Sistema interno de información, canal de información y protección del informante

Regulación, aportaciones y novedades de la Ley 2/2023, de 20 de febrero.

Muñoz de Priego & Pérez
ABOGADOS

Jesús Muñoz de Priego Alvear
ABOGADO
@JMunozdePriego

1. Finalidad de la ley.

- Trasposición de normativa europea. Directiva Europea 2019/1937 del Parlamento Europeo y del Consejo, de 23 de octubre de 2019.
- Protección del informante frente a represalias.
- Fomento de la cultura de información.
- Establecer normas mínimas de los canales de información.

De interés…

Amplía con mucho el ámbito material, de infracciones. No solo infracciones del Derecho de la Unión, sino infracciones penales y administrativas graves y muy graves del ordenamiento jurídico.

2. Ámbito material. ¿Qué se denuncia?

Protección de las personas que denuncien sobre:

- Infracciones de Derecho de la Unión Europea de la Directiva, que afecten a intereses financieros de la UE, que incidan en el mercado (incluidas competencias, ayudas, impuesto de sociedades o ventaja fiscal).
- Acciones u omisiones constitutivas de infracción penal o administrativa grave o muy grave.
- En cualquier caso, infracciones graves o muy graves que supongan quebranto a la Hacienda pública y la Seguridad Social.
- Infracciones de Derecho laboral en materia de seguridad y salud en el trabajo.

Se excluyen (no son objeto de protección):

- Informaciones clasificadas, sujetas a secreto profesional (médicos y abogados), confidencialidad de cuerpos y fuerzas de seguridad, secreto de deliberaciones judiciales.

3. Ámbito personal. ¿Quién denuncia?

Protección a informantes ¿Quiénes son informantes?:

- Empleados públicos.
- Trabajadores por cuenta ajena.
- Autónomos.
- Accionistas, partícipes, personas pertenecientes al órgano de administración, dirección o supervisión de la empresa.
- Cualquier persona que trabaje para contratistas, subcontratistas, proveedores.
- Persona con relación laboral o estatutaria ya finalizada.
- Voluntarios.
- Becarios.
- Trabajadores en formación (con o sin remuneración).
- Personas en proceso de selección o negociación precontractual.

3. Ámbito personal. ¿Quién denuncia?

También se protege:

- Representantes legales del informante.
- Asesores del informante.
- Asistentes en el proceso al informante.
- Personas relacionadas, como compañeros de trabajo o familia
- Personas jurídicas para quien trabaje el informante, mantenga relación, o tenga una participación significativa o de influencia (en cuanto a capital o voto).

<u>De interés…</u>

No solo se protege al informante, si no también asesores y personas físicas y jurídicas vinculadas que pudieran sufrir represalias.

4. Formas de denuncia:

- Sistema interno de información con su canal de información (“denuncia”) interno.

- Canal de “denuncia” externo de información de la Autoridad Independiente de Protección del Informante (AAI) y CCAA

- Revelación pública (puesta a disposición del público).

5. Obligados al Sistema interno de información en sector privado..

<u>Personas físicas o jurídicas con 50 o más trabajadores</u>.

Las personas jurídicas que entren en el ámbito de aplicación de actos de la UE de la Directiva (servicios, productos, mercados financieros, prevención blanqueo de capitales o financiación del terrorismo, seguridad del transporte, medio ambiente).

Partidos políticos, sindicatos, organizaciones empresariales y fundaciones creadas por uno u otro que reciban fondos públicos.

<u>De interés…</u>
Las personas jurídicas no obligadas podrán también tener Sistema interno de información, en cuyo caso deberán cumplir los requisitos de la ley.

6. Sistema interno de información.

Es el cauce preferente de información.

Responsable de implantación: Órgano de administración o gobierno de la entidad

Consulta previa con la representación de los trabajadores.

De interés…

A la representación de los trabajadores solo es una consulta previa. Pueden realizar informe, que no es vinculante.
La norma no recoge cómo debe procederse si la entidad no tiene representación de los trabajadores, o no la tiene en todos sus centros de trabajo. Hay quien sugiere actuar como en la regulación de los planes de igualdad con los sindicatos más representativos…

6. Sistema interno de información.

Características del Sistema interno de información (1):

- Permitir a todos los informantes comunicar todas las infracciones.
- Seguridad, que garantice confidencialidad de la identidad del informante y de cualquier tercero que se mencione, de las actuaciones que se desarrollen y la protección de datos.
- Permitir comunicaciones por escrito y verbalmente.
- Integrar los distintos canales internos de información.
- Garantizar tratamiento efectivo. Que el primero en conocer la irregularidad sea la entidad.

