Índice

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,** transpone la Directiva (UE) 2019/1937 (*whistleblowing*), convirtiendo en obligatorio el **"canal de denuncias"** para todas las entidades del sector público, incluidas todas las entidades locales, con independencia del tamaño; así como para las entidades jurídicas del sector privado que empleen a 50 o más trabajadores; y partidos políticos, sindicatos, patronales y fundaciones creadas por unos y otros, siempre que reciban o gestionen fondos públicos.

¿Qué pasa si no cumplo?

> *Las empresas obligadas a contar con un **canal denuncias** que no lo implanten conforme a la Ley 2/23, se exponen a multas de **600.001** a **1 millón** de euros*

La norma contempla un detallado régimen sancionador necesario para combatir con eficacia las acciones u omisiones que limiten los derechos y garantías introducidos por la Ley 2/23.

El procedimiento sancionador contempla **multas** que oscilan entre los 1.001 y los 300.000 euros, en el caso de personas físicas; y los 100.000 y el millón de euros, en el caso de las personas jurídicas.

Además en el caso de **infracciones muy graves** no podrás acceder a **subvenciones** o **beneficios fiscales** durante un plazo de 4 años ni **contratar con el sector público** durante un plazo de 3 años.

¿Qué pasa si pongo una "denuncia falsa"?

Hay que tener en cuenta que las "**denuncias falsas**" , consistentes en comunicar o revelar públicamente información a sabiendas de su falsedad, se consideran infracciones muy graves, con multa de 30.001 hasta 300.000 euros para personas físicas, y entre 600.001 y 1.000.000 de euros para personas jurídicas.

¿Quién está obligado?

Sujetos obligados a contar con un sistema interno de información (arts. 10 y 13 L 2/23)

- **Ámbito privado: todas las empresas** (personas físicas o jurídicas) que tengan contratados **50 o más trabajadores**. Además, con independencia del número de empleados, están obligados los partidos políticos, los sindicatos, las organizaciones empresariales y las fundaciones creadas por unos y otros, siempre que reciban o gestionen fondos públicos. Y también las empresas dedicadas a servicios, productos y mercados financieros, prevención del blanqueo de capitales o de la financiación del terrorismo, seguridad del transporte y protección del medio ambiente.
- **Sector público:** están obligadas todas las entidades que lo integran, si bien se permite que, por cuestiones de eficiencia, los municipios de menos de 10.000 habitantes lo compartan entre sí o con cualesquiera otras Administraciones públicas que se ubiquen dentro del territorio de la comunidad autónoma.

