POLÍTICA DE DENUNCIA DE IRREGULARIDADES

SSP

Rev. Mayo23

CONTENIDO

PREÁMBULO

Esta **política de denuncia de irregularidades**, denominada en SSP en inglés *"Speak Up",* ha sido emitida por el Grupo SSP, y traducida en cada país donde tiene presencia.
Se trata de una actualización de la hasta ahora denominada *"Whistleblowing Policy".*
Esta política se denomina en inglés "Whistleblowing Policy", ha sido emitida por el Grupo SSP, y traducida en cada país donde tiene presencia.

Tiene su fundamento legal 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, impone a los Estados Miembros el establecimiento, en el seno de las empresas (y de las administraciones públicas), de canales de denuncia efectivos, confidenciales y seguros, así como la adopción de medidas de protección de los denunciantes que utilicen esos canales internos, frente a posibles represalias de su empresa o de sus superiores.

En el BOE de 2 de febrero de2023 publico la ley 2/2023 de 20 de febrero de reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción", para transponer la citada Directiva.

Este término inglés, *whistleblowing* -que podríamos traducir como "toque de silbato"- se utiliza para nombrar a aquellos mecanismos y servicios que las empresas ponen a disposición de sus empleados (canales de denuncia, buzones de sugerencias...) para que puedan informar de una manera anónima, segura y sin el temor de posibles represalias de aquellas conductas o inacciones que pueden ser constitutivas de quebrantamiento de normas internas o políticas de la empresa.

Con las políticas de *whistleblowing* el personal tiene siempre abierto un canal para hacer llegar sus preocupaciones a las personas adecuadas dentro de la empresa, antes de que el problema se haga innecesariamente grande o desemboque en una denuncia ante un órgano jurisdiccional, y la empresa tiene la obligación de investigarlas desde que tenga conocimiento de ellas.

En el contexto de las prácticas de anticorrupción, el término inglés *whistleblower* se emplea para aludir a quienes, por su relación con una empresa —empleados, consultores…—, tienen conocimiento de irregularidades, infracciones o prácticas ilegales, y deciden denunciarlas, y se traduce como informante, que es de hecho el término empleado por el Parlamento Europeo.

1. DECLARACIÓN DE LA POLÍTICA

1.1 En SSP Group PLC, sus filiales y las Joint Ventures en las que participa (en adelante el "Grupo" o "SSP") nos comprometemos a llevar a cabo nuestro negocio con honestidad e integridad, y el Grupo espera que todo el personal mantenga los más altos estándares al respecto. Es esencial una cultura de transparencia y rendición de cuentas para evitar que se cometan actos ilícitos y para abordarlos cuando se produzcan.

2. PROPÓSITO

2.1 Los objetivos de esta política son:

2.1.1 **Alentar al personal a informar de las sospechas de irregularidades** que puedan tener, tan pronto como sea posible, sabiendo que sus denuncias serán tomadas en serio e investigadas según corresponda, y respetándose su confidencialidad;

2.1.2 Proporcionar al personal la **orientación necesaria sobre cómo denunciar esas sospechas**;

2.1.3 Que el personal pueda sentirse tranquilo al plantear una denuncia basada en una sospecha, **sin temor a represalias, incluso si se equivoca**.

2.2 Esta política responde a la **Directiva 2019/1937**, de Protección de los denunciantes de irregularidades y, en España, a la **Ley 2/2023**, de 20 de febrero, reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción, cuya finalidad es otorgar una protección adecuada frente a las represalias que puedan sufrir las personas físicas que informen sobre alguna de las acciones u omisiones a que se refiere el artículo 2, a través de los procedimientos previstos en la misma, así como 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. Como anexo a esta política se adjunta un resumen de la mencionada ley.
Además, esta política tiene en cuenta el *"WHISTLEBLOWING ARRANGEMENTS CODE OF PRACTICE",* Código de Práctica emitido por el *British Standards Institute and Public Concern at Work*.

2.3 Esta política no forma parte del contrato de trabajo de ningún empleado y puede ser modificada por el Grupo en cualquier momento.

2.4 Esta política debe leerse junto con otras políticas del Grupo, incluyendo el Código de Conducta y las Políticas de Autorización del Grupo (GAP).

3. ¿QUIÉN ESTÁ AMPARADO POR ESTA POLÍTICA?

3.1 Esta política se aplica a todas las personas que trabajan en el Grupo, con independencia del nivel, incluidos altos directivos, directores, empleados indefinidos y temporales, a tiempo completo o parcial, personal de ETT, consultores, contratistas, trabajadores a domicilio … (en adelante "plantilla" o "personal "), y en todas las divisiones y empresas del Grupo, y sus subsidiarias, y en todas las Joint Ventures, y sus subsidiarias, en que SSP sea mayoritaria.

