

G A _ P

Gómez-Acebo & Pombo

Sistemas de Información Interna (Sii)

Junio 2023

ÍNDICE

Introducción

1. Quiénes están obligados a tener un canal de denuncias	4
2. Quiénes pueden informar	5
3. Sobre qué se puede informar para obtener protección	5
4. Las denuncias anónimas	7
5. Dónde informar	7
6. El Responsable del sistema	9
7. El contenido de la denuncia y su tramitación	10
7.1 Gestión	10
7.2 Tramitación de las denuncias recibidas	12
7.3 Duración del proceso	14
7.4 Conclusión	14
7.5 Conservación de la documentación	16
8. Cómo se protege a los informantes	16
9. Los Sistemas de Información Interna	18
9.1 Protocolo societario o profesional que incluye Compliance Penal y de PBCFT..	19
9.2 Delitos e infracciones administrativas a los que se refiere la ley 2/2023 y otros...	20
9.3 Protocolo laboral de la Firma que cubre infracciones en el entorno laboral.....	20
9.4 Protocolo informático y de protección de datos, que cubre la infracción de todo orden en estos campos	21
9.5 Protocolo anticorrupción	21
9.6 Acoso, que incluye los 2 canales y los relativos a la igualdad de género y de identidad sexual	22
9.7 Protocolo ético profesional, que incluye las infracciones deontológicas propias de la profesión de abogado	23
9.8 El Catálogo sancionador	23
10. El Canal externo de información. La Autoridad Independiente de protección al informante	24
11. La revelación pública	28
12. La protección de datos personales en los Sistemas de Información	29
13. Sanciones	32
14. Formación e información a los empleados y directivos	36
15. Evaluaciones periódicas	37

INTRODUCCIÓN

La Ley Orgánica 5/2010, posteriormente modificada por la Ley Orgánica 1/2015, de 30 de marzo, introdujo la posibilidad de atribuir responsabilidad penal a las personas jurídicas respecto de determinados delitos recogidos en el Código Penal. Las personas jurídicas serán penalmente Responsables de los delitos cometidos en su nombre o por cuenta de ellas y en su beneficio directo o indirecto, por sus representantes legales o personas con capacidad de gestión o decisión —bien de forma individual, bien como miembros de un órgano colegiado—, así como por las personas que éstos tengan a su cargo cuando hayan incumplido gravemente el deber de control.

Y ello, sin perjuicio de la responsabilidad penal o de cualquier otra índole que pueda atribuírsele a la persona física que haya ejecutado materialmente el hecho presuntamente delictivo. De ello se derivarán para ésta una serie de consecuencias que pueden suponer graves perjuicios de tipo personal —como pena de privación de libertad o daños de imagen y reputacionales— y económico, pudiendo afectar al propio administrador o a cualquier directivo o empleado de Gómez-Acebo & Pombo Abogados, S. L. P., o cualquiera de sus filiales (en lo sucesivo referido indistintamente en este documento como «Gómez-Acebo & Pombo» o el «Despacho»).

A consecuencia de lo anterior, el Consejo de Administración aprobó poner en marcha un «Canal interno de comunicación y denuncia», que, unido a los distintos protocolos internos que Gómez-Acebo & Pombo tiene implantados en cada una de sus áreas de negocio para ejecutar las actividades propias de dichas áreas con la mayor diligencia posible, permitirá prevenir conductas ilícitas y, en caso de detectarse éstas o de tener conocimiento de cualquier tipo de imputación penal con motivo del desarrollo de la actividad, adoptar las medidas que en estos casos se han establecido al efecto.

Igualmente, la directiva (UE) 2019/1937 del Parlamento Europeo y del Consejo, conocida como de los “Whistleblowers”, exigía la existencia del Canal de Denuncias interno ya implantado y gestionado por el Despacho.

La reciente publicación de la ley 2/2023, reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción, que transpone la directiva europea, introduce algunos cambios más, por un lado, en la denominación de los comunicantes, que ya no tienen la consideración de denunciantes, al implicar el riesgo de connotaciones distintas en nuestro sistema legal, y pasando a ser denominados “informantes”, de ahí la existencia de “Sistemas de Información Interna”. Por otro lado, la gestión de los canales es holística y requiere la integración de todos los canales existentes en la Firma en un único sistema.

El Canal de Denuncias es una herramienta que permite una comunicación directa, segura, confidencial y anónima entre los trabajadores y los órganos de control, para que estos informen sobre irregularidades o sospechas de irregularidades ocurridas en la empresa.

Actualizaciones

Versión	Descripción del cambio	Fecha
2023	Exigencia de la existencia del SII el 9 de junio, tras la publicación de la ley 2/2023, de 20 de febrero 2023	_/5/2023

1. QUIÉNES ESTÁN OBLIGADOS A TENER UN CANAL DE DENUNCIAS

Las Entidades obligadas a disponer de un sistema interno de denuncias están señaladas en los artículos 10 y 13 de la Ley 2/2023, reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción:

SECTOR PRIVADO

- Las personas físicas o jurídicas del sector privado que tengan contratados cincuenta o más trabajadores
- 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.
 - o Se considerarán incluidas 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.
- Los partidos políticos, los sindicatos, las organizaciones empresariales y las fundaciones creadas por unos y otros, siempre que reciban o gestionen fondos públicos.
- Las personas jurídicas del sector privado que no estén vinculadas por la obligación impuesta, recogida en los párrafos anteriores, podrán establecer su propio Sistema interno de información, que deberá cumplir, en todo caso, los requisitos previstos en esta ley

SECTOR PÚBLICO

- Todas las entidades que integran el sector público estarán obligadas a disponer de un Sistema interno de información en los términos previstos en la ley 2/2023.

En el sector público no hay excepciones. Todas las entidades del sector público están obligadas a contar con un sistema interno de información

2. QUIÉNES PUEDEN INFORMAR

Extiende su aplicación no solo al ámbito laboral, sino también al profesional: trabajadores por cuenta ajena, empleados públicos, autónomos, accionistas y pertenecientes al órgano de administración, supervisión o dirección de una empresa, quienes trabajen bajo la supervisión y dirección de contratistas, subcontratistas o proveedores, quienes revelen información obtenida en el marco de una relación estatutaria ya finalizada, becarios y trabajadores en períodos de formación, aunque no reciban remuneración. E incluso en virtud de la información recibida durante una entrevista de trabajo o proceso de selección o de negociación precontractual.

3. SOBRE QUÉ SE PUEDE INFORMAR PARA OBTENER PROTECCIÓN

La ley 2/2023 protege a los comunicantes personas físicas que informen, por alguno de los canales establecidos, de la siguiente información:

- a) Infracciones penales (delitos).
- b) Infracciones administrativas graves o muy graves.
- c) Infracciones del derecho de la Unión Europea y que afecten a los intereses financieros de la Unión Europea el caso de que a través de estos canales se informe sobre acciones u omisiones distintas a las indicadas, los "informantes"

La protección dispensada por la ley no se extenderá a:

- Las informaciones que afecten a la información clasificada.
- Las obligaciones que resultan de la protección del secreto profesional de los profesionales de la medicina y de la abogacía y del deber de confidencialidad de las Fuerzas y Cuerpos de Seguridad del Estado,
- El secreto de las deliberaciones judiciales. No se aplicará la Ley a las informaciones relativas a infracciones en la tramitación de procedimientos de contratación que contengan información clasificada o hayan sido declarados secretos o reservados, o aquellos cuya ejecución deba ir acompañada de medidas de seguridad especiales o en los que lo exija la protección de intereses esenciales para la seguridad del Estado.

Se podrán comunicar las informaciones o denuncias que estén fuera del marco de la 2/2023, pero dentro del código ético de la firma o de sus protocolos de desarrollo:

- del Protocolo societario o profesional que incluye Compliance Penal y PBCFT.
- delitos e infracciones administrativas a los que se refiere la ley 2/2023 y otros.
- del Protocolo laboral de la Firma que cubre infracciones en el entorno laboral.
- del Protocolo informático y de protección de datos, que cubre la infracción de todo orden en estos campos.
- de las Políticas anticorrupción.
- del Protocolo de Acoso, que incluye los 2 canales y los relativos a la igualdad de género y de identidad sexual.
- del Protocolo ético profesional, que incluye las infracciones deontológicas propias de la profesión de abogado.