De interés…

Aunque habla de comunicaciones por escrito o verbalmente o de ambos modos, el resto de la regulación y el fin de la norma parece que debe optarse por ambos modos y ampliación de medios.

6. Sistema interno de información.

Características del Sistema Interno de Información (2):

- Ser independiente y diferenciado. Propio de la entidad y distinto.
- Contar con un responsable del sistema.
- Contar con una política con principios generales debidamente publicitada.

<u>De interés…</u>

- No deben compartirse sistemas de información, aunque en empresas de entre 50 y 249 trabajadores podrán compartirse Sistema interno de información (de gestión interna o externa) y recursos. A tener en cuenta en caso colegios, instituciones, fundaciones, asociaciones con distinto CIF pero vinculados institucional o carismáticamente.
- El responsable deberá ser directivo, salvo compliance officer en programa de cumplimiento ya en funcionamiento.
- Los documentos de política institucional en que se recogen los principios, valores y opciones, son, como en todo este tipo de documento, el primer paso.

6. Sistema interno de información.

Características del Sistema interno de información (y 3):

- Contar con un procedimiento de gestión de las informaciones.
- Establecer garantías de protección del informante.

Posibilidad de gestión externa del Sistema interno de información.

- En todo caso, el responsable será el órgano de gobierno.
- Exigirá, en todo caso, garantías de independencia. Confidencialidad, protección de datos y secreto de las comunicaciones.
- El tercero externo tendrá la consideración de encargado de protección de datos.

De interés…

El Canal interno de información es solo parte del Sistema interno de información, que debe recoger todos estos aspectos y documentarse, publicitarse,…

6. Sistema interno de información.

Responsable del Sistema Interno de Información.

- El órgano de administración o gobierno debe designar una persona física responsable del Sistema, que deberá ser un directivo.
- En caso de designar un órgano colegiado, este deberá delegar en uno de sus miembros la facultades de gestión del sistema, que deberá ser un directivo.
- El nombramiento y cese, con justificación del mismo, de la persona física o colegiada responsable del sistema deberá ser comunicado a la Autoridad estatal (AAI) o de las CCAA, en el plazo de diez días hábiles.
- Deberá actuar de forma independiente y autónoma al resto de órganos de la entidad, sin recibir instrucciones y con disposición de medios y recursos personales y materiales.

De interés…

En caso de tener ya un responsable de cumplimiento normativo podrá ser la persona responsable del sistema (parece que aunque no sea directivo)

7. Procedimiento de gestión de informaciones. Protocolo.

Será aprobado por el órgano de gobierno o administración y tramitado de forma diligente por el responsable del Sistema.

Contenido mínimo (1):

- Identificación de Canal Interno de Información.
- Información sobre los canales externos.
- Acuse de recibo de la comunicación del informante en siete días naturales, salvo riesgo de la confidencialidad.

<u>De interés…</u>

- Los sistemas informáticos actuales permiten acuse de recibo aún en comunicaciones anónimas no vinculadas a IP.

7. Procedimiento de gestión de informaciones. Protocolo.

Contenido mínimo (2):

- Plazo máximo de respuesta de tres meses (desde recepción o desde los siete días si no hubo acuse), ampliable hasta otros tres meses en caso de especial complejidad.
- Previsión de posibilidad de mantener comunicación con informante o de solicitarle información adicional.
- Garantía de confidencialidad de llegar por otros canales o por otras personas no responsables, a las que se les formará y advertirá de la obligación de remisión necesaria y consideración de infracción grave en caso de quebranto de la confidencialidad.

De interés…

- Debe informarse y formarse al personal de la entidad, no responsable, en caso de ser receptor de una información.

7. Procedimiento de gestión de informaciones. Protocolo.

Contenido mínimo (y 3):

- Establecimiento del derecho de la persona afectada (denunciada) a recibir información de acciones u omisiones que se le atribuyen y a ser oída en el momento adecuado.
- Respeto a la presunción de inocencia y al honor de las personas afectadas.
- Respeto a normativa de protección de datos.
- Remisión al Ministerio Fiscal con carácter inmediato cuando los hechos puedan ser constitutivos de delitos, o a la Fiscalía Europea en caso de afectación de intereses financieros de la UE.

