

Título:**LEY REGULADORA DE LA PROTECCIÓN DE LAS PERSONAS QUE
INFORMEN SOBRE INFRACCIONES NORMATIVAS Y
DE LUCHA CONTRA LA CORRUPCIÓN****Contenido:**

Adjunto se remite la **Ley 2/2023, de 20 de febrero, reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción**. Esta Ley transpone al ordenamiento jurídico español la conocida como Directiva de “*Whistleblowing*” y su objetivo es reforzar la cultura de cumplimiento de las entidades públicas y privadas mediante la protección de los denunciantes que informen sobre infracciones conocidas en el contexto laboral o profesional.

Esta normativa obliga a las entidades del sector privado y del sector público con **50 o más empleados** a implementar “sistemas internos de información” (canales de denuncia) que deben cumplir diversos requisitos y garantías.

De la presente Ley se destacan los siguientes aspectos:

1. OBJETO

El **objeto** de esta Ley es otorgar una protección adecuada frente a las represalias que puedan sufrir las personas físicas que informen sobre alguna de las acciones u omisiones a que se refiere su ámbito de aplicación, a través de los procedimientos previstos en la misma, así como el fortalecimiento de la cultura de la información, de las infraestructuras de integridad de las organizaciones y el fomento de la cultura de la información o comunicación como mecanismo para prevenir y detectar amenazas al interés público.

2. ÁMBITO DE APLICACIÓN

El **ámbito objetivo de aplicación** es:

- Infracciones del Derecho de la Unión Europea cuando:
 - a. Afecten a alguna de las materias señaladas en el Anexo I de la Directiva de Whistleblowing (Se adjunta)
 - b. Afecten a los intereses financieros de la Unión.
 - c. Incidan en el mercado interior.
- Infracciones administrativas graves o muy graves.
- Hechos delictivos.

Contenido:

Las comunicaciones pueden referirse a hechos conocidos en el ámbito de una relación laboral o profesional todavía en vigor, ya finalizada o incluso no iniciada (por ejemplo, si se refiere a infracciones relativas a procesos de selección o de negociación precontractual).

El **ámbito subjetivo de aplicación** viene referido a cualquier persona que en un contexto laboral o profesional haya obtenido información sobre presuntas infracciones, ya sea en el sector público o en el privado. La protección no se circunscribe a los empleados de los sujetos obligados, sino también a cualquier otra persona que, en el ejercicio profesional o en el marco de la prestación de servicios, haya interactuado con dichos sujetos.

La Ley 2/2023 incluye el siguiente **listado no exhaustivo**:

- empleados públicos.
- trabajadores por cuenta ajena.
- autónomos.
- accionistas, miembros del órgano de administración, dirección o supervisión de una entidad.
- voluntarios, becarios y trabajadores en períodos de formación.
- cualquier persona que trabaje para contratistas, subcontratistas y proveedores.

3. PROTECCIÓN AL DENUNCIANTE

El alcance de la protección se extiende a las personas relacionadas con el informante (compañeros de trabajo, familiares, personas jurídicas para las que trabaje o de las que sea titular, etc.). Asimismo, se extenderá a toda persona física que haya asistido al informante y, específicamente, a los representantes legales de los trabajadores en el ejercicio de sus funciones de asesoramiento y apoyo al informante

4. IMPLEMENTACIÓN DE UN SISTEMA INTERNO DE INFORMACIÓN

La implementación de un sistema interno de información obliga en el:

1. Ámbito público:

- Administraciones estatales, autonómicas y locales, así como sus organismos o entidades dependientes.
- Autoridades administrativas independientes (Banco de España, Seguridad Social, etc.). Universidades públicas.
- Corporaciones de Derecho Público.
- Fundaciones del sector público.
- Sociedades mercantiles participadas mayoritariamente por alguna de las entidades enumeradas anteriormente.
- Órganos constitucionales, de relevancia constitucional o análogos autonómicos.