Los Canales de Denuncias se identifican con la fase de “detección” de conductas irregulares, aunque su labor va más allá y su valor radica también en la “prevención”, porque promueven la comunicación de infracciones que aún no se han materializado, pero que probablemente se cometerán y saldrán a la luz.

En el apartado de exclusiones, es necesario advertir que no estarían amparadas por esa protección:

- Las informaciones vinculadas a reclamaciones sobre conflictos interpersonales, que deberían resolverse por otras vías.
- Las informaciones sobre irregularidades que ya estén completamente disponibles para el público, o que no contenga información nueva y significativa sobre infracciones por haber existido una comunicación anterior.
- Las informaciones sobre irregularidades que no sean más que meros rumores, las que afecten a hechos que carezcan de toda verosimilitud o las que se hayan obtenido mediante la comisión de un delito.

4. LAS DENUNCIAS ANÓNIMAS

El informante de la denuncia podría efectuarla de tres maneras distintas:

- De manera abierta, en la que el comunicante no oculta su identidad y puede recibir información sobre el trascurso de la denuncia.
- De manera confidencial, en la que el destinatario conoce la identidad del informante, que puede ser identificado a través de cierta información, pero que permanecerá en estricta confidencialidad y no será revelada a nadie, salvo que se trate de un caso de estricta necesidad, sin autorización del comunicante y por exigencias de la ley.
- De manera anónima, en la que el informante no se identifique.

La Directiva Europea 2019/1937 establece como principio el deber general de mantener al informante en el anonimato y así ha sido recogido por la ley 2/2023, como precepto fundamental para la existencia de un Canal Denuncias en la que se garantice la protección del comunicante. Ahora bien, este pilar esencial de la norma europea se exceptúa cuando, bien una norma nacional prevé revelar su identidad, o bien se solicita en el marco de un proceso judicial, argumentando el juzgador la necesidad de conocer la identidad de quien denunció, para garantizar el derecho de defensa del denunciado.

5. DÓNDE INFORMAR

El procedimiento se inicia en el momento de la recepción de la denuncia a través del canal establecido por el Despacho, que puede adoptar alguno de los siguientes formatos:

- Correo postal a la dirección: P.º de la Castellana, 216 - 28046 Madrid.
- Correo electrónico habilitado para ser utilizado en la comunicación de la información y que, en el Despacho, es informantes_sii@ga-p.com .
- O bien, mediante una comunicación verbal, por vía telefónica o mediante mensaje de voz. El Despacho ha habilitado un teléfono, que emitirá el mensaje siguiente:
"Está usted hablando con el buzón de voz del Sistema Interno de Información de Gómez-Acebo Pombo. Le informamos de que su mensaje va a ser grabado. En nuestra página Web, puede encontrar información sobre este Canal. A continuación, deje su comunicación, por favor. Nos pondremos en contacto con usted en un periodo no superior a 7 días. Indique el modo en que quiere que contactemos. Gracias."

La llamada se podrá efectuar desde:

- El móvil corporativo
- Un móvil/ teléfono externo
- Desde extensiones internas, que no aparecerán identificadas

La extensión para llamar desde el interior es **180**

El número para llamar desde el exterior es el **91 582 9180**

En ningún caso, se identificará al informante, puesto que no aparece la extensión, en el caso de la llamada interna, ni el teléfono en el caso de la llamada desde el exterior.

Siempre se pondrá en conocimiento del informante que su mensaje será grabado y se le informará de que el tratamiento de éste será acorde con la ley. Así mismo, se le informará sobre la conveniencia de consultar la página Web y la opción, no obligatoria, de proporcionarnos un método de contacto que nos permitiría proporcionarle información sobre el proceso iniciado.

En caso de que la comunicación se produzca de manera verbal, se procederá del siguiente modo:

- mediante una grabación del mensaje, o conversación, en un formato seguro, duradero y accesible, o
- a través de una transcripción completa y exacta de la conversación realizada por el personal Responsable de tratarla.

El Informante debe poder elegir el canal de denuncia más adecuado en función de las circunstancias particulares de su caso.

Una vez realizada la comunicación, se procederá a su registro, asignándole un código único de identificación.

En un plazo no superior a **7 días naturales**, el informante recibirá acuse de recibo de su comunicación, siempre que la denuncia no se formule de manera anónima. En todo caso, se preservará la confidencialidad de la identidad del denunciante, así como el contenido de la denuncia. Se informará al comunicante de que sus datos personales serán tratados conforme al Reglamento de Protección de datos.

6. EL RESPONSABLE DEL SISTEMA

Según lo establecido en el Artículo 5 de la Ley de Protección al Informante, el Responsable de la implantación del Sistema Interno de Información es el órgano de administración u órgano de gobierno de cada entidad, previa consulta con la representación legal de los trabajadores.

Sin embargo, debe existir la figura del Responsable del Sistema, que es la persona o departamento u órgano colegiado encargado de la recepción y seguimiento de las informaciones.

El órgano de administración de la empresa u órgano de gobierno de cada entidad u organismo público será el competente para su designación, destitución o cese, que deberán ser notificados a la Autoridad Independiente del Informante A.A.I.

Dado el carácter preventivo del canal de denuncias, el perfil para ocupar el puesto de Responsable del Sistema requiere contar con una cierta cualificación, mantener un contacto directo con el órgano de gobierno o de dirección y ofrecer garantías de confidencialidad e independencia.

En las entidades privadas, como es el caso de nuestra Firma, en la que ya existe un Responsable de Cumplimiento, será esta persona quien asuma la responsabilidad y quien continuará una labor que ya venía desarrollando en el Despacho.

Funciones del Responsable

El Responsable del Sistema tiene entre sus funciones:

- Garantizar el correcto funcionamiento del sistema de canal de denuncia.
- Aprobar el procedimiento de gestión de comunicaciones.
- Informar a cualquier persona interesada sobre los procedimientos de denuncia.
- Recibir y seguir denuncias, llevando los registros documentales correspondientes.
- Velar por que se lleven a cabo las investigaciones a las que haya lugar con respeto a los derechos de todas las partes involucradas y que se emitan los informes de culminación de las investigaciones en tiempo y forma.
- Mantener el contacto con el denunciante a los efectos de darle respuesta y de solicitarle información adicional en caso necesario.
- Proteger y velar por que se cumplan las garantías de confidencialidad de la identidad del denunciante y cualquier otra persona involucrada en la denuncia.
- Proteger y velar por que se cumplan las garantías de confidencialidad de las comunicaciones dentro del sistema del canal de denuncia.

7. EL CONTENIDO DE LA DENUNCIA Y SU TRAMITACIÓN

Con el fin de poder investigar la información recibida, es necesario que la denuncia incluya la información necesaria:

- La descripción de la conducta que se desea comunicar, incluyendo la información con el máximo detalle.
- La fecha y lugar en la que se ha producido.
- Identificación de la persona/as denunciadas.
- Si se dispone de alguna documentación relacionada, se debe adjuntar.
- El informante debe comunicar si considera que hay algún riesgo para él mismo u otras personas.
- Cualquier otro aspecto que el informante considere relevante: existencia de testigos, documentación etc.
- Medio de contacto sólo si desea recibir información y la notificación no es anónima.
- Fecha de envío de la comunicación.

7.1 Gestión.

El sistema de gestión de la denuncia debe recoger, de forma clara, cómo se efectúan y reciben las comunicaciones. Al mismo tiempo, el sistema de gestión de la denuncia de irregularidades debería permitir una evaluación del riesgo de perjuicio y el nivel de protección y apoyo necesarios para los denunciantes y otras personas involucradas. Es importante que la información se haya enviado a través de los medios puestos a disposición con este fin. En un plazo no superior a 7 días, el comunicante recibirá acuse de recibo de la denuncia.

