos, intimidaciones, trato desfavorable, daños reputacionales, etc.

La necesidad de garantizar la buena aplicación del ordenamiento hace que queden sin efecto cualesquiera cláusulas o disposiciones contractuales que impidan o pretendan limitar el derecho o la capacidad de informar, tales como cláusulas de confidencialidad o disposiciones que reflejan renunciaciones expresas; así como que se exima de responsabilidad ante la obtención de información relevante o que se invierta la carga de la prueba en aquellos procesos que inicie para exigir la reparación de daños. En fin, los informantes contarán con el apoyo necesario de la Autoridad Independiente de Protección del Informante, A.A.I. para que las medidas de protección establecidas en esta ley resulten eficaces.

Pero las medidas de protección no se dirigen sólo a favor de los informantes. También aquellas personas a las que se refieran los hechos relatados en la comunicación han de contar con una singular protección ante el riesgo de que la información, aun con aparentes visos de veracidad, haya sido manipulada, sea falsa o responda a motivaciones que el Derecho no puede amparar. Estas personas mantienen todos sus derechos de tutela judicial y defensa, de acceso al expediente, de confidencialidad y reserva de identidad y la presunción de inocencia; en fin, de los mismos derechos que goza el informante.

Las ventajas y eficacia que han demostrado los programas de clemencia en ciertos ámbitos sectoriales han llevado a incluir una regulación en la que se precisan las concretas condiciones para su correcta aplicación.

Artículo 35. Condiciones de protección.

1. Las personas que comuniquen o revelen infracciones previstas en el artículo 2 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 esta ley,

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

2. Quedan expresamente excluidos de la protección prevista en esta ley aquellas personas que comuniquen o revelen:

a) Informaciones contenidas en comunicaciones que hayan sido inadmitidas por algún canal interno de información o por alguna de las causas previstas en el artículo 18.2.a).

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 comprendidas en el artículo 2.

3. Las personas que hayan comunicado o revelado públicamente información sobre acciones u omisiones a que se refiere el artículo 2 de forma anónima pero que posteriormente hayan sido identificadas y cumplan las condiciones previstas en esta ley, tendrán derecho a la protección que la misma contiene.

4. Las personas que informen ante las instituciones, órganos u organismos pertinentes de la Unión Europea infracciones que entren en el ámbito de aplicación de la Directiva (UE) 2019/1937 del Parlamento Europeo y del Consejo, de 23 de octubre de 2019, tendrán derecho a protección con arreglo a lo dispuesto en esta ley en las mismas condiciones que una persona que haya informado por canales externos.

Artículo 36. Prohibición de represalias.

1. 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 esta ley.

2. 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.

3. A los efectos de lo previsto en esta ley, y 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.

4. 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.

5. 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.

6. La Autoridad Independiente de Protección del Informante, A.A.I. podrá, en el marco de los procedimientos sancionadores que instruya, adoptar medidas provisionales en los términos establecidos en el artículo 56 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

Artículo 38. Medidas de protección frente a represalias.

1. No se considerará que las personas que comuniquen información sobre las acciones u omisiones recogidas en esta ley o que hagan una revelación pública de conformidad con esta ley 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 esta ley, todo ello sin perjuicio de lo dispuesto en el artículo 2.3. 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.

2. 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.

3. Cualquier otra posible responsabilidad de los informantes derivada de actos u omisiones que no estén relacionados con la comunicación o la revelación pública o que no sean necesarios para revelar una infracción en virtud de esta ley será exigible conforme a la normativa aplicable.

4. *En los procedimientos ante un órgano jurisdiccional u otra autoridad relativos a los perjuicios sufridos por los informantes, una vez que el informante haya demostrado razonablemente que ha comunicado o ha hecho una revelación pública de conformidad con esta ley y que ha sufrido un perjuicio, se presumirá que el perjuicio se produjo como represalia por informar o por hacer una revelación pública. En tales casos, corresponderá a la persona que haya tomado la medida perjudicial probar que esa medida se basó en motivos debidamente justificados no vinculados a la comunicación o revelación pública.*

5. *En los procesos judiciales, incluidos los relativos a difamación, violación de derechos de autor, vulneración de secreto, infracción de las normas de protección de datos, revelación de secretos empresariales, o a solicitudes de indemnización basadas en el derecho laboral o estatutario, las personas a que se refiere el artículo 3 de esta ley no incurrirán en responsabilidad de ningún tipo como consecuencia de comunicaciones o de revelaciones públicas protegidas por la misma. Dichas personas tendrán derecho a alegar en su descargo y en el marco de los referidos procesos judiciales, el haber comunicado o haber hecho una revelación pública, siempre que tuvieran motivos razonables para pensar que la comunicación o revelación pública era necesaria para poner de manifiesto una infracción en virtud de esta ley.*

Artículo 39. 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 en los términos regulados en esta ley, así como a la misma protección establecida para los informantes, preservándose su identidad y garantizándose la confidencialidad de los hechos y datos del procedimiento.

Artículo 40. Supuestos de exención y atenuación de la sanción.

