

RocaJunyent Informa

Departamento Derecho Laboral y Protección de Datos
09 de Marzo de 2023



Ley 2/2023, reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción (Ley “Whistleblower”)

Aspectos de interés en el sector privado desde la perspectiva laboral y de protección de datos

El 13 de marzo de 2023 entra en vigor la **Ley 2/2023, reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción** (BOE de 21 de febrero de 2023). Esta alerta informativa complementa la elaborada y publicada por nuestro departamento de Laboral el [21 de febrero de 2023](#) y también aborda la perspectiva de protección de datos.

La citada Ley **traspone la Directiva (UE) 2019/1937**, de 23 de octubre de 2019, relativa a la protección de las personas que informen sobre infracciones del Derecho de la Unión (en adelante, “Directiva 2019/1937”), conocida como “**Directiva Whistleblowing**”.

La **finalidad de la norma** es proteger a las personas que, en un contexto laboral o profesional, hayan obtenido información sobre acciones u omisiones que puedan constituir **infracciones del Derecho de la Unión Europea**¹, así como acciones u omisiones que puedan ser constitutivas de **infracción penales o administrativa graves o muy graves**² y **que informen sobre las mismas**³. En todo caso, se entenderán comprendidas todas aquellas infracciones penales o administrativas graves o muy graves que impliquen quebranto económico para la Hacienda Pública y para la Seguridad Social.

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

Es importante destacar, desde la perspectiva laboral, que quedan expresamente **excluidas de la protección prevista en esta ley** aquellas personas que comuniquen o revelen informaciones vinculadas a **reclamaciones sobre conflictos interpersonales** o que afecten únicamente al informante y a las personas a las que se refiera la comunicación o revelación.

Esta ley prevé mecanismos y procedimientos aplicables a las informaciones obtenidas en el marco de una actividad laboral o profesional, así como medidas destinadas a proteger a los informantes (en esta Alerta se utiliza indistintamente el término “denunciante”).

¹ Siempre que (i) entren en el ámbito de aplicación de los actos de la Unión Europea enumerados en la Directiva 2019/1937 (contratación pública; servicios, productos y mercados financieros, prevención del blanqueo de capitales y la financiación del terrorismo; seguridad de los productos y conformidad; seguridad del transporte; protección del medio ambiente; protección frente a las radiaciones y seguridad nuclear; seguridad de los alimentos y los piensos, sanidad animal y bienestar de los animales; salud pública; protección de los consumidores; protección de la privacidad y de los datos personales, y seguridad de las redes y los sistemas de información; (ii) infracciones que afecten a los intereses financieros de la Unión; infracciones relativas al mercado interior, incluidas las infracciones de las normas de la Unión en materia de competencia y ayudas otorgadas por los Estados, así como (iii) las infracciones relativas al mercado interior en relación con los actos que infrinjan las normas del impuesto sobre sociedades o a prácticas cuya finalidad sea obtener una ventaja fiscal que desvirtúe el objeto o la finalidad de la legislación aplicable del impuesto sobre sociedades.

² Se ha ampliado el ámbito de aplicación material de la Directiva 2019/1937² a las infracciones de la legislación nacional, pero limitándolo a las infracciones penales y a las infracciones administrativas graves o muy graves, con el fin de permitir a los canales de información, tanto internos como externos, concentrar su actividad investigadora en las infracciones de la legislación nacional que se considera que tienen un mayor impacto en la sociedad en su conjunto.

³ La protección prevista en esta Ley no será de aplicación a la información clasificada y tampoco afectará a la protección del secreto profesional de los profesionales de la medicina y de la abogacía, al deber de confidencialidad de la Fuerzas y Cuerpos de Seguridad, así como al secreto de las deliberaciones judiciales.

Las **empresas a partir de 50 empleados**⁴ tendrán que crear un **Sistema interno de información** (“SII”).

La implantación del SII debe ser impulsado por el órgano de administración y debe **contar con un Responsable del Sistema** (directivo de la empresa, pudiendo recaer en la personas actualmente responsables de la función de cumplimiento normativo o políticas de integridad). **El SII deberá integrar los distintos canales de información existentes en la empresa**⁵.