El Despacho ya contaba, con anterioridad, con un sistema interno integrado de gestión de denuncias, dando trámite a las mismas, a través del Canal de Denuncia interno, si bien, el presente manual sirve de explicación sobre el funcionamiento del Sistema.

Existe un Protocolo, a disposición de toda la organización en la Intranet de la Firma que, aunque debe ser actualizado tras la publicación de la norma 2/2023 con terminología, ha arrojado resultados óptimos, alineados con las políticas de Compliance del Despacho, así como con la ley 2/2023. El documento se denomina "Canal interno de comunicación y denuncia" y es incluido, periódicamente, en las distintas formaciones de Compliance, explicando el uso del canal, el acceso y la propia gestión.

El canal interno del Despacho tiene por objeto establecer un procedimiento de comunicación entre el Responsable del Sistema, el Órgano de Compliance y los socios, administradores, directivos, empleados de Gómez-Acebo & Pombo con respecto a:

- a) Cualquier hecho o conducta de la que tengan conocimiento relacionada con una actuación u omisión presuntamente delictiva o generadora de un riesgo de imputación penal para Gómez-Acebo & Pombo o para cualesquiera de sus miembros.
- b) Cualquier noticia o requerimiento que reciban de cualquier autoridad u orden jurisdiccional o administrativo, el Ministerio Fiscal o el Tribunal de Cuentas, que será enviada al Canal para su resolución inmediata.
- c) Cualquier hecho o conducta que pudiera incumplir el Catálogo de conductas prohibidas.
- d) Cualquier denuncia de terceros externos a la organización en relación con cuestiones relativas a los estándares éticos o de corrupción.
- e) El hecho de que el Despacho o cualquiera de sus miembros esté incurso en un procedimiento judicial o administrativo motivado por hechos que estén relacionados con las actividades desarrolladas en las distintas líneas de negocio o que pudieran afectar al correcto desarrollo de las funciones que tengan encomendadas dentro de Gómez-Acebo & Pombo.

Admisión de la denuncia

El uso del Canal se hará de buena fe, con rigor y de forma seria y Responsable.

En caso de confirmarse que un miembro de Gómez-Acebo & Pombo ha formulado denuncia falsa, podrá ser objeto de procedimiento disciplinario conforme a la normativa laboral aplicable o con las políticas internas del Despacho.

Ningún miembro del Despacho podrá ser objeto de procedimiento disciplinario alguno por denunciar hechos que en su opinión infrinjan los estándares mínimos éticos de Gómez-Acebo & Pombo, siempre que su denuncia y actuación estén amparadas por la buena fe y por la convicción de estar actuando de forma correcta y dentro de dichos estándares mínimos éticos.

Las denuncias de hechos presentadas ante el Responsable del Sistema que puedan suponer la infracción de las obligaciones de carácter laboral de algún profesional miembro del despacho se trasladarán al departamento de RRHH en el caso de que la denuncia sea anónima y, sin perjuicio de se pueda hacer un seguimiento en caso de que proceda el mismo, corresponderá al departamento de RRHH el control de la infracción denunciada y, en su caso, la propuesta de sanción correspondiente. Si la denuncia se efectuara por un miembro identificado, el Responsable del Sistema le informará de la posibilidad de tramitar la denuncia ante el departamento de RRHH, advirtiéndole que la tramitación de la denuncia ante el Órgano de *Compliance* generará un expediente exento de carácter sancionador, pudiendo haber prescrito la falta laboral cuando aquél finalice. No obstante, si el denunciante persistiera en su deseo de mantener su actuación ante el

Responsable y el Órgano de *Compliance*, este último tramitará la misma en los términos previstos en este canal.

7.2 Tramitación de las denuncias recibidas

El procedimiento se iniciará mediante una denuncia o comunicación dirigida, por cualquier miembro de Gómez-Acebo & Pombo o por terceros interesados (clientes proveedores, etc.), al Responsable del Sistema, en la cual se ponga de manifiesto lo siguiente:

- a) Que ha tenido conocimiento de que en el Despacho se han producido o se están produciendo una serie de conductas que quedan al margen de los estándares mínimos éticos tal y como vienen definidas en distintos documentos de *Compliance* que aparecen recogidos en la Intranet y que son modificados según es pertinente y que, consecuentemente, son generadoras de un riesgo.
- b) Que ha tenido conocimiento de que el Despacho o uno de sus miembros está incurso en un procedimiento judicial o administrativo por hechos que están relacionados con las actividades desarrolladas en las distintas líneas de negocio o que pudieran afectar al correcto desarrollo de las funciones a ellos encomendadas dentro de Gómez-Acebo & Pombo.
- c) Que ha recibido un requerimiento de una autoridad judicial o administrativa, del Ministerio Fiscal o del Tribunal de Cuentas, a los fines de que facilite documentación o información relativa a Gómez-Acebo & Pombo o de uno de sus miembros.

La denuncia se efectuará mediante alguno de los medios ofrecidos por el Despacho en su página Web: dirigiéndose a la dirección de correo informantes_sii@ga-p.com , mediante un escrito a la dirección de correo postal que aparece en la página o bien, dejando un mensaje de voz en el buzón creado a tal efecto.

El informante tiene el deber de guardar secreto sobre la denuncia formulada, así como sobre la identidad de la persona o personas denunciadas y de los hechos y documentación objeto de la denuncia.

El denunciante guardará el número de registro asignado. Si ha proporcionado un correo electrónico o un teléfono, mediante este número de registro podrá obtener información acerca del proceso, bien porque la solicite, bien porque el Responsable le informe en el transcurso de la tramitación.

En caso de duda, y como criterio general, el informante o comunicante consultará con el Responsable de Sistemas cualquier conducta sospechosa o inusual que, en su opinión, pudiera implicar riesgo de cualquier tipo para Gómez-Acebo & Pombo, incluido el de imputación delictiva para Gómez-Acebo & Pombo o cualquiera de sus miembros. Para hacer la consulta se utilizarán los mismos cauces establecidos.

El Responsable de los Sistemas realizará un análisis *prima facie* y, a la vista de este:

- a) si considerara material la denuncia, procederá a tramitar la misma conforme al procedimiento descrito.
- b) si se tratara de un asunto de carácter laboral lo transmitirá al departamento de RRHH o seguirá con la tramitación.
- c) si apreciara que no es de su competencia o que no es relevante, lo archivará.
- d) si apreciara que es de competencia de otro departamento, lo trasladará a este último, y
- e) el Responsable de los Sistemas podrá actuar de oficio sin necesidad de denuncia.

Tras recibir la denuncia, el Responsable acusará recibo de esta en el plazo máximo de 7 días naturales. Si, tras el primer análisis, considera que no existe ningún modo de exclusión de los mencionados anteriormente, procederá a su trámite. Una vez estudiada la denuncia, si decide que debe ser objeto de investigación, abrirá el correspondiente procedimiento de investigación interna.

Abierto el procedimiento de investigación interna, el Responsable mantendrá una entrevista personal con la persona o personas presuntamente infractoras, quienes podrán estar asistidas por persona de su elección.

Igualmente, cualquiera de los miembros del Órgano de Compliance, que sirven de apoyo al Responsable, podrá recabar, en cualquier momento del procedimiento, la asistencia de cualquiera de los miembros de Gómez-Acebo & Pombo, así como de auditores, asesores y letrados externos. Cualquier tercero ajeno al procedimiento que participe en él estará sujeto al deber de confidencialidad.

En la entrevista, y no antes, se presentarán al presunto infractor los hechos y documentos que sustenten la supuesta conducta infractora, siempre protegiendo el anonimato del informante y respetando la presunción de inocencia y el derecho al honor de las personas afectadas.

Al terminar dicha entrevista, se levantará la correspondiente acta, en la que, al menos, se harán constar expresamente los siguientes extremos:

1. Fecha, hora y lugar de la entrevista.
2. Nombre, apellidos y funciones dentro del Despacho de las personas intervinientes.
3. Información suministrada a la persona o personas entrevistadas por el Responsable de los presuntos hechos que se les atribuyen.
4. Relación de los documentos soporte de la denuncia que se han puesto de manifiesto al presunto infractor entrevistado.
5. Firma de todos los intervinientes.
6. Cualquier manifestación de la que la persona o personas entrevistadas quieran dejar constancia por escrito.
7. Notificación expresa al presunto infractor de que dispone de un plazo de diez (10) días hábiles para formular alegaciones en su descargo y aportar la documentación que estime oportuna.