1. *Cuando una persona que hubiera participado en la comisión de la infracción administrativa objeto de la información sea la que informe de su existencia mediante la presentación de la información y siempre que la misma hubiera sido presentada con anterioridad a que hubiera sido notificada la incoación del procedimiento de investigación o sancionador, el órgano competente para resolver el procedimiento, mediante resolución motivada, podrá eximirle del cumplimiento de la sanción administrativa que le correspondiera siempre que resulten acreditados en el expediente los siguientes extremos:*

a) Haber cesado en la comisión de la infracción en el momento de presentación de la comunicación o revelación e identificado, en su caso, al resto de las personas que hayan participado o favorecido aquella.

b) Haber cooperado plena, continua y diligentemente a lo largo de todo el procedimiento de investigación.

c) Haber facilitado información veraz y relevante, medios de prueba o datos significativos para la acreditación de los hechos investigados, sin que haya procedido a la destrucción de estos o a su ocultación, ni haya revelado a terceros, directa o indirectamente su contenido.

d) Haber procedido a la reparación del daño causado que le sea imputable.

2. Cuando estos requisitos no se cumplan en su totalidad, incluida la reparación parcial del daño, quedará a criterio de la autoridad competente, previa valoración del grado de contribución a la resolución del expediente, la posibilidad de atenuar la sanción que habría correspondido a la infracción cometida, siempre que el informante o autor de la revelación no haya sido sancionado anteriormente por hechos de la misma naturaleza que dieron origen al inicio del procedimiento.

3. La atenuación de la sanción podrá extenderse al resto de los participantes en la comisión de la infracción, en función del grado de colaboración activa en el esclarecimiento de los hechos, identificación de otros participantes y reparación o minoración del daño causado, apreciado por el órgano encargado de la resolución.

4. Lo dispuesto en este artículo no será de aplicación a las infracciones establecidas en la Ley 15/2007, de 3 de julio, de Defensa de la Competencia.

6. SOBRE LA OBLIGACIÓN DE IDENTIFICAR EL CANAL EXTERNO DE INFORMACIÓN

El título III de la ley regula el canal externo de información, como medio complementario al canal interno. Con el fin de dar cumplimiento a los objetivos perseguidos por la Unión Europea y ahondar en la protección del informante, esta ley procede a la implementación de un canal externo cuya llevanza corresponde a la Autoridad Independiente de Protección del Informante, A.A.I. prevista en el título VIII. Todo ello sin perjuicio de las vigentes regulaciones autonómicas sobre los canales externos de denuncias. Conviene

recordar que la propia Ley 2/23 excluye de su ámbito de aplicación todas aquellas prácticas contrarias a la integridad que no integren el ámbito de la directiva o sean infracciones administrativas graves o muy graves, si bien deja claro el carácter eminentemente preventivo de la misma y de protección de la cultura de la integridad para proteger los intereses generales. Así, a los efectos de prácticas contrarias a la integridad, fraude y corrupción (incluyendo todo tipo de irregularidades para proteger toda clase de fondos públicos) podrá designarse como tal, al amparo de la Ley 1/2022, de Transparencia y Buen Gobierno de la Comunitat Valenciana, el buzón externo de denuncias de esta Agencia Valenciana Antifraude.

El título III aborda de manera sistemática la regulación específica del canal externo **ante el que podrán informar las personas físicas a las que se refiere el artículo 3 de la ley, ya sea directamente, ya con posterioridad a la previa formulación de información ante el canal interno.**

Artículo 16. Comunicación a través del canal externo de información de la Autoridad Independiente de Protección del Informante, A.A.I. o a través de las autoridades u órganos autonómicos.

1. Toda persona física podrá informar ante la Autoridad Independiente de Protección del Informante, A.A.I., o ante las autoridades u órganos autonómicos correspondientes, de la comisión de cualesquiera acciones u omisiones incluidas en el ámbito de aplicación de esta ley, ya sea directamente o previa comunicación a través del correspondiente canal interno.

2. Las referencias realizadas en este título III a la Autoridad Independiente de Protección del Informante, A.A.I., se entenderán hechas, en su caso, a las autoridades autonómicas competentes.

Tras detallar el **procedimiento de recepción de las comunicaciones**, que pueden llevarse a cabo de forma anónima o con reserva de la identidad del informante, y de su forma, escrita o verbal, el articulado de la norma aborda el trámite de admisión, en el que después de un análisis preliminar, se decide sobre su admisión a trámite, inadmisión motivada si concurre alguna de las causas tasadas que a tal efecto se prevén, comunicación inmediata al Ministerio Fiscal si la conducta pudiera ser constitutiva de

delito o remisión a otra Autoridad u Organismo que pudiera resultar competente para la tramitación de la comunicación.

Finalmente, cabe destacar que la resolución que adopte la Autoridad Independiente de Protección del Informante, A.A.I. no podrá ser objeto de recurso alguno, ni administrativo ni jurisdiccional, sin perjuicio de la posible impugnación de la resolución que ponga fin al procedimiento sancionador que se pudiera incoar a raíz de las investigaciones realizadas.