Es obligatorio permitir las **denuncias anónimas** y su tramitación como tales.

Se establece asimismo un **canal externo de información**⁶ a través de la **Autoridad Independiente de Protección del Informante** (o autoridades u organismos autonómicos correspondientes que puedan señalarse en cada CCAA), que podemos denominar “canal externo de denuncia”, para que todas las personas físicas puedan informar de la comisión de cualquiera de las acciones u omisiones incluidas en el ámbito de aplicación de esta ley.

Se puede acudir directamente a este canal externo o previa comunicación a través del correspondiente canal interno. El funcionamiento de este canal externo se desarrolla en los artículos 17 a 21 de la norma.

Es relevante destacar que este “canal externo” nacional es compatible con la información por parte de las personas físicas ante las instituciones, órganos u organismos pertinentes de la Unión Europea, en caso de infracciones que entren en el ámbito de aplicación de la Directiva 2019/1937 (esto es, para infracciones del Derecho de la Unión Europea).

Por otra parte, se regula la **revelación pública** de informaciones. Se puede hacer una divulgación pública en los medios de comunicación o en las redes sociales, etc., con la protección establecida en esta norma, en los siguientes supuestos:

- (i) cuando se hayan utilizado los canales internos y/o externos sin que se hayan tomado medidas apropiadas al respecto en el plazo establecido;

⁴ También están obligadas, con independencia del número de personas trabajadoras, (1) 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 las que se refieren las partes I.B y II del anexo de la Directiva 2019/1937; (2) los partidos políticos, los sindicatos, las organizaciones empresariales y las fundaciones creadas por unos y otros, siempre que reciban o gestionen fondos públicos.

⁵ Los canales internos de información podrán estar habilitados por la entidad que los gestione para la recepción de cualesquiera otras comunicaciones o informaciones fuera del ámbito establecido en esta Ley, si bien dichas comunicaciones y sus remitentes quedarán fuera de su ámbito de protección.

⁶ La implementación efectiva del canal externo (nacional o autonómico) está pendiente de desarrollo.

- (ii) cuando existan motivos razonables para pensar que la infracción puede constituir un peligro inminente o manifiesto para el interés público, exista riesgo de represalias o haya pocas probabilidades de que se dé un tratamiento debido a la información por las circunstancias particulares del caso.

Por último, destacamos que la Ley establece un **marco sancionador propio** para el incumplimiento de las medidas previstas en la misma, previendo un conjunto de infracciones administrativas leves, graves y muy graves, **con multas de hasta 300.000 € para personas físicas y de hasta 1.000.000 € para personas jurídicas**. Asimismo, se establecen penalizaciones accesorias en caso de infracción muy grave, tales como la **imposibilidad de contratar con la Administración**.

Ante la inminente entrada en vigor de la norma, continuación, desgranamos los aspectos de mayor interés desde la perspectiva laboral y de protección de datos, centrándonos en los Sistemas internos de información en el sector privado:

1. Nueva obligación empresarial: Sistema interno de información (SII)

Las empresas a partir de 50 empleados tendrán que crear un Sistema interno de información (en adelante, “SII”), o adaptar los ya existentes a los requerimientos de esta norma.

El **plazo para su efectiva implementación o adaptación** será el siguiente:

- **Empresas con 250 o más personas trabajadoras:** hasta el 13 de junio de 2023 (tres meses desde la entrada en vigor de la Ley).
- **Empresas de entre 50 y 249 personas trabajadores:** hasta el 1 de diciembre de 2023.

El órgano de administración será el responsable de la implantación del SII y tendrá la condición de responsable del tratamiento de datos personales.

El SII deberá:

- i) Permitir comunicar las infracciones previstas en esta norma.
- ii) Garantizar 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 comunicación.
- iii) Garantizar la protección de datos.
- iv) Impedir el acceso de personal no autorizado.