7.3 Duración del proceso

Transcurridos dichos diez (10) días hábiles, haya presentado o no el presunto infractor las alegaciones en su descargo y, en su caso, la correspondiente prueba documental, el Responsable, junto al Órgano de *Compliance* emitirá su dictamen en un plazo máximo de catorce (14) días hábiles.

El plazo máximo de tramitación será de 3 meses, a contar desde la recepción de la denuncia, ampliando el plazo por un periodo de 3 meses de manera justificada.

7.4 Conclusión

El Responsable, junto con el Órgano de *Compliance* adoptará en su dictamen alguna de las siguientes decisiones:

- a) Elevar al *Senior Partner* el resultado de la investigación por entender que la conducta analizada supone un incumplimiento de la normativa, interna o externa, o bien es contraria a los estándares mínimos éticos del Despacho.

Adicionalmente, en este caso, podrá incluir, además, estas recomendaciones:

1. Que se adopten determinadas medidas correctoras para prevenir que la conducta pueda volver a producirse.
2. Que se comuniquen los hechos a las autoridades judiciales o administrativas pertinentes.
3. O que se abra expediente disciplinario contra el presunto infractor, de conformidad con la normativa laboral aplicable o con la normativa interna del Despacho.

- b) Archivar la denuncia formulada frente al presunto infractor por entender que la conducta analizada no supone un incumplimiento normativo ni es contraria a los estándares mínimos éticos del Despacho.

En el supuesto de que el Responsable, junto al Órgano de Compliance, recomiende la apertura de un procedimiento disciplinario, se dará traslado del dictamen al *Senior Partner*, quien remitirá al Órgano de Compliance, en el plazo de siete (7) días hábiles, un escrito en el que, de manera motivada, manifieste su conformidad o disconformidad con la propuesta de apertura de procedimiento disciplinario. Una copia del citado escrito será remitida por el Órgano de Compliance al Órgano de Administración. El correspondiente procedimiento disciplinario se desarrollará conforme a la normativa aplicable y, en su caso, la normativa interna del Despacho.

La decisión adoptada en el expediente disciplinario será comunicada, de forma escrita, al Órgano de Compliance.

En cuanto a la recomendación del Órgano de Compliance al Órgano de Administración, con respecto a la comunicación de la conducta analizada a las autoridades judiciales o administrativas pertinentes, la correspondiente decisión habrá de adoptarse dentro del plazo de tres (3) meses, a contar desde la apertura del procedimiento de denuncia.

Información al comunicante

El Despacho, siempre y cuando no haya impedimento legal, o la denuncia no se haya formulado de manera anónima, informará al comunicante del resultado de su comunicación.

El informe que se facilite, en su caso, al comunicante, no podrá contener los detalles de la investigación ni referirse a personas concretas, sino que deberá ser redactado en términos genéricos, teniendo siempre en cuenta la naturaleza confidencial de la información y los derechos que puedan asistir a terceros, entre ellos, el presunto infractor —aunque no sólo él—. En dicho informe, se indicará expresamente si se han tomado medidas correctoras o se va a llevar a cabo cualquier tipo de actuación adicional al respecto, incluida la mejora de los procedimientos internos.

7.5 Conservación de la documentación

Será obligatorio conservar todos aquellos documentos que puedan servir de soporte probatorio de la conducta objeto de la denuncia, con especial observancia de la normativa en materia de protección de datos.

Tal y como se indica en la LO 3/2018 LOPDGDD, artículo 24, los datos se conservarán en el sistema de denuncias únicamente durante el tiempo imprescindible para decidir sobre la procedencia de iniciar una investigación sobre los hechos denunciados. Transcurridos tres meses desde la introducción de los datos, se procederá a su supresión del sistema de denuncias. Las denuncias a las que no se haya dado curso solamente podrán constar de forma anonimizada.

8. CÓMO SE PROTEGE A LOS INFORMANTES

La norma pretende que la protección a quienes informan de estas irregularidades sea lo más amplia posible. Para ello, se prohíbe expresamente y se declara la nulidad de pleno derecho de cualquier represalia laboral, incluyendo, entre otros:

- 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 la ley 2/2023.
- La ley 2/2023 define como 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
- También son consideradas por la Ley represalias:
 - La 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.

- Los daños, incluidos los de carácter reputacional, o pérdidas económicas, coacciones, intimidaciones, acoso u ostracismo.
- La evaluación o referencias negativas respecto al desempeño laboral o profesional.
- La 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.
- La denegación o anulación de una licencia o permiso.
- La denegación de formación.
- La discriminación, o trato desfavorable o injusto.

Más allá de lo anterior, la norma establece otras muchas garantías adicionales, entre las que cabe citar:

- Los informantes no incurrirán en responsabilidad por el acceso a la información de irregularidades, siempre que dicha adquisición o acceso no constituya un delito.
- La inversión de la carga de la prueba: En los procedimientos que se sigan ante un órgano jurisdiccional u otra autoridad por los perjuicios sufridos por quien ha informado de irregularidades, se presumirá que el perjuicio se produjo como represalia por tal actuación, de modo que corresponderá a la persona que haya tomado la medida perjudicial probar que la misma se basó en motivos justificados no vinculados a la comunicación o revelación pública.

Sin perjuicio de las facultades disciplinarias que en el ámbito interno de cada entidad puedan tener los órganos competentes, la protección a los trabajadores y demás personas que comunican de estas irregularidades se encomienda a autoridades independientes: una estatal y otra por Comunidad Autónoma. Sus funciones en este ámbito son de dos tipos:

- Medidas de protección y apoyo: información, asesoramiento, asistencia técnica y jurídica o, incluso, llegado el caso, apoyo financiero y psicológico.
- Potestad sancionadora, con competencia para sancionar cualquier conducta contraria a las previsiones de esta ley y, de forma particular, cualquier represalia contra quienes comuniquen estas irregularidades. La autoridad independiente de ámbito estatal, en el

ejercicio de su potestad sancionadora, tiene competencia respecto de las infracciones cometidas en el ámbito del sector público estatal. También lo será 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. Por su parte, las autoridades independientes de las Comunidades Autónomas tendrán competencia respecto de las infracciones cometidas en el ámbito del sector público autonómico y local del territorio de la comunidad autónoma, sin perjuicio de la posibilidad de que su normativa propia prevea que dichos órganos asuman también competencia para conocer de las infracciones cometidas en el ámbito del sector privado cuando afecten solamente a su ámbito territorial.

9. LOS SISTEMAS DE INFORMACIÓN INTERNA

La ley 2/2023 establece que debe existir un Sistema Interno de Información (SII), que gestione todos los canales de denuncia existentes en una entidad, tanto para las denuncias que se recojan en la propia ley, como aquellas que resulten de los otros canales existentes. Propugna, en definitiva, un sistema integrado con una gestión única para todos los canales a través de los que se pueda comunicar.

El artículo 5 de la ley 2/2023, establece que el órgano de administración u órgano de gobierno de cada entidad u organismo obligado por ella 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

La Ley habla de sistemas internos y externos de gestión, aunque prioriza los internos, siempre que la infracción se pueda tratar de modo efectivo vía interna y no haya riesgo de represalia para el informante.

La adaptación a la nueva normativa se lleva a cabo sin fricciones, puesto que los sistemas de comunicación ya se hallaban integrados en el Despacho, si bien era necesaria la creación de este manual explicativo y restaban por integrar algunas formas de comunicación alternativas de los sistemas informales. Además, el funcionamiento de los canales de comunicación de PBCFT no se puede integrar en su totalidad, como se puede observar en el apartado 9.1.

Características que debe tener el Canal interno de denuncias

- Debe garantizar la confidencialidad y el anonimato de las denuncias y garantizar la indemnidad del informante.