Debe tenerse en cuenta que el informante por el hecho de comunicar la existencia de una infracción penal o administrativa no tiene la condición de interesado, sino de colaborador con la Administración. De manera que las investigaciones que lleve a cabo tanto en el marco del Sistema interno de información del sector público como en el marco del procedimiento que desarrolla la Autoridad Independiente de Protección del Informante, A.A.I. se inician siempre de oficio y de conformidad con el procedimiento establecido en la LPAC.

Asimismo, prevé el título III (Artículo 21) el conjunto de derechos y garantías que ostenta el informante en el procedimiento de comunicación externa ante la Autoridad Independiente de Protección del Informante, A.A.I. y la exigencia de revisión de los procedimientos de recepción y seguimiento de informaciones, dando así cumplimiento al mandato de la Directiva.

Por último, conviene destacar la **posible implantación de canales externos de información por parte de las comunidades autónomas**. La llevanza de dichos canales externos será asumida por autoridades independientes autonómicas análogas a la Autoridad Independiente de Protección del Informante, A.A.I. cuya competencia podrá extenderse tanto a las informaciones sobre infracciones que, comprendidas en el ámbito de aplicación de esta ley, sean cometidas en el ámbito de las entidades del sector público autonómico y local del territorio de la correspondiente comunidad autónoma, como a las relativas a incumplimientos imputables a entidades del sector privado que produzcan efectos únicamente en el territorio de dicha comunidad autónoma.

Artículo 23. Traslado de la comunicación por otras autoridades a la Autoridad Independiente de Protección del Informante, A.A.I.

Cualquier autoridad que reciba una comunicación y no tenga competencias para investigar los hechos relatados por tratarse de alguna de las infracciones previstas en el título IX, deberá remitirla a la Autoridad Independiente de Protección del Informante, A.A.I.

dentro de los diez días siguientes a aquel en el que la hubiera recibido. La remisión se comunicará al informante dentro de dicho plazo.

Artículo 24. Informaciones sujetas a la competencia de las autoridades independientes de protección a informantes.

*1. La Autoridad Independiente de Protección del Informante, **A.A.I.** es la autoridad competente para la tramitación, a través del canal externo, de las informaciones que afecten a los siguientes sujetos:*

a) La Administración General del Estado y entidades que integran el sector público estatal.

b) Resto de entidades del sector público, los órganos constitucionales y los órganos de relevancia constitucional a que se refiere el artículo 13.

c) Entidades que integran el sector privado, cuando la infracción o el incumplimiento sobre el que se informe afecte o produzca sus efectos en el ámbito territorial de más de una comunidad autónoma.

d) Cuando se suscriba el oportuno convenio, las Administraciones de las comunidades autónomas, las entidades que integran la Administración y el sector público institucional autonómico o local.

2. La autoridad independiente o entidad que pueda señalarse en cada comunidad autónoma, lo será respecto de las informaciones que afecten:

a) al sector público autonómico y local de su respectivo territorio,

b) a las instituciones autonómicas a que se refiere el artículo 13.2, y

c) a las entidades que formen parte del sector privado, cuando el incumplimiento comunicado se circunscriba al ámbito territorial de la correspondiente comunidad autónoma.

3. Cuando se reciba una comunicación por un canal que no sea el competente o por los miembros del personal que no sean los responsables de su tratamiento, las autoridades competentes garantizarán, mediante el procedimiento de gestión del Sistema establecido, que el personal que la haya recibido no pueda revelar cualquier información

que pudiera permitir identificar al informante o a la persona afectada y que remitan con prontitud la comunicación, sin modificarla, al Responsable del Sistema de información.

En suma, tal y como hemos visto, en el ámbito de la Comunidad Valenciana, adicionalmente (pero no en sustitución del canal de la A.A.I.), podrá utilizarse el buzón externo de denuncias de la Agencia Valenciana Antifraude y, en todo caso, se utilizará para comunicar irregularidades contrarias a la integridad pública o potencialmente constitutivas de fraude o corrupción de ámbito autonómico (incluyendo todo tipo de irregularidades para proteger toda clase de fondos públicos). Y ello, al igual que convive con otros canales de denuncias externos como el habilitado por el SNCA (Infofraude), para la comunicación de información sobre fraudes o irregularidades que afecten a fondos europeos, el cual dispone de un apartado específico relativo al Mecanismo de Recuperación y Resiliencia, teniendo en cuenta lo dispuesto en la Comunicación 1/2017, de 6 de abril, 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.

Este canal existe desde hace cuatro años. Se crea por Resolución de 25 de abril de 2018, del director de la Agencia de Prevención y Lucha contra el Fraude y la Corrupción de la Comunitat Valenciana, de creación del Buzón de Denuncias de la Agencia y se regula su funcionamiento. Desde dicha fecha, el Buzón ha permitido ininterrumpidamente la recepción de alertas durante las 24 horas del día de los 365 días al año. Para ser admitidas, las comunicaciones efectuadas a través del Buzón de Denuncias deben referirse a acciones que se realicen en el ámbito de actuación de la Agencia: objetivo, subjetivo y territorial.