- v) Integrar los distintos canales internos de información que puedan existir en la empresa.
- vi) Garantizar que las comunicaciones presentadas se traten de manera efectiva con el objetivo de que el primero en conocer la posible irregularidad sea la propia entidad.
- vii) Ser independiente y aparecer diferenciado respecto de los sistemas internos de información de otras entidades.
- viii) Contar con un Responsable del Sistema.
- ix) Contar con una política o estrategia que enuncie sus principios generales y los de defensa del informante. Esta política o estrategia debe ser debidamente publicitada en el seno de la entidad.
- x) Contar con un procedimiento de gestión de las informaciones recibidas.
- xi) Establecer garantías para la protección de los informantes en el ámbito de la entidad.

Los sistemas internos de comunicación y sus correspondientes canales que, a la entrada en vigor de esta ley, tengan habilitados las empresas podrán servir para dar cumplimiento a las previsiones de esta ley siempre y cuando se ajusten a los requisitos establecidos en la misma en los plazos indicados (Disposición transitoria primera y segunda de la Ley 2/2023).

No se exige un formato específico para el canal, siempre y cuando cumpla los requisitos de seguridad, confidencialidad y protección de datos previstos en la Ley 2/2023.

Los distintos canales internos de información que puedan existir en la empresa (por ejemplo, contra el acoso, de prevención de delitos, etc.) **deberán integrarse en el SII.**

2. ¿El SII se debe acordar con la representación legal de las personas trabajadoras?

No es necesario acordarlo, pero sí se exige consulta previa con la representación legal de las personas trabajadoras ("RLPT") antes de su implantación por parte de la empresa. A falta de una regulación específica, entendemos aplicable el artículo 64.6 del Estatuto de los Trabajadores ("ET"), que en líneas generales establece que se debe facilitar a la RLPT la información necesaria para que pueda proceder a su examen y preparar, en su caso, la consulta e informe.

La consulta debe permitir a la RLPT reunirse con la empresa y obtener una respuesta justificada a su eventual informe. El plazo con el que cuenta la RLPT para poder emitir su informe es de un máximo de 15 días.

3. ¿Hay alguna previsión específica para los grupos de sociedades?

En el caso de un grupo de empresas conforme al artículo 42 del Código de Comercio, la empresa matriz aprobará una política general relativa al SII y a la defensa del informante, y asegurará la aplicación de sus principios en todas las entidades que lo integran, sin perjuicio de la independencia y autonomía de cada sociedad, subgrupo o conjunto de sociedades integrantes que, en su caso, pueda establecer el respectivo sistema de gobierno corporativo o de gobernanza del grupo.

Por tanto, **en el caso de grupo de sociedades conforme al art. 42 del Código de Comercio, el SII puede ser uno para todo el grupo.**

Tendrán no obstante que actualizarse los acuerdos en materia de protección de datos para la comunicación de datos entre empresas del grupo, a fin de recoger este nuevo tratamiento (y en su caso, el régimen de corresponsabilidad).

4. ¿Se puede compartir entre varias empresas el SII?

Las **empresas** que tengan **entre 50 y 249 personas trabajadoras pueden compartir el SII**, así como los recursos destinados a la gestión y tramitación de las comunicaciones (que puede ser gestionado de forma interna por cualquiera de ellas o de forma externalizada).

Si se determinan conjuntamente los medios y la forma de gestión, así como los canales que se van a integrar, ser necesario suscribir un acuerdo de corresponsabilidad conforme al artículo 26 del Reglamento 2016/679, General de Protección de Datos.

5. Responsable del Sistema interno de información (SII)

El **órgano de administración** será el **competente para la designación** de la persona física responsable del Sistema y de **su destitución** o cese. Si se opta por un órgano colegiado, este debe delegar en uno de sus miembros las facultades de gestión del SII y de tramitación de expedientes de investigación.

El **nombramiento y**, en su caso **cese**, del Responsable del SII **deberá notificarse a la Autoridad Independiente de Protección del Informante**⁷ (o autoridades u órganos competentes de las CCAA) en el plazo de los 10 días hábiles siguientes.

⁷ El cese exige especificar las razones que han justificado el mismo.

El Responsable del Sistema **deberá desarrollar sus funciones de forma independiente y autónoma** respecto del resto de órganos de la entidad.⁸ Deberá disponer de todos los **medios personales y materiales** necesarios para llevar a cabo sus funciones.