- El acceso a los datos contenidos en estos canales de denuncia debe quedar limitado exclusivamente a quienes, desarrollen las funciones de control interno y de cumplimiento, o a los encargados del tratamiento que eventualmente se designen a tal efecto.
- Se debe informar a los empleados y a terceros de la existencia de estos canales internos.
- El Despacho debe formar e informar a todos sus empleados y directivos sobre la implantación de estos sistemas integrados, de su finalidad, así como de su funcionamiento, la forma de presentación de la denuncia, su tramitación y plazos de resolución. Periódicamente, se informará sobre los distintos canales, su funcionamiento y la existencia de actualizaciones, en su caso.
- La persona afectada debe ser informada de la existencia de la denuncia formulada en su contra, respetándose la normativa existente en materia de protección de datos personales.
- Debe evaluarse periódicamente para comprobar su correcto funcionamiento y si existen errores o deficiencias de deben ser subsanadas.
- Debe existir un sistema disciplinario de incumplimientos.
- Debe comunicarse su existencia a los representantes legales de los trabajadores.

Documento donde se recogen los protocolos del Despacho

Debemos remitir al documento existente en el Despacho, a disposición de toda la organización en la Intranet de la Firma, y del que se hace entrega una copia a todas las nuevas incorporaciones, "Protocolo de conductas prohibidas y catálogo de sanciones de la Firma". El documento recoge la descripción de cuáles son las conductas, en cada uno de los ámbitos, susceptibles de ser incumplidas y posible objeto de comunicación, así como el sistema disciplinario que debe aplicarse para un correcto funcionamiento de los canales.

9.1 Protocolo societario o profesional que incluye Compliance Penal y de PBCFT

Como se mencionaba anteriormente, los canales de denuncia de PBCFT están adaptados a su normativa específica, no obstante, el canal exigido por el artículo 26.bis requiere de una gestión que puede perfectamente integrarse en el Sistema Interno, al desarrollarse como se gestionan el resto de denuncias.

Los canales de PBCFT son los siguientes:

Comunicación	Base normativa	Modo de comunicación	Anónimo	Quién gestiona
Por indicio	Art. 18 Ley 10/2010 PBC/FT	Mediante formulario incluido en la Intranet A través del correo Compliance@ga-p.com , dirigido a la Unidad Técnica	NO	Unidad Técnica que envía su investigación al OCI, quien toma la decisión final. En caso de falta de respuesta o desacuerdo con la resolución, el comunicante puede enviar su denuncia al SEPBLAC
Canal de denuncia interno	Art. 26.Bis Ley 10/2010 PBC/FT	A través del correo Compliance@ga-p.com , dirigido al "Managing Partner"	Puede ser anónimo	"Managing Partner"
Canal externo de denuncia	Art. 63 Ley 10/2010 PBC/FT	Directamente al SEPBLAC	NO	SEPBLAC

9.2 Delitos e infracciones administrativas a los que se refiere la ley 2/2023 y otros

La comunicación y gestión de las denuncias en el ámbito administrativo siguen los preceptos del Canal Interno de Denuncias y se desarrollan siguiendo el Protocolo establecido para ello.

9.3 Protocolo laboral de la Firma que cubre infracciones en el entorno laboral

El ámbito laboral dispone de su propio protocolo, aunque está igualmente incluido en el documento "Protocolo de conductas prohibidas y catálogo de sanciones de la Firma", que compila los relativos al Cumplimiento dentro de la Firma y la gestión de las denuncias se realiza a través del Canal Interno. Incluido en la Intranet, a disposición de toda la organización, el "Procedimiento sancionador en el ámbito laboral", recoge los formularios necesarios para la comunicación de la denuncia, el procedimiento de gestión y la aplicación de sanciones, en su caso.

9.4 Protocolo informático y de protección de datos, que cubre la infracción de todo orden en estos campos

La comunicación y gestión de las denuncias en el ámbito del departamento de Informática siguen los preceptos del Canal Interno de Denuncias y se desarrollan siguiendo el Protocolo establecido para ello.

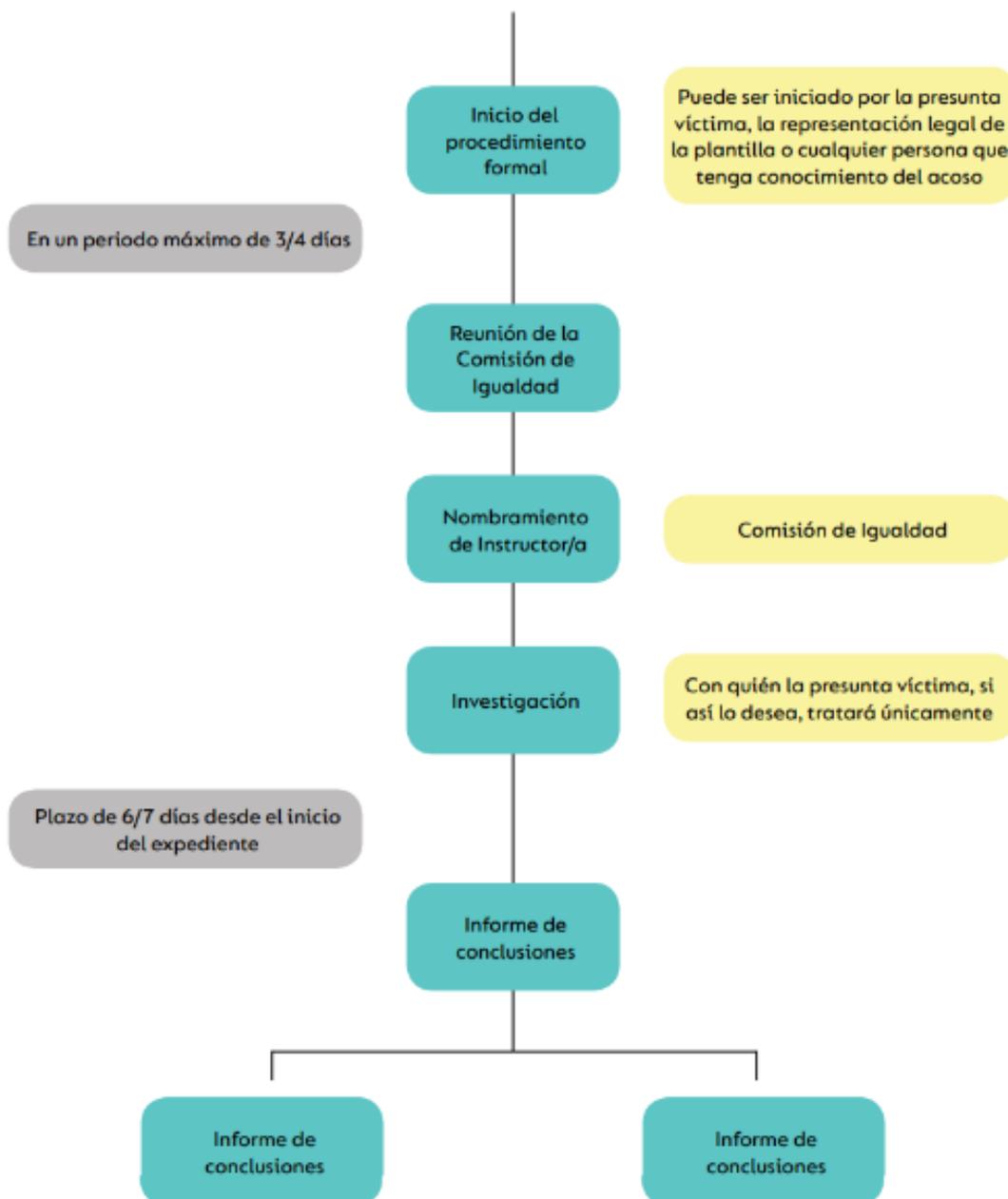
9.5 Protocolo anticorrupción

La comunicación y gestión de las denuncias relacionadas con la corrupción siguen los preceptos del Canal Interno de Denuncias y se desarrollan siguiendo el Protocolo establecido para ello.