3.2 Dependiendo de las circunstancias, esta política también puede aplicarse a Joint Ventures en las que una Compañía del Grupo tenga una participación minoritaria. Esto será determinado por el Grupo SSP, de acuerdo con el Oficial de Denuncia de País. Si no estás seguro de si una Joint Venture en concreto está sujeta a esta política, consulta a tu Gerente, Director de Recursos Humanos u Oficial de Denuncias.

4. ¿QUÉ ES LA DENUNCIA DE IRREGULARIDADES, (*SPEAK UP O WHISTLEBLOWING*)?

4.1 La denuncia de irregularidades, la divulgación de información que se relaciona con sospechas de irregularidades en el trabajo, que puede incluir: actividad criminal; injusticias; peligros para la seguridad y la salud; daños al medio ambiente; incumplimiento de cualquier obligación legal; soborno; negligencia; incumplimiento de nuestras políticas y procedimientos internos; o la ocultación deliberada de cualquiera de estos asuntos.

4.2 Debes plantear tus preocupaciones en el marco de esta política si tienes la creencia genuina de que una infracción o negligencia real o presunta puede haber afectado, está afectando, o afectará a cualquiera de las actividades de SSP.

4.3 Sin embargo, no debe usarse esta política para aquellas quejas relacionadas con tus circunstancias personales, como por ejemplo la forma en que has sido tratado en el trabajo, o para denuncias por acoso o "bullyng". En esos casos, debe utilizarse el Procedimiento de quejas.

4.4 Si no estás seguro de si algo está dentro del alcance de esta política, debes pedir consejo al Oficial de Denuncias de su país.

5. COMO PLANTEAR UNA DENUNCIA INTERNA

5.1 Esperamos que, en la mayoría de los casos, puedas plantear cualquier inquietud al departamento de Recursos Humanos. Puedes hablarlo en persona con ellos, o presentar el asunto por escrito si lo prefieres, mediante un email a la dirección de correo fernando.cabrera@ssp.es Es posible que ellos puedan encontrar una forma rápida y efectiva de resolver tu problema. En algunos casos, remitirán el asunto a Oficial de Denuncia de irregularidades del país.

5.2 Sin embargo, cuando el asunto es más grave, o sientas que tu superior jerárquico o el departamento de Recursos Humanos no han abordado su problema, o prefieres no plantearlo con ellos por alguna razón, debes contactar con:

5.2.1 El Oficial de Denuncia del País (en nuestro caso, Blanca Ripoll, blanca.ripoll@ssp.es o

5.2.2 La línea telefónica de ayuda confidencial del Grupo SSP (donde las inquietudes pueden ser informadas anónimamente si es necesario). Los números de teléfono de cada país se especifican al final de esta política, y el de España es el:

900 999 456

6. CONFIDENCIALIDAD

6.1 Esperamos que el personal se sienta capaz de expresar abiertamente sus preocupaciones bajo esta política. Sin embargo, si deseas plantear tu preocupación de manera confidencial, el Grupo hará todo lo posible por mantener tu identidad en secreto. Si es necesario que alguna de las personas que investigue tu inquietud conozca tu identidad, el Grupo lo acordará antes contigo. **Ningún miembro del personal será penalizado o sufrirá consecuencias adversas por expresar sus sospechas de irregularidades bajo esta política**, a menos que sean acusaciones falsas (según el párrafo 8 de esta política).

6.2 No alentamos a los miembros de la plantilla a que hagan denuncias anónimas. Una investigación adecuada puede ser más difícil, o imposible, si el Grupo no puede obtener más información de ti. Si te preocupan las posibles represalias en caso de que se revele tu identidad, debes hablar con el responsable de "*Speak Up*" de tu país o con uno de los otros puntos de contacto enumerados en el apartado 5, y entonces se podrán tomar las medidas adecuadas para preservar la confidencialidad. Si tienes alguna duda, puedes pedir consejo a nuestra línea de ayuda del Grupo SSP.

7. DENUNCIAS EXTERNAS

7.1 El objetivo de esta política es proporcionar un mecanismo interno para informar, investigar y remediar cualquier comportamiento deshonesto en el lugar de trabajo.

7.2 La ley reconoce que, en algunas circunstancias, puede ser apropiado que informes de tus inquietudes a un organismo externo. Rara vez será apropiado alertar a los medios. Te recomendamos encarecidamente que busque asesoramiento antes de informar una inquietud a alguien externo al Grupo.

Las preocupaciones de *Speak Up* suelen estar relacionadas con la conducta de nuestros compañeros de empresa, pero a veces pueden estar relacionadas con las acciones de un tercero, como un cliente, proveedor o prestador de servicios. La ley le permite plantear una inquietud a un tercero, cuando crea razonablemente que está relacionada principalmente con sus acciones o con algo que es legalmente su responsabilidad. Sin embargo, el Grupo te anima a que comuniques primero esas preocupaciones internamente. Deberás ponerte en contacto con tu superior jerárquico o con el departamento de Recursos Humanos o con alguna de las personas indicadas en el apartado 5 para que te orienten.