En el caso de grupo de sociedades conforme al art. 42 del Código de Comercio, el Responsable del Sistema puede ser uno para todo el grupo.

6. ¿Quién puede ser el Responsable del SII?

Una persona **directiva de la entidad**. Cuando la naturaleza o la dimensión de las actividades de la entidad no justifiquen o permitan la existencia de un directivo/a que se dedique exclusivamente a ser Responsable del Sistema, será posible el desempeño ordinario de las funciones del puesto con las de Responsable del Sistema.

Puede ser la **persona responsable de la función de cumplimiento normativo o de políticas de integridad** que ya existiera en la empresa.

7. Procedimiento de gestión de informaciones (“denuncias”)

El **órgano de administración aprobará el procedimiento de gestión de informaciones**, de cuyo cumplimiento diligente responderá el Responsable del SII.

El **contenido mínimo** de este procedimiento se desarrolla en el artículo 9 de la norma.

8. Principios generales del procedimiento de gestión de informaciones

El procedimiento establecerá las previsiones necesarias para que el SII y los canales internos de información existente cumplan con los requisitos establecidos en la ley. Se establecen los siguientes principios y el siguiente contenido mínimo:

- a) Identificación del canal o canales internos de información a los que se asocia.
- b) Inclusión de información clara y accesible sobre los canales externos de información antes las autoridades competentes y, en su caso, ante las instituciones, órganos u organismos de la Unión Europea.

⁸ No podrá recibir instrucciones de ningún tipo en su ejercicio.

- c) Envío de acuse de recibo de la comunicación al informante dentro de los 7 días naturales siguientes (salvo que ello pueda poner en peligro la confidencialidad de la comunicación).
- d) Plazo máximo para dar respuesta a las actuaciones de investigación (3 meses, con posibilidad de extensión hasta un máximo de 3 meses adicionales en supuestos de especial complejidad).
- e) Previsión de la posibilidad de mantener la comunicación con el informante y, si se considera necesario, solicitarle información adicional.
- f) Establecimiento del derecho de la persona afectada a que se le informe de las acciones u omisiones que se le atribuyen, y a ser oída en cualquier momento. Dicha comunicación tendrá lugar en el tiempo y forma que se considere adecuado para garantizar el buen fin de la investigación.
- g) Garantía de la confidencialidad cuando la comunicación sea remitida por canales de denuncia que no sean los establecidos o a miembros del personal no responsable de su tratamiento, al que se habrá formado en esta materia y advertido de la tipificación como infracción grave de su quebranto y, asimismo, el establecimiento de la obligación del receptor de la comunicación de remitirla inmediatamente al Responsable del Sistema.
- h) Exigencia del respeto a la presunción de inocencia y al honor de las personas afectadas.
- i) Respeto a las disposiciones sobre protección de datos.
- j) Remisión de la información al Ministerio Fiscal con carácter inmediato cuando los hechos pudieran ser indiciariamente constitutivos de delito. En el caso de que los hechos afecten a los intereses financieros de la Unión Europea, se remitirá a la Fiscalía Europea.⁹

9. ¿El canal interno de información debe constar en la página web de la empresa?

Sí, las empresas deben facilitar información clara y fácilmente accesible sobre el uso del canal interno implantado, así como sobre los principios esenciales del procedimiento. Dicha información deberá constar en la página de inicio de la web de la empresa, en una sección separada y fácilmente identificable.

⁹ Esta obligación debe ser analizada desde la óptica del Derecho Penal, y puede ser cuestionable por su colisión, entre otros, con el derecho constitucional a no declarar contra sí mismo del artículo 24 de la CE.

Deberá incluirse en la información el **contenido mínimo para los interesados respecto del tratamiento de sus datos**, conforme a lo dispuesto en los artículos 13 y 14 del Reglamento General de Protección de Datos.

También **deberá informarse a los empleados sobre el tratamiento de datos que se va a realizar por razón del SII.**

10. Registro de informaciones por parte de las empresas

Las empresas deberán contar con un **libro-registro de las informaciones recibidas y de las investigaciones internas** a que hayan dado lugar, garantizando en todo caso la confidencialidad.