El ámbito objetivo, tal y como se determina en la Resolución por la que se concreta el ámbito de actuación material de la AVAF (de 05-10-2020), se basa en tres principios: prevenir y erradicar el fraude y la corrupción; impulsar la integridad y la ética pública; y fomentar una cultura de buenas prácticas y de rechazo del fraude y la corrupción en políticas públicas, así como en la gestión de recursos públicos. A partir de ahí la AVAF es competente para determinar el grado de adecuación a Derecho de la actuación denunciada. El ámbito subjetivo es amplio, dentro de la tendencia, ya consolidada, de incluir todo el sector público en sentido amplio en el ámbito de aplicación subjetiva de las normas de Derecho público (Ley de contratos, Ley de transparencia, Ley de régimen jurídico, etc.). De este modo abarcaría no solo la Administración autonómica y local, y su

sector público, sino también otras entidades de derecho público, las estatutarias (en cuanto a su actividad administrativa), e incluso personas físicas y jurídicas, como perceptoras de fondos públicos. Por último, también los partidos políticos, sindicatos y organizaciones empresariales se encuentran incluidos en este ámbito de aplicación. En cuanto al ámbito territorial, evidentemente la AVAF, como entidad autonómica valenciana (dependiente de les Corts pero funcionando como entidad independiente dentro del entramado institucional de la Generalitat), debe restringir su actuación al territorio de la Comunitat Valenciana.

7. SOBRE LAS OBLIGACIONES EN MATERIA DE TRATAMIENTO Y PROTECCIÓN DE DATOS PERSONALES

El **título VI** regula el régimen del **tratamiento de datos personales** que deriven de la aplicación de esta ley.

El artículo 17 de la Directiva impone que todo tratamiento de datos personales realizado en aplicación de la misma se realizará de conformidad con el 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) y con la Directiva (UE) 2016/680. En este mismo sentido esta ley dispone que los tratamientos de datos personales deberán regirse por lo dispuesto en dicho **Reglamento y en la Ley Orgánica 3/2018**, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

Hasta ahora el artículo 24 de la citada ley orgánica regulaba la creación y mantenimiento de sistemas de información internos. El contenido de dicho precepto se ha incorporado a esta ley, pero era necesario completar las previsiones hasta ahora incluidas en la ley orgánica al objeto de extenderlas también a los tratamientos de datos que se lleven a cabo en los canales de comunicación externos y en los supuestos de revelación pública. Asimismo, y de acuerdo con lo que establece el artículo 6 del Reglamento general de protección de datos, procede indicar los títulos que hacen lícito el tratamiento de datos personales. Los tratamientos se entenderán necesarios para el cumplimiento de una obligación legal cuando deban llevarse a cabo en los supuestos en que sea obligatorio disponer de un Sistema interno de información y en los casos de canales de comunicación externos, mientras que se presumirán válidos al amparo de lo que establece el artículo 6.1.e) del Reglamento general de protección de datos cuando aquel sistema no sea

obligatorio o el tratamiento se lleve a cabo en el ámbito de la revelación pública que regula el título V. Se indica asimismo que en caso de que la persona investigada ejerza el derecho de oposición al tratamiento de sus datos personales se entiende que existen motivos legítimos imperiosos que legitiman continuar con dicho tratamiento, tal como permite el artículo 21.1 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016.

Artículo 32. Tratamiento de datos personales en el Sistema interno de información.

1. 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.*

2. 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 a las que se refiere el artículo 2, 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.

3. 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.

4. ***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.***

5. ***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.***

La ley también regula determinadas condiciones especiales en relación con los tratamientos de datos al objeto de garantizar plenamente el derecho a la protección de datos y en particular la identidad de los informantes y de las personas investigadas por la información suministrada. La preservación de la identidad del informante es una de las premisas esenciales para garantizar la efectividad de la protección que persigue esta ley. De ahí que se exija que en todo momento deba ser garantizada. En esta línea se dispone que el dato de la identidad del informante nunca será objeto del derecho de acceso a datos personales y se limita la posibilidad de comunicación de dicha identidad sólo a la autoridad judicial, el Ministerio Fiscal o la autoridad administrativa competente exigiendo que en todo caso se impida el acceso por terceros a la misma. Por otra parte, se exige que las entidades obligadas a disponer de un Sistema interno de información, los terceros externos que en su caso lo gestionen y la Autoridad Independiente de Protección de

Datos, A.A.I. así como las que en su caso se constituyan, cuenten con un delegado de protección de datos.

Artículo 33. Preservación de la identidad del informante y de las personas afectadas.

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

2. *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.*

3. *La identidad del informante solo podrá ser comunicada a la Autoridad judicial, al Ministerio Fiscal o a la autoridad administrativa competente en el marco de una investigación penal, disciplinaria o sancionadora.*

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

Artículo 34. Delegado de protección de datos.