8. Canal Interno de Información.

Forma parte del Sistema Interno de Información.

Debe dársele publicidad a su existencia y a los principios del procedimiento

Debe permitir realizar comunicaciones por escrito, o verbalmente, o de ambas formas. Correo postal, medio electrónico, teléfono, mensajería de voz y reunión presencial (en 7 días máximo desde su petición).

<u>De interés…</u>

- En caso de contar con página web la información (existencia del canal, principios, garantías y protección, procedimiento,…) debe constar en la página de inicio, en sección separada y fácilmente identificable.
- Entendemos que el listado de medios de comunicación no es un mínimo ni un máximo, aunque deberían, en la práctica habilitarse al menos todos los mencionados.
- Cabría además buzón físico, correo electrónico,…
- En caso de petición de entrevista física, debe recordarse el plazo máximo para fijarla de 7 días.

8. Canal Interno de Información.

En caso de comunicación verbal o física deberá ser grabada (formato seguro, duradero y accesible), previa información de ello al informante, o trascrita de forma completa y exacta, que podrá comprobar, rectificar y firmar.

A quienes utilicen el canal interno se les debe informar de forma clara y accesible de la existencia de canales externos ante las autoridades competentes (AAI, CCAA,…).

El informante podrá indicar domicilio, correo electrónico o lugar seguro para recibir notificaciones, o no, porque puede ser comunicación anónima.

<u>De interés…</u>
En caso de existir previamente un canal ético o de denuncia, deberá revisarse para cumplir todos los requisitos que prevé la ley.

8. Canal Interno de Información.

Se permite, por tanto, comunicación anónima.

El Canal interno puede incluir cualquier otra información ajena al ámbito material de la ley, pero esas quedan fuera del ámbito de protección de la ley.

9. Procedimiento de actuación.

No se establece en los Sistemas internos de información, pero al regular el canal externo de la AAI, regula:

- Recepción de informaciones.
- Trámite de admisión.
- Instrucción.
- Terminación de las actuaciones.
- Derechos y garantías del informante.
- Publicación y revisión del procedimiento de gestión de informaciones.

<u>De interés…</u>

- Pueden servir de base para la regulación del Sistema interno y del Canal interno.
- Incluye elementos como comunicar al informante la admisión y la inadmisión, información de derechos al afectado y trámite de audiencia, en ningún caso comunicación al investigado de identidad del informante, posibilidad de ser asistido por abogado

10. Registro en el Sistema de Información.

Necesidad de un libro-registro de las informaciones y las investigaciones.

Garantizando confidencialidad (solo será accesible bajo petición razonada de autoridad judicial en procedimiento).

Los datos personales solo se conservarán el periodo necesario y nunca más de diez años.

No se regula en el Sistema de información interno, pero en el externo se recoge (posible aplicación por analogía):

- El sistema de gestión de información le asignará un código de identificación.
- Estará contenido en una base de datos segura y de acceso restringido.
- Se registrarán todas las comunicaciones recibidas.
- Se registran con los siguientes datos: fecha de recepción, código de identificación, actuaciones desarrolladas, medidas adoptadas, fecha de cierre.

11. Tratamiento particular de protección de datos.

El acceso a los datos personales contenidos en el Sistema interno queda limitado a:

- Responsable del Sistema y quien lo gestione.
- Responsable de aplicar régimen sancionador en caso de proceder medidas disciplinarias.
- Responsable de servicios jurídicos, si procedieran medidas legales.
- Encargados de tratamiento de datos que se designen.
- Delegado de protección de datos.

Solo cabe tratamiento o comunicación a terceros en caso de ser necesario para medidas correctoras o procedimientos sancionadores o penales.

De interés…

Si la información no es veraz, o han trascurridos tres meses desde la recepción sin investigación, deberá suprimirse, quedando solo de forma anonimizada.

12. Garantía de confidencialidad.

Confidencialidad.

Al informante se le informará de forma expresa de que su identidad será reservada y que no se comunicará a afectados ni terceros.

Solo podrá ser comunicada a autoridad judicial, Ministerio fiscal o autoridad administrativa competente, en el marco de una investigación penal, disciplinaria o sancionadora.