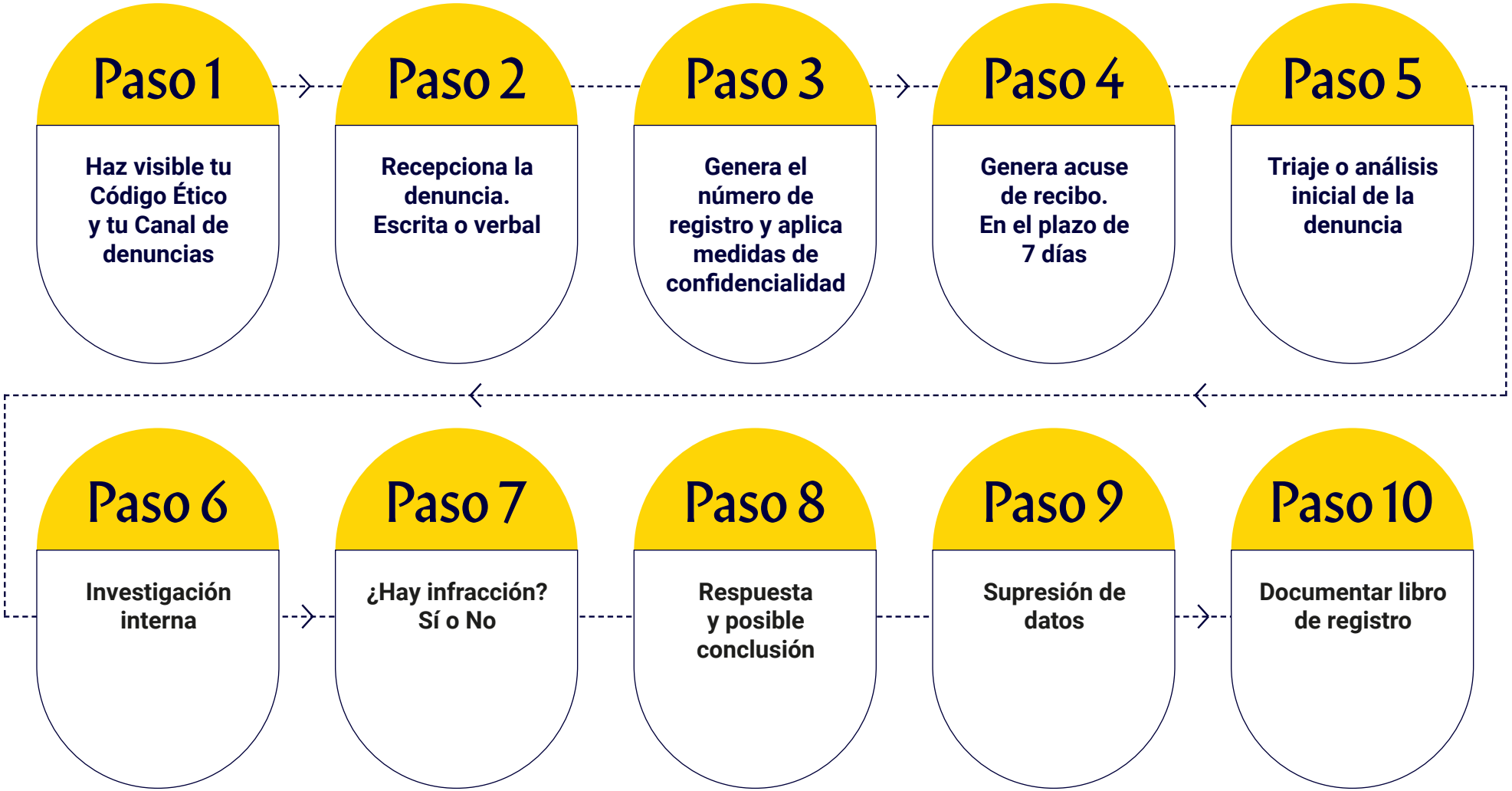
¿Cómo deben ser los sistemas de información y canales internos?

> *Es importante que el canal ofrezca la posibilidad de informar a los denunciantes sobre el estado de su denuncia y sobre los pasos dados*

Requisitos del sistema de información y canal/es interno/s (arts. 4 a 9 L 2/23)

- **Responsable del sistema**: debe ser designado por el órgano de administración u órgano de gobierno de cada entidad u organismo obligado, previa consulta con la representación legal de las personas trabajadoras. Su nombramiento debe notificarse a la AAI. Tiene la condición de responsable del tratamiento de los datos personales.
- Debe estar diseñado, establecido y gestionado de forma **segura**, garantizando la **confidencialidad** de la identidad del informante y de cualquier tercero mencionado en la comunicación, y de las actuaciones que se desarrollen en la gestión y tramitación de la misma, así como la **protección de datos**, impidiendo el acceso de personal no autorizado.
- Debe integrar los distintos canales internos de información que puedan establecerse dentro de la entidad.
- Debe contar con una política o estrategia que enuncie los principios generales en materia de Sistemas interno de información y defensa del informante y que sea debidamente publicitada en el seno de la entidad u organismo (**Código ético**).
- Debe contar con un **procedimiento de gestión** de las informaciones recibidas.
- Debe establecer las garantías para la protección de los informantes en el ámbito de la propia entidad u organismo.
- La gestión del Sistema interno de información se podrá llevar a cabo dentro de la propia entidad u organismo o acudiendo a un tercero externo.