De acuerdo con lo que dispone el artículo 37.1.a) del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, la Autoridad Independiente de Protección del Informante, A.A.I., y las autoridades independientes que en su caso se constituyan, deberán nombrar un delegado de protección de datos.

8. SOBRE EL RÉGIMEN SANCIONADOR

El texto articulado se cierra con un **título IX** que establece el **régimen sancionador**, necesario para combatir con eficacia aquellas actuaciones que impliquen represalias

contra los informantes, así como los incumplimientos en el establecimiento de las reglas de los canales de comunicación.

Artículo 61. Autoridad sancionadora.

*1. El ejercicio de la potestad sancionadora prevista en esta ley **corresponde a la Autoridad Independiente de Protección del Informante, A.A.I., y a los órganos competentes de las comunidades autónomas, sin perjuicio de las facultades disciplinarias que en el ámbito interno de cada organización pudieran tener los órganos competentes.***

2. La Autoridad Independiente de Protección del Informante, A.A.I. será competente respecto de las infracciones cometidas en el ámbito del sector público estatal. También será competente respecto a las infracciones cometidas en el ámbito del sector privado en todo el territorio, siempre que la normativa autonómica correspondiente no haya atribuido esta competencia a los organismos competentes de las respectivas comunidades autónomas. La competencia para la imposición de sanciones derivadas de los procedimientos competencia de la Autoridad Independiente de Protección del Informante, A.A.I. corresponderá a la persona titular de su presidencia.

3. Los órganos competentes de las comunidades autónomas lo serán exclusivamente respecto de las infracciones cometidas en el ámbito del sector público autonómico y local del territorio de la correspondiente comunidad autónoma. La normativa autonómica podrá prever que dichos órganos sean competentes respecto de las infracciones cometidas en el ámbito del sector privado cuando afecten solamente a su ámbito territorial.

Artículo 62. Sujetos responsables.

*1. **Estarán sujetos al régimen sancionador establecido en esta ley las personas físicas y jurídicas que realicen cualquiera de las actuaciones descritas como infracciones en el artículo 63.***

*2. Cuando la comisión de la infracción se atribuya a un **órgano colegiado** la responsabilidad será exigible en los términos que señale la resolución sancionadora. **Quedarán exentos de responsabilidad aquellos miembros que no hayan asistido por causa justificada a la reunión en que se adoptó el acuerdo o que hayan votado en contra del mismo.***

3. La exigencia de responsabilidades derivada de las infracciones tipificadas en esta ley se extenderá a los responsables incluso aunque haya desaparecido su relación o cesado en su actividad en o con la entidad respectiva.

Artículo 63. Infracciones.

1. Tendrán la consideración de **infracciones muy graves** las siguientes acciones u omisiones dolosas:

a) **Cualquier actuación que suponga una efectiva limitación de los derechos y garantías previstos en esta ley introducida a través de contratos o acuerdos a nivel individual o colectivo y en general cualquier intento o acción efectiva de obstaculizar la presentación de comunicaciones o de impedir, frustrar o ralentizar su seguimiento, incluida la aportación de información o documentación falsa por parte de los requeridos para ello.**

b) **La adopción de cualquier represalia derivada de la comunicación frente a los informantes o las demás personas incluidas en el ámbito de protección establecido en el artículo 3 de esta ley.**

c) **Vulnerar las garantías de confidencialidad y anonimato previstas en esta ley, y de forma particular cualquier acción u omisión tendente a revelar la identidad del informante cuando este haya optado por el anonimato, aunque no se llegue a producir la efectiva revelación de la misma.**

d) **Vulnerar el deber de mantener secreto sobre cualquier aspecto relacionado con la información.**

e) **La comisión de una infracción grave cuando el autor hubiera sido sancionado mediante resolución firme por dos infracciones graves o muy graves en los dos años anteriores a la comisión de la infracción, contados desde la firmeza de las sanciones.**

f) **Comunicar o revelar públicamente información a sabiendas de su falsedad.**

g) **Incumplimiento de la obligación de disponer de un Sistema interno de información en los términos exigidos en esta ley.**

2. Tendrán la consideración de **infracciones graves** las siguientes acciones u omisiones:

a) **Cualquier actuación que suponga limitación de los derechos y garantías previstos en esta ley o cualquier intento o acción efectiva de obstaculizar la presentación de informaciones o de impedir, frustrar o ralentizar su seguimiento que no tenga la consideración de infracción muy grave conforme al apartado 1.**

b) **Vulnerar las garantías de confidencialidad y anonimato previstas en esta ley cuando no tenga la consideración de infracción muy grave.**

c) **Vulnerar el deber de secreto en los supuestos en que no tenga la consideración de infracción muy grave.**

d) **Incumplimiento de la obligación de adoptar las medidas para garantizar la confidencialidad y secreto de las informaciones.**

e) **La comisión de una infracción leve cuando el autor hubiera sido sancionado por dos infracciones leves, graves o muy graves en los dos años anteriores a la comisión de la infracción, contados desde la firmeza de las sanciones.**

3. **Tendrán la consideración de infracciones leves las siguientes acciones u omisiones:**

a) **Remisión de información de forma incompleta, de manera deliberada por parte del Responsable del Sistema a la Autoridad, o fuera del plazo concedido para ello.**

b) **Incumplimiento de la obligación de colaboración con la investigación de informaciones.**

c) **Cualquier incumplimiento de las obligaciones previstas en esta ley que no esté tipificado como infracción muy grave o grave.**

Artículo 64. Prescripción de las infracciones.