En dicho caso, se informará previamente al informante, salvo riesgo de comprometer la investigación o el procedimiento judicial.

13. Medidas de protección.

Condiciones para la protección:

- Veracidad en el momento de la comunicación, aunque no haya pruebas concluyentes.
- Que la información entre en el ámbito material de infracciones de la ley.
- Cumplimiento de los requerimientos de la ley.
- Encargados de tratamiento de datos que se designen.

Se excluyen: comunicaciones inadmitidas, informaciones de conflictos exclusivamente interpersonales, informaciones ya disponibles al público o rumores, informaciones que no entren en el ámbito material de infracciones de la ley.

13. Medidas de protección

1. Prohibición de represalias.

- “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”.
- Como: suspensión del contrato, despido, extinción de relación laboral, no renovación de contrato, terminación anticipada de trabajo temporal tras periodo de prueba, terminación anticipada contrato prestación de servicios, imposición de medidas disciplinarias, degradación, denegación de ascensos, modificación sustancial de las condiciones de contrato, no conversión de contrato temporal a indefinido, daño, daño reputacional, pérdidas económicas, coacciones, intimidaciones, acoso, ostracismo, evaluación o referencias negativas, inclusión en listas negras, denegación de licencia o permiso, denegación de formación, discriminación, trato desfavorable o injusto.

13. Medidas de protección

1. Prohibición de represalias.

- Durante dos años, que podrán extenderse (de forma excepcional y justificada).

<u>De interés…</u>

- Cuidado con los efectos perversos de la norma, pues puede blindar a un trabajador.
- Si hay perjuicio se presumirá que es por represalia.

13. Medidas de protección

2. Medidas de apoyo.

- Información y asesoramiento gratuito sobre procedimientos, recursos, protección frente a represalias y derechos de la persona afectada.
- Asistencia efectiva de autoridad competente ante cualquier autoridad implicada en protección frente a represalias.
- Asistencia jurídica en procesos penales y civiles transfronterizos.
- Apoyo financiero y psicológico, de forma excepcional.

13. Medidas de protección

3. Medidas de protección frente a represalias.

- No se considerará que el informante infringe restricción de revelación de información reservada u obligación de sigilo; ni en responsabilidad por adquisición de la información, salvo en caso de acceso por delito; ni en responsabilidad por la información en procesos judiciales por difamación, violación de derechos de autor, vulneración de secretos, infracción de normas de protección de datos, revelación de secretos empresariales, solicitudes de indemnización por derecho laboral o estatutario
- En caso de perjuicio del informante se presumirá que es represalia (presunción iuris tantum).

13. Medidas de protección

4. Medidas de protección a personas afectadas.

Presunción de inocencia, derecho a la defensa, derecho de acceso al expediente, preservación de identidad y confidencialidad de hechos y datos del procedimiento.

5. Programa de clemencia en infracciones administrativas (exención y atenuación de la sanción).

Exención si el informante ha participado en la comisión de infracción administrativa; se ha informado antes de incoación de procedimiento investigador o sancionador; haya cesado en la comisión de la infracción; identificado al resto de personas participantes; ha cooperado plena, continua y diligentemente; ha facilitado información veraz y relevante, ha procedido a reparar el daño causado. Si solo parcialmente, atenuación.

14. Régimen sancionador.

Infracciones muy graves (1).

- Limitación de derechos y garantías previstos en la ley, por contratos, acuerdos o cualquier intento de obstaculizar la presentación de comunicaciones o de impedir, frustrar o ralentizar su seguimiento.
- La adopción de represalias.
- Vulnerar garantías de confidencialidad y anonimato, o cualquier acción para revelar la identidad del informante, aunque no se llegue a conseguir.
- Vulnerar el mantener secreto sobre la información.
- La comisión de infracción grave, cuando ya se hubiese sido sancionado por resolución firme por dos infracciones graves o muy graves en los dos años anteriores, a contar desde la firmeza de esas sanciones.

14. Régimen sancionador.

Infracciones muy graves (y 2).

- Comunicar o desvelar información a sabiendas de su falsedad.
- Incumplimiento de la obligación de disponer de un Sistema interno de información.

De interés…

No disponer de un Sistema interno de información acorde a la ley, en entidades de 50 o más trabajadores, puede ser infracción muy grave y alcanzar la sanción de un millón de euros

14. Régimen sancionador.

Prescripción de infracción muy grave a los tres años, a contar desde que se comete la infracción o del último acto de ser continuada. La prescripción se interrumpe por la iniciación, con conocimiento del interesado del procedimiento sancionador, reanudándose si el expediente permanece paralizado durante tres meses por causas no imputables al afectado.