En España es posible denunciar de forma externa 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.

8. INVESTIGACIÓN Y RESULTADO

8.1 Una vez tengamos conocimiento de tu denuncia organizaremos una reunión contigo lo antes posible, para analizar tu inquietud. Podrás traer a un/a compañero/a o representante sindical a cualquier reunión celebrada bajo esta política. Tu acompañante deberá respetar la confidencialidad de la reunión, y de cualquier investigación posterior.

8.2 Tras esa reunión, el Grupo llevará a cabo una evaluación inicial para determinar el alcance de cualquier investigación. Te informaremos del resultado de nuestra evaluación. Es posible que debas asistir a reuniones adicionales para proporcionar más información.

8.3 En algunos casos el Grupo puede designar un investigador/a, o equipo de investigadores, que puede incluir algún miembro de la plantilla con experiencia en investigaciones o con conocimiento especializado del tema a investigar. El/los investigador/es puede/n hacer recomendaciones de cambio que nos permitan minimizar el riesgo de errores futuros.

8.4 Nuestro objetivo es mantenerte informado del progreso de investigación y de los tiempos de la misma. Sin embargo, la necesidad de confidencialidad supondrá que, a veces, no te proporcionemos detalles específicos de la investigación, o de cualquier acción disciplinaria que se tomase como resultado de la misma. Debes tratar cualquier información sobre la investigación como confidencial.

8.5 Si el Grupo concluye que un denunciante ha hecho deliberadamente denuncias falsas, el denunciante podrá ser objeto de medidas disciplinarias.

9. SI NO QUEDAS SATISFECHO/A

9.1 Aunque el Grupo no siempre puede garantizar el resultado que buscas, intentaremos tratar tu preocupación de manera justa y adecuada. Utilizando esta política puedes ayudarnos a conseguirlo.

9.2 Si no estás satisfecho/a con la forma en que se ha gestionado tu preocupación, puedes plantearla con uno de los otros contactos clave enumerados en el párrafo 5.

10. PROTECCIÓN Y APOYO A LOS DENUNCIANTES

10.1 Es comprensible que los denunciantes puedan preocuparse por las posibles repercusiones de su denuncia. Nuestro objetivo es alentar la transparencia y apoyaremos al personal que plantea preocupaciones sinceras y legítimas bajo esta política, incluso si se equivocan.

10.2 El personal no debe sufrir ningún perjuicio como consecuencia de elevar una denuncia, como despido, medidas disciplinarias, amenazas u otro tratamiento desfavorable relacionado con el hecho de haber denunciado. Si crees que has sufrido algún tratamiento de este tipo, debes informar de inmediato al Oficial de Denuncia de Irregularidades de tu país. De no remediarse la situación, debes plantearlo formalmente usando nuestro Procedimiento de Quejas.

10.3 El personal no debe amenazar ni tomar ningún tipo de represalia contra los denunciantes. Cualquier persona involucrada en dichas conductas estará sujeta a medidas disciplinarias.

11. RESPONSABILIDAD DEL EXITO DE ESTA POLÍTICA

11.1 El Consejo de Dirección de cada país tiene la responsabilidad general sobre esta política, y la de revisar la efectividad de las acciones tomadas en respuesta a las denuncias planteadas bajo la misma.

Cada país tiene un Oficial de Denuncias, su Director General. En el caso de España es Blanca Ripoll, blanca.ripoll@ssp.es Puede solicitar la lista de Oficiales de Denuncia de Irregularidades por país enviando un mail a Global.HR@ssp.uk.com.

11.2 El Oficial de Denuncia de Irregularidades de tu país tiene la responsabilidad final de (i) garantizar que sus distintas áreas de negocio establezcan sistemas y controles para cumplir con esta política y (ii) supervisarla periódicamente. Esto incluye:

- Responsabilidad operacional diaria sobre esta política;
- Implementar mecanismos de comunicación para garantizar que esta política se incorpore y comprenda en toda la organización;
- Garantizar niveles adecuados de personal para cumplir con los requisitos de esta política;
- Garantizar que todos/as los empleados/as relevantes reciban la capacitación adecuada;
- Garantizar la efectividad de los controles que implementan esta política;
- Garantizar una presentación de informes fluida y rápida según esta política.

11.3 La persona designada con la responsabilidad general de esta Política es Jonathan Davies, Director Financiero de SSP Group plc, que discutirá los resultados de la actividad de supervisión y revisión con el Comité de Riesgos de SSP. Este Comité informará periódicamente al Comité de Auditoría del Grupo y al Consejo de Administración. de SSP Group plc. Las personas relevantes que están obligadas a cumplir con esta política serán notificadas de cualquier cambio en la misma.