Contenido:

2. **Ámbito privado:**

- Personas físicas o jurídicas que tengan contratados a 50 o más trabajadores.
- Personas jurídicas que entren en el ámbito de aplicación del Derecho comunitario en materia de servicios, productos y mercados financieros, prevención del blanqueo de capitales y financiación del terrorismo, seguridad del transporte o protección del medio ambiente.
- Partidos políticos, sindicatos, así como las organizaciones empresariales y fundaciones creadas por ellos que reciban fondos públicos.

En los **grupos de empresas**, la sociedad dominante aprobará una política general relativa al sistema interno de información y a la defensa del informante y se asegurará de la aplicación de sus principios por todas las sociedades que conformen el grupo, sin perjuicio de la independencia y autonomía de cada sociedad en función del sistema de gobierno corporativo del grupo del que se trate y de las modificaciones o adaptaciones que fueran necesarias para el cumplimiento de la normativa que les resulte aplicable. **Las entidades entre 50 y 249 trabajadores** podrán compartir entre sí el sistema interno de información y los recursos destinados a la tramitación de las comunicaciones, respetando en todo caso las garantías previstas en la ley.

5. **PLAZO DE IMPLEMENTACIÓN**

El **plazo máximo de implementación** de sistema interno de información será de 3 meses a partir de la entrada en vigor de la ley, hasta el **13 de junio de 2023**. Excepcionalmente, para **las entidades con menos de 250 empleados**, se amplía este plazo **hasta el 1 de diciembre de 2023** para cumplir con la normativa.

6. **RESPONSABLE DE LA IMPLEMENTACION DEL SISTEMA INTERNO DE INFORMACIÓN**

El responsable de la implementación del sistema será el **órgano de administración** o de gobierno de cada entidad, que deberá seguir un trámite de consulta con los representantes legales de los trabajadores a tal efecto y tendrá la condición de responsable del tratamiento de los datos personales del sistema interno de información. En lo que respecta a la gestión del sistema y la tramitación de las comunicaciones, las entidades deberán contar con un responsable del sistema interno de información (podrá recaer en una única persona o un **órgano colegiado** designado a tal efecto por el órgano de administración) que deberá cumplir los una serie de requisitos marcados en la normativa.

7. **REQUISITOS DEL SISTEMA DEL SISTEMA INTERNO DE INFORMACIÓN**

El sistema interno de información constituirá el **cauce preferente para la comunicación y tramitación de denuncias** (frente al canal externo o la revelación pública).

Contenido:

Los principios esenciales del sistema interno de información pueden sintetizarse en los siguientes:

- Garantía de confidencialidad de la identidad del informante y de cualquier tercero mencionado, así como del tratamiento de la información y su investigación.
- Garantías frente a la adopción de represalias.
- Respeto al principio de presunción de inocencia y derecho de defensa de las partes afectadas.
- Garantía de independencia, imparcialidad y ausencia de conflictos de interés.
- Tramitación efectiva de las comunicaciones.

Asimismo, esta Ley exige a los sujetos obligados la integración de todos los canales internos operativos en la entidad para la denuncia de posibles infracciones (tales como, por ejemplo, canales de prevención del acoso, de la prevención de delitos o infracciones del código ético de la entidad, etc.). Adicionalmente, las entidades estarán obligadas a disponer de una política que enuncie los principios generales del sistema y un procedimiento de gestión de comunicaciones, que deberá ser aprobado por el órgano de administración o de gobierno y de cuya efectiva implementación responderá el responsable del sistema interno de información.

El sistema de información contará con **un canal interno para la gestión de las comunicaciones**, con la posibilidad de externalizarlo a través de un tercero, que deberá ofrecer garantías adecuadas de respeto de la independencia, la confidencialidad, la protección de datos y el secreto de las comunicaciones, y que tendrá la consideración de encargado del tratamiento a efectos de la legislación sobre protección de datos personales. En todo caso, la gestión por un tercero externo no podrá suponer un traslado de las obligaciones atribuidas al responsable del sistema en persona distinta.

El canal interno de información deberá permitir la presentación de **denuncias anónimas**, cuestión que la Directiva de *Whistleblowing* había dejado a elección de cada uno de los Estados miembros.