Sanciones (1):

- Personas físicas: de 30.001 a 300.000 €.

- Personas jurídicas: de 600.001 a 1.000.000 €

14. Régimen sancionador.

Sanciones (y 2):

- Adicionalmente: Amonestación pública, prohibición de obtener subvenciones u otros beneficios fiscales durante un plazo máximo de cuatro años; prohibición de contratar con sector público durante un plazo máximo de tres años; si superan los 600.001 podrán ser publicadas en BOE.

Prescripción de las sanciones muy graves: 3 años, desde el día siguiente a que fuera ejecutable la sanción. La prescripción se interrumpe por la iniciación, con conocimiento del interesado, del procedimiento de ejecución, reanudándose si permanece paralizado durante más de un mes por causas no imputables al afectado.

14. Régimen sancionador.

Infracciones graves.

- Limitación de derechos y garantías previstos en la ley o cualquier intento de obstaculizar la presentación de comunicaciones o de impedir, frustrar o ralentizar su seguimiento, que no sean infracciones muy graves.
- Vulnerar garantías de confidencialidad y anonimato, cuando no tengan la consideración de muy grave.
- Vulnerar el deber de secreto, cuando no tenga la consideración de infracción muy grave.
- Incumplimiento de obligación de adoptar medidas para garantizar confidencialidad y secreto de las informaciones.
- La comisión de infracción leve, cuando ya se hubiese sido sancionado por dos infracciones leves, graves o muy graves en los dos años anteriores, a contar desde la firmeza de esas sanciones.

14. Régimen sancionador.

Prescripción de infracción grave a los dos años, a contar desde que se comete la infracción o del último acto de ser continuada. La prescripción se interrumpe por la iniciación, con conocimiento del interesado del procedimiento sancionador, reanudándose si el expediente permanece paralizado durante tres meses por causas no imputables al afectado.

Sanciones:

- Personas físicas: de 10.001 a 30.000 €.

- Personas jurídicas: de 100.001 a 600.000 €

Prescripción de las sanciones graves: 2 años, desde el día siguiente a que fuera ejecutable la sanción. La prescripción se interrumpe por la iniciación, con conocimiento del interesado, del procedimiento de ejecución, reanudándose si permanece paralizado durante más de un mes por causas no imputables al afectado.

14. Régimen sancionador.

Infracciones leves.

- Remisión de información incompleta por el responsable del Sistema, de forma deliberada, o fuera de plazo.
- Incumplimiento de la obligación de colaboración en la investigación.
- Incumplimiento de obligaciones previstas en la ley que no estén fijadas como muy grave o grave.

Prescripción de infracción leve a los seis meses, a contar desde que se comete la infracción o del último acto de ser continuada. La prescripción se interrumpe por la iniciación, con conocimiento del interesado del procedimiento sancionador, reanudándose si el expediente permanece paralizado durante tres meses por causas no imputables al afectado.

14. Régimen sancionador.

Sanciones:

- Personas físicas: de 1.001 a 10.000 €.

- Personas jurídicas: de hasta 100.000 €

Prescripción de las sanciones leves: 1 año, desde el día siguiente a que fuera ejecutable la sanción. La prescripción se interrumpe por la iniciación, con conocimiento del interesado, del procedimiento de ejecución, reanudándose si permanece paralizado durante más de un mes por causas no imputables al afectado.

14. Régimen sancionador.

Gradación de sanciones: reincidencia, entidad y persistencia del daño, intencionalidad o culpabilidad, resultado económico del ejercicio anterior de infractor, , haber o no subsanado el incumplimiento por propia iniciativa, reparación de daños, colaboración con autoridades.

15. Plazo máximo de implantación de Sistema interno de información o adaptación de los existentes.

- En general: tres meses desde la entrada en vigor de la ley (13 de junio de 2023).

- Entidades con 250 trabajadores o menos: hasta el 1 de diciembre de 2023.

<u>De interés…</u>

- Entidades de 50 o más trabajadores y hasta 250, hasta el 31 de diciembre de 2023.

- Entidades no obligadas, pero que tengan canal de denuncia, consideramos que también.