11.4 SSP mantendrá un registro de todos los informes realizados bajo esta política para incluir detalles de la investigación y el resultado de esas investigaciones. Estos registros se conservarán durante al menos cinco años a partir de la fecha de registro.

11.5 Todo el personal es responsable del éxito de esta política y debe asegurarse de que la usen para divulgar cualquier sospecha de irregularidad. Las consultas sobre la política deben dirigirse al Oficial de Denuncia de Irregularidades de tu país.

12.- CONTROL Y REVISIÓN

12.1 SSP revisará periódicamente la implementación de esta política con respecto a su idoneidad, adecuación y efectividad, y se compromete a realizar mejoras, según corresponda.

Solo para uso interno

Version 1	Agosto 2018	
Version 2	Julio 2022	Pequeños cambios “whistleblowing” a “speak-up”
Version 3	Mayo 2023	Cambios menores adaptación Ley 2/2023, de 20 de febrero

Puedes informar de un incidente llamando al número que proceda del listado de más abajo o hacerlo on-line en

www.sspgroup.ethicspoint.com

Por favor, ten en cuenta que en **Finlandia** y **Catar,** por el momento, solo pueden hacerlo on-line

País:	Número de teléfono:	País:	Número de teléfono::
Austria	0800 068792	Hong Kong	800 906 570
Bélgica	0800 75 973	Hungría	(80) 088 414
Brasil	08005917317	Israel	1-809-399-883
Canadá	(833) 646-0064	Luxemburgo	800 24 602
China	400 120 0201	Países bajos	0800 3510049
Chipre	80 077008	España	900 999 456
Egipto	0800 006 0184	Suecia	020- 12 70 17
Estonia	8000 100 861	Suiza	0800 223 029
Francia	0 800 99 07 62	Taiwán	00801-49-1615
Alemania	0800 1817635	Tailandia	1800014586
Grecia	800 848 1585	Estados Unidos	(833) 646-0064

Los países de más abajo necesitan marcar dos veces. Sigue los pasos a continuación para informar de un incidente:

1. Marca el número de tu país.
2. Cuando se solicite, marcar el número 833 646 0064.
3. Serás transferido con un especialista en comunicación que gestionará tu información.

País:	Número de teléfono:	Introducir número:
Australia	1-800-551-155 (Optus) or 1-800-881-011 (Telstra)	(833) 646-0064
Baréin	800-00-001 or 800-000-05 (Cellular)	(833) 646-0064
Dinamarca	800-100-10	(833) 646-0064
India	000-117	(833) 646-0064
Irlanda	00-800-222-55288 (UIFN) or 1-800-550-000	(833) 646-0064
Malasia	1-800-80-0011	(833) 646-0064
Noruega	800-190-11	(833) 646-0064
Filipinas	1010-5511-00 (PLDT) or 105-11 (Globe, Philcom, Digitel, Smart)	(833) 646-0064
Singapur	800-001-0001 (StarHub) or 800-011-1111 (Singtel)	(833) 646-0064
Emiratos Árabes Unidos	8000-021 or 8000-555-66 (du) or 8000-061 (cellular)	(833) 646-0064
Reino Unido	0-800-89-0011	(833) 646-0064

Anexo: Resumen de 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.

Puede accederse al texto completo de la Ley en el siguiente link:

https://www.boe.es/eli/es/l/2023/02/20/2/con

TÍTULO I

Finalidad de la ley y ámbito de aplicación

Artículo 1. Finalidad de la ley.

1. La presente ley tiene por finalidad otorgar una protección adecuada frente a las represalias que puedan sufrir las personas físicas que informen sobre alguna de las acciones u omisiones a que se refiere el artículo 2, a través de los procedimientos previstos en la misma.

2. También tiene como finalidad 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.

Artículo 2. Ámbito material de aplicación.

1. La presente ley protege a las personas físicas que informen, a través de alguno de los procedimientos previstos en ella de:

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 contempla 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.

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

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

4. La protección prevista en esta ley no será de aplicación a las informaciones que afecten a la información clasificada. Tampoco afectará a las obligaciones que resultan de la protección del secreto profesional de los profesionales de la medicina y de la abogacía, del deber de confidencialidad de las Fuerzas y Cuerpos de Seguridad en el ámbito de sus actuaciones, así como del secreto de las deliberaciones judiciales.

5. No se aplicarán las previsiones de esta ley a las informaciones relativas a infracciones en la tramitación de procedimientos de contratación que contengan información clasificada o que hayan sido declarados secretos o reservados, o aquellos cuya ejecución deba ir acompañada de medidas de seguridad especiales conforme a la legislación vigente, o en los que lo exija la protección de intereses esenciales para la seguridad del Estado.