9.6 Acoso, que incluye los 2 canales y los relativos a la igualdad de género y de identidad sexual

El Protocolo de acoso, también dispone de canales de denuncia que se integran en este Sistema. Disponible para toda la organización, en la Intranet, el Protocolo muestra que hay dos modos de comunicar y gestionar las comunicaciones sobre irregularidades referidas a acoso e igualdad:

Procedimiento informal para la tramitación de las reclamaciones o denuncias de acoso sexual o por razón de sexo



Procedimiento formal

El procedimiento formal supone la elaboración de una actuación clara y precisa, complementaria o alternativa al procedimiento informal, para denunciar e investigar situaciones de acoso y será tramitado por el Compliance Officer y las personas que éste designe de conformidad con los procedimientos aplicables.

La denuncia se efectuará rellenando el correspondiente formulario disponible en la intranet corporativa y se deberá adjuntar toda la documentación de que se disponga y que sirva de soporte justificativo de la denuncia. Seguirá lo dispuesto en el Canal Interno de Comunicación y Denuncia, y se tramitará según lo allí establecido.

El procedimiento deberá ser rápido, tanto para poner fin lo antes posible a la conducta de acoso y mitigar los posibles efectos sobre la víctima como para no perjudicar los intereses de la persona denunciada.

Se debe garantizar la audiencia a las partes implicadas, permitiendo a éstas formular alegaciones e informándoles de los elementos, objetivos y resultados del procedimiento; y que tanto las personas denunciadas como la denunciada podrán acompañarse en todos los trámites de una persona de la Representación Legal de la plantilla.

En todo el proceso se deberá mantener el respeto a una confidencialidad estricta y al derecho a la intimidad, no sólo de la presunta víctima sino también de la persona objeto de la acusación. Se debe informar a cuantas personas participen en el procedimiento, de su deber de guardar confidencialidad y sigilo sobre su intervención y sobre cuanta información conocieran por su comparecencia en la misma.

9.7 Protocolo ético profesional, que incluye las infracciones deontológicas propias de la profesión de abogado

La comunicación y gestión de las denuncias relacionadas con el Código Deontológico siguen los preceptos del Canal Interno de Denuncias y se desarrollan siguiendo el Protocolo establecido para ello.

9.8 El Catálogo sancionador

Recogido, como se mencionaba, en el documento de referencia "Protocolo de conductas prohibidas y catálogo de sanciones de la Firma":

La potestad sancionadora del Despacho, tanto de las normas societarias como laborales, permite establecer la posibilidad de extinguir la relación con el Despacho ante incumplimientos que supongan una manifiesta y grave quiebra de la confianza, de la transgresión de la buena fe contractual o de la pérdida de adecuación profesional.

Salvo en el supuesto de relaciones laborales comunes, sometidas a un Convenio Colectivo específico, y cuya tipificación tanto en incumplimientos como en sanciones se impone, a excepción de aquellas conductas no recogidas en el mismo, el resto de supuestos pueden suponer una extinción unilateral por parte de la Firma.

No obstante, y atendiendo a la distinta naturaleza de las observaciones indicadas en el Catálogo de Conductas Prohibidas, y salvo que la conducta tenga inicialmente una naturaleza grave y culpable o derive en un daño contrastado para la Firma, se optará por una amonestación escrita, en caso de reiteración en el incumplimiento por una suspensión de empleo y sueldo proporcionada al mismo, y, de existir reincidencia y, por tanto, gravedad y culpabilidad en el comportamiento, se rescindirá la relación contractual.

En todo caso, la falta de seguimiento de las indicaciones de correcta actuación o el desarrollo de conductas prohibidas se recogerá en la evaluación anual del miembro de la Firma, con la debida repercusión en su promoción profesional y económica.

Los miembros de la Firma con relaciones mercantiles, societarias o civiles se registrarán por lo dispuesto en sus contratos que se considerarán integrados a efectos de lo que la Firma estima conforme a la buena fe y a la confianza exigible por los Protocolos de conductas prohibidas, así como el catálogo y procedimiento aquí contenidos.

10. EL CANAL EXTERNO DE INFORMACIÓN. LA AUTORIDAD INDEPENDIENTE DE PROTECCIÓN AL FIRMANTE

La gestión de la información puede realizarse internamente o encargarse a un tercero externo (art. 15 L. 2/2023). Se entiende por gestión de la información por un tercero externo la recepción de informaciones sobre infracciones y, en todo caso, tendrá carácter exclusivamente instrumental. La mención a esta posibilidad de externalización contenida en la Ley tiene como objetivo diferenciar la externalización del Canal de denuncias, de la gestión del Canal Externo de Información.

La existencia de canal de denuncia o de información externo, se entiende como un medio complementario al canal interno. En la Ley se ha constituido como canal externo de información a la Autoridad Independiente de Protección del Informante (A.A.I.) o a las autoridades u órganos autonómicos correspondientes (art. 16 L. 2/2023).

Funciones

- la Gestión del Canal Externo de comunicaciones,
- la adopción de medidas de protección al informante,
- tramitar procedimientos sancionadores e imponer las sanciones que procedan.

Cualquier autoridad que reciba una comunicación y no tenga competencias por tratarse de alguna de las infracciones sobre las que es competente la AAI, deberá remitirla a esta última.

Las informaciones sujetas a la competencia de las AAI son las que provengan de la Administración General del Estado y entidades que integran el sector público estatal, resto de entidades del sector público, órganos constitucionales, órganos de relevancia constitucional, entidades que integran el sector privado cuando la comunicación afecte al ámbito territorial de más de una comunidad autónoma, cuando se suscriba el oportuno convenio, las Administraciones y entidades establecidas.

La autoridad Independiente u órgano o entidad en cada comunidad autónoma, será competente respecto de las informaciones que afecten al sector público autonómico y local de su respectivo territorio, instituciones autonómicas y entidades que formen parte del sector privado, cuando el incumplimiento comunicado se circunscriba al ámbito territorial de la correspondiente comunidad autónoma.

Una cuestión relevante es que las decisiones adoptadas por la A.A.I. en el curso del procedimiento iniciado tras una comunicación, no serán recurribles en vía administrativa ni en vía contencioso-administrativa. El resto de actos y decisiones serán recurribles vía administrativa o ante la jurisdicción contencioso-administrativa.

Cómo se gestiona la información recibida

El Canal Externo gestiona la información del mismo modo que lo hace el Canal Interno:

- Por escrito: correo postal o por medio electrónico habilitado.
- Verbalmente: vía telefónica o a través de otros sistemas de mensajería de voz. Previa solicitud del denunciante, se podrá celebrar una reunión presencial en el plazo de 7 días.
- De ambos modos.

Se advertirá al informante de que la comunicación será grabada, en su caso, y de que sus datos personales serán tratados conforme al Reglamento de Protección de datos. Además, podrá indicar un domicilio, correo o lugar a efectos de notificaciones. Y, una vez presentada la información, se registrará en el Sistema de Gestión de Información y se le asignará un Código de identificación.

Recibida la información se acusará recibo en un plazo no superior a 5 días hábiles, salvo que se trate de una información anónima y el informante haya renunciado expresamente a recibir comunicaciones. Realizado un 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:

INADMISIÓN MOTIVADA DE LA DENUNCIA	ADMISIÓN DE LA DENUNCIA	REMISIÓN
<p>Inadmitir la comunicación en los casos establecidos: por falta de verosimilitud de los hechos; porque no se trate de una infracción incluida en el ámbito de aplicación de la Ley; porque carezca de fundamento o existan indicios de que se ha obtenido delictivamente; porque no contenga información nueva o significativa respecto otras comunicaciones anteriores. La inadmisión de comunicará al informante en los 5 días hábiles siguientes, salvo si la comunicación es anónima o hay renuncia a recibir notificaciones.</p>	<p>Admitir a trámite la comunicación: se comunicará al informante dentro de los cinco días hábiles siguientes, salvo denuncia anónima o previa renuncia a recibir notificaciones.</p>	<ul style="list-style-type: none"> - Remitir la información al Ministerio Fiscal o a la Fiscalía Europea, en su caso. - Remitir la comunicación a la autoridad, entidad u organismo que se considere competente para su tramitación.