8. RÉGIMEN DE PUBLICIDAD Y REGISTRO

La norma establece, entre otros, determinados **plazos que deben cumplirse en materia de publicidad y registro**:

- En caso de que el informante solicite mantener una **reunión presencial**, la entidad deberá fijarla dentro del plazo máximo de siete días desde la formulación de la petición. Tras la recepción de la comunicación, la entidad deberá enviar acuse de recibo al informante en el plazo máximo de siete días.
- El plazo máximo para dar respuesta a las **actuaciones de investigación** se establece en tres meses a partir del vencimiento del plazo de siete días después de efectuarse la

Contenido:

comunicación, salvo casos de especial complejidad que requirieran una ampliación del plazo, en cuyo caso este podrá extenderse hasta un máximo de otros tres meses adicionales.

- El plazo de **conservación y eliminación de datos personales** están en línea con los previstos hasta ahora en la normativa previa de protección de datos. En particular, se establece que las comunicaciones podrán 7 mantenerse dentro del sistema de información únicamente durante el tiempo imprescindible para decidir sobre si procede o no iniciar una investigación. Si esta decisión no se adoptara en un plazo de tres meses, deberá suprimirse del sistema la comunicación, salvo con el fin de mantener evidencia del funcionamiento del sistema y de forma anonimizada si fueran comunicaciones no cursadas.

9. PROHIBICIÓN DE REPRESARIAS

La norma ofrece una **enunciación amplia** sobre qué puede entenderse por represalia:

- Suspensión del contrato de trabajo, despido o extinción de la relación.
- Anulación de contratos de bienes o servicios.
- Imposición de cualquier medida disciplinaria.
- Degradación o denegación de ascensos o modificación sustancial de las condiciones de trabajo.
- Daños económicos o reputacionales.
- Evaluación negativa del desempeño profesional.
- Inclusión en listas negras.
- Denegación de formación.
- Trato desfavorable o injusto.

Además, siempre que **el informante actúe de buena fe**, esto es, sin incurrir en falsedades o tergiversaciones de los hechos, **la protección se extenderá también a:**

- Personas físicas que, en el marco de la organización en la que preste servicios el informante, asistan al mismo en el proceso.
- Personas físicas que estén relacionadas con el informante y que puedan sufrir represalias, como compañeros de trabajo o familiares del informante.
- Personas jurídicas, para las que trabaje el informante o con las que mantenga cualquier otro tipo de relación en un contexto laboral u ostente una participación significativa.

Asimismo, se establecen otras medidas de protección de diversa naturaleza, incluyendo de tipo asistencial (asesoramiento e información, asistencia jurídica, apoyo financiero, apoyo psicológico, etc.), a cargo de la **Autoridad Independiente de Protección**.

Contenido:

10. TRATAMIENTO DE DATOS PERSONALES

La Ley regula de pormenorizadamente cómo deben tratarse los **datos personales de los informantes y demás personas involucradas** en una comunicación e investigación posterior y deroga expresamente la regulación previa de esta materia contenida en la normativa de protección de datos.

11. SANCIONES

En caso de **incumplimiento o implementación deficiente de los sistemas de información**, las entidades podrían enfrentarse a sanciones que, en caso de infracciones muy graves, podrían alcanzar:

- Multas de hasta 1.000.000 de euros para las personas jurídicas y 300.000 euros para las personas físicas.
- Amonestaciones públicas.
- Prohibición de obtener subvenciones u otros beneficios fiscales durante un plazo de 4 años.
- **Prohibición de contratar con el sector público durante un plazo de 3 años.**

Las sanciones por infracciones muy graves de cuantía igual o superior a 600.001 euros impuestas a personas jurídicas **podrían ser publicadas en el Boletín Oficial del Estado** tras la firmeza de la resolución en vía administrativa. Asimismo, y puesto que la norma recoge una serie de reglas específicas en materia de protección de datos personales, el incumplimiento de estas podría dar lugar a sanciones administrativas bajo el Reglamento General de Protección de Datos.

La presente Ley **entrará en vigor el próximo 13 de marzo de 2023**, a los veinte días de su publicación en el Boletín Oficial del Estado.

Madrid, 28 de febrero de 2023

Fdo.: Mariano Sanz Lorient
Secretario General