1. **Las infracciones muy graves prescribirán a los tres años, las graves a los dos años y las leves a los seis meses.**

2. **El plazo de prescripción de las infracciones comenzará a contarse desde el día en que la infracción hubiera sido cometida. En las infracciones derivadas de una actividad continuada, la fecha inicial del cómputo será la de finalización de la actividad o la del último acto con el que la infracción se consume.**

3. **La prescripción se interrumpirá por la iniciación, con conocimiento del interesado, del procedimiento sancionador, reanudándose el plazo de prescripción si el expediente**

sancionador permaneciera paralizado durante tres meses por causa no imputable a aquellos contra quienes se dirija.

Artículo 65. Sanciones.

1. La comisión de infracciones previstas en esta ley llevará aparejada la imposición de las siguientes **multas**:

a) **Si son personas físicas** las responsables de las infracciones, serán multadas con una cuantía de **1.001 hasta 10.000 euros** por la comisión de infracciones leves; de **10.001 hasta 30.000 euros** por la comisión de infracciones graves y de **30.001 hasta 300.000 euros** por la comisión de infracciones muy graves.

b) **Si son personas jurídicas** serán multadas con una cuantía **hasta 100.000 euros** en caso de infracciones leves, entre **100.001 y 600.000 euros** en caso de infracciones graves y entre **600.001 y 1.000.000 de euros** en caso de infracciones muy graves.

2. **Adicionalmente, en el caso de infracciones muy graves, la Autoridad Independiente de Protección del Informante, A.A.I., podrá acordar:**

a) La amonestación pública.

b) La **prohibición de obtener subvenciones** u otros beneficios fiscales durante un plazo máximo de **cuatro años**.

c) La **prohibición de contratar con el sector público durante un plazo máximo de tres años** de conformidad con lo previsto en la 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.

3. Las sanciones por infracciones muy graves de cuantía igual o superior a 600.001 euros impuestas a entidades jurídicas podrán ser publicadas en el «Boletín Oficial del Estado», tras la firmeza de la resolución en vía administrativa. La publicación deberá contener, al menos, información sobre el tipo y naturaleza de la infracción y, en su caso, la identidad de las personas responsables de las mismas de acuerdo con la normativa en materia de protección de datos.

Artículo 66. Graduación.

1. Para la graduación de las infracciones se podrán tener en cuenta los **criterios siguientes**:

a) *La reincidencia, siempre que no hubiera sido tenido en cuenta en los supuestos del artículo 63.1.e) y 2.e).*

b) *La entidad y persistencia temporal del daño o perjuicio causado.*

c) *La intencionalidad y culpabilidad del autor.*

d) *El resultado económico del ejercicio anterior del infractor.*

e) *La circunstancia de haber procedido a la subsanación del incumplimiento que dio lugar a la infracción por propia iniciativa.*

f) *La reparación de los daños o perjuicios causados.*

g) *La colaboración con la Autoridad Independiente de Protección del Informante, A.A.I., u otras autoridades administrativas.*

2. *Las sanciones a imponer como consecuencia de la comisión de infracciones tipificadas en esta ley se graduarán teniendo en cuenta la naturaleza de la infracción y las circunstancias concurrentes en cada caso. De modo especial, y siempre que no se hubieran tenido en cuenta para la graduación de la infracción, la ponderación de las sanciones atenderá a los criterios del apartado anterior.*

Artículo 67. Concurrencia.

*El ejercicio de la potestad sancionadora previsto en este título es autónomo y **podrá concurrir con el régimen disciplinario del personal funcionario, estatutario o laboral que resulte de aplicación en cada caso.***

Artículo 68. Prescripción de las sanciones.

Las sanciones impuestas por infracciones muy graves prescribirán a los tres años, las impuestas por infracciones graves a los dos años y las impuestas por infracciones leves al año.

El plazo de prescripción de las sanciones comenzará a contarse desde el día siguiente a aquel en que sea ejecutable la resolución por la que se impone la sanción.

Interrumpirá la prescripción la iniciación, con conocimiento del interesado, del procedimiento de ejecución, volviendo a transcurrir el plazo si aquel está paralizado durante más de un mes por causa no imputable al infractor.

Nótese que el incumplimiento de las obligaciones expuestas en la presente comunicación lleva aparejadas cuantiosas sanciones, por lo que procede que los órganos de gobierno responsables de su cumplimiento en plazo adopten con celeridad las medidas necesarias para su puesta en marcha. A tales efectos, cuentan con el asesoramiento y colaboración de esta Agencia Valenciana Antifraude.

9. PLAZOS PARA ADAPTARSE A LA LEY

Disposición transitoria primera. Adaptación de los Sistemas y canales internos de información existentes.