Fase de instrucción

Durante la fase de instrucción, la persona afectada por la información tiene derecho a tener noticia de la información. Nunca se le desvelará la identidad del informante ni se le permitirá acceder a la comunicación, aunque sí obtendrá una sucinta relación de los hechos y podrá presentar alegaciones. La instrucción comprenderá, siempre que sea posible, una entrevista con la persona afectada.

Tendrá acceso al expediente sin que se pueda identificar al informante, podrá ser oída en cualquier momento y tendrá posibilidad de comparecer asistida de abogado.

Informe de la AAI y decisión

Concluidas las actuaciones la AAI emitirá un informe y adoptará alguna de las siguientes decisiones:

- Archivo del expediente.
- Remisión al Ministerio Fiscal o a la Fiscalía Europea, en su caso.
- Traspaso de lo actuado a la autoridad competente.
- Adopción de acuerdo de inicio de un procedimiento sancionador.

El plazo del que se dispone no puede superar los 3 meses y se puede ampliar a 6 meses en casos justificados.

Las decisiones adoptadas por la Autoridad Independiente de Protección del Informante, A.A.I., no serán recurribles en vía administrativa ni en vía contencioso-administrativa.

La protección a los informantes

Los informantes tendrán derecho a la protección prevista en la Ley siempre que tengan motivos razonables de verosimilitud de la información, sin que sea preciso que aporten pruebas concluyentes y hayan realizado la comunicación a través de los sistemas internos o externos previstos en ella.

Esta protección 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.

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 ni delito ni falta muy grave.

En los procedimientos laborales ante un órgano jurisdiccional relativos a los perjuicios sufridos por los informantes, se presumirá que el perjuicio se produjo como represalia por informar o por hacer una revelación pública. Corresponderá a la persona que haya tomado la medida perjudicial probar que esa medida se basó en motivos debidamente justificados no vinculadas a la comunicación o revelación pública.

En los procesos judiciales civiles o laborales, los informantes no incurrirán en responsabilidad de ningún tipo como consecuencia de comunicaciones o de revelaciones públicas protegidas por la ley. Dichas personas tendrán derecho a alegar motivos razonables para pensar que la comunicación o revelación pública era necesaria para poner de manifiesto una infracción en virtud de lo previsto en la Ley de protección del denunciante.

Quedan fuera de protección los informantes cuyas comunicaciones:

- Se inadmitieron por el canal interno de información (falta de verosimilitud).
- No se trate de una infracción incluida en el ámbito de aplicación de la Ley.
- Carezca de fundamento o existan indicios de que se ha obtenido delictivamente.
- No contenga información nueva o significativa (respecto otras comunicaciones anteriores)
- Las vinculadas a reclamaciones sobre conflictos interpersonales o que afecten únicamente al informante y a las personas a las que se refiera la comunicación.
- Recogían informaciones ya disponibles o se trataba de meros rumores.
- Versaban sobre informaciones excluidas del ámbito de aplicación de la ley.

En lo que a protección se refiere, queda prohibida toda represalia contra el informante, incluso la mera tentativa. La relación de represalias incluidas en la Ley es meramente enunciativa (art. 36 L2/2023). El período de protección es de dos años, pero excepcionalmente y de forma justificada, podrá extenderse dicho período. Incluso se prevén medidas de apoyo (información y asesoramiento; asistencia efectiva por las autoridades competentes; apoyo financiero y psicológico, de forma excepcional, si así lo decidiese la A.A.I.; asistencia jurídica gratuita para la representación y defensa en procedimientos judiciales).

Se prevé una cláusula de clemencia para el informante que hubiese participado en la comisión de la infracción administrativa (salvo para infracciones relacionadas con el Derecho de la Competencia, art. 40 L. 2/2023).

11. LA REVELACIÓN PÚBLICA

La ley también otorga protección al informante que hubiera acudido a la opinión pública, lo que se denomina revelación pública en la ley 2/2023, en aquellos casos en que hubiera informado previamente, a través de los cauces internos y externos, sin éxito, o cuando exista una situación de riesgo inminente o manifiesto para el interés público que así lo justifique.

La ley 2/2023 dedica el título V a la revelación pública, definiéndola como “la puesta a disposición del público de información sobre acciones u omisiones en los términos previstos en esta ley”.

Las condiciones para acogerse a protección previstas en la Ley, y recogidas en el artículo 28.1 de esta, 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.

Es importante señalar que la protección no se pierde si posteriormente llega a verificarse que la información facilitada sobre esas presuntas irregularidades era inexacta o que quien la proporcionó se equivocó en cuanto a la importancia del asunto, si ello se debió a un error cometido de buena fe. Tampoco se pierde cuando la amenaza percibida para el interés público no se hubiere materializado finalmente.

Lo determinante es que quien haya dado la voz de alarma sobre la infracción tenga motivos razonables para pensar que la información que facilita es veraz en el momento de hacer la comunicación, aun cuando no hubiera aportado pruebas concluyentes, siendo suficiente con una sospecha razonable.

Tampoco debe olvidarse que la propia norma resulta muy estricta respecto de las denuncias maliciosas, hasta el punto de que prevé que la comunicación o revelación de informaciones falsas, a sabiendas de su falsedad, constituiría una infracción muy grave, que podría sancionarse con multas de hasta 300.000 euros.

A los informantes y a quienes lleven a cabo una revelación pública se les informará de que su identidad será en todo caso reservada, que no se comunicará a las personas a las que se refieren los hechos relatados ni a terceros. La persona a la que se refieran los hechos relatados no será en ningún caso informada de la identidad del informante o de quien haya llevado a cabo la revelación pública.

12. LA PROTECCIÓN DE DATOS PERSONALES EN LOS SISTEMAS DE INFORMACIÓN

La protección de datos personales es un derecho fundamental que tienen todas las personas a que sus datos personales se traten de manera leal y lícita, con un fin concreto y específico, y con su consentimiento.

Los datos personales se regirán, además de por la ley 2/2023 reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción, que en su Título VI recoge la Protección de datos personales, por lo contenido en la normativa:

- Directiva (EU) 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, Capítulo VI-Medidas de Protección.

- Reglamento (UE) 2016/679 (RGPD), 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.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos y garantía de los derechos digitales.
- 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.

De acuerdo con la normativa en protección de datos y la relativa a la protección de los informantes, los datos personales deben de cumplir con los siguientes principios:

- Deben ser tratados de manera lícita, leal y transparente.
- Deben de tener un fin determinado, explícito y legítimo.
- Con fines adecuados, pertinentes y limitados a lo justo y necesario.
- Exactos y actualizados.
- Por un tiempo determinado.
- Se debe garantizar la seguridad y protección adecuada de los datos personales suministrados.

El tratamiento de los datos será lícito cuando el interesado dé su consentimiento o bien el tratamiento resida sobre la base del cumplimiento de una obligación legal, es decir, tratamiento necesario para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluidas la protección y prevención frente a las amenazas contra la seguridad pública, realizado por una autoridad competente en ejercicio de sus funciones.

El responsable de los datos

El órgano de administración u órgano de gobierno de cada entidad u organismo obligado a contar con un Canal de denuncias tendrá la condición de "Responsable del tratamiento de los datos personales".

Qué datos deben recopilarse

Sólo deben recopilarse los datos personales necesarios para la tramitación de la denuncia.

En el momento en el que se recogen los datos personales, el Responsable debe informar al titular de:

- La finalidad del tratamiento de los datos.
- Tipos de datos objeto del tratamiento.
- Base de legitimación del tratamiento.
- Entidades interesadas o parte del proceso.

- Fines de la comunicación de datos.
- Existencia de transferencias internacionales de datos.
- Tiempo de conservación de los datos personales.
- Dirección a la que dirigirse para el ejercicio de derechos.
- Datos del Delegado de Protección de Datos para contacto.

De acuerdo con la normativa vigente, es necesario que el Responsable de los datos personales pueda demostrar que, efectivamente, el interesado consistió el tratamiento de sus datos personales para esos fines específicos, con una clara acción afirmativa.