6. En el supuesto de información o revelación pública de alguna de las infracciones a las que se refiere la parte II del anexo de la Directiva (UE) 2019/1937 del Parlamento Europeo y del Consejo, de 23 de octubre de 2019, resultará de aplicación la normativa específica sobre comunicación de infracciones en dichas materias.

Artículo 3. Ámbito personal de aplicación.

1. La presente ley se aplicará a los 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 empleados públicos o trabajadores por cuenta ajena;

b) los autónomos;

c) los accionistas, partícipes y personas pertenecientes al órgano de administración, dirección o supervisión de una empresa, incluidos los miembros no ejecutivos;

d) cualquier persona que trabaje para o bajo la supervisión y la dirección de contratistas, subcontratistas y proveedores.

2. La presente ley también se aplicará a los informantes que comuniquen o revelen públicamente información sobre infracciones obtenida en el marco de una relación laboral o

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

3. Las medidas de protección del informante previstas en el título VII también se aplicarán, en su caso, específicamente a los representantes legales de las personas trabajadoras en el ejercicio de sus funciones de asesoramiento y apoyo al informante.

4. Las medidas de protección del informante previstas en el título VII también se aplicarán, en su caso, a:

a) personas físicas que, en el marco de la organización en la que preste servicios el informante, asistan al mismo en el proceso,

b) personas físicas que estén relacionadas con el informante y que puedan sufrir represalias, como compañeros de trabajo o familiares del informante, y

c) personas jurídicas, para las que trabaje o con las que mantenga cualquier otro tipo de relación en un contexto laboral o en las que ostente una participación significativa. A estos efectos, se entiende que la participación en el capital o en los derechos de voto correspondientes a acciones o participaciones es significativa cuando, por su proporción, permite a la persona que la posea tener capacidad de influencia en la persona jurídica participada.

TÍTULO II

Sistema interno de información

CAPÍTULO I

Disposiciones generales

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.

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 Sistemas 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.

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 regirá 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 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 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.

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.

CAPÍTULO II

Sistema interno de información en el sector privado

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.

Artículo 11. Grupos de sociedades.

1. En el caso de un grupo de empresas conforme al artículo 42 del Código de Comercio, la sociedad dominante aprobará una política general relativa al Sistema interno de información a que se refiere el artículo 5 y a la defensa del informante, y asegurará la aplicación de sus principios en todas las entidades que lo integran, sin perjuicio de la autonomía e independencia de cada sociedad, subgrupo o conjunto de sociedades integrantes que, en su caso, pueda establecer el respectivo sistema de gobierno corporativo o de gobernanza del grupo, y de las modificaciones o adaptaciones que resulten necesarias para el cumplimiento de la normativa aplicable en cada caso.

2. El Responsable del Sistema podrá ser uno para todo el grupo, o bien uno para cada sociedad integrante del mismo, subgrupo o conjunto de sociedades, en los términos que se establezcan por la citada política. Por su parte, el Sistema interno de información podrá ser uno para todo el grupo.

3. Será admisible el intercambio de información entre los diferentes Responsables del Sistema del grupo, si los hubiera, para la adecuada coordinación y el mejor desempeño de sus funciones.

Artículo 12. Medios compartidos en el sector privado.

Las personas jurídicas en el sector privado que tengan entre cincuenta y doscientos cuarenta y nueve trabajadores y que así lo decidan, podrán compartir entre sí el Sistema interno de información y los recursos destinados a la gestión y tramitación de las comunicaciones, tanto si la gestión se lleva a cabo por cualquiera de ellas como si se ha externalizado, respetándose en todo caso las garantías previstas en esta ley.

CAPÍTULO III

Sistema interno de información en el sector público

(Se omite en este resumen)

TÍTULO III

Canal externo de información de la Autoridad Independiente de Protección del Informante, A.A.I.

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.

Artículo 17. Recepción de informaciones.

1. La información puede llevarse a cabo de forma anónima. En otro caso, se reservará la identidad del informante en los términos del artículo 33, debiendo adoptarse las medidas en él previstas.

2. La información se podrá realizar por escrito, a través de correo postal o a través de cualquier medio electrónico habilitado al efecto dirigido al canal externo de informaciones de la Autoridad Independiente de Protección del Informante, A.A.I., 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 los casos de comunicación verbal se advertirá al informante de que la comunicación será grabada y se le informará del tratamiento de sus datos de acuerdo con lo que establecen el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, y la Ley Orgánica 3/2018, de 5 de diciembre.

Al presentar la información, el informante podrá indicar 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 la Autoridad Independiente de Protección del Informante, A.A.I. como consecuencia de la información.

En caso de comunicación verbal, incluidas las realizadas a través de reunión presencial, telefónicamente o mediante sistema de mensajería de voz, la Autoridad Independiente de Protección del Informante, A.A.I. deberá documentarla de alguna de las maneras siguientes:

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 del mensaje.