Este registro no será público y solo se podrá acceder a su contenido mediante Auto de la Autoridad judicial competente.

Este registro es independiente del Registro de Actividades del Tratamiento previsto en el art. 30 del Reglamento General de Protección de Datos, y 31 de la Ley Orgánica 3/2018 de Protección de Datos Personales y Garantía de los Derechos Digitales (Ley de Protección de Datos) el cual también **deberá actualizarse conforme al funcionamiento y configuración del SII.**

11. ¿Quién puede ser considerado informante, protegido por las garantías de la presente norma?

Esta ley se aplicará a los **informantes** que trabajen en el sector privado o público y que hayan obtenido información sobre infracciones en un contexto laboral o profesional, comprendiendo.

El concepto de informante es muy amplio, incluyendo a administradores, accionistas, partícipes, trabajadores por cuenta propia o ajena, extrabajadores, voluntarios, becarios, trabajadores en períodos de formación, candidatos en procesos de selección o negociación precontractual, autónomos o personal vinculado a empresas contratistas, subcontratistas y proveedores.

El derecho a la protección otorgada por esta ley exige que concurren las circunstancias siguientes:

- (i) que las personas que comuniquen o revelen infracciones tengan motivos razonables para pensar que la información recibida es veraz en el momento de la comunicación o revelación, aun cuando no aporten pruebas concluyentes, y que la citada información entra dentro del ámbito de aplicación de esta ley;
- (ii) que la comunicación o revelación se haya realizado conforme a los requerimientos previstos en la ley.

En cambio, quedan expresamente **excluidas de la protección prevista en esta ley** aquellas personas que comuniquen o revelen:

- (i) informaciones contenidas en **comunicaciones que hayan sido inadmitidas**;
- (ii) informaciones vinculadas a **reclamaciones sobre conflictos interpersonales** o que afecten únicamente al informante y a las personas a las que se refiera la comunicación o revelación, y
- (iii) **informaciones que ya estén disponibles para el público o que constituyan meros rumores.**

12. ¿Los representantes legales de las personas trabajadoras también están protegidos por las garantías de la presente norma?

Sí, así como las personas físicas o jurídicas relacionadas con el informante y que le presten apoyo, para prevenir represalias.

Concretamente, **se extenderán las medidas de protección del informante a:**

- a) los **representantes legales de las personas trabajadoras** en el ejercicio de sus funciones de asesoramiento y apoyo al informante;
- b) **personas físicas que**, en el marco de la organización en la que preste servicios el informante, **asistan al mismo en el proceso**;
- c) personas físicas relacionadas con el informante y que puedan sufrir represalias, como **compañeros de trabajo o familiares del informante**;
- d) **personas jurídicas, para las que trabaje el informante o con las que mantenga cualquier otro tipo de relación** en un contexto laboral o en las que ostente una participación significativa.

13. ¿Se puede externalizar la gestión de la recepción de las informaciones (“denuncias”)?

Sí. Este **tercero externo deberá ofrecer garantías adecuadas** en materia de independencia, confidencialidad, protección de datos y secreto de las comunicaciones.

Asimismo, **tendrá la consideración de encargado del tratamiento de datos** a efectos de la legislación sobre protección de datos personales y deberá suscribir el acuerdo regulado en el art. 28.3 del Reglamento General de Protección de Datos.

14. ¿Se puede “denunciar” indistintamente a través del canal interno o externo?

Sí, las denuncias pueden presentarse **a través de canales internos o externos**, como se ha expuesto.

El canal interno- Sistema interno de información (SII)- **es el cauce preferente para informar**, siempre que pueda tramitarse eficazmente y si el informante considera que no hay riesgo de represalias.

No obstante lo anterior, **cualquier persona física podrá denunciar ante la "Autoridad Independiente de Protección del Informante"** (o ante las autoridades u organismos autonómicos competentes) bien **directamente o previa comunicación a través del correspondiente canal interno**.

15. ¿Se pueden presentar “denuncias” de forma anónima?