El procedimiento de gestión de las informaciones o denuncias en 10 pasos



Esquema en 10 pasos. **Procedimiento de gestión de las informaciones o denuncias**

Paso 1 Haz visible tu Código Ético y tu Canal de denuncias

- ✓ La organización debe proporcionar, de manera accesible y visible, información sobre su Código Ético y sobre el Canal de denuncias (para qué es, cómo funciona, cómo es el proceso) [arts. 5.2.h) e i) y 9 L 2/23] [4.4.a) y 5.2 ISO 37002]
- ✓ La **información sobre el uso de todo canal interno** se debe ofrecer de manera adecuada, de **forma clara y fácilmente accesible**, incluyendo los principios esenciales del procedimiento de gestión. En caso de contar con una **página web**, dicha información deberá constar en la **página de inicio**, en una **sección separada y fácilmente identificable** (art. 25 L 2/23)

Cabe la **gestión por tercero externo** (arts. 6 y 15 L 2/23) así como reglas para **compartir medios** (arts. 12 y 14 L 2/23)

En el ámbito privado, cabe la **delegación de funciones** del responsable del sistema (art. 8.3 L 2/23) (5.3.3 ISO 37002)

La organización puede decidir (Apdo. 4.3 ISO 37002):

- ✓ Ámbito geográfico
- ✓ Si caben solo denuncias o se usa el canal también para consultas o quejas
- ✓ Si caben denuncias solo internas o también externas, y en ese caso, de quién (cualquiera / solo proveedores/ clientes/otros).

Posibles campos del formulario de "denuncia" (art. 2 L 2/23) (8.2 ISO 37002)

- ✓ Datos del denunciante, o posibilidad de "denuncia" anónima.
- ✓ Hechos relevantes sobre los que se informa.
- ✓ Relación con la organización (laboral, proveedor, cliente, etc.).
- ✓ En su caso, información sobre grupo de empresas.
- ✓ Dónde ocurrieron los hechos.
- ✓ Cuándo ocurrieron los hechos.
- ✓ Posible tipificación de los hechos.
- ✓ Personas implicadas.
- ✓ Otro/as afectado/as o participantes.
- ✓ Área de negocio afectada.
- ✓ Fuente de conocimiento del problema.
- ✓ ¿Conocimiento del problema por la dirección?
- ✓ Personas que han intentado ocultar el problema.
- ✓ Campo libre para otros datos.
- ✓ Campo para adjuntar ficheros. Ojo a los metadatos y datos personales que puedan incorporar.

Además

- ✓ Se deben aceptar los términos y condiciones de uso.
- ✓ Código ético y procedimiento de gestión del sistema interno accesibles.
- ✓ Se debe informar de los derechos del informante, así como de los riesgos de las denuncias falsas.

Paso 2

Recepciona la denuncia

Denuncia

La Ley usa los términos "información" o "comunicación": puede ser escrita o verbal (art. 7 L 2/23) (7.4 ISO 37002)

Anónima

Identificada

A solicitud del informante, también puede presentarse mediante una reunión presencial, dentro del plazo máximo de 7 días (art.7.2 L 2/23)

Paso 3

Genera el número de registro y aplica medidas de confidencialidad

- ✓ **Genera número** de registro (art. 26.1 L 2/23)
- ✓ **Medidas de confidencialidad,** protección de datos, seguridad de datos, etc. (arts. 4 a 9 y 29 y ss. L 2/23)

Paso 4

Genera acuse de recibo. En el plazo de 7 días

Acuse de recibo en el plazo de 7 días [art. 9.2.c) L 2/23]

- ✓ En caso de anónima, puede generarse vía web, aportando número de registro y copia de los campos rellenados (PDF descargable, por ejemplo).
- ✓ En caso de nominativa, puede optarse por el sistema anterior y/o envío de correo.