3. Presentada la información, se procederá a su registro en el Sistema de Gestión de Información, siéndole asignado un código de identificación. El Sistema de Gestión de Información estará contenido en una base de datos segura y de acceso restringido exclusivamente al personal de la Autoridad Independiente de Protección del Informante, A.A.I. convenientemente autorizado, en la que se registrarán todas las comunicaciones recibidas, cumplimentando los siguientes datos:

a) Fecha de recepción.

b) Código de identificación.

c) Actuaciones desarrolladas.

d) Medidas adoptadas.

e) Fecha de cierre.

4. Recibida la información, en un plazo no superior a cinco días hábiles desde dicha recepción se procederá a acusar recibo de la misma, a menos que el informante expresamente haya renunciado a recibir comunicaciones relativas a la investigación o que la Autoridad

Independiente de Protección del Informante, A.A.I. considere razonablemente que el acuse de recibo de la información comprometería la protección de la identidad del informante.

Artículo 18. Trámite de admisión.

1. Registrada la información, la Autoridad Independiente de Protección del Informante, A.A.I., deberá comprobar si aquella expone hechos o conductas que se encuentran dentro del ámbito de aplicación recogido en el artículo 2.

2. Realizado este análisis preliminar, la Autoridad Independiente de Protección del Informante, A.A.I., decidirá, en un plazo que no podrá ser superior a diez días hábiles desde la fecha de entrada en el registro de la información:

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

1.º Cuando los hechos relatados carezcan de toda verosimilitud.

2.º Cuando los hechos relatados no sean constitutivos de infracción del ordenamiento jurídico incluida en el ámbito de aplicación de esta ley.

3.º Cuando la comunicación carezca manifiestamente de fundamento o existan, a juicio de la Autoridad Independiente de Protección del Informante, A.A.I., 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 Autoridad Independiente de Protección del Informante, A.A.I., notificará la resolución de manera motivada.

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

b) Admitir a trámite la comunicación.

La admisión a trámite se comunicará al informante dentro de los cinco días hábiles siguientes, salvo que la comunicación fuera anónima o el informante hubiera renunciado a recibir comunicaciones de la Autoridad Independiente de Protección del Informante, A.A.I.

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.

Artículo 19. Instrucción.

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

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

En ningún caso se comunicará a los sujetos afectados la identidad del informante ni se dará acceso a la comunicación. Durante la instrucción se dará noticia de la comunicación con sucinta relación de hechos al investigado. Esta información 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.

3. Sin perjuicio del derecho a formular alegaciones por escrito, la instrucción comprenderá, siempre que sea posible, una entrevista con la persona afectada en la que, siempre con absoluto respeto a la presunción de inocencia, se le invitará a exponer su versión de los hechos y a aportar aquellos medios de prueba que considere adecuados y pertinentes.

A fin de garantizar el derecho de defensa de la persona afectada, la misma tendrá acceso al expediente sin revelar información que pudiera identificar a la persona informante, pudiendo ser oída en cualquier momento, y se le advertirá de la posibilidad de comparecer asistida de abogado.

4. Los funcionarios de la Autoridad Independiente de Protección del Informante, A.A.I. que desarrollen actividades de investigación tendrán la consideración de agentes de la autoridad en el ejercicio de sus funciones y estarán obligados a guardar secreto sobre las informaciones que conozcan con ocasión de dicho ejercicio.

5. Todas las personas naturales o jurídicas, privadas o públicas, deberán colaborar con las autoridades competentes y estarán obligadas a atender los requerimientos que se les dirijan para aportar documentación, datos o cualquier información relacionada con los procedimientos que se estén tramitando, incluso los datos personales que le fueran requeridos.

Artículo 20. Terminación de las actuaciones.

1. Concluidas todas las actuaciones, la Autoridad Independiente de Protección del Informante, A.A.I. emitirá un informe que contendrá al menos:

a) Una exposición de los hechos relatados junto con el código de identificación de la comunicación y la fecha de registro.

b) La clasificación de la comunicación a efectos de conocer su prioridad o no en su tramitación.

c) Las actuaciones realizadas con el fin de comprobar la verosimilitud de los hechos.

d) Las conclusiones alcanzadas en la instrucción y la valoración de las diligencias y de los indicios que las sustentan.