Sí, pueden presentarse de forma anónima o con identificación del informante. La tramitación posterior de las comunicaciones también puede ser anónima, en cuyo caso debe habilitarse un canal para que el informante pueda recibir comunicaciones en relación con la denuncia.

16. ¿Cómo pueden presentarse las “denuncias” en el canal interno de información?

Por escrito, a través de correo postal o a través de cualquier medio electrónico habilitado al efecto, **o verbalmente**, por vía telefónica o a través de un sistema de mensajería de voz. A solicitud del informante, también podrá presentarse mediante una **reunión presencial** dentro del plazo máximo de 7 días.¹⁰

Las **comunicaciones verbales**, incluidas las realizadas a través de reunión presencial, telefónicamente o mediante sistema de mensajería de voz, **deberán documentarse** de alguna de las maneras siguientes, previo consentimiento del informante:

¹⁰ En todos estos formatos deberá proporcionarse al menos la información básica de primera capa sobre el tratamiento de datos personales para cumplir con el deber de información previsto en el artículo 13 del Reglamento General de Protección de Datos y el artículo 11 de la Ley de Protección de Datos.

- a) Mediante grabación de la conversación en un formato seguro, duradero y accesible, o
- b) A través de una transcripción completa y exacta de la conversación realizada por la persona responsable de tratarla.¹¹

En aquellos casos en que la comunicación no sea remitida por los canales de denuncia establecidos o sea remitida a miembros del personal no responsable de su tratamiento, el receptor de la comunicación debe remitirla inmediatamente al Responsable del Sistema (art. 9.2.g) de la Ley 2/2023).

17. Plazos generales del proceso del canal interno de información

En un **plazo de 7 días** a partir de la recepción de la comunicación (“denuncia”), debe **acusarse recibo al informante**, salvo que ello pueda poner en peligro la confidencialidad de la comunicación.

El **plazo máximo para dar respuesta a las actuaciones de investigación** no podrá ser superior a **3 meses**, salvo en casos de especial complejidad, en cuyo caso podrá prorrogarse otros 3 meses adicionales.

El plazo general de 3 meses se computa desde la recepción de la comunicación. Si no se remitió acuse de recibo al informante, el plazo de 3 meses se computa desde el vencimiento del plazo de 7 días después de efectuarse la comunicación.

Se establecen plazos específicos para la conservación y supresión de los datos personales y de las comunicaciones, en línea con la normativa de protección de datos:

- a) deben eliminarse tan pronto como dejen de ser necesarios.
- b) Si no se da curso a la investigación, deberán suprimirse tan pronto como se decida no dar curso a la misma, y/o en todo caso, transcurridos tres meses desde la recepción de la comunicación sin que se hubiese iniciado la investigación, salvo que se preserven con la finalidad de evidenciar el funcionamiento del sistema, y en ese caso, hasta un máximo de 3 años¹².
- c) En ningún caso pueden conservarse por un plazo superior a 10 años.

18. Acceso a los datos personales contenidos en el SII

¹¹ Se ofrecerá al informante la oportunidad de comprobar, rectificar y aceptar mediante su firma la transcripción de la conversación.

¹² Período de prescripción de las infracciones muy graves previstas en esta norma.

La norma contiene un **desarrollo específico del tratamiento de datos personales** (artículos 29 a 34).

Los datos serán tratados en base al cumplimiento de obligaciones legales, en los casos en que sea obligatoria la implantación del SII (artículo 6.1.c del Reglamento General de Protección de Datos), o bien en base al cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento (artículo 6.1.e del Reglamento General de Protección de Datos).

En cuanto **al acceso a los datos personales contenidos en el SII, quedará limitado a:**

- a) Responsable del SII y quien lo gestione directamente.
- b) El responsable de recursos humanos o el órgano competente debidamente designado, sólo cuando pudiera proceder la adopción de medidas disciplinarias contra un trabajador.
- c) El responsable de los servicios jurídicos de la entidad, si procediera la adopción de medidas legales en relación con los hechos relatados en la comunicación.
- d) Los encargados del tratamiento que eventualmente se designen.
- e) El delegado de protección de datos.