Paso 5 Triaje o análisis inicial de la denuncia

"Triaje" [art. 9.2.j) y e) L 2/23] (8.4 ISO 37002)

- ✓ Primera valoración sobre si la denuncia está fundada o hay sospechas de que pueda ser una conducta delictiva y/o pueda ocasionar daños que requieran acciones inmediatas para proteger al denunciante, a terceros o a la propia organización.
- ✓ Posible comunicación con el informante y, si se considera necesario, solicitud a la persona informante de información adicional.
- ✓ Remisión de la información al Ministerio Fiscal con carácter inmediato cuando los hechos pudieran ser indiciariamente constitutivos de delito. En el caso de que los hechos afecten a los intereses financieros de la Unión Europea, se remitirá a la Fiscalía Europea.

En todo caso, abre los mecanismos internos de protección al denunciante y preservación de identidad y respeto a la presunción de inocencia y al honor de las personas afectadas [art. 9.2.f) L 2/23]

Paso 6 Investigación interna

Investigación interna (8.4.1 ISO 37002)

- ✓ Protege la información y custodia de documentos.
- ✓ No interfiere en investigaciones policiales o judiciales.

Eventual investigación judicial/policial

Según el tipo de infracción y los indicios

Paso 7 ¿Hay infracción? Sí o No

Se detecta infracción // Comunicaciones de pasos intermedios (8.5 ISO 37002)

- ✓ La organización adopta medidas para resolverla y para monitorizar que no vuelva a suceder, conforme a las políticas/código ético.
- ✓ En su caso, impone las sanciones internas.
- ✓ En su caso, monitoriza los resultados de las investigaciones judiciales/ policiales.
- ✓ Posible reconocimiento al denunciante.

No se detecta infracción (8.4.1 ISO 37002)

- ✓ Protege la información y custodia de documentos.
- ✓ No interfiere en investigaciones policiales o judiciales.

Paso 8 Respuesta y posible conclusión del procedimiento

Respuesta y posible conclusión del procedimiento

El plazo máximo para dar respuesta a las actuaciones de investigación no puede ser superior a 3 meses a contar desde la recepción de la comunicación o, si no se remitió un acuse de recibo al informante, a 3 meses a partir del vencimiento del plazo de 7 días después de efectuarse la comunicación, salvo casos de especial complejidad que requieran una ampliación del plazo, en cuyo caso, este podrá extenderse hasta un máximo de otros 3 meses adicionales [art. 9.2.d) L 2/23]

Paso 9 Supresión de datos

Obligación de supresión de datos en los casos del art. 32.3 L 2/23. En todo caso, transcurridos 3 meses desde la recepción de la comunicación sin que se hayan iniciado actuaciones de investigación, debe procederse a la supresión de los datos personales de la denuncia, salvo que la finalidad de la conservación sea dejar evidencia del funcionamiento del sistema (art. 32.4 L 2/23)

Supuestos (8.5 ISO 37002):

a) No ha habido que tomar medidas.

b) De los hechos no se desprende que haya que investigar.

c) Hay que acudir a otro procedimiento (judicial, policial).

d) La investigación ha finalizado (con infracción detectada o no).

Puede incluir: hallazgos, medidas adoptadas, lecciones aprendidas, …

Paso 10 Documentar libro de registro

Se deben documentar en el libro-registro las informaciones recibidas y las investigaciones internas a que hayan dado lugar, garantizando, en todo caso, los requisitos de confidencialidad legalmente previstos (art. 26 L 2/23). Sugerencia de documentación:

- ✓ Fecha de conclusión del expediente.
- ✓ Quién aprueba la conclusión.
- ✓ Qué medidas se adoptaron.
- ✓ Evidencias relevantes.