Como regla general, queda prohibido el tratamiento de los datos personales de categoría especial, recogidos en el art. 9 del RGPD, aunque pueden ser tratados si concurre alguna de las circunstancias siguientes:

- Consentimiento explícito del tratamiento del interesado de dichos datos para uno o más fines especificados en dicho consentimiento.
- Sean necesario para el cumplimiento de una obligación y/o el ejercicio de un derecho, siempre y cuando existan las garantías necesarias y adecuadas para el respeto de los derechos del interesado.
- Para proteger intereses vitales del interesado.
- Los datos personales suministrados por el interesado sean públicos.
- Sean necesario para la formulación, ejercicio o defensa de reclamaciones.
- Por razones de interés público esencial.
- Para fines de medicina preventiva, diagnósticos, entre otros.
- Con fines de interés público como investigaciones científicas o históricas, siempre respetando las garantías y lo establecido en el Derecho.

Además, se les comunicará, de forma expresa, que su identidad será en todo caso reservada y permanecerá anónima para las personas a las que se refieren los hechos relatados o para terceros.

La persona denunciada no será en ningún caso informada de la identidad del informante o de quien haya llevado a cabo la revelación pública.

Quién tiene acceso a los datos

Se limita el acceso a los datos personales en el sistema interno de información a una serie de personas:

- al Responsable del sistema y a quien lo gestione directamente.

- al Responsable de RRHH, 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.
- al Responsable de los servicios jurídicos.
- a los encargados del tratamiento.
- al delegado de protección de datos.

Será lícito el tratamiento de los datos por otras personas, o incluso su comunicación a terceros, cuando resulte necesario para la tramitación de los procedimientos sancionadores o penales. En ningún caso serán objeto de tratamiento los datos personales que no sean necesarios.

Conservación de los datos

Los datos que sean objeto de tratamiento podrán conservarse en el sistema de informaciones únicamente durante el tiempo imprescindible para decidir si iniciar o no la investigación. No obstante, 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.

Revelación de la identidad del informante

La identidad del informante solo puede ser comunicada a las autoridades competentes en el marco de una investigación penal, disciplinaria o sancionadora.

La necesidad de un delegado de protección de datos

Se establece la obligatoriedad de nombrar un Delegado de Protección de Datos para todos los tratamientos derivados del sistema interno de información. Y para el caso de que el tratamiento lo lleve a cabo una autoridad u organismo público, la AAI o autoridad autonómica equivalente, serán las encargadas de nombrarlo.

13. SANCIONES

Las sanciones penales, civiles o administrativas son un mecanismo adicional de protección al Informante, ya que disuaden a las empresas u organizaciones de ejecutar acciones de represalia contra ellos, u obstruir el derecho de los trabajadores a Informar libremente y de forma segura irregularidades ocurridas dentro de la empresa.

Como ya se mencionaba en un apartado anterior, la potestad sancionadora en la ley 2/2023 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.

Tal y como se recoge en la propia Ley, la 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. 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.

Quiénes son Responsables

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 o que hayan votado en contra del acuerdo.

La exigencia de responsabilidades derivada de las infracciones tipificadas en la Ley de Protección del Informante se extenderá a los Responsables incluso aunque haya desaparecido su relación o cesado en su actividad en o con la entidad respectiva.

Qué se considera infracciones muy graves

- Obstrucción al derecho de informar.
- Actos de represalia por acción u omisión.
- Revelación de la identidad del informante.
- Revelación de otras información o datos confidenciales de la investigación.
- Conducta ilegal reincidente. 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.
- Denuncias de mala fe. Comunicar o revelar públicamente información a sabiendas de su falsedad.
- Incumplimiento de la obligación de disponer de un Sistema interno de información en los términos exigidos en la ley 2/2023.

Qué se considera infracciones graves

- Cualquier actuación que suponga limitación de los derechos y garantías previstos en la ley 2/2023 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.
- Vulnerar las garantías de confidencialidad y anonimato previstas en esta ley cuando no tenga la consideración de infracción muy grave.
- Vulnerar el deber de secreto en los supuestos en que no tenga la consideración de infracción muy grave.
- Incumplimiento de la obligación de adoptar las medidas para garantizar la confidencialidad y secreto de las informaciones.
- La comisión de una infracción leve cuando el autor hubiera sido sancionado por dos infracciones leves o graves o muy graves en los dos años anteriores a la comisión de la infracción, contados desde la firmeza de las sanciones.

Qué se considera infracciones leves

- 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.
- Incumplimiento de la obligación de colaboración con la investigación de informaciones.
- Incumplimiento de la obligación de colaboración con la investigación de informaciones.

Prescripción de las infracciones

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.

- Muy graves: prescribirán a los 3 años
- Graves: prescribirán a los 2 años
- Leves: prescribirán a los 6 meses

Sanciones

La comisión de infracciones previstas en la ley llevará aparejada la imposición de las siguientes multas:

PERSONAS FÍSICAS	PERSONAS JURÍDICAS
— una cuantía de 1.001 hasta 10.000 euros por la comisión de infracciones leves ;	— una cuantía hasta 100.000 euros en caso de infracciones leves ,

<ul style="list-style-type: none"> — 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 	<ul style="list-style-type: none"> — entre 100.001 y 600.000 euros en caso de infracciones graves y — entre 600.001 y 1.000.000 euros en caso de infracciones muy graves
---	--

Adicionalmente, en el caso de infracciones muy graves, la Autoridad Independiente de Protección del Informante, podrá acordar:

- La amonestación pública.
- La prohibición de obtener subvenciones u otros beneficios fiscales durante un plazo máximo de cuatro años.
- 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.

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.

Graduación

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

- Reincidencia
- La entidad y persistencia temporal del daño o perjuicio causado.
- La intencionalidad y culpabilidad del autor.
- El resultado económico del ejercicio anterior del infractor.
- La circunstancia de haber procedido a la subsanación del incumplimiento que dio lugar a la infracción por propia iniciativa.
- La reparación de los daños o perjuicios causados.
- La colaboración con la Autoridad Independiente de Protección del Informante, u otras autoridades administrativas.

Concurrencia

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

Prescripción de las sanciones

- Muy graves: prescribirán a los 3 años
- Graves: prescribirán a los 2 años
- Leves: prescribirán al 1 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.

14. FORMACIÓN E INFORMACIÓN A LOS EMPLEADOS Y DIRECTIVOS

El Despacho debe informar y formar a sus empleados y directivos, sobre el Canal de denuncias. Si bien el Canal interno ya estaba implantado con anterioridad y se informaba, con periodicidad anual, en la formación de Compliance, a todos los empleados y directivos acerca de su funcionamiento, así como del Protocolo existente y disponible en la Intranet del Despacho, para toda la organización, se informa ahora acerca de las novedades contenidas en la ley 2/2023, así como de la implantación de un Sistema Integrado de Información, para las irregularidades observadas, no sólo recogidas en la Ley, sino también en los Protocolos descritos en el punto 9 del presente manual. Igualmente, se formará e informará sobre la existencia del Canal externo de denuncias, A.A.I., así como de su utilización y funcionamiento.

La formación específica sobre el canal exigido por la nueva normativa, aunque similar a la que se venía observando en el Canal de Denuncias Interno, tendrá carácter anual y versará sobre:

- La existencia, finalidad y funcionamiento del canal ético o de denuncias y Sistemas Internos de Información.
- La forma de presentación de la denuncia, tramitación y plazos de resolución.
- La información a la persona afectada de la existencia de la denuncia formulada en su contra, respetándose la normativa existente en materia de protección de datos personales.
- Otras cuestiones contenidas en el presente manual.

En la formación, se informará del sistema disciplinario de incumplimientos, remitiendo, como ya venía siendo habitual, al documento disponible en la Intranet, para toda la organización, denominado "Protocolos de conductas prohibidas y catálogo de sanciones de la Firma".

15. EVALUACIONES PERIÓDICAS

Periódicamente, se evaluará el funcionamiento del canal de denuncias, para detectar posibles deficiencias y errores, que deberán subsanarse y analizarse, de manera que los resultados estén alineados con la política de Cumplimiento normativo del Despacho.

Los reportes se incluyen en las auditorías externas anuales de los Estados de Información No Financieros (EINF), siendo también evaluados por los auditores.