Los sistemas internos de comunicación y sus correspondientes canales que, a la entrada en vigor de esta ley, tengan habilitados las entidades u organismos obligados podrán servir para dar cumplimiento a las previsiones de esta ley siempre y cuando se ajusten a los requisitos establecidos en la misma.

Disposición transitoria segunda. Plazo máximo para el establecimiento de Sistemas internos de información y adaptación de los ya existentes.

1. Las Administraciones, organismos, empresas y demás entidades obligadas a contar con un Sistema interno de información deberán implantarlo en el plazo máximo de tres meses a partir de la entrada en vigor de esta ley.

2. Como excepción, en el caso de las entidades jurídicas del sector privado con doscientos cuarenta y nueve trabajadores o menos, así como de los municipios de menos de diez mil habitantes, el plazo previsto en el párrafo anterior se extenderá hasta el 1 de diciembre de 2023.

3. Los canales y procedimientos de información externa se regirán por su normativa específica resultando de aplicación las disposiciones de esta ley en aquellos aspectos en los que no se adecúen a la Directiva (UE) 2019/1937 del Parlamento Europeo y del Consejo, de 23 de octubre de 2019. Dicha adaptación deberá producirse en el plazo de seis meses desde la entrada en vigor de esta ley.

En estos supuestos, el informante gozará de la protección establecida en esta ley siempre que la relación laboral o profesional en cuyo contexto se produzca la infracción, se rija por la ley española y, en su caso, adicionalmente de la protección establecida en la normativa específica.

En efecto, los órganos de gobierno de las entidades del sector público de la Comunitat Valenciana tenían hasta el día 13 de junio de 2023 para contar con su propio Sistema interno de información, lo que requiere celeridad en la toma de decisiones necesarias al efecto.

10. POSIBILIDAD DE SUSCRIBIR UN PROTOCOLO DE COLABORACIÓN CON LA AVAF Y DIRECCIONES DE CONTACTO PARA CONSULTAS Y APOYO EN NUESTRO ÁMBITO DE APLICACIÓN

Los canales de información arriba analizados resultan uno de los principales mecanismos de detección de prácticas contrarias a la integridad, posibilitando tanto la elaboración de banderas rojas (*red flags*) de cada entidad y la idoneidad de la autoevaluación de riesgos de fraude, corrupción y conflictos de interés, como la adopción de las medidas necesarias para minimizar que tales riesgos sean contingentes y el refuerzo de los controles atenuantes e internos. Ello contribuirá asimismo a dar cumplimiento a las obligaciones ya exigibles, en el ámbito autonómico, en el Título III de la Ley 1/2022, de 13 de abril, de la Generalitat, de Transparencia y Buen Gobierno de la Comunitat Valenciana, (DOGV de 22/04/2022): contar con códigos éticos y de conducta con un contenido mínimo legal y, de manera complementaria a su adopción, *“se fomentará la elaboración y aprobación de planes de prevención de riesgos para la integridad a partir del autodiagnóstico e identificación de los riesgos de mayor relevancia en la organización”*.

Para facilitar el cumplimiento de las obligaciones estatales y autonómicas referidas, las entidades incluidas en el ámbito de actuación de la AVAF tienen la posibilidad de suscribir un Protocolo de colaboración funcional con la Agencia, cuyo contenido puede resumirse en los siguientes aspectos:

- a) La colaboración en el fomento de las actividades de prevención del fraude y la corrupción y de integridad y ética pública para mejorar las funciones y fines respectivos que tienen encomendados.
- b) Con la finalidad de dar cumplimiento a las exigencias de la citada Ley 2/2023, de 20 de febrero, el reconocimiento como canal externo de denuncias del Buzón de la AVAF y su adhesión al mismo.
- c) En cumplimiento de los plazos fijados por la señalada Ley 2/2023 en su disposición transitoria segunda, la puesta en marcha por la entidad correspondiente de su canal de

denuncias interno, debiendo remitir a la AVAF el nombramiento del Responsable del Sistema interno de información, para lo cual, como ya se ha mencionado, la Resolución número 504, de 10 de mayo de 2023, del director de la AVAF (DOGV núm. 9601 de 23.05.2023), creó el Registro de responsables de sistemas internos de información de la Agencia de Prevención y Lucha contra el Fraude y la Corrupción de la Comunitat Valenciana (RRSII), regulándose su funcionamiento.

d) El auxilio de autoridades y personal de la entidad, con celeridad y diligencia, a la AVAF en el ejercicio de las funciones que a esta le corresponden.

e) Por parte de la AVAF, en materia de prevención de la corrupción y fraude y de fomento de la integridad y ética pública, la colaboración se llevará a cabo facilitando las siguientes actuaciones:

- El fomento de la implementación de un Plan de Integridad, facilitando una propuesta de contenido mínimo del Plan y algunos modelos como anexos al Plan, así mismo se asesorará para que el Ayuntamiento elabore su autodiagnóstico previo de riesgos contrarios a la integridad pública.
- La puesta a disposición del Ayuntamiento de mecanismos de prevención de los riesgos contrarios a la integridad pública contenidos en las Recomendaciones generales de la AVAF y/o en otros de los materiales elaborados por la AVAF.
- La elaboración por la AVAF de catálogos genéricos de riesgos (comunes y sectoriales) contrarios a la integridad pública en los procesos de toma de decisiones y puesta a disposición de los mismos para su adaptación por parte del Ayuntamiento.
- La colaboración de la AVAF en las acciones de formación de la necesidad y contenido mínimo del Plan de Integridad.
- El asesoramiento en la elaboración de códigos éticos como marco de integridad pública.

f) Además de la colaboración en materia de prevención, la AVAF y el Ayuntamiento podrán realizar actividades formativas, internas y externas, o cualesquiera otras que permiten conseguir objetivos de interés común.

Respecto al alcance de la colaboración a desarrollar, se indican a continuación las unidades administrativas de la Agencia a las que podrá dirigirse concretamente para resolver cualquier duda o requerir información adicional:

a) Al Servicio de Prevención, sobre planes, mapas de riesgos y fomento de la ética e integridad pública **prevencion@antifraucv.es**

b) Al Servicio de Formación, en relación con cualquier actividad de esta índole **formacion@antifraucv.es**

c) Al Servicio de Sistemas de Información, sobre la tecnología de canales o buzones de denuncias internos y externo **servicio.tic@antifraucv.es**

d) A la Dirección de Análisis e Investigación, en cuanto a gestión de los canales o buzones y actuaciones de investigación de denuncias **investigacion@antifraucv.es**

e) A la Dirección de Asuntos Jurídicos, respecto de la protección de personas que denuncian o alertan de actuaciones contrarias a la ley y al interés general **juridico@antifraucv.es**

Para formalizar el Protocolo, deberán solicitarlo a la Dirección de Asuntos Jurídicos, a efectos de recibir la propuesta de texto del mismo, completarlo y remitirlo, con carácter previo a su aprobación por la entidad correspondiente, a juridico@antifraucv.es para su revisión final. En este sentido, como se ha adelantado, la AVAF ha publicado en su página web <https://www.antifraucv.es> un compendio con 36 preguntas y respuestas sobre la Ley 2/2023, incluyendo en la cuestión correspondiente un enlace al modelo de protocolo.

En cualquier caso, también pueden ponerse en contacto con nosotros llamando a centralita 96 278 74 50, solicitando que le pasen con la unidad correspondiente.

ANEXO I: MARCO NORMATIVO

[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.](#)

[Ley 11/2016, de 28 de noviembre, de la Agencia de Prevención y Lucha contra el Fraude y la Corrupción de la Comunitat Valenciana.](#)

[Reglamento de funcionamiento y régimen interior de la Agencia](#)

[Modificación del Reglamento de funcionamiento y régimen interior](#)

[Resolución por la que se crea el Buzón de Denuncias de la Agencia y se regula su funcionamiento](#)

[Resolución por la que se crea el Registro de Responsables de Sistemas Internos de Información y se regula su funcionamiento](#)

ANEXO II: DOCUMENTOS DE CONSULTA

[Decálogo para la protección de las personas denunciantes y alertadoras, aprobado por el Consejo de Participación de la AVAF](#)

[36 preguntas y respuestas sobre la Ley 2/2023 en la web de la AVAF](#)

[Código de Integridad de la Comunitat Valenciana, elaborado por la AVAF](#)

RECOMENDACIONES, GUÍAS Y MANUALES AVAF:

- [Recomendación general. La ejecución de los contratos en clave de integridad pública.](#)
- [FAQ: Preguntas más frecuentes sobre Planes de Medidas Antifraude – Actualización abril 2023](#)
- [Checklist: implantación de la administración electrónica en una entidad local.](#)
- [Reflexiones sobre conflictos de interés: su desconocimiento la antesala de la corrupción.](#)
- [La planificación: herramienta clave para prevenir los riesgos de corrupción en las organizaciones.](#)
- [La vía del enriquecimiento injusto en el sector público: ¿uso o abuso?](#)
- [Reflexiones en el estado de alarma declarado ante la pandemia del COVID-19.](#)
- [Manual AVAF – El ejercicio del cargo público con integridad: Antes, durante y después del proceso electoral.](#)
- [Guía AVAF: El Plan de Integridad Pública: Hoja de Ruta y Anexos Facilitadores.](#)
- [Manual didáctico visual: Los conflictos de interés en clave de integridad.](#)

CATÁLOGOS DE RIESGOS Y FICHAS DE SISTEMATIZACIÓN:

- [Riesgos contrarios a la integridad pública en el sector público instrumental valenciano.](#)
- [Catálogos de riesgos comunes en los procesos de toma de decisiones y](#)

algunos mecanismos de prevención.

- Fichas de Sistematización: Control Interno.
- Fichas de Sistematización: Gestión de Riesgos.
- Fichas de Sistematización: Control Externo.
- Fichas de Sistematización: Marcos de Integridad.