2. Emitido el informe, la Autoridad Independiente de Protección del Informante, A.A.I., adoptará alguna de las siguientes decisiones:

a) Archivo del expediente, que será notificado al informante y, en su caso, a la persona afectada. En estos supuestos, el informante tendrá derecho a la protección prevista en esta ley, salvo que, como consecuencia de las actuaciones llevadas a cabo en fase de instrucción, se concluyera que la información a la vista de la información recabada, debía haber sido inadmitida por concurrir alguna de las causas previstas en el artículo 18.2.a).

b) Remisión al Ministerio Fiscal si, pese a no apreciar inicialmente indicios de que los hechos pudieran revestir el carácter de delito, así resultase del curso de la instrucción. Si el delito afectase a los intereses financieros de la Unión Europea, se remitirá a la Fiscalía Europea.

c) Traslado de todo lo actuado a la autoridad competente, de conformidad con lo dispuesto en el artículo 18.2.d).

d) Adopción de acuerdo de inicio de un procedimiento sancionador en los términos previstos en el título IX.

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

4. Las decisiones adoptadas por la Autoridad Independiente de Protección del Informante, A.A.I., en las presentes actuaciones no serán recurribles en vía administrativa ni en vía contencioso administrativa, sin perjuicio del recurso administrativo o contencioso administrativo que pudiera interponerse frente a la eventual resolución que ponga fin al procedimiento sancionador que pudiera incoarse con ocasión de los hechos relatados.

5. La presentación de una comunicación por el informante no le confiere, por si sola, la condición de interesado.

Artículo 21. Derechos y garantías del informante ante la Autoridad Independiente de Protección del Informante, A.A.I.

El informante tendrá las siguientes garantías en sus actuaciones ante la Autoridad Independiente de Protección del Informante, A.A.I.:

1.º Decidir si desea formular la comunicación de forma anónima o no anónima; en este segundo caso se garantizará la reserva de identidad del informante, de modo que esta no sea revelada a terceras personas.

2.º Formular la comunicación verbalmente o por escrito.

3.º Indicar un domicilio, correo electrónico o lugar seguro donde recibir las comunicaciones que realice la Autoridad Independiente de Protección del Informante, A.A.I. a propósito de la investigación.

4.º Renunciar, en su caso, a recibir comunicaciones de la Autoridad Independiente de Protección del Informante, A.A.I.

5.º Comparecer ante la Autoridad Independiente de Protección del Informante, A.A.I., por propia iniciativa o cuando sea requerido por esta, siendo asistido, en su caso y si lo considera oportuno, por abogado.

6.º Solicitar a la Autoridad Independiente de Protección del Informante, A.A.I. que la comparecencia ante la misma sea realizada por videoconferencia u otros medios telemáticos seguros que garanticen la identidad del informante, y la seguridad y fidelidad de la comunicación.

7.º Ejercer los derechos que le confiere la legislación de protección de datos de carácter personal.

8.º Conocer el estado de la tramitación de su denuncia y los resultados de la investigación.

Artículo 22. Publicación y revisión del procedimiento de gestión de informaciones.

La Autoridad Independiente de Protección del Informante, A.A.I. deberá publicar su procedimiento de gestión de informaciones.

Cada tres años revisará y, en su caso, modificará dicho procedimiento teniendo en cuenta su experiencia y la de otras autoridades competentes. La modificación será asimismo objeto de publicación.

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.

TÍTULO IV

Publicidad de la información y Registro de informaciones

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.

De igual modo, las autoridades competentes a las que se refiere el artículo 24 publicarán, en una sección separada, fácilmente identificable y accesible de su sede electrónica, como mínimo, la información siguiente:

a) las condiciones para poder acogerse a la protección en virtud de esta ley;

b) los datos de contacto para los canales externos de información previstos en el título III, 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 al informante aclaraciones sobre la información comunicada o que proporcione información adicional, el plazo para dar respuesta al informante, en su caso, y el tipo y contenido de dicha respuesta;

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, y en el título VII de esta ley.

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 de atenuación de la sanción a las que se refiere el artículo 40.

f) los datos de contacto de la Autoridad Independiente de Protección del Informante, A.A.I. o de la autoridad u organismo competente de que se trate.

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.

TÍTULO V

Revelación pública

Artículo 27. Concepto.

1. Se entenderá por revelación pública la puesta a disposición del público de información sobre acciones u omisiones en los términos previstos en esta ley.

2. A las personas que hagan una revelación pública de las acciones u omisiones previstas en el artículo 2 les será aplicable el régimen de protección establecido en el título VII cuando se cumpla alguna de las condiciones establecidas en el artículo siguiente.

Artículo 28. Condiciones de protección.

1. La persona que haga una revelación pública podrá acogerse a protección en virtud de esta ley si se cumplen las condiciones de protección reguladas en el título VII y alguna de las condiciones siguientes:

a) Que haya realizado la comunicación primero por canales internos y externos, o directamente por canales externos, de conformidad con los títulos II y III, sin que se hayan tomado medidas apropiadas al respecto en el plazo establecido.

b) Que tenga motivos razonables para pensar que, o bien la infracción puede constituir un peligro inminente o manifiesto para el interés público, en particular cuando se da una situación de emergencia, o existe un riesgo de daños irreversibles, incluido un peligro para la integridad física de una persona; o bien, en caso de comunicación a través de canal externo de información, exista riesgo de represalias o haya pocas probabilidades de que se dé un tratamiento efectivo a la información debido a las circunstancias particulares del caso, tales como la ocultación o destrucción de pruebas, la connivencia de una autoridad con el autor de la infracción, o que esta esté implicada en la infracción.