Será lícito el tratamiento de los datos por otras personas, o incluso su comunicación a terceros, en determinados **supuestos tasados**: cuando resulte necesario para la adopción de medidas correctoras en la entidad o la tramitación de los procedimientos sancionadores o penales que, en su caso, procedan.

Todo esto deberá informarse en la política de privacidad y los procedimientos internos en materia de protección de datos y seguridad de la información (particularmente, los que definan los roles y los permisos de acceso a los sistemas y las políticas internas de empleados).

19. Preservación de la identidad del informante

Toda persona que realice una comunicación o divulgación pública tiene **derecho a que no se revele su identidad a terceros**.

La identidad del informante sólo podrá comunicarse a la Autoridad judicial, al Ministerio Fiscal o a la autoridad administrativa competente en el marco de una investigación penal, disciplinaria o criminal.

20. Prohibición de represalias contra los informantes

Quedan expresamente prohibidos los actos que constituyan represalias, incluidas las amenazas de represalias y los intentos de represalias contra los informantes.

Se considerarán represalias, a título enunciativo:

- a) Suspensión del contrato de trabajo, despido o extinción de la relación laboral, incluida la no renovación o la terminación anticipada de un contrato de trabajo temporal tras el período de prueba; rescisión 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, así como la no conversión de un contrato de trabajo temporal en indefinido, salvo que dichas medidas se hayan llevado a cabo en el ejercicio regular del poder de dirección en virtud de la legislación laboral, por hechos o infracciones acreditadas y ajenas a la presentación de la denuncia.
- b) Daños, incluidos los de carácter reputacional, o pérdidas económicas, coacción, intimidación, acoso u ostracismo.
- c) Evaluación o referencias negativas sobre el desempeño laboral o profesional.
- d) Inclusión en listas negras o difusión de información en un ámbito sectorial concreto, que dificulten o impidan el acceso al empleo o la contratación de obras o servicios.
- e) Denegación o anulación de una licencia o permiso.
- f) Denegación de formación.
- g) Discriminación, o trato desfavorable o injusto.

El período general de la protección frente a represalias es de dos años.

21. Presunción de perjuicio en determinados supuestos

En los procedimientos ante un órgano jurisdiccional u otra autoridad en relación con los daños sufridos por los informantes, una vez que el informante haya demostrado razonablemente que ha comunicado o ha hecho una revelación pública de conformidad con esta Ley y que ha sufrido un perjuicio, **se presumirá que el perjuicio fue una represalia** por informar o hacer una revelación pública. En tales casos, corresponde a la persona que hay tomado la medida perjudicial probar que esa medida se basó en motivos debidamente justificados no vinculados a la comunicación o revelación pública.

22. Medidas de protección de las personas afectadas

Durante la tramitación del expediente las personas afectadas por la comunicación (“persona denunciada”) tendrán derecho a la **presunción de inocencia, derecho de defensa y derecho de acceso al expediente**, así como a la **misma protección establecida para los informantes, preservándose su identidad** y garantizándose la **confidencialidad** de los hechos y datos del procedimiento.

23. Sistema de sanciones

Esta Ley establece un **marco sancionador propio** para el incumplimiento de las medidas previstas en la misma. El ejercicio de la potestad sancionadora corresponde a la “Autoridad Independiente de Protección del Informante” (o a los órganos competentes de las CCAA).

La norma prevé un conjunto de infracciones administrativas leves, graves y muy graves, con **multas de hasta 300.000 € para personas físicas y de hasta 1.000.000 € para personas jurídicas**. Se tipifica como infracción muy grave, entre otras, el incumplimiento de la obligación de disponer de un Sistema interno de información en los términos establecidos en la Ley (con multa mínima de 30.001€ para personas físicas y de 600.001€ para personas jurídicas).

Adicionalmente, en el caso de infracciones muy graves, se podrán acordar **sanciones complementarias**: (i) la amonestación pública; (ii) la prohibición de obtener subvenciones u otros beneficios fiscales durante un máximo de 4 años, así como (iii) la prohibición de contratar con el sector público durante un máximo 3 años.

Las sanciones por infracciones muy graves impuestas a personas jurídicas, una vez firmes en vía administrativa, podrán ser publicada en el “BOE”.