2. Las condiciones para acogerse a protección previstas en el apartado anterior no serán exigibles cuando la persona haya revelado información directamente a la prensa con arreglo al ejercicio de la libertad de expresión y de información veraz previstas constitucionalmente y en su legislación de desarrollo.

TÍTULO VI

Protección de datos personales

Artículo 29. Régimen jurídico del tratamiento de datos personales.

Los tratamientos de datos personales que deriven de la aplicación de esta ley 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, de Protección de Datos Personales y garantía de los derechos digitales, 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 presente título.

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

Artículo 30. Licitud de los tratamientos de datos personales.

1. Se considerarán lícitos los tratamientos de datos personales necesarios para la aplicación de esta ley.

2. El tratamiento de datos personales, en los supuestos de comunicación internos, se entenderá lícito en virtud de lo que disponen los artículos 6.1.c) del Reglamento (UE) 2016/679

del Parlamento Europeo y del Consejo, de 27 de abril de 2016, 8 de la Ley Orgánica 3/2018, de 5 de diciembre, y 11 de la Ley Orgánica 7/2021, de 26 de mayo, cuando, de acuerdo a lo establecido en los artículos 10 y 13 de la presente ley, sea obligatorio disponer de un sistema interno de información.

Si no fuese obligatorio, el tratamiento se presumirá amparado en el artículo 6.1.e) del citado reglamento.

3. El tratamiento de datos personales en los supuestos de canales de comunicación externos se entenderá lícito en virtud de lo que disponen los artículos 6.1.c) del Reglamento (UE) 2016/679, 8 de la Ley Orgánica 3/2018, de 5 de diciembre, y 11 de la Ley Orgánica 7/2021, de 26 de mayo.

4. El tratamiento de datos personales derivado de una revelación pública se presumirá amparado en lo dispuesto en los artículos 6.1.e) del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, y 11 de la Ley Orgánica 7/2021, de 26 de mayo.

5. El tratamiento de las categorías especiales de datos personales por razones de un interés público esencial se podrá realizar conforme a lo previsto en el artículo 9.2.g) del Reglamento (UE) 2016/679.

Artículo 31. Información sobre protección de datos personales y ejercicio de derechos.

1. Cuando se obtengan directamente de los interesados sus datos personales se les facilitará la información a que se refieren los artículos 13 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, y 11 de la Ley Orgánica 3/2018, de 5 de diciembre.

A los informantes y a quienes lleven a cabo una revelación pública se les informará, además, de forma expresa, de que su identidad será en todo caso reservada, que no se comunicará a las personas a las que se refieren los hechos relatados ni a terceros.

2. La persona a la que se refieran los hechos relatados no será en ningún caso informada de la identidad del informante o de quien haya llevado a cabo la revelación pública.

3. Los interesados podrán ejercer los derechos a que se refieren los artículos 15 a 22 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016.

4. 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.

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.

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.

TÍTULO VII

Medidas de protección

Artículo 35. Condiciones de protección.

1. Las personas que comuniquen o revelen infracciones previstas en el artículo 2 tendrán derecho a protección siempre que concurran 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 37. Medidas de apoyo.

1. Las personas que comuniquen o revelen infracciones previstas en el artículo 2 a través de los procedimientos previstos en esta ley accederán a las medidas de apoyo siguientes:

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

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

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

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

2. Todo ello, con independencia de la asistencia que pudiera corresponder al amparo de la Ley 1/1996, de 10 de enero, de asistencia jurídica gratuita, para la representación y defensa en procedimientos judiciales derivados de la presentación de la comunicación o revelación pública.

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.

Artículo 41. Autoridades competentes.

Las medidas de apoyo previstas en el presente título serán prestadas por la Autoridad Independiente de Protección del Informante, A.A.I., cuando se trate de infracciones cometidas en el ámbito del sector privado y en el sector público estatal, y, en su caso, por los órganos competentes de las comunidades autónomas, respecto de las infracciones en el ámbito del sector público autonómico y local del territorio de la respectiva comunidad autónoma, así como las infracciones en el ámbito del sector privado, cuando el incumplimiento comunicado se circunscriba al ámbito territorial de la correspondiente comunidad autónoma.

Lo anterior debe entenderse sin perjuicio de las medidas de apoyo y asistencia específicas que puedan articularse por las entidades del sector público y privado.

Anexo 2

Funcionamiento del canal externo de comunicaciones de la Autoridad Independiente de Protección del Informante